Trust factor validation for distributed denial of service attack detection using machine learning

Manju Jayakumar Raghvin, Manjula R. Bharamagoudra, Ritesh Dash
School of Electronics and Communication Engineering, Reva University, Karnataka, India

Article Info

Article history:

Received Jun 10, 2024
Revised Oct 29, 2024
Accepted Nov 20, 2024

Keywords:

Distributed denial of service
Distributed reflection denial of service
Intrusion detection
Machine learning
Node validation
Time interval
Trust factor

ABSTRACT

Distributed denial of service (DDoS) attacks, predicted to be 100 Gbps and greater, are expected to begin in the first quarter of 2019, with 77% of all attacks concentrated on at least two vectors. According to a Neustar Research Agency assessment, DDoS attacks are becoming more powerful and common. Among many other issues, distributed denial of service is a notable security issue. A large number of research projects have been conducted to address this issue, but their methodologies are either inaccurate or computationally expensive, making developing an effective DDoS assault detection method a critical demand of current research. A DDoS attack employs a huge number of agents or resources to carry out the attack, resulting in a large-scale attack power. The attackers use their intelligence to discover the weak system, which is then coordinated and managed remotely. The suggested detection framework uses a frequent time interval balancing module with node trust factor validation (FTIBM-NTFV) that is used to identify the DDoS attacks in the system for improving the security levels of the network. The proposed model is compared with the traditional methods and the results are analyzed that represents the proposed model is achieving better outcomes.

Corresponding Author:

Manju Jayakumar Raghvin
School of Electronics and Communication Engineering, Reva University
Yelahanka, Karnataka, India
Email: manjuraghvin@gmail.com

1. INTRODUCTION

Designing intrusion detection systems (IDS) is becoming increasingly difficult due to the ever-changing nature of malicious software (malware). Malware authors use various evasion tactics for information concealment to avoid detection by an IDS, making the identification of unknown and obfuscated malware the major problem in today's more complex malicious attacks. Security risks, such as zero-day attacks, have also been on the rise and are specifically targeting internet users. Since information technology is now integral to our daily lives, computer security is of the utmost importance.

Monitoring network performance and investigating any indications of anomalies over the network is the primary objective of an IDS. Intruder detection systems have recently begun to use machine learning approaches since these methods have shown to be both adaptable and capable of learning, which allows for a faster response time. In this paper, we present a model for detecting and classifying intrusions using machine learning.

Distributed denial of service is a major threat to network security. A distributed denial of service (DDoS) attack is frequently carried out by creating a massive amount of traffic in order to overwhelm the target system's resources [1]. This attack has caused significant damage across the Internet and has resulted in massive financial loss. To prevent DDoS attacks, researchers have created a number of detection technologies [2], each of which use a distinct technology. Some of these systems have made use of data mining techniques [3], such as machine learning (ML) approaches. It is nevertheless an interesting study to suggest more efficient detection systems for DDoS attacks [4]. Researchers are looking for low false alarm rates as well as a high detection rate [5]. A detection engine must be able to manage a large amount of real-time network traffic. This suggested work provides a novel and more efficient DDoS attack detection system implementation technique. First, a trust factor validation model is created to reduce the number of dimensions and processing needs by validating the nodes, and then a machine learning approach is utilized to create a frequent time interval based balancing module [6].

The security of IDS depends on the needs of the user and can be implemented either on the server side or on the client side [7]. Automated decisions are made possible by combining IDS with machine learning techniques [8]. By classifying different kinds of intrusions, machine learning algorithms can process them in a manner that protects the network's integrity, confidentiality, and security [9]. Another misconception is that distributed denial of service attacks are always the same [10]. While some DDoS techniques use a lot of resources, others use very little. Therefore, there may be countless variants of DDoS attacks that machine learning algorithms miss. A difficult-to-detect assault strategy is signature-based learning, which involves learning to recognize new threats [11].

Smurf attacks, user datagram protocol (UDP) floods, and transmission control protocol (TCP) floods are only a few examples of the many types of DDoS assaults targeting networks today. An assault that overwhelms a computer network by sending massive amounts of data to the targeted systems is known as a UDP or TCP flood. When machines get ping requests from unknown sources, they will react. The literature depicts real-world DDoS attack situations using benchmark datasets [12]. Despite their initial utility, these datasets are now considered outdated because attack criteria are constantly evolving. Malware and publicly available tools are used by attackers [13]. To identify DDoS attacks in real-time, more recent datasets are required.

The authors used the CICDDOS 2019 dataset, which contains a wide spectrum of dangerous threats. Attacks by perpetrators of distributed denial of service have regularly been recognized and remedied using ML approaches. When compared to ML algorithms, traditional DDoS attack detection methods are faster, more exact, and provide the most accurate results [14]. DDoS attacks are designed to reduce the availability of internet services to those who actually use them. In this scenario, the attacker installs malware on computers via the internet without the computer user's or owner's knowledge or consent when they visit malicious websites [15]. Computers that are known as bot machines are typically compromised due to malware. The attacker gets malware onto several computers across multiple places using the internet as a medium to build a botnet [16].

In order to identify suspicious behavior on a particular network segment or device, network intrusion detection system (NIDS) analyzes packets sent over the network [17]. In order to identify intrusions, host intrusion detection system (HIDS) watches the host's behavior. Also, there are usually three ways to categorize an IDS: by signature, by anomaly, or by hybrid detection [18]. We find patterns of intrusions that happen often and utilize them to foretell when they will happen again. A hybrid approach of anomaly detection is the third type of IDS. It combines two existing methods of detection in order to enhance their capabilities. Combining the anomalous approach with the known misuse method allows for the detection of unexpected attacks. The system's overall performance will be enhanced [19].

The primary objective of this study is to design an anomaly-based system for detecting distributed denial-of-service attacks on networks. The initial stage in creating a successful DDoS detection system is to gain knowledge of the technologies that are already in use. There are primarily three technologies used by intrusion detection systems: network anomaly detection, host intrusion detection, and network intrusion detection [20]. Machine learning is used as an initial method during testing and learning, and it gets better with time. It establishes a system that optimizes performance by iteratively processing feedback data [21].

In this research work, the problems faced by companies from which DDoS attacks can originate is considered and suggests a new defensive method to help counter these problems. In addition to storing information, the suggested system functions as a sensor, and the acquired data can be used to determine how online traffic is classified and the inferences that are made from randomized traffic samples collected on network devices using stream protocol [22]. The proposal will not require software or hardware updates, and it is compatible with the current internet infrastructure. It is a given that the privacy of the users' data is upheld at all stages of system functioning.

2. PROPOSED MODEL

Load forecasting is challenging since there are so many possible variables. A substantial relationship between load change and these variables has not been found yet because there are so many possible influences [23]. Even collecting the necessary data was a pain until recently. We can now record and evaluate any repercussions on a large scale thanks to new smart meter networks, efficient sensing methods, and internet of things (IoT) technology [24]. Because they have so many sensors, smart meters can gather a lot of data about their surroundings without human intervention. They can also access the data that other IoT devices have shared [25]. The primary command center will receive all of the data in this upload [26]. This will allow for the collection of massive amounts of data for future research. Using consumption patterns as inputs, this study develops a method for load balancing on a single distribution transformer, node, or feeder. The idea behind this method is that different people consume power at different times and have different electrical needs [22]. This technology can also be used to disperse the load more evenly on a distribution transformer. Therefore, smart grids that have measurement infrastructure are ideal for using the approach. Consequently, the method works well with smart grids.

In the proposed work, a frequent time interval balancing module with node trust factor validation (FTIBM-NTFV) model is used to identify the DDoS attacks in the system. The proposed work begins by taking network traffic into account using a dataset that records details of network traffic. This dataset is then used to detect DDoS. From the extracted dataset features, a feature selection model chooses the most accurate and relevant features for attack identification. The proposed model architecture is indicated in Figure 1.

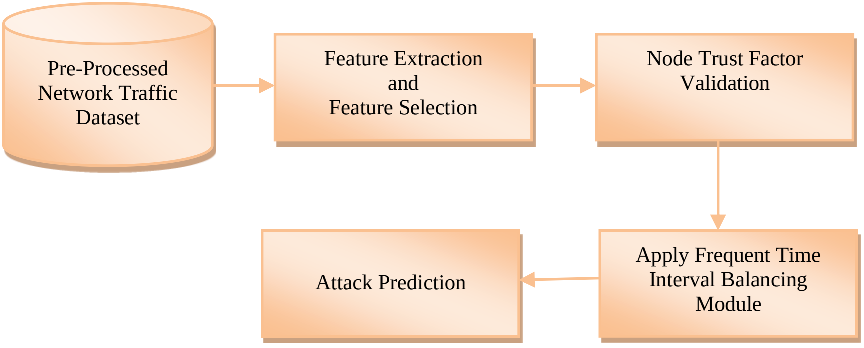
Pre-Processed Network Traffic Dataset
Feature Extraction and Feature Selection
Node Trust Factor Validation
Apply Frequent Time Interval Balancing Module
Attack Prediction

Figure 1. Proposed model architecture

Feature extraction is the first step in effective intrusion detection. It involves selecting and identifying significant qualities or characteristics from the information. In order to make sure the logistic regression model can handle the features consistently; data preparation could include standardizing input values. Important features with wider ranges are filtered out of the learning process at this stage, allowing the model to function at its best. To fit the model, logistic regression is used after the data is prepared. Estimating the parameters (coefficients) that govern the impact of each characteristic on the incursion likelihood is an important part of this process. To forecast the likelihood of each data instance being labeled as an intrusion, the model uses these coefficients. In order to determine the parameter values that maximize the likelihood of the observed data, the fitting procedure employs maximum likelihood estimation.

The features are extracted from the dataset DS considered and all the features are extracted using (1).

$$FS[DS(\mathrm{i},\mathrm{M})] = \left(\sum_{i\in M_1^N}^{M} \{\frac{\left\||N_j - mean(i)|\right\|}{\left\||N_i - mean(j)|\right\|}\} * OT_{ij}^{l}\right) \tag{1}$$

Here, N is the count of total records considered in the dataset, M is the last record in the dataset, OT is the optimum threshold value. The feature set is calculated based on the optimum threshold selected for analyzing the traffic rate. The optimum threshold is calculated as (2).

$$OT_i^M = \frac{\sum_i^M \sum_j^{\mathrm{N}} \left|FS[DS(i)]_i^{i+1} - FS[DS(i+1,M)]\right|^N}{\sum_i^N \sum_j^M \max\left(DS(i,M)\right)} \tag{2}$$

Let $\{P_1, P_2 \ldots \ldots . P_n\}$ is the set of packets travelling in the network. Let R be a random variable with probability levels.

$$P(R = P_i) = \frac{Packets\_travelling\_towards\_Destination\ P_D}{Totalpacketstravellingtowards\ var\ iousdestinations} \tag{3}$$

The nodes trust factor that involved in transmission is calculated as (4).

$$Trust_F\big(\mathrm{N(i)}\big) = \sum_{i=1}^{M} \delta\left(\omega - count(M)\right)^{i} + \min(P_i) + \max(P_i) \tag{4}$$

where M is the total network nodes count, δ indicates the network range, ω indicates nodes within the range, P represents probability index of instant node in the range. The probability index of an instant node is calculated as (5).

$$P_i = \frac{p_r - p_s}{t_s + T_s} \tag{5}$$

where p_r is the total packets received, p_s is the packets transferred and t_s is the time taken for node to data transfer and T_s is the total packets generated that is transferred to various destinations.

The trust factor validation of all the nodes involved in the network transmission is validated as (6).

```
$If\ (Trust_F(\mathrm{N(i)})\ \varepsilon\ set\ (Trust_F)$
{
$Validator(N(i))_N = \frac{P_i}{|R(OT)|+p_i^{(\mathrm{FS(i)})}+F_j^{(C_i)}} + Trust_F(\mathrm{N(i)})$          (6)
}
$Else$
{
$Node\ will\ be\ marked\ with$ '0'.
}
```

Each feature weight is calculated from each pixel for final vector generation that is performed as (7).

$$FV(N(i)\varepsilon DS) = \int_{i=1}^{N} Fi(i, i+1) + \int_{j=i}^{N} validator(N(i)) + \omega + \sum_{i=1}^{M} OT_i^N (Trust_F - P_i^{(N)})(7)$$

The final feature vector set is generated as (8).

$$TF(N(i)) = \sum_{i=1}^{n} W(FV(N(i, i+1))) - \frac{1}{N}\{\sum_{i=1}^{M} \mathrm{validator}(N(i))\} \tag{8}$$

The feature set is finalized and relevant features are extracted. The traffic analysis of every node is performed using frequent time interval balancing model to balance the node monitoring such that all nodes traffic needs to be analyzed. The node balancing in frequent time interval is performed as (9).

$$NB(N(i)) = \sum_{i=1}^{\infty} TF(N(i) + T_{s,e}^{N}(OT) * \min(P_i) + \max(P_i) \tag{9}$$

Here T is the time interval, s, e are the starting and ending time levels for traffic analysis. OT is the optimum Threshold.

```
$If\ (NB(N(i)) < Threshold\_Time\_Interval)$
{
$updateNB(N(i)) = \sum_{i=1}^{N}\sum_{j=i}^{N} minT\left(NB\big(N(i)\big)\right) + \mathrm{validator(N(i))}$          (10)

$updateNB(N(i)) = updateNB(N(i)) + \sum_{i=1}^{N}\sum_{j=i}^{M-1} FV\left(N(i)\right) + OT(DS\big(N(i)\big) + \sum_{i=1}^{M} OT_i^N (Trust_F - P_i^{(N)})$          (11)
}
$Else$
{
$Discard\ the\ node$
```

```
        $DiscSet[] = N(i)$
        }
```

The nodes that cause the unnecessary traffic in the network is identified and the attacks causing nodes are identified as (12).

$$attackSet(N(i)\varepsilon DS) = DiscSet[(N(i))] + N(i)\,! = NB(N(i)) \tag{12}$$

3. RESULTS AND DISCUSSION

There is no greater cyber threat than DDoS attacks right now. Resources like bandwidth and buffer capacity on the impacted server are reduced because the server cannot supply them to legitimate clients. One of the most significant forms of these attacks is the DDoS attack, which slows down the network and causes many legitimate user requests to be delayed. Despite the numerous proposed DDoS mitigation schemes, the difficult task of distinguishing between valid and fraudulent requests remains unaddressed. Research shows that machine learning algorithms may successfully identify DDoS assaults in network data. The proposed model considers dataset from the link *https://www.kaggle.com/datasets/yashwanthkumbam/apaddos-dataset*. The detection of malicious connections has become more of a tough undertaking due to the exponential proliferation of connected devices. One common technique utilized for these goals is IDS. Machine learning is quickly becoming a standard tool in IDS because to the increasing complexity of assaults and the wide variety of typical traffic patterns. Machine learning techniques require access to attack patterns that depict various types of attacking traffic in order to identify the enemy's face. The datasets that the machine learning community has access to do not, unfortunately, include all patterns for notorious assaults. Common attack patterns, such as ACK and PUSH-ACK flooding DDoS attacks, have been underrepresented in current datasets; this project aims to rectify that. Developers of intrusion detection systems can use the created dataset to improve the detection ratio of detection modules. The dataset contains 151,200 node samples and 23 features for the detection of intrusion.

The proposed model is implemented in python and executed in Google Colab. Metrics including F1 score, recall, accuracy, and precision were used to assess the efficacy of various machine learning algorithms. The suggested detection framework uses a FTIBM-NTFV that is used. The proposed model is compared with the traditional physical assessment of an SDN-based security framework for DDoS attack mitigation (PASF-DDoS-AM) model, protocol-based deep intrusion detection (PbDID) for DoS and DDoS attacks using UNSW-NB15 and Bot-IoT data-sets and intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system (CNBF-DDoS-IDPS). The results represent that the proposed model performance in attack detection is high.

The node behavior analysis and performance analysis are required to know the network performance. Each node packet delivery rate is calculated and the loss rate can be analyzed. The packet delivery represents the node behavior. The random node packet delivery levels are shown in Figure 2.

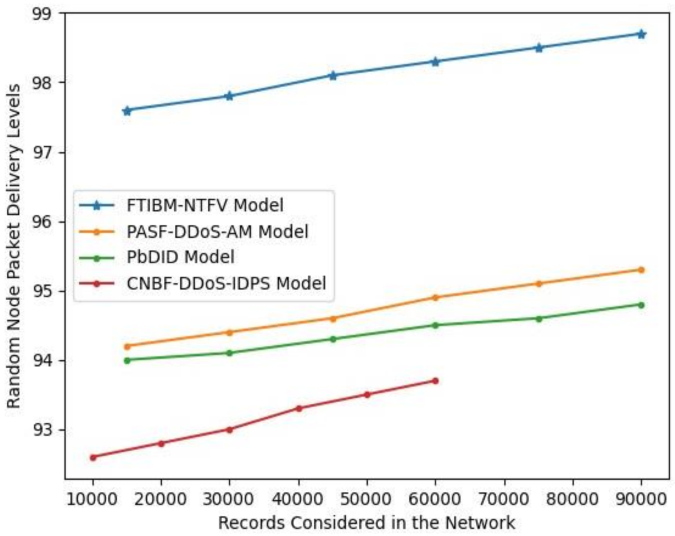

Figure 2. Random node packet delivery levels

Trust factor of every node is calculated based on nodes performance and each node trust factor is considered by analyzing the complexity levels, packet delivery rate, energy consumption. The trust factor of nodes are used to analyze the node behavior and consider a node as a trusted node or malicious nodes. The trust factor validation accuracy levels are represented in Figure 3.

The features extracted are allocated with weights in the network. The weight allocation is performed that are used to consider for training. The features having less dependency are considered and features are allocated with highest weight that is highly independent. The feature weight allocation time levels are indicated in Figure 4.

A DDoS assault is when hackers try to overwhelm a server's infrastructure by flooding it with traffic. Sites experience significant slowdowns or even crashes as a result, preventing legitimate traffic from reaching them. The DDoS attack detection accuracy levels of the proposed and existing models are shown in Figure 5.

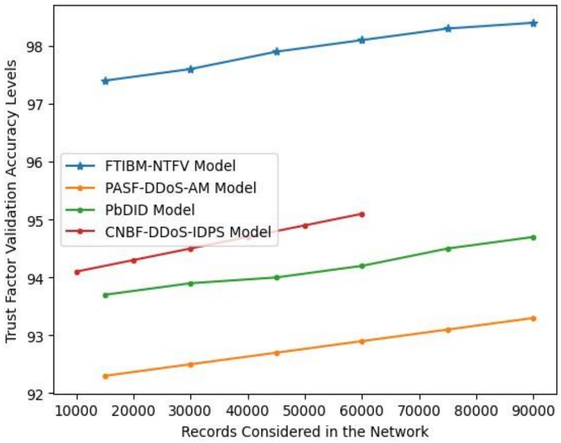

Figure 3. Trust factor validation accuracy levels

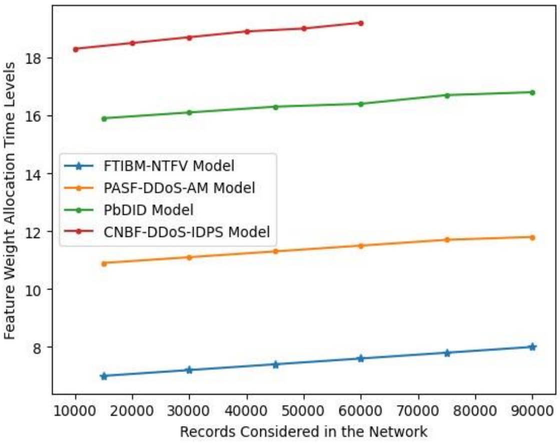

Figure 4. Feature weight allocation time levels

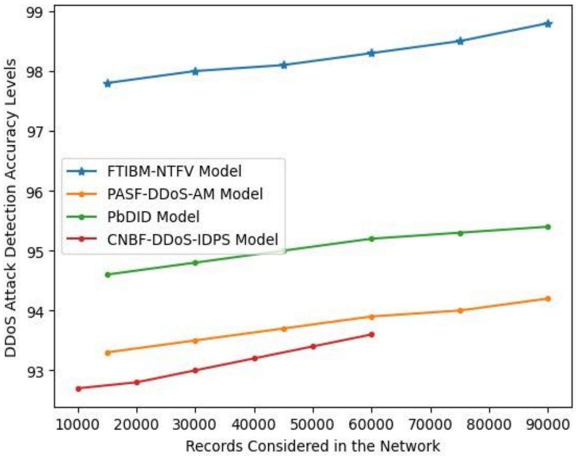

Figure 5. DDoS attack detection accuracy levels

4. CONCLUSION

The distributed denial-of-service assault, known as a DDoS attack, is one of the most common network attacks today. DDoS attacks are becoming more damaging due to the rapid advancement of computer and communication technology. As a result, research into DDoS attack detection is becoming increasingly important. There has now been some scientific investigation and progress in this area. A detection approach with a decent detection accuracy has not been provided due to the diversity of DDoS attack modes and the variable quantity of traffic attack. DDoS attacks pose a significant security risk to networks. This study proposes a machine learning-based frequent time interval-based balancing approach with node trust factor validation to prevent DDoS attacks on the source side. Our proposed method is capable of detecting assaults with a low false positive rate (1.6%) and excellent accuracy (98.4%). Protecting the network provider's reputation entails "nipping DDoS attacks in the bud" by detecting and handling DDoS attacks before they escalate. To achieve improved overall performance in the future, the usage of several machine learning techniques such as unsupervised learning and supervised models will be crucial. In order to improve the precision rate, the training samples considered should be upgraded in the future.

ACKNOWLEDGEMENT

The authors would like to thank REVA University for continuous support, infrastructure, and encouragement in carrying out the research, fostering a collaborative academic environment.

REFERENCES

[1] M. Nadeem, A. Arshad, S. Riaz, S. S. Band, and A. Mosavi, "Intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system," *IEEE Access*, vol. 9, pp. 152300–152309, 2021, doi: 10.1109/ACCESS.2021.3126535.

[2] N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Perez-Diaz, E. Jacob, and C. Martinez-Cagnazzo, "Physical assessment of an SDN-based security framework for DDoS attack mitigation: introducing the SDN-slowrate-DDoS dataset," *IEEE Access*, vol. 11, pp. 46820–46831, 2023, doi: 10.1109/ACCESS.2023.3274577.

[3] M. Zeeshan *et al.*, "Protocol-based deep intrusion detection for DoS and DDoS attacks using UNSW-NB15 and Bot-IoT data-sets," *IEEE Access*, vol. 10, pp. 2269–2283, 2022, doi: 10.1109/ACCESS.2021.3137201.

[4] J. G. Almaraz-Rivera, J. A. Perez-Diaz, J. A. Cantoral-Ceballos, J. F. Botero, and L. A. Trejo, "Toward the protection of IoT networks: introducing the LATAM-DDoS-IoT dataset," *IEEE Access*, vol. 10, pp. 106909–106920, 2022, doi: 10.1109/ACCESS.2022.3211513.

[5] J. E. Varghese and B. Muniyal, "An efficient IDS framework for DDoS attacks in SDN environment," *IEEE Access*, vol. 9, pp. 69680–69699, 2021, doi: 10.1109/ACCESS.2021.3078065.

[6] T. V Phan and M. Park, "Efficient distributed denial-of-service attack defense in sdn-based cloud," *IEEE Access*, vol. 7, pp. 18701–18714, 2019, doi: 10.1109/ACCESS.2019.2896783.

[7] J. John and J. Norman, "Major vulnerabilities and their prevention methods in cloud computing," *Advances in Intelligent Systems and Computing*, vol. 750, pp. 11–26, 2019, doi: 10.1007/978-981-13-1882-5_2.

[8] A. Bhardwaj, A. Sharma, V. Mangat, K. Kumar, and R. Vig, "Experimental analysis of DDoS attacks on OpenStack cloud platform," *Lecture Notes in Networks and Systems*, vol. 46, pp. 3–13, 2019, doi: 10.1007/978-981-13-1217-5_1.

[9] K. Singh, P. Singh, and K. Kumar, "User behavior analytics-based classification of application layer HTTP-GET flood attacks," *Journal of Network and Computer Applications*, vol. 112, pp. 97–114, 2018, doi: 10.1016/j.jnca.2018.03.030.

[10] M. Idhammad, K. Afdel, and M. Belouch, "DoS detection method based on artificial neural networks," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 4, 2017, doi: 10.14569/ijacsa.2017.080461.

[11] L. Zhou, Y. Zhu, Y. Xiang, and T. Zong, "A novel feature-based framework enabling multi-type DDoS attacks detection," *World Wide Web*, vol. 26, no. 1, pp. 163–185, 2023, doi: 10.1007/s11280-022-01040-3.

[12] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 12, no. 2, pp. 930–939, 2023, doi: 10.11591/eei.v12i2.4466.

[13] K. Kalegele, K. Sasai, H. Takahashi, G. Kitagata, and T. Kinoshita, "Four decades of data mining in network and systems management," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 10, pp. 2700–2716, 2015, doi: 10.1109/TKDE.2015.2426713.

[14] S. Badotra and S. N. Panda, "SNORT based early DDoS detection system using Opendaylight and open networking operating system in software defined networking," *Cluster Computing*, vol. 24, no. 1, pp. 501–513, 2021, doi: 10.1007/s10586-020-03133-y.

[15] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Towards a lightweight detection system for cyber attacks in the IoT environment using corresponding features," *Electronics*, vol. 9, no. 1, pp. 1–19, Jan. 2020, doi: 10.3390/electronics9010144.

[16] A. M. da S. Cardoso, R. F. Lopes, A. S. Teles, and F. B. V Magalhães, "Real-time DDoS detection based on complex event processing for IoT," *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 273–274, 2018.

[17] T. L. Von Sperling, F. L. De Caldas Filho, R. T. De Sousa, M. C. E. Martins Lucas, and R. L. Rocha, "Tracking intruders in IoT networks by means of DNS traffic analysis," in *Proceedings - 2nd Workshop on Communication Networks and Power Systems, WCNPS 2017*, 2017, pp. 1–4, doi: 10.1109/WCNPS.2017.8252938.

[18] H. Zhao, Y. Feng, H. Koide, and K. Sakurai, "An ANN based sequential detection method for balancing performance indicators of IDS," in *Proceedings - 2019 7th International Symposium on Computing and Networking, CANDAR 2019*, 2019, pp. 239–244, doi: 10.1109/CANDAR.2019.00039.

[19] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020, doi: 10.1016/j.future.2020.02.017.

[20] J. Habibi, D. Midi, A. Mudgerikar, and E. Bertino, "Heimdall: mitigating the internet of insecure things," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 968–978, 2017, doi: 10.1109/JIOT.2017.2704093.

[21] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K. K. R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 314–323, 2019, doi: 10.1109/TETC.2016.2633228.

[22] T. Lukaseder, L. Maile, B. Erb, and F. Kargl, "SDN-assisted network-based mitigation of slow DDoS attacks," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 255, pp. 102–121, 2018, doi: 10.1007/978-3-030-01704-0_6.

[23] V. Thangavelu, D. M. Divakaran, R. Sairam, S. S. Bhunia, and M. Gurusamy, "Deft: a distributed iot fingerprinting technique," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 940–952, 2019, doi: 10.1109/JIOT.2018.2865604.

[24] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, “Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things,” in *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, 2015, pp. 606–611, doi: 10.1109/INM.2015.7140344.

[25] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini, and N. T. K. Son, “Performance evaluation of Botnet DDoS attack detection using machine learning,” *Evolutionary Intelligence*, vol. 13, no. 2, pp. 283–294, 2020, doi: 10.1007/s12065-019-00310-w.

[26] M. Hawedi, C. Talhi, and H. Boucheneb, “Multi-tenant intrusion detection system for public cloud (MTIDS),” *Journal of Supercomputing*, vol. 74, no. 10, pp. 5199–5230, 2018, doi: 10.1007/s11227-018-2572-6.

BIOGRAPHIES OF AUTHORS

Manju Jayakumar Raghvin received B.E degree in ECE from Nagarjuna College of Engineering and Technology, Bangalore, affiliated to VTU, Belgaum, Karnataka in 2009. M.Tech. degree in electronics from R V College of Engineering, Bangalore, affiliated to VTU, Belgaum, Karnataka in 2011. He is currently working towards the Ph.D. degree at the School of Electronics and Communication Engineering, Reva University, Yelahanka, Karnataka, India. His research interests include artificial intelligence and machine learning application in power system engineering. He can be contacted at: manjuraghvin@gmail.com.

Manjula R. Bharamagoudra professor School of ECE has 17+ year experience in teaching, administration in higher education and research. She is excellent in team building and motivating teams to focus on their goals. A team player who believes in capacity building and create an atmosphere that encourages team members to be dedicated, accountable and provide enough opportunity to express their creativity and develop their capacity. She is an active researcher having research accomplishments in the areas of funded projects, consultancy, quality publications, patents, innovative projects and products. She has 3 ongoing funded projects worth 20 lakhs from VGST, REVA University and ATAL Incubation Centre – Pondicherry Engineering College Foundation. Research publications are in reputed national/international journals and conferences. Some of the journals where research articles published are Elsevier, Springer and Wiley, having good impact factors. She has published 26 papers in peer reviewed national and international journals, 19 papers in reputed national and international conferences and 2 book chapter/book. She has an Indian patent granted and 2 Australian patents granted; 4 patents published and 2 patents are filed. As per Google Scholar, there are more than 370 citations (h-index = 10 and i-10index = 11) (as on Sept. 2023). Her research interests are in the areas related to underwater communication, internet of things and robotics. She is reviewer for IEEE conferences and peer reviewed journals such as Elsevier, Wiley, Springer, IEEE systems and so on. She has been invited as session chair in various reputed conferences. Currently guiding six Ph.D. scholars (Since 2017 and one has received the awarded) from REVA University in the areas internet of things, Underwater IoT. She is contributing to the society through HAM member with a call sign of VU3UFS. She is also active professional member @ IETE (IETE) India, member ISTE (MISTE) India and member of IEEE (MIEEE), USA, IEEE Education Society. She is actively involved in motivating students and scholars to work on innovative projects, participate in national and international competitions. Few of the teams working in her guidance have received best paper awards, won the hackathons and competitions. She has received best researcher award and has been cited in Wiley Women in Engineering. She can be contacted at email: manjula.rb@reva.edu.in.

Ritesh Dash presently working as a professor at School of EEE, REVA University, Bengaluru. Before his current assignment, he has also served as design engineer, electrical at WAPCOS Ltd. He has a vast experience in the field of solar energy practices and energy auditing. He received the Ph.D. degree from the School of Electrical Engineering, KIIT University. He has a research experience of over 14 years and has sound knowledge in the field of artificial intelligence, FACTS, and machine learning. He has published more than 130 numbers of research papers both in international journals and conferences. He has received Madhusudan Memorial Award, IEI Young Engineers Award, Green Energy Award by KREEPA and the Institutional Award from the Institution of Engineers, India. He is associated with Many International Bodies, such as IEEE, Indian Science Congress, The Institution of Engineers, Solar Energy Society of India, and Carbon Society of India. He has handled many research projects funded by DST, SERB, CGCOST, TEQUIP-III. He can be contacted at email: ritesh.dash@reva.edu.in.