

An efficient security framework for intrusion detection and prevention in internet-of-things using machine learning technique

Tejashwini Nagaraj¹, Rajani Kallhalli Channarayappa²

¹Department of Computer Science and Engineering, Sai Vidya Institute of Technology, Bangalore, India

²Department of Artificial Intelligence and Machine Learning, Cambridge Institute of Technology, Bangalore, India

Article Info

Article history:

Received Mar 6, 2023

Revised Nov 27, 2023

Accepted Dec 15, 2023

Keywords:

Clustering techniques

Internet of things

Intrusion detection

Network security

Supervised learning

ABSTRACT

Over the past few years, the internet of things (IoT) has advanced to connect billions of smart devices to improve quality of life. However, anomalies or malicious intrusions pose several security loopholes, leading to performance degradation and threat to data security in IoT operations. Thereby, IoT security systems must keep an eye on and restrict unwanted events from occurring in the IoT network. Recently, various technical solutions based on machine learning (ML) models have been derived towards identifying and restricting unwanted events in IoT. However, most ML-based approaches are prone to miss-classification due to inappropriate feature selection. Additionally, most ML approaches applied to intrusion detection and prevention consider supervised learning, which requires a large amount of labeled data to be trained. Consequently, such complex datasets are impossible to source in a large network like IoT. To address this problem, this proposed study introduces an efficient learning mechanism to strengthen the IoT security aspects. The proposed algorithm incorporates supervised and unsupervised approaches to improve the learning models for intrusion detection and mitigation. Compared with the related works, the experimental outcome shows that the model performs well in a benchmark dataset. It accomplishes an improved detection accuracy of approximately 99.21%.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Tejashwini Nagaraj

Department of Computer Science and Engineering, Sai Vidya Institute of Technology

Bangalore, Karnataka 560064, India

Email: tejashwini.n@gmail.com

1. INTRODUCTION

The idea of internet of things (IoT) has evolved with a vision to advance the technological paradigm towards connecting numerous devices or smart objects to make our daily life more convenient and well-organized [1]. The core operations associated with IoT involve devices that sense the environment and collect data which is further forwarded to the respective location with technology-driven services [2], [3]. The recent publications on IoT demonstrate its initial implications, which were limited to only small offices and homes. However, its extended broad range spectrum can now be integrated into industries for more reliable and smart operations, saving significant time and cost [4]. The tremendous growth of IoT devices will also make a technological shift soon, where the possibilities of unknown cyber-attacks increase. This situation is becoming challenging and will continue to increase with network heterogeneity. In this regard, a wide range of research-based strategic solutions has been proposed in the past that could address the cyber-security loopholes and protect and verify the information flow within the network. The prime motive was laid on the

basis of protecting the information confidentiality and make the system sustainable and robust to different forms of threats and unauthorized access [5], [6]. This way, the concern rises gradually for IoT security. A considerable effort is being emphasized to protect the data traffic from IoT cyber-attacks, which could be in known/unknown forms. Thereby, the need to provide effective security modules arises that can detect attacks early and restore network operations to normal at the earliest. The heterogeneity of different IoT devices and user requirements also poses the problem of implementing cross-device security solutions in IoT, where the traditional intrusion detection models fail to provide a full-proof defense.

Recently, machine learning (ML) based intrusion detection approaches gained much popularity owing to their potential advantages in resisting several security threats in IoT, where distributed denial-of-services (DDoS) is one of the most hazardous threats in the IoT network environment [7]–[9]. ML-based approaches have a much broader scope toward effectively identifying intrusions, which is crucial in IoT security monitoring and traffic management. An ML-based approach from the security point of view can learn about the intrinsic details regarding threats. It can have the capability to identify even very minute mutations in the data traffic of IoT operations [10], [11]. This introduces the realization that an appropriate ML model can be designed, which could accomplish better attack detection accuracy and ensure lower execution time for identification in IoT.

The relevant literature on ML-based intrusion detection and mitigation strategies are discussed as follows: recently, Alharbi *et al.* [12] introduced a novel security system that targets to identify malware threats in IoT network environment. The prime motive of this approach was to protect the IoT systems against any form of cyber-attacks. The system has been mechanized in a way that is operated on top of the fog-computing architecture. The presented system leverages the potential of a virtual private network (VPN) to safeguard the communication channel with a novel security approach of challenge-response authentication. The study outcome demonstrates the system's effectiveness with a proof-of-concept prototype and shows experimental results to justify the performance metric. The experiment's outcome also shows that the system is highly robust against identifying malicious attacks with low response time and consumes minimal network resources. A similar study by Tian *et al.* [13] also introduces a deep learning-based security system to protect IoT edge devices from web attacks. The study formulates web-attack detection systems that consider the advantages of uniform resource locator (URLs). Multiple concurrent deep models are incorporated to make the system more consistent in detecting edge-device web attacks. The outcome of the system shows that it accomplishes a 98.91% true positive rate (TPR) and 99.410% accuracy, which makes it competitive in the direction of intrusion detection.

The adoption of ML models has been widely employed in the detection of cyber-attacks in IoT network environments, as seen in the studies of Ventura *et al.* [14], Xue *et al.* [15], and Alsheikh *et al.* [16]. These authors have suggested one thing in common IoT traffic identification is crucial in IoT security management. These studies also claimed that the extraction of significant feature sets plays a crucial role in accurate threat identification extraction results. Effective features indicate appropriate information to be fed to the ML technique. These effective feature sets include both training and testing sets.

Koroniotis *et al.* [17] introduced a new dataset named Bot-IoT. The study formulates a system to assess the legitimate and simulated IoT network traffic based on the new dataset and various attacks. The authors formulate a realistic test-bed ecosystem to identify the limitations of the existing approaches in capturing the complete vital network information. It also highlights the need for precise data labelling and analysis of complex attack diversity so that understanding the unknown and unknown forms of attacks in the IoT ecosystem could be easier. The study further evaluated the reliability factors associated with the Bot-IoT data set. In this regard, the system applies several statistical and ML methods for forensics, and the validity is further compared with the benchmark datasets. Shafiq and Yu [18] also emphasizes accurate traffic classification problems at early stages for IoT-based 5G network applications. The authors have encouraged the ML models toward accurate and timely Internet traffic classification. The study evaluated ten different prominent ML algorithms using the crossover classification method. It applied two statistical analysis tests, such as Friedman and Wilcoxon pairwise tests, to compute the results of experiments. The study outcome exhibited the effectiveness of the random forest ML classifier for early stage and accurate classification of internet traffic. The study by Shafiq *et al.* [19] also introduces a network traffic classification technique considering the ML approaches for IoT. On the other hand, another study by Shafiq *et al.* [20] emphasizes appropriate feature selection problems [21]–[23] from the IoT network dataset. The study introduces a wrapper-based feature selection mechanism for identifying network intrusion from malicious IoT traffic. The other related studies by the authors in [24]–[27] also talk about the need for IoT security and the implications of ML approaches toward accurately identifying network threats. The critical review of literature clearly outlines that the matter of fact that: i) existing ML approaches are mostly based on supervised learning, where labeling the big dataset generated from the complex IoT network is a laborious task and also prone to human error; ii) the unsupervised ML approaches also do not ensure better intrusion detection accuracy and

have a track record of degrading the performance of IoT operations; iii) in the existing studies, most ML-based approaches incorporate deep learning, which generates computational overhead to the systems of fog nodes associated with IoT, restricting the timely response for attack/intrusion detection. The accurate identification of intrusion within a shorter time can control the malicious event from propagating severe consequences; iv) most of the existing intrusion detection system in IoT mostly overlooks the problem of appropriate feature exploration and selection paradigm leading to misclassification and a higher false alarm rate for malicious intrusion detection and v) existing system has reported very less focus towards intrusion prevention strategies even though the focus is more towards intrusion detection. These factors motivated the study to design a suitable simplistic ML approach for intrusion detection and mitigation in IoT. The system's strategic design contributes to developing a methodology that solely focuses on lowering attack detection time with enhanced accuracy levels. It introduces a semi-supervised learning-based strategic model which could address the potential limitations of both supervised and unsupervised learning models and provide improved detection accuracy with timely execution.

The contribution of the study is as follows: i) the study contributes towards developing a simplified computational framework of ML which can ensure considerable intrusion detection time with accurate identification metrics; ii) it also addresses the research challenges to avoid the pitfalls associated with the existing supervised ML approaches and attempts to improve the accuracy of intrusion detection; iii) the proposed system also contributes towards designing unsupervised clustering techniques that strengthen IoT data transmission's security aspects; iv) the evaluation of the proposed methodology is performed under the simulation considering IoT-fog devices where the robustness is checked for validating its real-time working prospects and v) the system performance shows effectiveness under the benchmark dataset of network security layer-knowledge discovery in database (NSL-KDD), and the experimental outcome shows that the study not only accomplishes improved detection accuracy but also ensures lower testing time. It makes sure of the system's applicability to delay-sensitive use-cases. The next section discusses about adopted method of proposed study.

2. METHOD

The prime aim of the proposed system is to leverage the enhanced working operations of semi-supervised learning modeling toward effective intrusion detection in the IoT ecosystem. The proposed study designs and mechanizes the algorithms deployed on the fog devices between IoT-network and cloud layers. The study also addresses the data overfitting problem of the NSL-KDD dataset [28], which is less likely to be explored in the existing system. The system design modeling executes three distinct modules simultaneously. The modules are: i) data collection functional unit (DCFU); ii) semi-supervised training unit (SSTU) and iii) intrusion detection and mitigation strategy (IDMS). The following Figure 1 shows the overview of the IoT-fog network.

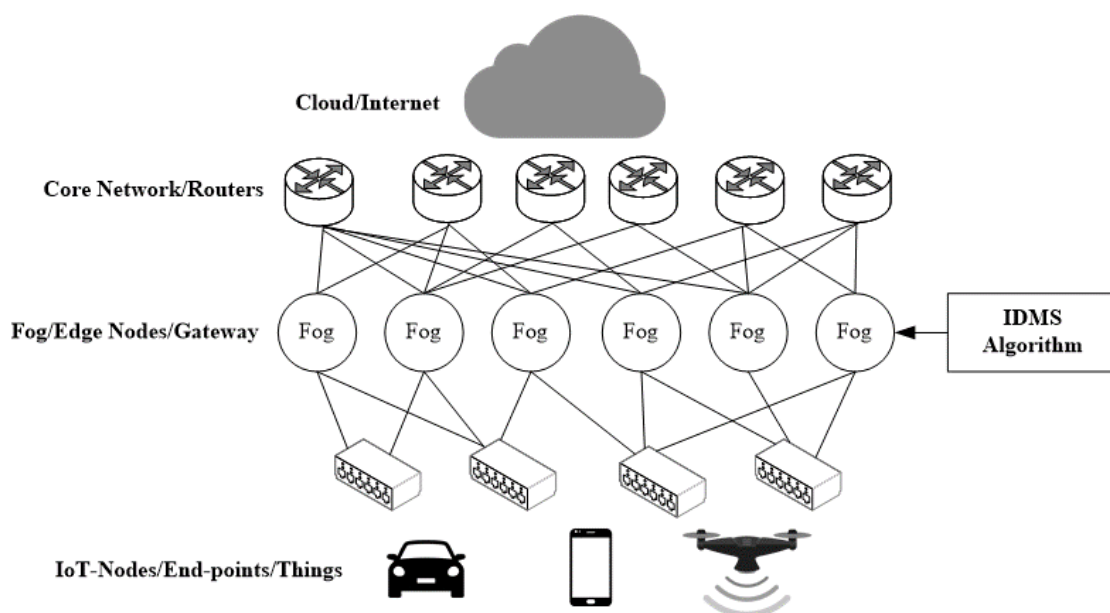


Figure 1. IoT-fog network in the proposed system formulation

According to Figure 1, a comprehensive network of end-point nodes, gateway nodes, and core network is exhibited where IDMS algorithm is exhibited to be implemented in gateway nodes. Further, the proposed SSTU unit combines the strengths associated with supervised and unsupervised learning paradigms. Apart from this agenda of proposed scheme, the security functionality is targeted to be deployed to the fog-node (FN) by offloading paradigm.

2.1. Data collection functional unit

This functional unit basically considers the FN as a gateway for the IoT network. The data-traffic basically flows through foreground (FG) prior reaching to the server unit (SU) in IoT. The study formulates the proposed methodology in such a way where the DCFU unit initially verifies the incoming traffic flow and incorporates a rule-based authentication mechanism to check the authenticity of the packets. This entire operation takes place in the fog-node as highlighted in the Figure 1. In case the system finds that the traffic flow does not obey the rules then the packet is further dropped as per the action taken by the DCFU unit. The NSL-KDD dataset consists of 22 statistical attributes which are obtained from the IoT traffic. The features could also provide better insight towards identifying unknown forms of intrusion in IoT. The data collection phase basically considers the incoming flow of traffic $I_{Traffic}$ and further extracts the essential features E_{fet} . The proposed modeling of data collection further checks the internet protocol (IP) address of the fog-node as $IP \leftarrow FN_i$ and also checks the IoT device IP which attempts to connect the FN. The rule-based mechanism further verifies the $I_{Traffic}$. For each $i \in IoT$, the system assigns the FN_{IP} to the gateway device (G). Further the DCFU unit checks the $I_{Traffic}$ under the rule-based traffic validation mechanism (RTV) and if the action indicates the Flag-1 then the system drops the packet, else it further performs essential feature extraction E_{fet} with imitating.

2.2. Feature modeling

Incase if the traffic validation is successful then the system computes the essential features of traffic with imitating. The essential features include i) size of the packet and ii) packet count. These attributes are essential for the detection of intrusion from the IoT traffic flow. The study contributes towards the dataset where the details of the features associated with critical IoT attacks are also considered. The extracted imitating packets from the $I_{Traffic}$ further undergoes through a pre-processing mechanism for the effective data-cleaning operations. The proposed system considers a set of feature attributes which are appropriately selected from the incoming traffic which are-count of the packet, link estimation for used bandwidth, standard deviation, average, weighted moving average, magnitude, radius, covariance, correlation factor, entropy estimation, and information distance computation.

2.3. Semi-supervised training unit

The proposed system designs the concept of semi-supervised unit considering the potential features of deep neural networks (DNN). The study mechanizes the learning function of SSTU in such a way where it combines the DNN potential features with K-means clustering mechanism. However, the single layer feed-forward neural network is not suitable for providing ample information on the size of the network despite its capability of providing higher accuracy in classification problems. The algorithm for SSTU unit is provided in Algorithm 1.

This has been justified by the universal approximation theorem [29]. This limitation is addressed in the proposed system by studying the properties of deep feed forward neural network (DFNN) not only reduces the generalization error but also verify the count of the nodes in the hidden units. The proposed study introduces a customized function $f_{DFNN}(x)$ that considers the size of the network for training and also aims to reduce the generalization error with web of interconnected neurons across several hidden layers. Here the neurons non-linear characteristics basically helps the model to understand the pattern of attack from the data traffic with adjustments in input-output combinations. The limitations associated with the DFNN is also addressed in the proposed study and it is observed that DFNN all alone cannot be robust against new form of attack strategy and in that case, it will not be able to predict the attack with higher level of accuracy. The SSTU component further also introduces another customized functional module $f_{DFNN}(x)$ of enhanced K-means clustering which when combined with the enhanced DFNN provides significant outcome. The study considers the strength factors of K-means clustering approach which have enough capability to appropriately classify the unknown traffic data. The function $f_{DFNN}(x)$ basically runs on the top of proposed $f_{DFNN}(x)$. Initially the DFNN dataset is labeled and the intermediate training model is prepared. Further the trained model of $f_{DFNN}(x)$ divide the classes into a set of classes such as $DC \leftarrow \{AC_1, AC_2, \dots, AC_j \dots NC\}$. Here DC represents the divided class whereas AC represent attack classes and NC refers to normal class. Here the role of the supervised DFNN model is it provides nearly perfect initial data points to the K-means for clustering

which improves the accuracy of attack identification. The proposed K-means clustering further computes the random samples of attack classes and computes Euclidian distance between and points considering the unlabeled dataset and further classify the adversarial cluster unit and normal cluster unit which is further again forwarded to the trained model.

The algorithm design and modeling are numerically performed and it clearly shows that from step-1 to step-18 has already been covered up in the above segment of the study. However, the further portion of the algorithm activates the proposed clustering mechanism of $f_{DFNN}(x)$ which considers the training model-1 T_{model1} which is computed from the $f_{DFNN}(x)$ computation. The algorithm further optimizes the process of computation of predictor classes and also performs the clustering of training data (TD). The function further also approximate the random samples $RN(i)$ which are further assigned to each of the clusters. It also incorporates unlabeled training data $uL_TD(i)$ and assign the datapoints into the clusters and compute the Euclidian distance $ED(RN - TD)$ between the samples and the training data. Further the proposed method also introduces a thresholding mechanism (T) which assists in finding the appropriate cluster for intrusion criticality analysis. Finally, the SSTU system returns the trained model to the output.

Algorithm 1. Proposed semi-supervised learning model

```

Input:  $I_{Traffic}$ 
Output: Trained Model  $T_{model2}$ 
Begin
  IP-FNi
  For each  $i \in IoT$ 
    Assign  $FN_{ip} \rightarrow G$ 
  End
  Employ (RTV)
  IF ( $I_{Traffic}$  against RTV)
    Drop(packet)
  Else
    Extract ( $E_{fet}$ )
  Enable:  $f_{DFNN}(x)$ :pass in  $E_{fet}$ 
  DC  $\leftarrow \{AC_1, AC_2, \dots, AC_j, \dots, NC\}$ 
  Labeling of training data (TD) of n samples
  Init: layers, neurons, bias, weight, learning rate, epoch, accuracy
  Compute: accuracy  $\leftarrow \#(actual == observed)/n \times 100$ 
  If (accuracy is not satisfactory)
    change training attributes
  Else
    return  $\rightarrow$  trained model  $T_{model1}$ 
  Enable:  $f_{kmeans}(x)$ :pass in:  $T_{model1}$ 
  Compute predictor classes
  Perform clustering of TD
  Random samples of  $RN(i) \leftarrow C_i$ 
  Add  $uL\_TD(i) \rightarrow C_i, ED(RN - TD)$ 
  Thresholding (T)
  Final  $C_i$ 
  Return Trained Model  $T_{model2}$ 
End

```

2.4. Proposed intrusion detection and mitigation strategy

The proposed intrusion detection strategy basically takes the input of E_{fet} and with the feature it trains the model T_{model2} and computes the intrusion status. If the intrusion is found to be normal then the IDMS module continues the normal IoT operations. If the intrusion is of known class, then it generates the status accordingly. If incase the intrusion is found to be of unknown form then the IDMS system generates alert. The IDMS unit further also functionalizes intrusion mitigation strategy where it considers the assessment of attack status. If the intrusion is found to be of unknown class, then the IDMS system enables drop rules to the media access control internet protocol (MAC_IP) from FN. Here the MAC_IP belongs to the intruder IoT node that has transmitted the malicious packets. The drop rule is set considering a defined random time-stamp. Once the random time stamp expires then the drop rule is revoked from the ruleset. Here the time stamp remains unknown so that intruder cannot properly understand the time-strategy. If the intrusion is found to be of unknown form, then the IDMS system also employ the drop-rule but for limited random time-stamp. Here the time-stamp is set to small random timer as IDMS is not sure about the type of intrusion. In that case the IDMS system also verifies the traffic behavior if it is found suspicious then again drop-rule is set. Else no rule is set. Further the system updates the traffic instances with new observed data. The next section further illustrates the experimental results obtained from simulating the proposed algorithm in a simulation environmental testbed.

3. RESULTS AND DISCUSSION

In this section, the results obtained from the simulation of the presented approach is demonstrated. The study considers a simulation testbed of IoT-fog cloud [30] to evaluate the performance of the proposed system. The fog-node is configured with a component of Cisco Nexus switch device of 5672UP. It considers Cisco NX-OS operating system with other programmable features. The cloud comprises of Quadcore Intel CPU E5620 @2.40 GHz and Xen PVM hypervisor. The simulation testbed also considers total 30 IoT nodes which are connected with the Raspberry Pi connected to various sensor nodes. The Raspberry Pi consists of 1.2 GHz 64-bit quad-core ARMv8 processor with 1 GB RAM size and Strech OS with 64 GB memory. The Fog-Node is programmable in the proposed study where the rule-based mechanism can be employed for mitigating the attacks considering the traffic assessment. The optimal training parameter values in the proposed system for the training of SSTU which are shown with the following Table 1.

Serial number	Parameter	Optimal value
1	Hidden layer count	7-8
2	Neuron count	100-200
3	Activation function	Sigmoid
4	Learning rate	0.04-0.06
5	No of epoch	700-900

In the proposed system a total number of approximately 120,000 tuples are generated from the traffic dataset of NSL-KDD, where a total of 11,530 tuples are labeled for initial input of training. The performance metric to evaluate the effectiveness of the proposed system considers a set of parameters which are accuracy of intrusion detection, detection rate and response time of detection. The metric accuracy indicates the percentage of correctly identified network intrusion from the traffic instances. It also indicates whether the traffic is suspicious or not. The measure of accuracy in (1) is computed for the performance evaluation of the proposed system.

$$Acc = \left(\frac{TP+TN}{TP+TN+FN+FP} \right) \quad (1)$$

The accuracy Acc parameter computation considers the values of true positive score (TP), along with the true negative score TN , false negative score FN and false positive score FP . In (2), the intrusion detection rate D_{rate} is measured for the purpose of numerical evaluation. The Figure 2 shows the comparative outcome of the proposed system towards accuracy of the intrusion detection. The comparison has been performed with the conventional popular related approaches of intrusion detection in IoT eco-system.

$$D_{rate} = \left(\frac{TP}{TP+FN} \right) \quad (2)$$

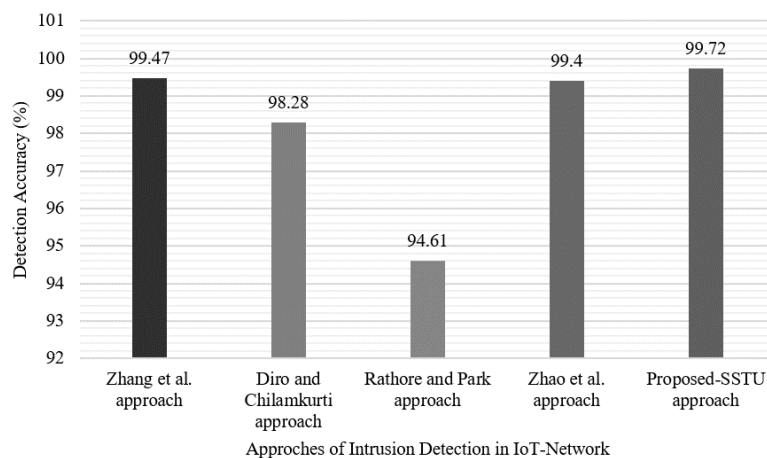


Figure 2. Comparing simulation results of detection accuracy (%)

The proposed study considers the much popular related works of Zhang *et al.* [31], Diro and Chilamkurti [32], Rathore and Park [33], and Zhao *et al.* [34] for the purpose of comparison and it clearly shows that when it comes to detection accuracy the proposed SSTU outperforms the existing system by approximately 99.72% of detection accuracy. The prime reason is that it applies the proposed semi-supervised learning model which is trained with the appropriate features. The simulation results comparison is illustrated in Figure 3. The Figure 3(a) and Figure 3(b) further also shows the analysis of detection rate and detection time respectively. The outcome shows that proposed scheme adopting semi-supervised learning methods excels better performance in contrast to existing studies. Proposed scheme achieves 99.81% of accurate in detection rate that is higher enough to facilitate better resistivity towards various threats. Further, it is also seen that work carried out by [31], [34] attains comparable outcome owing to the adoption of neural network.

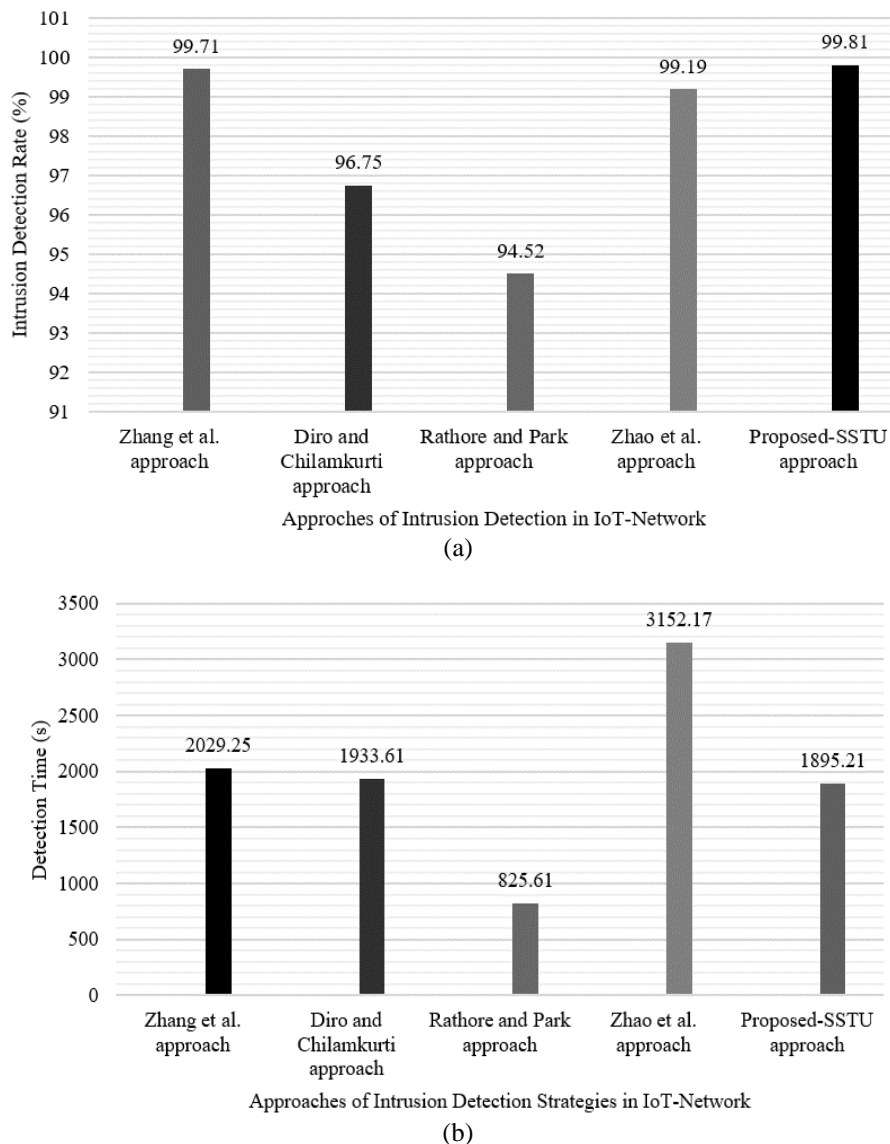


Figure 3. Comparing simulation results for (a) intrusion detection rate and (b) detection time (s)

In the context of detection time analysis, it is quite clear that the approach of [33] attains better detection time but it comes with a cost of lesser detection accuracy which is approximately 94.61%. However, the proposed system of semi-supervised learning improves the detection time to 1895.21 which is quite superior and balanced in comparison to supervised learning models. Hence, the proposed system attains a balanced outcome towards identifying the network intrusions in IoT and also contributes to the security functionalities in fog-computing.

4. CONCLUSION

The study introduces a novel security framework of intrusion detection and prevention system for IoT-network operations. It realizes the advantages and popularity of ML techniques towards identifying the network intrusion from the traffic flows that pass-through fog-nodes inside the IoT eco-system. However, the study also addresses the pitfalls associated with the supervised and unsupervised learning approaches towards improving the accuracy of attack detection. The prime reason came out to be the inappropriateness in feature selection and also the problem of exhaustive network data labeling in supervised learning models. Addressing the potential research problems in existing system. The proposed study introduces a novel SSTU learning framework that functionalize the deep learning on the top of K-means clustering approach towards identifying the network intrusions in IoT. The proposed study also contributes towards feature labeling considering the NSL-KDD dataset. This approach of appropriate feature selection has enhanced the learning accuracy which have resulted in better intrusion detection and prevention considering huge network traffic. The contribution of the study are as follows: i) unlike related works the proposed system simplifies the design of semi-supervised learning where it also contributes towards feature selection; ii) the proposed study outcome yields a balanced performance between attack detection accuracy and detection time which is still a missing gap and research challenge in the existing research trend; iii) the proposed study also contributes towards identifying unknown forms of adversaries in the IoT-network whereas in the existing system majority of the approaches are specific towards particular form of attacks and iv) unlike existing system it also introduces attack prevention strategy and also outperforms the existing system in attack detection accuracy which approximately 99.72%. The future research work will be carried out towards optimizing the outcome of computational time complexity of the proposed SSTU-approach. It also furthers targets to optimize the learning parameters of SSTU approach so that accuracy of attack detection should be improved to more extent.





REFERENCES

- [1] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4682–4696, Jun. 2020, doi: 10.1109/JIOT.2020.2969326.
- [2] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Implementing lightweight IoT-IDS on raspberry pi using correlation based feature selection and its performance evaluation," in *International Conference on Advanced Information Networking and Applications*, Springer, 2020, pp. 458–469, doi: 10.1007/978-3-030-15032-7_39.
- [3] A. Hamdan, B. Alareeni, R. Hamdan, and M. A. Dahlan, "Incorporation of artificial intelligence, big data, and internet of things (IoT): an insight into the technological implementations in business success," *Journal of Decision Systems*, pp. 1–4, Nov. 2022, doi: 10.1080/12460125.2022.2143618.
- [4] J. Qiu, L. Du, D. Zhang, S. Su, and Z. Tian, "Nei-TTE: intelligent traffic time estimation based on fine-grained time derivation of road segments for smart city," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2659–2666, Apr. 2020, doi: 10.1109/TII.2019.2943906.
- [5] F. Schuster and A. Habibipour, "Users' privacy and security concerns that affect IoT adoption in the home domain," *International Journal of Human-Computer Interaction*, pp. 1–12, Nov. 2022, doi: 10.1080/10447318.2022.2147302.
- [6] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222–232, Feb. 1987, doi: 10.1109/TSE.1987.232894.
- [7] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Defending DoS attacks on broadcast authentication in wireless sensor networks," in *2008 IEEE International Conference on Communications*, 2008, pp. 1653–1657, doi: 10.1109/ICC.2008.319.
- [8] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for internet of things using blockchain technology," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, Mar. 2018, pp. 769–773, doi: 10.1109/ICCNC.2018.8390280.
- [9] Z. Tian, X. Gao, S. Su, and J. Qiu, "Vcash: a novel reputation framework for identifying denial of traffic service in internet of connected vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3901–3909, May 2020, doi: 10.1109/JIOT.2019.2951620.
- [10] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in internet of things," *Journal of Communications and Networks*, vol. 20, no. 3, pp. 291–298, Jun. 2018, doi: 10.1109/JCN.2018.000041.
- [11] A. Abeshu and N. Chilamkurti, "Deep learning: the frontier for distributed attack detection in fog-to-things computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, Feb. 2018, doi: 10.1109/MCOM.2018.1700332.
- [12] S. Alharbi, P. Rodriguez, R. Maharaja, P. Iyer, N. Bose, and Z. Ye, "FOCUS: a fog computing-based security system for the internet of things," in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Jan. 2018, pp. 1–5, doi: 10.1109/CCNC.2018.8319238.
- [13] Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1963–1971, Mar. 2020, doi: 10.1109/TII.2019.2938778.
- [14] D. Ventura, D. Casado-Mansilla, J. López-de-Armentia, P. Garaizar, D. López-de-Ipiña, and V. Catania, "ARIIMA: a real IoT implementation of a machine-learning architecture for reducing energy consumption," in *International Conference on Ubiquitous Computing and Ambient Intelligence*, Springer, 2014, pp. 444–451, doi: 10.1007/978-3-319-13102-3_72.
- [15] R. Xue, L. Wang, and J. Chen, "Using the IoT to construct ubiquitous learning environment," in *2011 Second International Conference on Mechanic Automation and Control Engineering*, Jul. 2011, pp. 7878–7880, doi: 10.1109/MACE.2011.5988881.
- [16] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: algorithms, strategies, and applications," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1996–2018, 2014, doi: 10.1109/COMST.2014.2320099.
- [17] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, Nov. 2019, doi: 10.1016/j.future.2019.05.041.





- [18] M. Shafiq and X. Yu, "Effective packet number for 5G IM wechat application at early stage traffic classification," *Mobile Information Systems*, vol. 2017, pp. 1–22, 2017, doi: 10.1155/2017/3146868.
- [19] M. Shafiq, X. Yu, A. A. Laghari, L. Yao, N. K. Karn, and F. Abdessamia, "Network traffic classification techniques and comparative analysis using machine learning algorithms," in *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, Oct. 2016, pp. 2451–2455, doi: 10.1109/CompComm.2016.7925139.
- [20] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Computers & Security*, vol. 94, p. 101863, Jul. 2020, doi: 10.1016/j.cose.2020.101863.
- [21] 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, Jun. 2020, doi: 10.1016/j.future.2020.02.017.
- [22] S. Egea, A. Rego Manez, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, "Intelligent IoT traffic classification using novel search strategy for fast-based-correlation feature selection in industrial environments," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1616–1624, Jun. 2018, doi: 10.1109/JIOT.2017.2787959.
- [23] S. Su, Y. Sun, X. Gao, J. Qiu, and Z. Tian, "A correlation-change based feature selection method for IoT equipment anomaly detection," *Applied Sciences*, vol. 9, no. 3, pp. 1–14, Jan. 2019, doi: 10.3390/app9030437.
- [24] M. R. Belgaum, Z. Alansari, S. Musa, M. Mansoor Alam, and M. S. Mazliham, "Role of artificial intelligence in cloud computing, IoT and SDN: reliability and scalability issues," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 5, pp. 4458–4470, Oct. 2021, doi: 10.11591/ijece.v11i5.pp4458-4470.
- [25] D. Khwailleh and F. Al-balas, "A dynamic data encryption method based on addressing the data importance on the internet of things," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 2, pp. 2139–2146, Apr. 2022, doi: 10.11591/ijece.v12i2.pp2139-2146.
- [26] H. A. Khan, R. Abdulla, S. K. Selvaperumal, and A. Bathich, "IoT based on secure personal healthcare using RFID technology and steganography," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 4, pp. 3300–3309, Aug. 2021, doi: 10.11591/ijece.v11i4.pp3300-3309.
- [27] R. Zhao *et al.*, "A novel intrusion detection method based on lightweight neural network for internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9960–9972, Jun. 2022, doi: 10.1109/JIOT.2021.3119055.
- [28] A. Shiravani, M. H. Sadreddini, and H. N. Nahook, "Network intrusion detection using data dimensions reduction techniques," *Journal of Big Data*, vol. 10, no. 1, pp. 1–25, Mar. 2023, doi: 10.1186/s40537-023-00697-5.
- [29] M.-X. Wang and Y. Qu, "Approximation capabilities of neural networks on unbounded domains," *Neural Networks*, vol. 145, pp. 56–67, Jan. 2022, doi: 10.1016/j.neunet.2021.10.001.
- [30] N. Ravi and M. S. Selvaraj, "TeFENS: testbed for experimenting next-generation-network security," in *2018 IEEE 5G World Forum (5GWF)*, Jul. 2018, pp. 204–209, doi: 10.1109/5GWF.2018.8516708.
- [31] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019, doi: 10.1109/ACCESS.2019.2903723.
- [32] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for internet of things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, May 2018, doi: 10.1016/j.future.2017.08.043.
- [33] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Applied Soft Computing*, vol. 72, pp. 79–89, Nov. 2018, doi: 10.1016/j.asoc.2018.05.049.
- [34] J. Li, Z. Zhao, R. Li, and H. Zhang, "AI-based two-stage intrusion detection for software defined IoT networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2093–2102, Apr. 2019, doi: 10.1109/JIOT.2018.2883344.

BIOGRAPHIES OF AUTHORS



Tejashwini Nagaraj     she has completed her B.E from SVCE, Bengaluru Karnataka and M. Tech is from Dr. AIT, Bengaluru, Karanataka, and Ph.D with research topic "Design of energy efficient and secure algorithm for wireless environment using public key encryption" in network security in wireless sensor networks under Visvesvaraya Technological University in the year 2022. She is having six years of teaching and research experience in respective engineering colleges under Visvesvaraya Technological University, Belagavi, and Karnataka, India. Her interest includes digital image communication, wireless communication, wireless sensor network and operating system. Currently she is pursuing her research for PhD under Visvesvaraya Technological University, Belagavi, and Karnataka. She has published her work in various international conferences and journals. She can be contacted at email: tejashwini.n@gmail.com.



Rajani Kallhalli Channarayappa     is the assistant professor in Department of Artificial Intelligence and Machine Learning in the Cambridge Institute of Technology, K R Puram, Blore at VTU, Belgaum. She completed B.E from NCET, and MTech from Atria Institute of Technology. She submitted thesis and pursuing research work under VTU. Her research interest focuses on mobile ad-hoc networks, wireless sensor networks, WANET'S and machine learning. She has many publications on isolating routing misbehavior problems in mobile ad hoc networks. She had more than 8 years of teaching experience worked as assistant professor in various colleges like NCET, SRSIT, and Presidency University. During her career she taught students with various subjects to students like C# programming and .net, DBMS, OOMD, FS, SE, ST, web programming, CO, C-Programming and C++. My vision is to be to be a successful teacher by incorporating good teaching values and to provide students a quality in teaching. She can be contacted at email: rajanikcc009@gmail.com.