Intrusion Detection and Prevention Using RNN in WSN

Ashok Yadav and Arun Kumar

Abstract The wireless sensor network involves sensor nodes, communicating protocols, and gateways for interaction with the Internet. Due to limited memory availability in wireless sensor network, the advanced encryption algorithm of securities and authentication protocol is not deployable due to which wireless sensor networks are prone to attacks such as distributed denial of service and distributed denial of service attacks. The intrusion detection and prevention is used to detect, notify malware activities, avoid, and stop them. The proposed system is mainly to detect and prevent the distributed denial of service and denial of service attack in wireless sensor network. In the proposed model, recurrent neural network is taken as a classifier. The model is validated using the ten-fold cross validation in nine is to one repeated iteration and is then tested for making of false positive alerts on data set (WSN-DS). The accuracy of this model is 99.8% with positive fault rate of 0.3%.

Keywords Recurrent neural network · WSN-DS · SVM · Random forest · Decision tree · CNN

1 Introduction

The wireless sensor networks have many applications in the field of detection of the air quality, volcanoes, earthquake, flood, health care, and in telecommunication. The wireless sensor network has physical insecurities, limited processing power, less availability of memory, and no well-defined boundaries; i.e., the boundaries are changed on the movement of either device or users; due to these, the wireless sensor network is prone to threat. The distributed denial of service attack and denial of service attacks are easily deployable attack in the wireless sensor network [1]. The intrusion detection and prevention mechanism is more important because in wireless sensor network the implementation of advanced encryption algorithm, large

A. Yadav (✉) · A. Kumar
Centre for Advanced Studies, AKTU, Lucknow, Uttar Pradesh, India

A. Kumar
e-mail: drarun@cas.res.in

S. Smys et al. (eds.), *Inventive Computation and Information Technologies*, Lecture Notes in Networks and Systems 336, https://doi.org/10.1007/978-981-16-6723-7_40

authentication protocols, and other cryptographic algorithm are not feasible [2]. The intrusion detection is done easily using the concept of deep learning as well as machine learning techniques. The wireless network mainly threatens in areas such as attack on sensors, attack on the network service, and attacks on the application services.

The attacks which mainly occur on sensors are location tracking, device cloning, and physical attacks. Similarly, attacks on network service are routing attacks and on application services are distributed denial of service, denial of service attack, and eavesdropping etc. The intrusion detection main aim is to avoid compromises to confidentiality, and availability [3]. Due to the advancement in the field of IOT devices, automation system results in the smart parking system, automated homes, smart cities, smart traffic light system, smart electric meters, and sensors nodes, etc. These are interconnected with communication protocols, and gateway is used to connect with Internet due to which the securities attack increased [4]. The devices which are used in wireless sensor network mainly have less memory and also depend upon the batteries.

These devices have almost negligible security because of lack of deployment of encryption algorithm, antivirus, and other cryptographic techniques. The propositioned tactic is centered on the anomaly intrusion detection, and their prevention with the recurrent neural networks as classifier and validation of the model takes place using tenfold cross-validation mechanism on the wireless sensor network data set (WSN-DS). The feature which is generally used for classification is the abnormal traffic on network, data transfer rate, etc. The proposed model easily detects the attacks in the network. The recurrent neural network is trained for detecting the attack such as user to root attack, remote to local, denial of service, and distributed denial of service attack. Some artificial neural network-based mechanism is proposed such as backpropagation which is not lightweight and attack type is flooding attack whose accuracy is closer to 90%, and the feedforward algorithm which is lightweight in nature and attack type which is malicious node, and accuracy which is almost 95%.The remaining paper is described as follows. Section 2 describes the related work, Sect. 3 describes the proposed methodology, Sect. 4 involves the result section of the paper, and Sect. 5 has the conclusion of the paper.

2 Related Work

One of previously proposed models for detection of denial of service attack and the KDD Cup99 data set is used, and this model is capable of detecting the flooding attack and denial of service attack with higher precision and accuracy [5]. Papers [6] and [7] have proposed a model in which the artificial neural network is used for detection of the intrusions. The KDD Cup99 data set is used, and the feature selection takes place using backpropagation algorithm. This model is suitable for the real-time applications also, and with this, gray-hole attack as well as denial of service attack is easily detected with higher accuracy. Papers [8] and [9] have proposed a model for intrusion detection using artificial neural network, and in this, the classification can be done using backpropagation algorithm, and the KDD Cup99 data set is used for training and testing purposes. Papers [5] and [10] have defined a model in which layered categories are used for the classification purpose to detect intrusions and the artificial neural network as well as the support vector machine and KDD Cup99 data set is used in the implementation of model. Papers [11] and [12] have proposed a model in which the machine learning classifier such as random forest and artificial neural network are used for the classification, detection and prevention of network-based intrusion respectively. Papers [8] and [13] have given a model in which the machine learning classifier such as decision tree is for the classification and artificial neural network is for detection and prevention of network-based intrusion. Paper [14] has proposed a technique for intrusion detection and classification of the attacks with help of the artificial neural network. In this, the multi-layer perceptron architecture is used. The KDD Cup99 data set is used for training and testing the model, and it detects various attacks and after that classifies in into six different clusters. Paper [15] proposed model for detection of network intrusion with the help of the multi-layer perceptron architecture and the artificial neural network. In this, some relevant features of attacks are used instead of all features of the packet. The model accuracy is better in case of detection of denial of service attack. Papers [16] and [17] proposed a model which is based on feature-reduced intrusion detection, and it analyzed important features of data dimensionality reduction take place then the reduced features are feed to feed-forward neural network for training and testing using the KDD Cup99 data set, and this model uses artificial neural network classify normal and abnormal data. In papers [15] and [18], the given model for detection of intrusion in wireless sensor network is based on the mechanism of the genetic programming. The genetic programming involves gene-expression mechanism, linear genetic programming mechanism, and multi-programming mechanism for the detection of the intrusions, and the accuracy of the model is more than 95%. In papers [2] and [19], another model is proposed which is totally based on the fuzzy logic for intrusion detection in wireless sensor network. In this, the author claims that using this model, all types of the intrusions are detected easily with accuracy of 100%. Papers [14] and [20] have given a mechanism which is based on the concept of rule-based decentralized mechanism which detects the different type attacks of the wireless sensor network such as black hole attack, worm hole attack, and selective hole attack. The accuracy of the model is better, and the positive fault rate is minimal. Papers [6] and [21] have proposed a model which is based on the concept of the clustering mechanism. In this, the detection of intrusions takes place on the basis of differentiating between the abnormal traffic on the network and normal traffic on the network. Have proposed one of the models in which support vector machine is used as a classifier and for training and testing the model using distributed learning algorithm is used. Papers [5] and [22] have proposed one of the models in which decision tree is used as a classifier, and for training and testing, distributed learning algorithm is used. Papers [3] and [11] have proposed one of the models in which convolution neural network is used as a classifier, and for training and testing, distributed learning algorithm is used. Papers [4] and [10] have proposed one of the models in which random forest is used as a classifier, and for training and testing, the distributed learning algorithm is used. The detection of malicious file in this model is more accurate and also applicable in real-life scenario. One of models is proposed in which deep learning algorithm is used. In this, the fog node used is of high bandwidth and power of computation enhanced the deployment of the deep learning services. The farmer's get more information about their crop, and also the quality of life of farmers is improved. The result of the proposed work shows that accuracy of the model is good [23]. One model is proposed for addressing the data mining chaos such as scalability, security and privacy, and efficiency. The complexity of the model is linear in nature due to which the model is more efficient. The model provides more resistant to the system from attacks, and also, the accuracy of model is better [24]. A technique to decide highest quality time and highest quality fee to withdraw a voluntary retirement scheme thinking about chance of recognition of a retirement request of a retirement request fee because of saying voluntary retirement scheme and to the enterprise because of one-time unique bills to folks that voluntarily retire for the duration of the term is discussed. A specific case wherein a Poisson n a Poisson manner is believe for the statement of the voluntary retirement scheme [25]. One of the models is proposed which helps in the identification of the name of the resources which are allocated in the cloud. The mechanism used is round robin and first come first serve for minimizing the cost of demand and time [26].

3 Method and Material

In the intrusion detection and prevention system proposed involves the following stages such as feature extraction, classifier, training and testing, data set, and decision. At the stage of feature extraction, some features are extricated from the provided data and used as a feature and also some features are mixed with other features and considered as single feature for classification with the help of which the classification result accuracy is improved. The next stage is of classifier, and recurrent neural network is used as a classifier. In the papers [19] and [8], training and testing are done using the WSN-DS. The resilient backpropagation learning strategy is applied for training neural network in which rate of learning is 0.01, and to train, 1000 epochs are used. According to received data at classifier stage, the classification take place and then result is forwarded at the decision stage and decision stage decisions are made either data packet is accepted or rejected and automatically notify at the base station. The given model in the paper [13] intrusion detection and prevention system uses the only header of the data, but in this, both header and the payload of the data are considered for making decision due to which the accuracy of the model is enhanced [13]. The anomaly-based intrusion detection system is mainly compromises of only two phases that is training phase and testing phase. In this, the deviation between the perceived behavior and the model is regarded as an abnormality and the feature selection is considered during the training phase of the recurrent neural network [27]. The ability of learning from data set depends upon neural network used, and categorizing the file or packet coming through network as abnormal or normal will

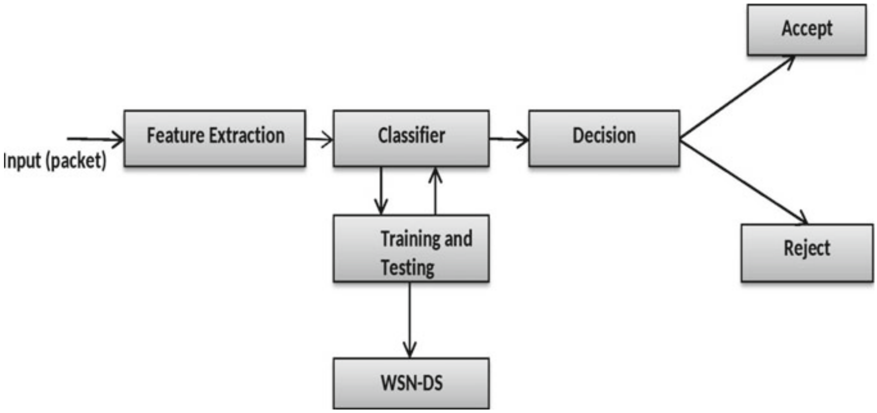

Fig. 1 Model of IDPS using RNN

be done by some computing techniques of neural network. The network traffic data is collected using image, library files, log file, dynamic link, and other files such as log file, music file, and word file documents (Fig. 1).

4 Result and Discussion

In our proposed model, recurrent neural network is trained using the WSN-DS data set with help of the tenfold cross validation method in nine is to one iteration with two hidden layers and three hidden layers. The classification of the attacks classified correctly up to 98.6% with two hidden layers and error is approximately 0.0343, when three hidden layer are used for the classification of attacks take place correctly up to 98.34 with error of 0.0643. In case of the using two hidden layers, at first layer, the number of neurons used is 11, and in the second layer, the number of neurons is five, and in case of three hidden layers, the number of neurons at first layer is 11, and at second hidden layer, five neurons are used, and at last hidden layer, the number neurons used is two. The number of passes or epochs used through training data is 1000. The proportion of validation set from the data used for training is 20%, the learning rate in proposed model is used for the adjustment of the weight at each iteration, and the learning rate of this model is approximately 0.3, and the momentum of model is used for adjustment of weight during the backpropagation in order to prevent local minima and speed up convergence, and momentum of this model is 0.2. The tenfold cross-validation method is used in (9:1) repeated manner with the help of which the accuracy of classification is enhanced. Some of the term is used for showing the result of the model which is the true negative means of the number of normal attacks that are classified as normal (no attack), as well as false negative, which refers to the number of attack cases that are wrongly classified as normal (no attack), and the false positive which means the normal (no attack) cases classified incorrectly as attack. The rate of true positive and false positive is calculated with the help of formulae (Figs. 2, 3 and 4; Tables 1 and 2).

$$
\begin{aligned}
&(\mathrm{TPR} = (\mathrm{TP}/(\mathrm{TP}+\mathrm{FN}))\\
&(\mathrm{TNR} = (\mathrm{TN}/(\mathrm{FN}+\mathrm{TP}))\\
&(\mathrm{FPR} = (\mathrm{FP}/(\mathrm{FP}+\mathrm{TN}))
\end{aligned}
$$

The receiver operating characteristic curve is used to describe the total distinction of the classification model. If the area under the curve is high, then it means that the classifier used is better. In the above ROC curve, bold blue indicates the norm of receiver operating characteristics curve of all 500 iterations of the repeated tenfold cross-validation, and the gray-shaded area directs the extent of the receiver operating characteristic curve produced over all iterations. The dashed red line in the curve indicates the ability of the classifier that is the accuracy of the classification of files either it is malicious or no malicious to which class it belongs to at random a baseline for the worst case class. In another way the red dashed line is the base line for worst case classification performance.

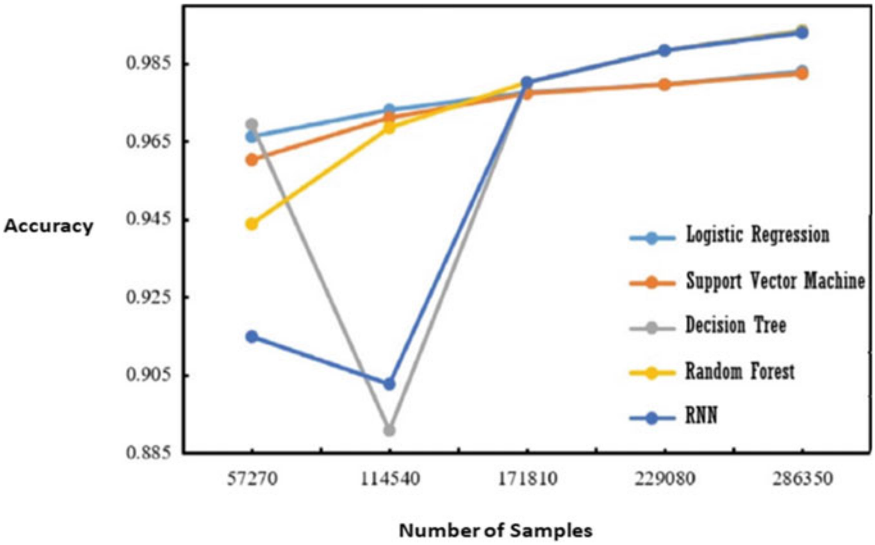

Fig. 2 Training of model using multiple classifiers

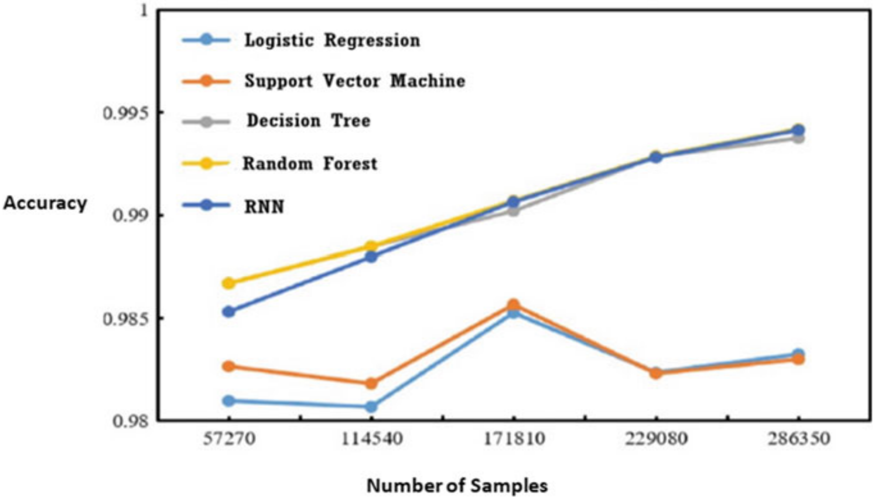

Fig. 3 Testing ROC curve using multiple classifiers

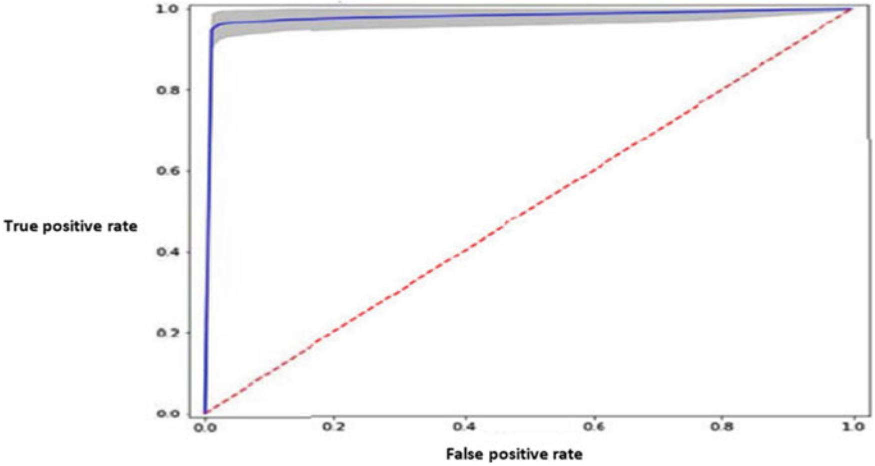

Fig. 4 ROC curve of RNN

Table 1 Result using two hidden layer

	TPR	FPR	FNR	TNR	P
Normal	0.998	0.02	0.002	0.98	0.998
DDOS	0.979	0.006	0.211	0.899	0.899
DOS	0.924	0	0.079	1	0.979
Flooding	0.898	0.002	0.005	0.979	0.969
Scheduling	0.798	0.02	0.004	0.897	0.991
AVG	0.985	0.004	0.014	0.962	0.999

Table 2 Result using three hidden layer

	TPR	FPR	FNR	TNR	P
Normal	0.984	0.046	0.007	0.896	0.995
DDOS	0.843	0.013	0.157	0.987	0.938
DOS	0.769	0.01	0.311	0.99	0.946
Flooding	0.789	0.001	0.219	0.977	0.976
Scheduling	0.0.874	0.002	0.196	0.988	0.989
AVG	0.969	0.041	0.028	0.959	0.963

5 Conclusion

The main aim of intrusion detection system is to avert compromise to CIA triads of security model of the system. In the proposed method, RNN is used as classifier using which the classification of malicious and non-malicious file is detected. The data set used is WSN-DS which is created using the leach protocol. A WSN-DS data set consists of 17 attributes and 374,000 rows. The accuracy of the model is better with two hidden layer in detection of distributed denial of service attack and denial of service attack with positive fault rate of 0.3. The validation of model is done using of tenfold in nine is to one repeated iteration mechanism due to which the fault rate is minimal and the accuracy is better. The flooding attack, gray-hole attack, and other attacks are also detected with better accuracy.

References

1. H. Mi, Z. Wang, A. Ittycheriah, Supervised attentions for neural machine translation. EMNLP 2016—Conf. Empir. Methods Nat. Lang. Process. Proc. **4**, 2283–2288 (2016). https://doi.org/10.18653/v1/d16-1249
2. V. Jyothsna, V.V. Rama Prasad, K. Munivara Prasad, A review of anomaly based intrusion detection systems. Int. J. Comput. Appl. **28**(7), 26–35 (2011). https://doi.org/10.5120/3399-4730
3. E.G. Dada, J.S. Bassi, O.O. Adekunle, *An Investigation Into the Effectiveness of Machine Learning Techniques for Intrusion Detection*, vol. 13, no. 6, pp. 764–778 (2017). Available: www.azojete.com.ng
4. J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, A. Wahab, A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. Electron **9**(7) (2020). https://doi.org/10.3390/electronics9071177
5. A. Saeed, A. Ahmadinia, A. Javed, H. Larijani, Random neural network based intelligent intrusion detection for wireless sensor networks. Procedia Comput. Sci. **80**, 2372–2376 (2016). https://doi.org/10.1016/j.procs.2016.05.453
6. R. Krishnan, Y.H. Robinson, E.G. Julie, *An Intrusion Detection and Prevention Protocol for Internet of Things Based Wireless Sensor Networks*, pp. 0–18
7. K.A. Molinaro, M.L. Bolton, Evaluating the applicability of the double system lens model to the analysis of phishing email judgments. Comput. Secur. **77**, 128–137 (2018). https://doi.org/10.1016/j.cose.2018.03.012

8. O.E. Elejla, B. Belaton, M. Anbar, A. Alnajjar, Intrusion detection systems of ICMPv6-based DDoS attacks. Neural Comput. Appl. **30**(1), 45–56 (2018). https://doi.org/10.1007/s00521-016-2812-8
9. R. Chen, J. Gaia, H.R. Rao, An examination of the effect of recent phishing encounters on phishing susceptibility. Decis. Support Syst. **133**, 113287 (2020). https://doi.org/10.1016/j.dss.2020.113287
10. M.A. Rezvi, S. Moontaha, K.A. Trisha, S.T. Cynthia, S. Ripon, Data mining approach to analyzing intrusion detection of wireless sensor network. Indones. J. Electr. Eng. Comput. Sci. **21**(1), 516–523 (2021). https://doi.org/10.11591/ijeecs.v21.i1.pp516-523
11. Y. Fu, Z. Yan, J. Cao, O. Koné, X. Cao, An automata based intrusion detection method for internet of things. Mob. Inf. Syst. **2017**, 6–10 (2017). https://doi.org/10.1155/2017/1750637
12. M. Jakobsson, Modeling and preventing phishing attacks. Lect. Notes Comput. Sci. **3570**, 89 (2005). https://doi.org/10.1007/11507840_9
13. S. Duque, M.N. Bin Omar, Using data mining algorithms for developing a model for intrusion detection system (IDS). Procedia Comput. Sci. **61**, 46–51 (2015). https://doi.org/10.1016/j.procs.2015.09.145
14. A. Hendrawan, A.F. Daru, A.M. Hirzan, Intrusion detection with wireless sensor network (WSN) internet of things. EEE Access **13**(2), 45–48 (2021)
15. J.P. Ananth, S. Balakrishnan, S.P. Premnath, Logo based pattern matching algorithm for intrusion detection system in wireless sensor network. Int. J. Pure Appl. Math. **119**(12), 753–762 (2018). https://acadpubl.eu/hub/2018-119-12/articles/7/1636.pdf
16. M. Hasan, M.M. Islam, M.I.I. Zarif, M.M.A. Hashem, Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things **7**, 100059 (2019). https://doi.org/10.1016/j.iot.2019.100059
17. A.S. Ahmed, R. Hassan, N.E. Othman, Denial of service attack over secure neighbor discovery (SeND). Int. J. Adv. Sci. Eng. Inf. Technol. **8**(5), 1897–1904 (2018). https://doi.org/10.18517/ijaseit.8.5.6427
18. L. Alsulaiman, S. Al-Ahmadi, Performance evaluation of machine learning techniques for DOS detection in wireless sensor network. Int. J. Netw. Secur. Its Appl. **13**(2), 21–29 (2021). https://doi.org/10.5121/ijnsa.2021.13202
19. L. Ashiku, C. Dagli, Network intrusion detection system using deep learning. Procedia Comput. Sci. **185**(June), 239–247 (2021). https://doi.org/10.1016/j.procs.2021.05.025
20. V. Suryani, S. Sulistyo, W. Widyawan, Two-phase security protection for the Internet of Things object. J. Inf. Process. Syst. **14**(6), 1431–1437 (2018). https://doi.org/10.3745/JIPS.03.0106
21. N. Kaur, P. Rattan, A critical review of intrusion detection systems in WSN: challenges & future directions. IDS WSN **25**(4), 3020–3028 (2021)
22. N.A. Alrajeh, S. Khan, B. Shams, Intrusion detection systems in wireless sensor networks: a review. Int. J. Distrib. Sens. Netw. (2013). https://doi.org/10.1155/2013/167575
23. K. Lee, B.N. Silva, K. Han, Deep learning entrusted to fog nodes (DLEFN) based smart agriculture. Appl. Sci. **10**(4) (2020). https://doi.org/10.3390/app10041544
24. W. Haoxiang, S. Smys, Big data analysis and perturbation using data mining algorithm. J. Soft. Comput. Paradig. **3**(1), 19–28 (2021). https://doi.org/10.36548/jscp.2021.1.003
25. B. Thilaka, N. Theetharappan, Optimal time for withdrawal of voluntary retirement scheme with a time—varying threshold, in *The second International Conference on Innovative Mechanisms for Industry Applications ICIMIA 2020—Conference Proceedings*, vol. 02, no. 04, pp. 598–602 (2020). https://doi.org/10.1109/ICIMIA48430.2020.9074885
26. D.W. Haoxiang, D.S. Smys, MC-SVM based work flow preparation in cloud with named entity identification. J. Soft Comput. Paradig. **2**(2), 130–139 (2020). https://doi.org/10.36548/jscp.2020.2.006
27. A. Martin, N.B. Anutthamaa, M. Sathyavathy, M.M. Saint Francois, D.V.P. Venkatesan, A framework for predicting phishing websites using neural networks. Int. J. Comput. Sci. **8**(2), 330–336 (2011). Available: http://arxiv.org/abs/1109.1074