Table 4: Accuracy

Dataset	Number of Training Samples	Number of Testing Samples	Training Accuracy	Testing accuracy
network-intrusion-detection	125973	10000	94.04	92.08

Table 5 shows the confusion matrix of the proposed algorithm. The accuracy for each category off the attack in the testing dataset is shown here.

Table 5: network-intrusion-detection confusion matrix

Normal	DOS	R2L	U2R	Probing	Accuracy of each attack
3981	51	197		0	3981/4229=94.13
0	3132	200	0	0	3132/3332 = 87.99
0	159	931	13	0	931/1103 = 84.40
0	116	44	1119	0	1119/1279 = 87.49
0	0	10	2	45	45/57 = 78.94

Neural Network Analysis

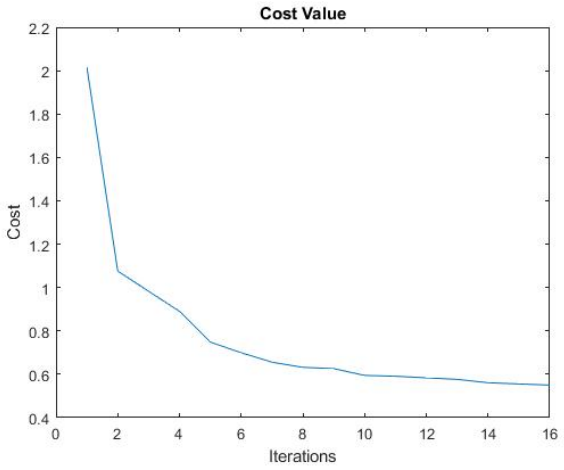

Fig. 4. Cost value of the NN weights over iteration

- Input size – 15
- Number of classes – 5

Fig 4 shows the cost function value of the proposed algorithm. During the training phase, the cost function of the NN reduced to 0.6 after 15 iterations. This lower cost function is an indication towards optimal training of the weights. The comparison of the proposed algorithm with other NN optimizations is listed in table 6.

Table 6: Comparison Results with complete dataset

S. No.	Optimization Algorithm	Train Accuracy	Test Accuracy
1.	Genetic	94.06	92.22
2.	Whale	93.28	90.63
3.	Proposed Grey Wolf	94.05	92.08

The experimental results on both the datasets prove that the proposed method of SOANN produces better result in classification of the attacks. The accuracies are shown in tables 3 and 6.

5. Conclusion

An Intruder Detection System needs to detect anomalies in the network based on the input parameters. This paper proposed a Swarm optimization based NN for the purpose of identifying the attacks. The experiments have been carried out on KDD Cup data set and Kaggle dataset. The proposed method produced better accuracy when compared to the existing optimization techniques.

References

[1] Hoang, X.D. A Website Defacement Detection Method based on Machine Learning. In Proceedings of the International Conference on Engineering Research and Applications (ICERA 2018), Thai-Nguyen, Vietnam, 1–2 December 2018.
[2] X. Liang and J. Xu, "Control for networked control systems with remote and local controllers over unreliable communication channel," arXiv preprint arXiv:1803.01336, 2018.
[3] XueliHu, Qi Xi, and Zhenxing Wang. Monitoring of root privilege escalation in android kernel. In International Conference on Cloud Computing and Security, pages 491–503. Springer, 2018.
[4] EnamulKabir, JiankunHu, Hua Wang, GuangpingZhuo, A novel statistical technique for intrusion detection systems, Future Generation Computer Systems, 2017, ISSN 0167-739X.
[5] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, ''Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection,'' IEEE Access, vol. 6, pp. 33789–33795, 2018.
[6] V. Patel, H. Madhukar, and S. Ravichandran, ''Variability index constant false alarm rate for marine target detection,'' in Proc. Conf. Signal Process. Commun. Eng. Syst. (SPACES), Jan. 2018, pp. 171–175.
[7] F. Farahnakian and J. Heikkonen, "A deep auto-encoder based approach for intrusion detection system," in Advanced Communication Technology (ICACT), 2018 20th International Conference on. IEEE, 2018, pp. 178–183.
[8] Wenjuan Li, Steven Tug, WeizhiMeng, and Yu Wang. Designing collaborative blockchained signature-based intrusion detection in iot environments. Future Generation Computer Systems, 96:481 – 489, 2019.
[9] R. Colelli, S. Panzieri, F. Pascucci, "Exploiting system model for securing cps: the anomaly based ids perspective", 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), vol. 1, pp. 1171-1174, Sep. 2018.
[10] S. J. Horng, M. Y. Su, Y. H. Chen, T. W. Kao, R. J. Chen, J. L. Lai and C. D. Perkasa, "A novel intrusion detection system based on hierarchical clustering and support vector machines," in Expert systems with Applications, vol. 38, no. 1, pp. 306–313, 2011.
[11] F. Amiri, M. R. Yousefi, C. Lucas, A. Shakery and N. Yazdani, "Mutual information-based feature selection for intrusion detection systems," in Journal of Network and Computer Applications, vol. 34, no. 4, pp.1184–1199, 2011.
[12] A. Gouveia and M. Correia, "Feature set tuning in statistical learning network intrusion detection," 2016 IEEE 15th International Symposium on Network Computing and Applications, 2016, pp. 68–75.
[13] S. O. Al-mamory and F. S. Jassim, "Evaluation of different data mining algorithms with KDD Cup 99 dataset," in Journal of Babylon University/Pure and Applied Sciences, vol. 21, no. 8, pp. 2663–2681, 2013.
[14] D. Deepika and V. Richhariya, "Intrusion detection withkNN classification and DS-Theory," in International Journal of Computer Science and Information Technology and Security, vol. 2, no.2, pp.274–281, 2012.
[15] B. Subba, S. Biswas and S. Karmakar, "Intrusion detection systems using linear discriminant analysis and logistic regression," 2015 Annual IEEE India Conference (INDICON), New Delhi, 2015, pp. 1-6.
[16] S. Devaraju and S. Ramakrishnan, "Performance comparison for intrusion detection system using neural network with KDD dataset," ICTACT Journal on Soft Computing, vol. 4, no. 3, 2014.
[17] A. A. Olusola, A. S. Oladele and D. O. Abosede, "Analysis of KDD'99 intrusion detection dataset for selection of relevance features," World Congress on Engineering and Computer Science, San Francisco, USA, 2010, vol. 1, pp. 20–22.
[18] R. Chitrakar and C. Huang, "Anomaly based intrusion detection using hybrid learning approach of combining k-medoids clustering and Na¨ıve Bayes classification," 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), Shanghai, 2012, pp. 1-5.