instances and this has high precedence over a slightly better training model created using two classes model creation strategy.

The second stage of the proposed model (reasoning mechanism) was built using a hybrid approach. The hybrid approach in this paper uses both neural network and fuzzy logic. The benefit of using the hybrid approach is increasing the intrusion detection rate, some of attacks may not be detected by one of the modules but the other one may be able to detect them. The results obtained by this approach achieves a higher detection rate than both the neural network and fuzzy logic each one individually. However, it has a higher false positive rate.

11. Future Work

For the next phase of research work, the authors are working on decreasing the false positive rate of the reasoning mechanism by trying a different neural network structure, and different membership functions in the fuzzy module. The authors will also consider developing the proposed model to handle multi-stage attacks by analysing and modelling different multi-stage attacks scenarios.

12. References

[1] H.-J. Liao, et al., "Intrusion detection system: A comprehensive review," Journal of Network and Computer Applications, 2013, vol.36, n.1, pp. 16-24.

[2] D.-K. Kang, D. Fuller, and V. Honavar, "Learning classifiers for misuse and anomaly detection using a bag of system calls representation," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop (IAW'05)*, 2005, pp. 118-125.

[3] M. Roesch, "Snort: Lightweight Intrusion Detection for Networks," in *LISA*. 1999, vol.99, pp. 229-238.

[4] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," Expert Systems with Applications, 2014. vol.41, n.4, pp. 1690-1700.

[5] KDD'99. *KDD Cup 1999 Data*. 1999. Available from: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (Access Date: 17 July, 2014).

[6] S. Axelsson, "The base-rate fallacy and its implications for the difficulty of intrusion detection," in *Proceedings of the 6th ACM Conference on Computer and Communications Security*. 1999, pp.1-7.

[7] T. Abraham, "IDDM: Intrusion detection using data mining techniques," 2001.

[8] W. Lee, and S.J. Stolfo, "A framework for constructing features and models for intrusion detection systems," ACM transactions on Information and system security (TiSSEC), 2000, vol.3, n.4, pp. 227-261.

[9] R.-I. Chang, et al., "Intrusion detection by backpropagation neural networks with sample-query and attribute-query," International Journal of Computational Intelligence Research, 2007, vol.3, n.1, pp. 6-10.

[10] D. Barbara, et al., "ADAM: a testbed for exploring the use of data mining in intrusion detection," ACM Sigmod Record, 2001, vol. 30, n.4, pp. 15-24.

[11] N. Bhargava, et al., "Decision Tree Analysis on J48 Algorithm for Data Mining," International Journal, 2013. vol.3, n.6.

[12] H. Altwaijry, "Bayesian based intrusion detection system," in *IAENG Transactions on Engineering Technologies*, 2013, Springer. pp. 29-44.

[13] M. Hall, et al., "The WEKA Data Mining Software: An Update. SIGKDD Explorations," 2009, vol.11, n.1, pp. 10-18.

[14] M. Anthony., P.L. Bartlett, "Neural Network Learning: Theoretical Foundations" 2009, Campridge University.

[15] S. Rajasekaran, G.A. Pai, "Neural Networks, Fuzzy |Logic and Genetic Algorithm: Synthesis and Applications" 2003, PHI Learning Pvt. Ltd.

[16] D.-z. Wei, Q.-g. Wang, and L.-n. Lin, "Design and Application of a Snort System Based on Data Mining," Journal of Jimei University (Natural Science), 2011, vol.5, pp. 016.

[17] M.A. Hall, "Correlation-based feature selection for machine learning," 2009, The University of Waikato.

[18] J.J. Davis, and A.J. Clark, "Data preprocessing for anomaly based network intrusion detection: A review. computers & security," 2011, vol.30, n.6, pp. 353-375.

[19] P. Kukiełka, Z. Kotulski, (2010) "Adaptation of the neural network-based IDS to new attacks detection", Available from: http://arxiv.org/abs/1009.2406 (Access Date: 17 Oct, 2014).

[20] B. Shanmugam, "Improved Intrusion Detection System Using Fuzzy Logic for Detecting Anamoly and Misuse Type of Attacks" in *Proceedings of the Conference of Soft Computing and Pattern Recognition*. 2009, pp.212-217.

