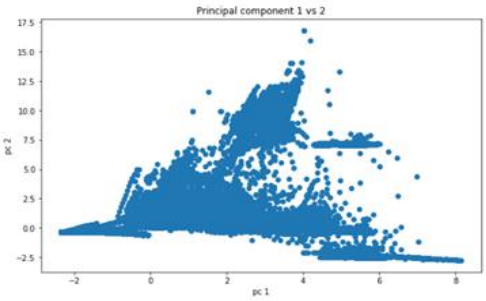

Out[61]:

	principal component 1	principal component 2	target
0	0.560535	1.428889	1.0
1	0.561570	1.404599	1.0
2	0.541429	1.380523	1.0
3	0.514420	1.354875	1.0
4	0.488805	1.329314	1.0

Fig. 9 Principle component 1vs 2

This dataset is considered as for evaluating within NIDS research. Further, using of these datasets helps in conducting a meaningful comparison with existing working models and research work. The detection rate obtained as part of the result showed that the proposed model obtained an accuracy of 99.87%.On the basis of the keen observation and evaluation; it is proved that our deep learning model has produced a promising set of results. As compared to the other machine learning algorithms like Naïve bayes, random forest, kNN using the same dataset the detection rate of the implemented method was exceptionally high. Another important matter is the time it takes to complete the entire function, the time required to train our model is drastically and commendably reduced. While classifying the KDD Cup '99 dataset, [3] Kim *et al.*, achieved an accuracy of 96.93%. Also, Gao *et al.*, [6] developed a deep learning based DBN model and it achieved an accuracy of 93.49%. As compared to both the methods, the proposed model obtained much better accuracy. These comparisons show that the result of the proposed is very promising and very much successful and when compared to other existing current deep learning based methods it is proved to have shown better efficiency.

V. CONCLUSION

In this paper a detailed description about Intrusion detection system and its different types have been discussed. A brief definition on deep learning is also included. The dataset that is employed is the KDD Cup dataset. Lot of issues persists in this dataset and these issues have been discussed in detail and the various methods that can be implemented in order to eliminate those problems have also been discussed. The result has been showcased in a graphical representation to get a clear understanding of the problem. A deep learning based model was proposed for the IDS and was implemented using tensorflow. The obtained results show an outstanding accuracy for the proposed system. The results have demonstrated that the proposed approach offers high levels of accuracy and precision along with reduced training time. As future scope, the detection can be done in real-time bases for a better performance based intrusion detection system. In real-time detection lot of advantages as well as disadvantages are present. If the intrusion detection system is able to detect the threat and reports it immediately, then the damage caused by the intrusion can be limited. In this particular work, intrusion detection is performed, as a future expansion of this work, prevention methods can also be included. Intrusion prevention system is able to block potential threats. They monitor log and report activities similar to IDS but they are also capable of stopping threats without the administrator getting involved.

REFERENCES

[1] Inadyuti Dutt, Samarjeet Borah, Indra Kanta Maitra, Kuharan Bhowmik, Ayindrilla Maity and Suvosmita Das *"*Real-Time Hybrid Intrusion Detection System Using Machine Learning Techniques", *Springer*, Vol. 462, pp. 885-894, 2018

[2] Jabez, and Dr. B. Muthukumar, *"*Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach*"*, *Procedia Computer Science*, Vol. 48, pp. 338-346, 2015

[3] Dongseong Kim, Hanam Nguyen, Syngyup Ohn, and Jongsou Park, "Fusions of GA and SVM for anomaly detection in intrusion detection system", *Springer*, Vol. 3498, pp. 415-420, 2005

[4] Kwangjo, Kim, Muhamad Erza, Aminanto, Harry Chandra and Tanuwidjaja, "Network Intrusion Detection using Deep Learning ", *Springer Briefs on Cyber Security Systems and Networks*, pp. 978-981, 2018

[5] Wathiq Laftah Al-Yaseen, Zulaiha Ali Othman and Mohd Zakree Ahmad Nazri, "Real-Time Intrusion Detection System Using Multi-agent System", *IAENG International Journal of Computer Science*, pp.1-11, 2016

[6] N. Gao, L. Gao, Q. Gao and H. Wang, "An Intrusion Detection Model Based on Deep Belief Networks," *2014 2nd Intl.Conf. on Advanced Cloud and Big Data*, Huangshan, pp. 247-252, 2014.

[7] Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam *"A Deep Learning Approach for Network Intrusion Detection System"*, BICT, 2016 pp. 03-05 ICST , December 2015.

[8] N. Shone, T.N. Ngoc, V.D. Phai and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," in *IEEE Transactions on Emerging Topics in Computational Intelligence*, Vol. 2, No. 1, pp. 41-50, Feb. 2018.

[9] A.S Sodiya, O.A Ojesanmi, O.C Akinola. and O. Aborisade "Article: Neural Network based Intrusion Detection Systems*"*. *International Journal of Computer Applications*, Vol.106, pp. 19-24, Nov. 2018.

[10] B. Subba, S. Biswas and S. Karmakar, "Enhancing effectiveness of intrusion detection systems: A hybrid approach," *2016 IEEE International Conference on Advanced Networks and Tele communications Systems (ANTS)*, Bangalore, pp. 1-6, 2016

[11] Sumanta Kumar Deb, Ankan Bhowmik, Biswajit Maity, Abhijit Sarkar, and Amitava Chattopadhyay "Wi-Fi Optimization Using Parabolic Reflector and Blocking Materials in Intrusion Detection Systems,*" Emerging Technologies in Data Mining and Information Security*, Vol. 814, pp. 761–771, 2018.

[12] T.A. Tang, L. Mhamdi, D. McLernon, S.A.R. Zaidi and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," *2016 Intl.Conf. on Wireless Networks and Mobile Communications*(WINCOM), pp. 258-263, 2016.

[13] Nabil El Kadhi, Karim Hadjar and Nahla El Zant, "A Mobile Agents and Artificial Neural Networks For Intrusion Detection", *Journal Of Software*, Vol. 7, No. 1, pp. 156-160, 2012

[14] Z. Wang "Deep Learning-Based Intrusion Detection with Adversaries", *IEEE Access*,Vol. 6, pp. 38367-38384, 2018

[15] Berlin H. Lekagning Djionang and Gilbert Tindo, "Network Intrusion Detection Systems based on Neural Network: A Comparative Study*"*, *International Journal of Computer Applications* Vol. 157, No. 5, pp. 42-47, 2017