# Comparison Between Extreme Learning Machine and Fast Learning Network Based on Intrusion Detection System

Mohammed Hasan Ali and Mustafa Musa Jaber

March 4, 2021

# Comparison between Extreme Learning Machine and Fast Learning Network Based on Intrusion Detection System

**Mohammed Hasan Ali**[1]**, Mustafa Musa Jaber**
[1] Computer Techniques Engineering Department, Faculty of Information Technology, Imam Ja'afar Al-sadiq University, Najaf, Iraq
Department of Computer Science, Dijlah University College, Baghdad, Iraq

**Abstract: Currently, Intrusion Detection System (IDS) design based on machine learning algorithms achieved better results in compare with traditional intrusion detection system. Moreover, Extreme Learning Machine (ELM) and Fast Learning Network (FLN) are represents a popular machine learning Algorithms that had been gives promising results when applied in several fields. This work proposed a comparison between ELM and FLN based on intrusion detection system with different numbers of Neurons to analysis the impact of algorithms architecture based IDS accuracy.**

**Keywords:** Fast Learning Network, Intrusion Detection System, Machine learning

## 1.Introduction

Technology has over the many years impacted the current days based on several applications like marketing, shopping, and messaging [1]. A major problem is that these networks are steadily exposed to numerous online threats which threaten their availability and integrity and as such, demands to be protected from intrusion and violation. In 2015, the U.S. Director of NSA, Adm. Michael Rogers, in the House Intelligence Committee, warned of an impending major security attack in the U.S. in the next decade. In his words, "It's only a matter of the 'when,' not 'if,' that we are going to see something dramatic." Several state-backed hackers have continuously launched attacks on industrial control systems that manage vital infrastructures, such as nuclear power, power grid, transportation systems, and air-traffic control. The NSA director also opined that, based on his own assessment, the U.S. may fall into these attacks [2].

Furthermore, Intrusion Detection System (IDS) is one of the powerful software or hardware [3] that is used to monitor computer network for the detection of normal or abnormal behaviors [4][5]. An IDS monitors a network for signs of invasion which could manifest in abnormal system behaviors or violation of network security policies. Moreover, there are several limitations of the conventional IDS [6], [7], such as high rate false alarms, lack of continuous adaptation to changing malicious behaviors, and highly uneven data distribution. Furthermore, the incorporation of machine learning (ML) can enhance the performance of IDS [8], [9] as the ML algorithms can ensure optimum performance. This work provides several contributions based on ML models: firstly, analysis of the most popular machine learning algorithms Extreme Learning Machine (ELM) and Fast Learning Network (FLN) algorithm based on IDS, secondly, proposed different neurons number in hidden layer to analysis the impact of both algorithms architecture, which can fill the gaps in the current ML models based on IDS.

## 2. Overview of Intrusion Detection System

Technological advancements in the present world have made connectivity easier than ever [10]. A large amount of information (personal, military, government, and commercial) are hosted on network infrastructures worldwide. The security of network infrastructures is attracting great research interest due to the huge number of intellectual properties which can be easily acquired through the internet. The society has become over-reliant on technology as people depend on computer systems for their daily information and entertainment [11].

Moreover, IDS represents one of powerful security tool which monitoring the system activities for any abnormal system behaviors or violation of network security policies. Moreover, IDS perform several functions [12] such as Monitors and analyzes the activity of the system users and Checks the critical system and data file integrity. In general IDS techniques divided into anomalies or signatures of attack are used by the detection system for the detection of attacks, and these techniques determine the effectiveness of an IDS [9], [13]. In addition, machine learning algorithms based intrusion detection system achieved promising results in several works [14], [15][16] which represent a motivation for analysis the most popular machine learning algorithms(ELM) and (FLN) and their architecture impact based on IDS.

## 3. Overview of Machine Learning Based IDS

The conventional techniques like firewalls, encryption, and access control have been proven inefficient in adequately protecting networks from the ever-increasingly forms of attacks and malware [12]. Consequently, the IDS have been developed as an indispensable aspect of security systems which is used for the detection of attacks even before they occur [17] [18]. There are certain issues to consider when building IDS, issues like data collection, intrusion recognition, data pre-processing, reporting, and response. The most important among these issues is intrusion recognition.

There are several machine learning algorithms have been proposed as IDS models such as Support vector machine (SVM) and Artificial neural network (ANN) [19], ELM[20][21]. This work proposes most popular machine learning algorithms (ELM and FLN) to analysis the performance based IDS and explain the number of neurons impact based on IDS

## 4. Results of ELM Vs FLN Comparison

In order to validate the efficiency of FLN[22] and ELM[23] based classification NSL-KDD data set [24] which represent one of accurate IDS Dataset, results of accuracy as the best and mean of all runs, detection rate (DR), false alarm rate (FAR), recall, precision, F-measure (F.M), Maximum accuracy (MAX.Acc), Average accuracy (AVR. Acc) and G-mean (G.M) are compared with ELM. Moreover, in Figure 4.1 which provides different structure based on number of neurons, it can be concluded that FLN has outperformed ELM from the perspective of all measures. In following Table.1 shown the comparison results are between FLN and ELM based standard evaluations.

Table .1 The Comparison result between ELM and FLN

| No.Neurons | Model | MAX.Acc | AVR.Acc | DR | FAR | Precision | Recall | F.M | G.M |
|---|---|---|---|---|---|---|---|---|---|
| **10** | ELM | 0.9255 | 0.8956 | 0.9047 | 0.1545 | 0.8956 | 0.8955 | 0.8955 | 0.8061 |
| | **FLN** | **0.9641** | **0.9591** | **0.9586** | **0.0485** | **0.9588** | **0.9591** | **0.9587** | **0.9216** |
| **25** | ELM | 0.9521 | 0.9471 | 0.9418 | 0.0695 | 0.9469 | 0.9472 | 0.9471 | 0.8977 |
| | **FLN** | **0.9738** | **0.9669** | **0.9624** | **0.0441** | **0.9668** | **0.9666** | **0.9665** | **0.9367** |
| **35** | ELM | 0.9631 | 0.9548 | 0.9501 | 0.0591 | 0.9632 | 0.9628 | 0.9629 | 0.9124 |
| | **FLN** | **0.9785** | **0.9735** | **0.9696** | **0.0301** | **0.9781** | **0.9779** | **0.9783** | **0.9479** |
| **50** | ELM | 0.9709 | 0.9652 | 0.9593 | 0.0478 | 0.9706 | 0.9701 | 0.9709 | 0.9321 |
| | **FLN** | **0.9821** | **0.9803** | **0.9808** | **0.0247** | **0.9818** | **0.9822** | **0.9821** | **0.9606** |

The Table.1, shown the maximum (Best) and average accuracy (Mean), are computed for each algorithms (ELM, FLN), the experiments results taken as average for fifteen runs. The results of FLN based on a double parallel forward neural network, with this parallel connection of a multilayer feedforward neural network and a single layer feedforward neural network, and the DPFNN's output nodes not only receive the recodification of the external information through the hidden nodes, but also receive the external information itself directly through the input nodes.

This extra information will increase the learning rate of the model, which lead to make the FLN represented with less number of hidden neurons in hidden layer higher accuracy than the ELM as showed in Figure.1. Moreover, ELM shown higher false alarm rate in compare with FLN because of less number of weights in ELM in compare with FLN. In the following figures shown the comparisons between ELM and FLN with consideration for each part of number of neurons (10, 25, 35 and 50). Moreover, the average accuracy that FLN achieved better that ELM in all proposed different structures in this work with maximum accuracy 0.9821 achieved by FLN with 50 neurons in hidden layer.  In both algorithms showed the impact of neurons in hidden layer based accuracy. Moreover, the FLN with only 10 neurons in the hidden layer got higher accuracy than ELM with 10,25 and 35 neurons in the hidden layer, which means achieved high accuracy with less complexity.

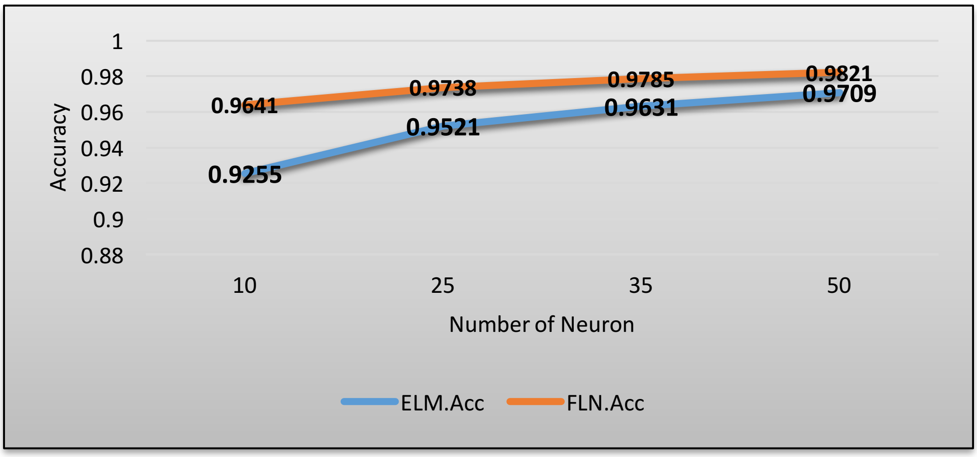

Figure .1 comparison of ELM vs FLN accuracy based number of neurons

In Figure.1, showed how the accuracy increase not in the same rate for both algorithms. The increase rate of accuracy is less in ELM algorithm because its start with low accuracy in compare with FLN in 10 hidden neurons which means based on the 2.6.1 section that represents the impact of double parallel forward neural network in FLN instead of single hidden layer in ELM algorithm. And even with 50 neurons the ELM accuracy didn't get equivalent FLN accuracy, which mean still need more hidden neurons to reach the same level with FLN accuracy.

## Conclusion

In general intrusion detection system based on machine learning achieved better results in compare with traditional methods of intrusion detection system. moreover, the results of this work showed the impact directly of both the increase in learning rate and number of neurons based on the intrusion detection performance and that which make FLN achieved better accuracy than ELM. As future work most of machine learning algorithms still facing limitation that can represent negative effect based on intrusion detection performance.

**Reference**

[1] H. A. S. Ahmed, M. H. Ali, L. M. Kadhum, M. Fadli, B. Zolkipli, and Y. A. Alsariera, "A Review of Challenges and Security Risks of Cloud Computing," *J. Telecommun. Electron. Comput. Eng.*, vol. 9, no. 1, pp. 87–91, 2016.

[2] J. M. Fossaceca, "Application of a Novel Multiple Kernel Learning Framework for Improving the Robustness of Network Intrusion Detection," no. December 1992, 2015.

[3] M. H. Ali, M. F. Zolkipli, M. M. Jaber, and M. A. Mohammed, "Intrusion detection system based on machine learning in cloud computing," *J. Eng. Appl. Sci.*, vol. 12, no. 16, pp. 4241–4245, 2017.

[4] E. Vasilomanolakis, S. Karuppayah, M. A. X. M. Uhlh, and M. Fischer, "55 Taxonomy and Survey of Collaborative Intrusion Detection ¨ ¨," vol. 47, no. 4, pp. 1–33, 2015.

[5] M. H. Ali, M. Fadlizolkipi, A. Firdaus, and N. Z. Khidzir, "A hybrid Particle swarm optimization -Extreme Learning Machine approach for Intrusion Detection System," *2018 IEEE Student Conf. Res. Dev.*, pp. 1–4, 2019.

[6] S. A. R. Shah and B. Issac, "Performance comparison of intrusion detection systems and application of machine learning to Snort system," *Futur. Gener. Comput. Syst.*, vol. 80, pp. 157–170, 2018.

[7] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Syst. Appl.*, vol. 67, pp. 296–303, 2017.

[8] M. H. Ali, K. Moorthy, M. Morad, and M. A. Mohammed, "Propose a New Machine Learning Algorithm based on Cancer Diagnosis," no. October 2018, 2019.

[9] M. H. Ali and M. F. Zolkipli, "Review on Hybrid Extreme Learning Machine and Genetic Algorithm To Work As Intrusion Detection System in Cloud Computing," vol. 11, no. 1, pp. 460–464, 2016.

[10] M. H. Ali1, "TOWARDS A EXCEPTIONAL DISTRIBUTED DATABASE MODEL FOR MULTI DBMS." pp. 553–560, 2014.

[11] Bhavya Daya, "Network security: History, importance, and future," *Univ. Florida Dep. Electr. ...*, p. 13, 2013.

[12] T. Kaur, V. Malhotra, and D. Singh, "Comparison of network security tools-Firewall,

Intrusion Detection System and Honeypot," *Int. J. Enhanc. Res. Sci. Technol. Eng.*, vol. 3, no. 2, pp. 200–204, 2014.

[13] U. Kumar, "A Survey on Intrusion Detection Systems for Cloud Computing Environment," vol. 109, no. 1, pp. 6–15, 2015.

[14] M. H. Ali, "Review on hybrid extreme learning machine and genetic algorithm to work as intrusion detection system in cloud computing," no. January, 2016.

[15] M. H. Ali and M. F. Zolkipli, "Model of Improved a Kernel Fast Learning Network Based on Intrusion Detection System," pp. 1–12, 2019.

[16] W. L. Al-yaseen, Z. Ali, M. Zakree, and A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Syst. Appl.*, vol. 67, pp. 296–303, 2017.

[17] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Intrusion Detection Techniques in Cloud Environment: A Survey," *J. Netw. Comput. Appl.*, vol. 77, no. October 2016, pp. 18–47, 2016.

[18] M. H. Ali and M. F. Zolkipli, "Model of Improved a Kernel Fast Learning Network Based on Intrusion Detection System Model of Improved a Kernel Fast Learning Network Based on Intrusion Detection System," no. January, 2019.

[19] W. H. Chen, S. H. Hsu, and H. P. Shen, "Application of SVM and ANN for intrusion detection," *Comput. Oper. Res.*, vol. 32, no. 10, pp. 2617–2634, 2005.

[20] J. M. Fossaceca, T. A. Mazzuchi, and S. Sarkani, "Expert Systems with Applications MARK-ELM : Application of a novel Multiple Kernel Learning framework for improving the robustness of Network Intrusion Detection," *Expert Syst. Appl.*, vol. 42, no. 8, pp. 4062–4080, 2015.

[21] M. H. Ali, M. F. Zolkipli, M. A. Mohammed, and M. M. Jaber, "Enhance of extreme learning machine-genetic algorithm hybrid based on intrusion detection system," *J. Eng. Appl. Sci.*, vol. 12, no. 16, pp. 4180–4185, 2017.

[22] P. Niu, K. Chen, Y. Ma, X. Li, A. Liu, and G. Li, "Model turbine heat rate by fast learning network with tuning based on ameliorated krill herd algorithm," *Knowledge-Based Syst.*, vol. 118, pp. 80–92, 2017.

[23] G. Huang *et al.*, "Extreme learning machine: a new learning scheme of feedforward neural networks," *Neural Networks, 2004. Proceedings. 2004 IEEE Int. Jt. Conf.*, vol. 2, no. August 2004, pp. 985–990 vol.2, 2004.

[24] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *IEEE Symp. Comput. Intell. Secur. Def. Appl. CISDA 2009*, no. June, 2009.