An Overview of Machine Learning Optimization Model for Network Intrusion Detection (MLOM-NID).

Yoro R.E.
Department of Computer Science
Delta State Polytechnic
Ogwashi-Uku, Delta State, Nigeria
E-mail: rumerisky@yahoo.com; rumerisky5@gmail.com

ABSTRACT

Network attacks across the globe, has become the largest threat to organizations proprietary data, with the possibility of it affecting every organization. With the rapid growth of technological advancement affecting networked devices, hackers have improved their fastidious intent, perfectly exploring vulnerabilities from ignorant security breaches created by organizations, individuals and poor systems monitoring. Intrusion Detection Systems (IDSs) are an integral facet of system and organization security which has gained recognition across the globe. The effectiveness and efficiency of these systems are usually determined by prompt and reliable response in detecting unauthorized network access from network intruders- malicious system hackers. In other to address these issues, prerequisite knowledge was drawn from notable journals while network experts were randomly interviewed for information pertaining to network traffic abnormalities, network size and uniformity of data. The prerequisite knowledge was studied carefully in close collaboration with platform integration techniques. The Machine Learning Optimization Model for Network Intrusion Detection (MLOM-NID) was built on the premise of Genetic Algorithm (GA) and Modular Neural Network (MNN) which was the anchor for the model. GA provides feature selection while MNN provides a flexible machine learning paradigm. The Machine Learning Optimization Model for Network Intrusion Detection (MLOM-NID) was designed, implemented and validated for network intrusion detection solely. The designed model was not initiated with prevention and correction of network features as additional functionalities. Consequently, the possibility of prevention time, correction time, resources lost and resources management were not considered. These issues are beyond the scope of this research and further researchers can do well do delve into this.

Keywords: MNN, MLOM, NID, Intrusion, Genetic Algorithms, Optimization, Model, Machine Learning

iSTEAMS Conference Proceedings Paper Citation Format
Ojo, A.K. & Akinnifesi, A.S. (2019): An Overview of Machine Learning Optimization Model for Network Intrusion Detection (MLOM-NID)..
Proceedings of the 14th iSTEAMS International Multidisciplinary Conference, AlHikmah University, Ilorin, Nigeria, Vol. 14, No 2 Pp 275-286

1. INTRODUCTION

Information is crucial to organizational survival, efficiency and effectiveness. It is the bedrock of today society, which is disseminated through Information and Communication Technology (ICT) supported with numerous multimedia devices to enhance human productivity in daily activities (Samantha, 2014). Despite, the fundamental benefits obtained from the amalgamation of machine learning in predicting Intrusion Detection System (IDS) features in different models, its prediction, possibly has been questionable due to the escalation of intrusion even with these trained models (Kruegel et al. 2003; Nahla et al. 2004; Sampada et al. 2004; Adel et al. 2006; Mehdi et al, 2007; Shanmugavadivu and Nagarajan, 2011, Nitin et al. 2013, Angel and Ramamoorthy, 2015, Nenekazi 2017). Could this issue be traced to poor features (noisy or vilest features) used for machine learning?
These devilments of intrusion, could be linked to lack of features optimization prior to machine learning. With an

intrusion attack recorded every 44 seconds, 58, 727 per hour, 2645 per minutes and large scale distributed denial of services (DDOS) increasing by 500%, only 38% of organization globally claim preparedness in handling sophisticated attack, in spite of the huge connected networked devices (roughly 200 billion) and the total cost for intrusion attacked estimated globally at $1trillion dollars as at 2018 (Cybint, 2018). Intrusion Detection Systems (IDSs) are an integral facet of system and organization security which has gained recognition across the globe. The effectiveness and efficiency of these systems are usually determined by prompt and reliable response in detecting unauthorized network access from network intruders- malicious system hackers (Sampada et al. 2004, Adel et al., 2006; Samantha, 2014).

2. RELATED WORK

Hussain et al., (2014) presented an Overview of Intrusion Detection System (IDS) along with its commonly used techniques and classifications. The research focused on the types and different techniques which are commonly applied. This research also focal innovative approach for new knowledge in providing Intrusion detection system. The network-based IDS, Host-Based IDS and Hybrid Based IDS were also consider and discussed. It was observed finally, that the system detects intrusion and attack more accurately than other security systems providing less fewer false positive alarm rate.

Chia-Mei et al. (2016), applied Hidden Markov Model in identifying anomaly in network intrusion detection due to the inability of the current defence products failing to providing sensor input diversity. The research provides a sequence of attack corresponding to stages attacks and the proposed system adopted. The experimental results show that the proposed detection system has the potential of identifying attacks efficiently. Priyanka and Rakesh (2016), provided a comprehensive review of different soft-computing approaches applicable in solving intrusion detection. The research considers fuzzy logic, support vector machine, neural network and even evolutionary computing. The research also briefly explores certain cyber security challenges- cutting across vulnerability and intrusion. Finally, it was established that soft computing should be explored fully in most endeavours.

Mohit et al., (2017) provided an Intrusion Detection System (IDS) survey focused on types of intrusion methods, attacks types, varied tools and techniques, research needs and challenges. The research finally developed an IDS tools research purpose. The system comprises of IDS-Sensor (packet and behavior signatures), Backend (Event recording of database) and Frontend (user interface, control and commands). The system is capable of addressing denial of services, distributed denial of services and SYN- synchronization. Conclusively, the system was citified performance efficient. Nenekazi et al. (2017) provided an intrusion detection system for predicting Neptune (TCP SYN) flooding attack based on Fuzzy logic. The research was employed based on the fundamentals of fuzzy logic- fuzzification, membership function attainment, rule generation and defuzzification. In this research a NSL KDD which is an extended form of KDD99 dataset was employed in experimental analysis. The experimental result was subsequently compared with decision tree result which shows that the performance differ in terms of predicting Neptune proportion cases were negligible.

Shahid et al. (2017) provided a fundamental survey cutting across intrusion response system and intrusion detection system relying on an in-depth understanding of the response option for varied network attack. The claims the usefulness of the survey is based on an in-depth understanding of response option tied to varied network. The research claims that relevant findings will assist network administrator and network staffs in understanding tackling methods. Yuancheng et al., (2017) presented an Intrusion Detection System using Sequence Extreme Learning Machine (OSELM) in advance metering infrastructure of Smart grid. These was subsequently used in AMI and carrying out a comparative analysis with other algorithms. The research employed Home Area Network (HAN), Wireless Area Network (WAN), Far Area Network (FAN) and Near Area Network (NAN).

The research also employed data preprocessing, initialization phase, online sequence learning phase. The Simulation

results when compared with other intrusion detection methods, intrusion detection method based on OS-ELM is more superior in detection speed and accuracy. Mageswary and Karthikeyan (2018) used K-Means algorithms in determining Denial of service (DOS) attack. The failure rate of various approaches- clustering and classification approach was identified due to anomaly detection methods generate high false positive and negative. Using K- means clustering algorithms, the KDD cup 1999 dataset was analyzed.

Table 2.1: Literature Review (LR) pertaining to Intrusion detection System (IDS) and Artificial Intelligence (AI)

SN	Author (Year of Research)	LR of Evaluation Components				Explored Methods
		Intrusion Detection System (IDS)	Data Optimization	Model Classification	Machine Learning	
1.	Wenke et al. (1998)	✓			✓	Association Rule (AR)
2.	Kruegel et al. (2003)	✓			✓	Bayesian Network (BN)
3.	Nahla et al. (2004)	✓			✓	Naïve Baye (NB) + Decision Tree (DT)
4.	Sampada et al. (2004)	✓		✓	✓	SNORT- Artificial Neural Networks (ANN)+ Fuzzy inference System (FIS
5.	Adel et al. (2006)	✓		✓	✓	Adaptive Neuro Fuzzy Inference System (ANFIS)
6.	Mehdi et al.(2007)	✓		✓	✓	Bayesian Classification Procedure (BCP) + Artificial Neural Network (ANN)
7.	Shanmugavadivu and Nagarajan (2011)	✓		✓		Fuzzy Logic (FL)
8.	Nitin et al. (2013)	✓		✓	✓	ANFIS
9.	Angel and Ramamoorthy (2015)	✓	✓	✓		Genetic Algorithm (GA) + Fuzzy Logic (FL) +
10.	Nenekazi (2017)	✓		✓		Fuzzy Logic (FL)
11.	Yuancheng et al., (2017)	✓			✓	Sequence Extreme Learning Machine (OSELM)
MLOM-NID PROJECTION						
12.	MLOM-NID	✓	✓	✓	✓	Genetic Algorithm (GA) + Modular Neural Network (MNN)

Compared with other approaches the K-clustering algorithms generated better results with low false positive rate achieved. Umesh (2018), presented a Log Based Intrusion Detection System based on the failures in preventing cyber-

attack in spite of tremendous technologically innovative growth. The research presented an extension Host- Based Intrusion (HIDS) - Log Based Intrusion System. Each log is monitored based on services provided by the system in collaboration with light-weight agent installed on the system. Conclusively, the research extended current log-based Intrusion Detection System.

Table 2.1 identify two fundamental limitations associated with existing intrusion detection models.

a. Most reviewed literatures focused sparsely on data optimization prior to machine learning.
b. Most literature focused on data classification ignoring data optimization

Concept of Optimization: Optimization is concerned with minimizing or maximizing cost function tied to certain constraint with the essence of obtaining desired results. Optimization processes are carried out iteratively or incrementally comparing obtained solutions until optimum (optima) solution are obtained. The technological development of computers and computer-based technologies has fostered the need in applying optimization within computer-based design and processes.

Optimization can be seen from two main perspectives

a. Deterministic Optimization: These optimizations apply rule generalization in obtaining best. It is an iterative process with its rules moving the solution toward optimal end.
b. Stochastic Optimization: Stochastic optimization apply probabilistic rules in obtaining desired results.

Optimization are usually obtained comparing few alternative generated results with potential generated solutions. This is combined with prior problem knowledge investigating the reliability of each generated result based on their objective function of each solution with weaker solution dropped. These integral components vary greatly with each problem domain. The first thumb rule of the formulation of an optimization problem is to choose as few design variables as possible. Feature Selection (FS): They are closely aligned toward soft computing. FS are employed in identifying best features used in constructing mathematical induced of non-mathematical model (Bermingham et al., 2005). Features selection enhances simplification for model classification and rule classification. Overtime, data redundancy and poor accuracy in prediction has attuned feature selection in obtaining best features. Redundant or irrelevant features are intricately linked which must be cater for data optimization

Feature Selection Algorithms (FSA): Feature selection algorithms are meta-heuristic algorithms designed for searching experimental data and obtaining relevant (optimal features). Usually these algorithms maybe computationally intensive, less optimal and less evolving depending on designed techniques, goal and result attainment. The three main categories of feature selection and extraction algorithms (Gareth, 2013 and Bermingham, et al., 2015): Wrappers, Filters and Embedded selection.

a. Wrapper Selection these techniques are one of the fore most feature selection techniques. These techniques encompass certain algorithms which are designed to apply a certain score based on features evaluation and objective function presentation. This approach counts and records usually the number of mismatch (errors or variances) for each feature which has been subsequently identified by the algorithm. These scores are compared and subsequently evaluated in determining iterative movement to subsequent generation. Wrapper model are usually computationally intensive and promises optimal features. Wrapper selection usually present specific model features are which are incompatible with models in general
b. Filter Selection methods are concerned with determining closeness of potential solution as opposed to error or mismatch counts. These approaches are opted for due to speed and optimization time- less computationally intensive which usually result in less optimal features and models generic features. Overtime approaches such as point –wise, SNP, Weich-Test, Eigenvector Centrality FS and Infinite Eigenvector has largely implemented filter selection. These approaches are locked ranking and ranking techniques (Guyon and Elisseeff, 2003). Some implementation has used filter methods as pre-processor prior to varied techniques.
c. Embedded Selection is an amalgamation between wrapper and filter methods. These approaches identify the best advantage of both and applied them in bringing up an optimal algorithm capable of addressing feature

selection. Therefore, it enacts both feature selection as part of the optimization, identify generic or eccentric feature, and employ computational intensiveness while providing model specific or generic features (Zares, 2013). Recursive Feature Elimination (RFE) + Support Vector Machine (SVM). Genetic Algorithm (GA) + Iterative Local Search are all algorithms implementing embodied selection.

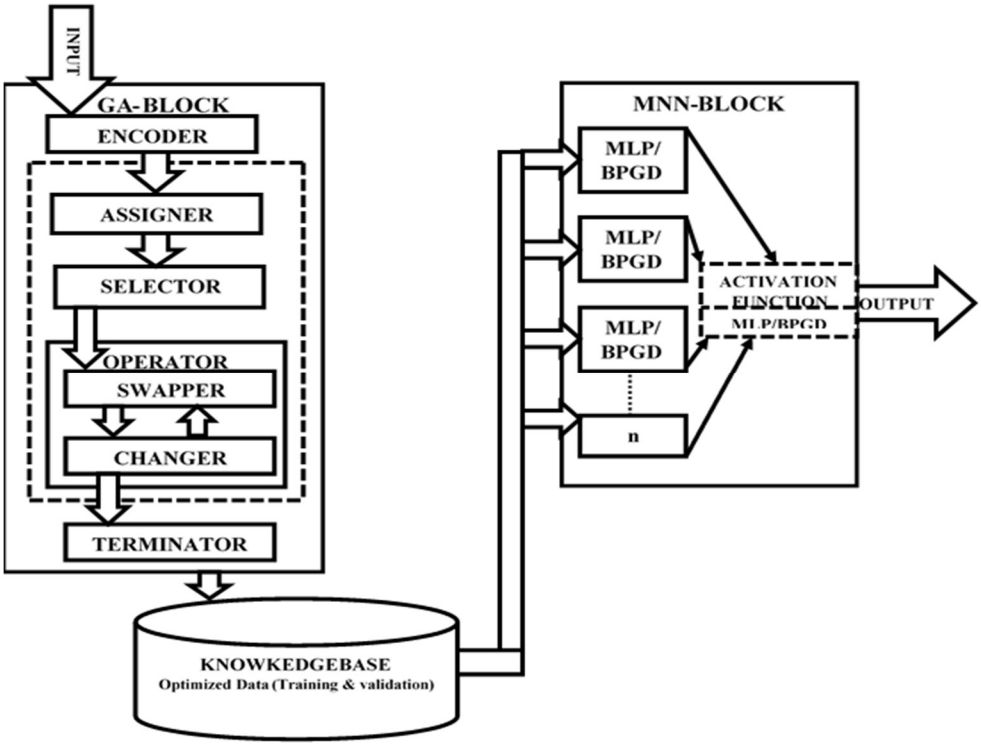
3. METHODOLOGY

The research methodology was conceived after an extensive literature reviews of associated works boarding on network intrusion detection. Prerequisite knowledge was studied carefully in close collaboration with platform integration techniques described in Gheorghe P. and Bogdan, 2011 Shanmugavadivu and Nagarajan, 2011; Pandeeswari and Ganeshkumar 2015; Mageswary and Karthikeyan 2018. Subsequently, a Machine Learning Optimization Model for Network Intrusion Detection (MLOM-NID) was conceptualized toward addressing feature optimization and machine learning combining the strength of Genetic Algorithm (GA) and Modular Neural Network (MNN).

4. RESULT/DISCUSSION

Malicious attacks sponsored by cyber hackers has bedevilled network system continually is an enhanced model conceptualized intuitionally and computationally understudying the demerits of existing intrusion detection models as presented in Wenke et al. 1998, Kruegel et al. 2003, Nahla et al. 2004, Sampada et al. 2004, Adel et al. 2006, Mehdi et al.2007, Shanmugavadivu and Nagarajan 2011, Nitin et al. 2013, Angel and Ramamoorthy 2015 and Nenekazi 2017 Yuancheng et al., 2017 which has thrust this model - Machine Learning Optimization Model for Network Intrusion Detection (MLOM-NID) toward the pinnacle in addressing these issues. MLOM-NID was proposed taking cognizant of present constraints which has bedeviled current models – an appropriate machine learning technique with the capability of offsetting the current rigid approach adopted in predictive machine learning was employed. Optimization has overtime been seen as the pinnacle in machine learning due to its propensity in presenting clear, clean and optimized data with minima noise (errors in variances) and preventing over fitting and under fitting - this has been sparsely utilized in existing models. MLOM-NID was designed to address these issues. MLOD-NID is trained with the most appropriate machine learning tool. MLOD-NID is built on current network intrusion data. MLOD-NID is built to address dataset optimization prior to machine learning using the most appropriate optimization tools (stochastic search/meta-search algorithm). This algorithm is all compassing, it is flexible and adaptive to its iterative sequence eliminating pros and cons for ambiguity and ingenuity in optimization.

The Machine Learning Optimization Model for Network Intrusion Detection (MLOM-NID) was built on the premise of Genetic Algorithm (GA) and Modular Neural Network (MNN) which was the anchor for the model. GA provides feature selection while MNN provides a flexible machine learning paradigm. The model was conceptualized after a careful study of the models presented in Gheorghe P. and Bogdan, 2011 Shanmugavadivu and Nagarajan, 2011; Pandeeswari and Ganeshkumar 2015; Mageswary and Karthikeyan 2018. The MLOM-NID designed model is depicted on Figure 4.1



Keys
MLP: Multi-layered Perceptron
BPGD: Back Propagation Gradient Descent
n: Number of network attacks subsequently trained using MNN

Figure 4.1: Machine Learning Optimization Model for Network Intrusion Detection (MLOM-NID)

The functional design of the Machine Learning Optimization Model for Network Intrusion Detection (MLOM-NID) identify associated tools used for the design. These design concept spans both the integral tools and techniques for the Genetic Algorithm (GA) block and the Modular Neural Network (MNN) blocks. The GA-Block is the first facet of the MLOM-NID while the MNN is the second phase of the MLOM-NID. Where the input interface is the frontier of the MLOM-NID. It is linked with the GA-Block and tasked with receiving the ADFA-ID dataset in its rawest format and transmitting it to the first GA component-encoder. The GA-Block is the facets of the MLOM-NID tasked with dataset optimization. It received these datasets as input from the input module and apply GA- fundamentals in repositioning these datasets into an optimized data. It applies the fundamentals of GA of a seen as: ENCODER, ASSIGNER, SELECTOR, OPERATORS (SWAPPER and CHANGER) and TERMINATOR.

These components are applied iteratively until termination, at which point an optimal dataset has been obtained. The encoder is the first GA-Block component, it collects the dataset from the input module of the MLOM-NID and apply encoding techniques in reorganizing the dataset in GA simulation format. It is the encoding that supports value placement and repositioning within the MLOP-NID. The GA-Block under the MLOM-NID implement value-encoding due to real value structure, usability in neural network (NN) and positioning placement. It also supports machine learning through the provision of label greater than two (2), an added advantage not simplified, possibly with another encoding scheme. The assigner is the second GA-Block component, it accepts the encoder dataset from the encoder module of the GA-Block and assign an appropriate fitness function. It is the objective function and the fitness function that subsequently fostered selection and operator's enactment.

This fitness function assignment is based on the adaptation of a Mohammed et al. (2012) objective function was subsequently adapted based on selective features, total feature and external feature not currently exhibited or presented within our dataset. It is the assignment of these fitness values through the objective function that invariably paved the way in identifying optimal features from less optimal feature.

The selector is the third GA-Block component, it accepts the fitness assigned dataset from the assigner module of the GA-Block and apply, probability, cumulative probability and Roulette Wheel Selection (RWS) in distinctly separating highly optimal dataset features from less optimal dataset features. The probability determines the overall probability of selecting an individual from the overall population space. It is the probability that determines chance and selection. The cumulative probability provides for probability accuracy through the provision of cumulative summation with the range of one. This value determines that all probability values have been accurately assigned. It is on the premise of this, that RWS apply a dual selection rule which must be true in other to obtain optimal features. The RWS was employed due to its ability in obtaining optimal features, although the issues of premature converge was addressed through sequential arrangement of successive feature and case. The operator is the fourth GA-Block component, it accepts the selected optimal feature samples and apply GA-operator in other to create diversity within dataset space. Its operator application also presents or eliminate dataset stagnation toward a local optimum or global. It is the operator that create novel features within the dataset state space. MLOM-NID implement swapper and changer operators. The swapper is modelled after the single point crossover while the changer is modelled after non-uniform mutation in addressing GA operators.

The terminator is the fifth GA-Block component, it accepts the selected optimal feature which has subsequently be optimized applying fitness value, selection, operator iteratively for each GA-generation. The stochastic nature of GA optimization can ensure infinite optimization for the MLOM-NID. Therefore, in truncating the MLOM-NID, a Stall generation stopping criteria was applied. The MLOM-NID knowledge-Base (KB) is a specialized database employed in accommodating process component- optimized dataset, machine learning and validation data. Therefore, structure and unstructured processing is allowed within this domain. The knowledgebase component serves as operational input for the Modular Neural Network (MNN). This contains are sequentially obtained. The MNN-Block is the facet of the MLOM-NID tasked with the machine learning. It received as input, the optimized machine learning dataset from the GA-Block subsequently partitioned. The MNN-Block comprises of modules of Neural Network (NN) each dedicated to a particular attack. The multilayer feed forward or multi-layer perceptron (MLP) was applied for each module. The MLP apply a Back Propagation Gradient Descent (BPGD) algorithm in addressing machine learning. The number of modular MLP is consistent with the number of network attacks (n) domiciled with our dataset. These respective NN are subsequently passed to the activation function which invariably arrive at the final summation value.
The final summation values are a concatenation of all independent multilayer feed forward neural network. This value gives the final prediction.

5. CONCLUSION

Unauthorized access to network resources has been predicted to reach an unprecedented height, with 2020 projecting more attacks. Its prediction of unwanted attacks has indeed been worrisome due to the increase of malicious hackers, loss of proprietary properties and the cost implication incurred to many organizations due to these unwanted losses. Although several intelligent models for Intrusion Detection (ID) has been developed for network intrusion, model optimization and machine learning model for these purposes are scanty, thus the need to explore a novel feature selection tools within this area. Although several intelligent models have been developed for network intrusion, the significance of a unified model capable of addressing optimization and machine learning has not been explored, thus the need to explore such model unification.

6. SUGGESTION TO FURTHER WORKS

The Machine Learning Optimization Model for Network Intrusion Detection (MLOM-NID) was designed, implemented and validated for network intrusion detection solely. The designed model was not initiated with prevention and correction of network features as additional functionalities. Consequently, the possibility of prevention time, correction time, resources lost and resources management were not considered. These issues are beyond the scope of this research and further researchers can do well do dive into this.

REFERENCES

1. Abraham, A. (2005), Adaptation of Fuzzy Inference System Using Neural Learning", in Nedjah, Nadia; de Macedo Mourelle, Luiza, Fuzzy Systems Engineering: Theory and Practice, Studies in Fuzziness and Soft Computing 181, Germany: Springer Verlag, pp. 53–83, doi:10.1007/11339366_3.
2. Adel N. T., Mohsen K. Reza M. (2006), Network Intrusion Detection Based on Neuro-Fuzzy Classification, retrieved online from http://cloudbus.org/~adel/pdf/ICOCI2006.pdf.
3. Albrecht S. (1996), A Modular Neural Network Architecture with Additional Generalization Abilities for High Dimensional Input Vectors, retrieved online from http://teco.du/ ~albrecht/neuro/report/.pdf
4. Anderson, R. (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons. pp. 387–388
5. Alabsi, F. and Naoum, R. (2012), Comparison of Selection Methods and crossover Operation using Steady State Genetic Based Intrusion Detection System, Journal of Emerging Trends in computing and information Science, Vol 3. No 7, Pp.11-20.
6. Alabsi, F. and Naoum, R. (2012), Fitness Function for Genetic Algorithm used in Intrusion Detection System, International journal of Applied Science and Technology, Vol. 2 (4): 129-134.
7. Angel A. C. and Ramamoorthy S. (2015), Intrusion Detection System by Combining Fuzzy Logic with Genetic Algorithm, Global Journal of Pure and Applied Mathematics (GJPAM), Volume 11, Number 1, PP. 105 – 110.
8. Babak K. and Jamal B. (2008), An Experience Improving Intrusion Detection Systems False Alarm Ratio by Using Honeypot, 22nd International Conference on Advanced Information Networking and Applications, Pp.997 – 1004.
9. Barron, A. R. (1993), Universal Approximation bounds for Super-positions of a sigmoidal function, IEEE Transactions on Information Theory, IT-39, Pp.930-945.
10. Beale, R. and Jackson, I. (1990), Neural Computing: An Introduction, CRC Press Book, United States. July, 2015.
11. Benedetti, S., Saverio, M., Anna, G. S. and Gian, L.M. (2005), Electronic nose and neural network use for the classification of honeypot retrieved citeseerx.ist.psu. September 4, 2014.
12. *Bermingham, M. L., Pong-Wong, R., Spiliopoulou, A., Hayward, C., Rudan, I., Campbell, H., Wright, A. F., Wilson, J. F., Agakov, F., Navarro, P. and Haley, C. S. (2015). Application of high-dimensional feature selection: evaluation for genomic prediction in man, Sci. Rep. 5.*
13. Bhattacharjya, R. K. (2013), Introduction to Genetic Algorithm, retrieved from www.iitg.ernet.in/rkbc/CE602/CE602/Genetic%20Algorithms.pdf, July, 2015.
14. Boyfriend N.W.M. (2011), The Role of Intrusion Detection Systems in Electronic Information Security: From the activity theory perspective, retrieved online from https; //www.emeraldinsight.com/doi/abs/10.1108/17260531111179915
15. Cao, Y. J. and Wu, Q. H. (1999), Teaching Genetic Algorithm Using Matlab, International Journal of Electrical Engineering and Education (IJEEE), Vol. 36, Pp. 139–153.
16. Chia-Mei C., Dah-Jyh G., Yu-Zhi H. And Ya-Hui O. (2015), Anomaly Network Intrusion Detection Using Hidden Markov Model, International Journal of Innovative Computing, Information and Control ICIC International, Volume 12, Number 2, Pp.569 -580
17. Cybint (2018), 13Alarming Cyber Security Facts and Stats, retrieved online from https://www.cybintsolutions.com/cyber-security-facts-stats/ December, 2018
18. Czogala, K. and Leski J. (2000), Neuro-Fuzzy Intelligent Systems, Studies in Fuzziness and Soft Computing", Springer Verlag, Germany,
19. Dayhoff, J. E. (1990), Neural Network Architecture: An Introduction, retrieved from https://catalyst.library.jhu.edu/July 10, 2015.
20. Deepa A.J. and Kavitha D. (2012), A comprehensive Survey on Approaches to Intrusion Detection System, International Conference on modelling Optimisation and Computing, Procedia Engineering 38, Pp. 2063 –

2069
21. *Engin K.; Somesh J; Davide B. (2009).* Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23–25, 2009, Proceedings
22. *França, A. L.; Jasinski, R.; Cemin, P.; Pedroni, V. A.; Santin, A. O. (2015).* The energy cost of network security: A hardware vs. software comparison*, 2015 IEEE International Symposium on Circuits and Systems (ISCAS). pp. 81–84.*
23. Diaz-Gomez, P. A. and Hougen, D. F., (2005): Improved off-line intrusion detection using a genetic algorithm, http://cameron.edu/~pdiaz-go/Art_ICEIS.pdf. January, 2018
24. Gareth J., Daniela W., Trevor H. and Robert T. (2013), An introduction to Statistical Learning, Springer, P. 204.
25. Garzia, F. Lombardi, M. Ramalingam, S. (2017). An integrated internet of everything - Genetic algorithms controller, artificial neural networks framework for security/safety systems management and support, International Carnahan Conference on Security Technology (ICCST). IEEE. doi:10.1109/ccst.2017.8167863.
26. Guyon, I. and Elisseeff, A. (2003), An Introduction to Variable and Feature Selection", Journal of machine Learning research *Vol.* 3. Retrieved online from http://clopinet.com/fextract-book/IntroFS.pdf.
27. Hao Li., Zhijian L. Kejun L., and Zhien Z. (2017), Predictive Power of Machine Learning for Optimizing Solar Water Heater Performance: The Potential Application of High-Throughput Screening, International Journal of Photoenergy, Volume 2017, Pp. 1 – 10
28. Hornik, K. M. S. and White, H. (1991), Universal approximation of an unknown mapping and its derivatives using multilayer feed forward networks, Journal of Neural Networks. Vol. 3: Pp.551-560.
29. Hornik, K. (1993), Some New Results on Neural Network Approximation: Journal of Neural Networks, Vol.6, 1069-1072.
30. Hussain A. M. U., Memoona J. and. Arshad M.J. (2014), An Overview of Intrusion detection System (IDS) along with its commonly used techniques and Classification, International Journal of Computer Science and Telecommunications, Vol. 5, Iss 2. Pp. 20 – 24
31. Jang, J. R (1991), Fuzzy Modelling Using Generalized Neural Networks and Kalman Filter Algorithm, Proceedings of the 9th National Conference on Artificial Intelligence, 2. pp. 762–767.
32. Jang, J. R. (1993), ANFIS: Adaptive Network Based Fuzzy Inference System retrieved from citeseer. Ist.psu.edu/viewdoc/summary?doi=10.1.1.42.2913, May, 2013.
33. Jang, S. (1997), Neuro-Fuzzy and Soft-Computing, Prentice Hall, Pp. 335-368.
34. John R. V. (2010). Managing Information Security. Syngress. p. 137. ISBN 978-1-59749-533-2. retrieved February, 2019.
35. Karthikeyan K.R. and Indra. A. (2010), Intrusion Detection Tools and Techniques –A Survey, International Journal of Computer Theory and Engineering, Vol.2, No.6, Pp.1793-8201.
36. Kruegel C. D., Mutz W. R. and Valeur F. (2003), Bayesian Event Classification for intrusion Detection, Porc. 19th Ann. Computer Security Application Conf. (ACSAC' 03), Pp. 14 – 23,
37. Kosko, B. (1992), "Neural Networks and Fuzzy Systems: A Dynamical System Approach to
    i. Machine Intelligence", Prentice Hall, Englewood Cliffs, New Jersey.
38. Kuan, C. M. and White, H. (1994), Artificial Neural Networks: An Econometric Perspective, Econometric Reviews, Vol.13, Pp.1-91 and 139-143.
39. Kumar, R. and Jyotishree, K. (2012), "Novel Encoding Scheme in Genetic Algorithms for Better
40. Fitness", International Journal of Engineering and Advanced Technology, Volume-1, Issue-6, pp. 214-218, ISSN: 2249-8958.
41. Kumar, R. and Jyotishree K. (2012), "Blending Roulette Wheel Selection & Rank Selection in Genetic Algorithms", International Journal of Machine Learning and Computing, Vol. 2, No. 4, pp.365-370.
42. Kumar, A. (2013), Encoding Schemes in Genetic Algorithm, International Journal of Advanced Research in IT and Engineering, Vol.2, (3), Pp. 1-7
43. Iaroslav O. (2017), Applying Deep Machine Learning for psycho-demographic profiling of Internet users using

O.C.E.A.N. model of personality, retrieved online from pdfs.semanticscholar.org/
44. Liu H. Y., Xiangdong C. And Shalini L. (2013), Understanding Modern Intrusion Detection Systems: A Survey, retrieved https://arxiv.org/ftp/arxiv/papers/1708/1708.07174.pdf, January, 2019
45. Mageswary G. and Karthikeyan M. (2018), Intrusion Detection Using Data Mining Techniques, International Journal of Engineering Science Invention (IJESI), Pp. 2319 -6726.
46. Mehdi, M. S. Zair, A. A. and Bensebti M. (2007), A Bayesian Networks in Intrusion Detection Systems, Journal of Computer Science 3 (5): Pp.259- 265,
47. Mohit T., Raj K., Akash B., Jai K. (2017), Intrusion Detection System, International Journal of Technical Research and Applications, Volume 5, Issue 2, Pp.38 – 44
48. Nahla B.A., Salem B., Zied E. (2004), Naive Bayes vs Decision Trees in Intrusion Detection Systems,retrievedhttp://static.aminer.org/pdf/PDF/000566/404/naive_bayes_vs_decision_trees__intrusion_detection_systems.pdf
49. Nauck, D., Klawon F., and Kruse R. (1997), Foundation of Neuro-Fuzzy System, J.Wiley and Sons, Pp.312
50. Negnevitsky, M. (2005), Artificial Intelligence: a guide to Intelligent Systems, retrieved online from http://www.amazon.co.uk/Artificial-Intelligence-Guide Intelligent-System /dp/May 19, 2011
51. Nenekazi N. Penelope M. and Fulufhelo V. N. (2017), A Fuzzy Logic Based Network Intrusion Detection System for Predicting the TCP SYN Flooding Attack, retrieved online https://pdfs.semanticscholar.org/3ff0/98c99400b920257538849e0031af9379957d.pdf
52. Nitin S. K., Deepak S. T. , Amit S. (2013), Development Of Adaptive Neuro-Fuzzy Inference System Based Network Intrusion Detection System, International Journal of Scientific & Engineering Research, Volume 4, Issue 10, Pp. 1568 -1572.
53. Pandeeswari N., Ganeshkumar P. (2015), A Neuro Fuzzy Based Intrusion Detection Systemfor a Cloud Data Center Using Adaptive Learning, retrieved online from https://pdfs.semanticscholar.org/ab8b/d93
54. Peter, D. (1998), Unsupervised learning, The MIT Encyclopaedia of the Cognitive Science, retrieved online from www.gatsby.ucl.ac.uk/~dayan/papers/dun99b.pdf
55. Portnoy L. Eskin E. and Stolfo S. (2001), Intrusion Detection with Unlabeled Data using Clustering Pro. ACM Workshop Data Mining Applied to Security (DMSA).
56. Priyanka S. and Rakesh S. K. (2016), Cyber Attacks On Intrusion Detection System, International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, Pp. 191 – 196
57. Rajasekaren, S. and Vijayalakshmi P. G. A. (2012), Neural Network, Fuzzy Logic and Genetic Algorithms; Synthesis and Applications, published by soke.K.Ghosh, PHI learning provate limited, Sinepat, Haryana, ISBN-978-81-203-2186-1.
58. Randy, L. H. and Sue E. H. A. (1998), Practical Genetic Algorithm, John Wiley & Sons, Inc., Hoboken, New Jersey
59. Ricardo K., Raju R., Joseph M., Igor H., Geoffrey S., Mandy B., Silviu N., S. Masoud S., Tao L., and Krista M. (2008), Anatomy of a Real-time Intrusion Prevention System, International Conference on Autonomic Computing, IEEE, Pp. 151 – 160.
60. Richard, S. S. and Andrew, G. B. (2011), Reinforcement learning: an Introduction, retrieved from http://books.google.com/books/March 11, 2013.
61. Robert, F. (2000) Introduction to Neuro-Fuzzy Systems, Advances in Soft Computing Series, Springer-Verlag, Berlin/Heidelberg, Germany.
62. Russell, S. and Norvig, P. (2003) Artificial Intelligence: A Modern Approach (2nd ed.). Prentice Hall. ISBN 978-0137903955.
63. Samantha C. (2014), Building a strong society requires effective family policy, retrived online from http://www.qscience.com/doi/pdf/10.5339/difi.2014.1
64. Sampada C., Khusbu S., Neha D. and Sanghamitra M. (2004), Adaptive Neuro-Fuzzy Intrusion Detection Systems, Proceedings of the International Conference on Information Technology: Coding and Computing

(ITCC'04)
65. Santos K. B, Chandra S. P. R., .Ratnakar M., Dawood B., Sudhakar N. (2013), Intrusion Detection System-Types and Prevention, International Journal of Computer Science and Information Technologies, Vol. 4 (1),Pp. 77 – 82.
66. Schank, R. C. (1991). "Where's the AI". AI magazine. Vol. 12 no. 4. p. 38.
67. Shahid A. Jasni M. Z., Mohamad F. Z. Zakira I. Suleman K. Bokolo A. and Victor C. (2017), From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions, retrieved online from https://www.mdpi.com/1999-4893/10/2/39/pdf, November, 2018.
68. Shanmugavadivu R and Nagarajan N. (2011), Network Intrusion Detection System Using Fuzzy Logic, Indian Journal of Computer Science and Engineering (IJCSE), Pp. 101 – 111.
69. Shannon M. O. (2009), Information Access, retrieved online from http://bpm.ils.indiana.edu/scholarship
70. Stefan A. (2010), Intrusion Detection Systems: A Survey and Taxonomy, retrieved online from http://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf, January, 2018
71. Suresh N. Chari P. C. (1998), BlueBoX: A Policy–driven, Host–Based Intrusion Detection system, retrieved http: www.ndss-symposium.org/wp-ndsssymposium.org/wp- December 2018.
72. Umesh K. R. (2018), Log Based Intrusion Detection System, IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 20, Issue 5, Vol. I, PP 15-22.
73. Vacca, J. R. (2013). Network and System Security. Elsevier.
74. Warrender C. S. F., Stephanie F. and Pearlmutter B. (1999), Determining Intrusion using System Calls: Alternative Data Models, "Proc. IEEE symp. Security and Privacy (SP'99) Pp. 120 - 128
75. Wenke L., Salvatore J. S. and Kui W. M. (1998), Mining Audit Data to Build Intrusion Detection Models, retrieved online from http: citeseerx.ist.psu.edu/viewdoc/download?
76. Wernick, Y., Brankov, Y. and Strother (2010), Machine Learning in Medical Imaging, IEEE Signal Processing Magazine, vol. 27, no. 4, July 2010, pp. 25–38.
77. Yang, K Y. McLaughlin, S. S., Littler, E. G T., Pranggono B., and Wang H. F (2011), Multiattribute SCADA-Specific Intrusion Detection System for Power Networks, retrieved online from http://shura.shu.ac.uk/11129/
78. Yuancheng L., Rixuan Q., Sitong J. (2017), Intrusion detection system using Online Sequence Extreme Learning Machine (OSELM) in advanced metering infrastructure of smart grid, retrieved online from https://doi.org/10.1371/journal.pone.0192216
79. Zhang, D.F., Patuwo, B. E. and Hu, M. Y. (1998), Forecasting with artificial neural networks: The state of the art, International Journal of Forecasting, Vol.14, Pp.35-62.
80. Zare, H. (2013), Scoring relevancy of features based on combinatorial analysis of Lasso with application to lymphoma diagnosis, BMC Genomics S14.