**An Analysis Of Hybrid Approaches For Intrusion Detection**

**Group No**. : **13**

**Group Members :** **Mentors:**

Abhinav Jaiswal 2016-IPG-004 Dr. Saumya Bhadauria

Mohit Kumar 2016-IPG-053 Dr. Santosh Singh Rathore

Surendra Singh Gangwar 2016-IPG-107

**Background:**

In recent years, there has been a revolutionary change in the field of networking, use of the internet is growing day by day and so is a risk of intrusion.

Nowadays it is very crucial to have a secure network because of increasing dependability on the internet and to achieve high-level security, the only way it can be possible is through intrusion detection, it is an efficient technique which is capable of the classifying the network attacks.

Today[1], the web is broadly utilized in various organizations and the business prerequisites have caused enterprises to convey their very own data frameworks on the web, Due to large dependability on an information system, it became a major bottleneck, and thus the target for the intruders.

Advancement in Machine learning (ML) and Deep learning (DL) techniques made IDS algorithms result in less error rate and more accurate to classify various attacks. In this work, we present an ensembling approach with a mixture of expert for intrusion detection that would provide a better prediction performance than any single classifier.

**Motivation:**

Intrusion detection is the problem of identifying unauthorized users accessing the system in an unauthorized manner and authorized users who exceed their privileges. Detecting an intrusion is based on the belief that intruder’s behavior differs from a legitimate user. An intrusion detection system monitors security related events and continuously check for malicious activity.

Previous work in intrusion detection in the field of machine learning includes implementation of different models of both supervised and unsupervised learning algorithms to solve the classification problem of intrusion detection whether a given connection is normal or malicious. It may be possible that some feature in the trace file is not recognized by one model and another one can handle it so using more than one models together can increase the accuracy of result from the previous one.

The goal of any machine learning problem is to develop a single model that predict or classify the required outcome. Ensemble learning is an effective technique to increase classification and prediction accuracy. Motivation includes the ensemble approach combines several machine learning techniques into one model in order to reduce loss and variance. Ensemble learning algorithms include namely stacking and the mixture of experts. Stacking trains different models with the entire dataset, then a new model trained with the predictions of the previously trained models. Advantage of using such type of learning is overcome the feature capturing that is not handled by one model can be handled by other models. The mixture-of-expert method based on the divide and conquer approach technique that subdivides the problem based on input regions and trains different models with specific input regions of the problem. So that each model has its own contribution in the final output of the problem.

**Objective:**

The main objectives of our project can be summarized in the following points:

* Our main goal is to propose a method using Mixture of experts technique that would provide a high accuracy rate for intrusion detection with the deep learning approach

* To prepare a comparative study of our proposed model with other existing approaches.

**Timeline:**

In order to achieve our aforementioned objective, we can divide our project work into various phases, each phase has its own subphases. We summarize the workflow of our project through the following given Gantt chart.

**Phase 1**

* Literature Review
* Identifying the research gap
* Selection of the problem

**Phase 2**

* Data Preprocessing
* In-depth analysis of various ensemble model approaches

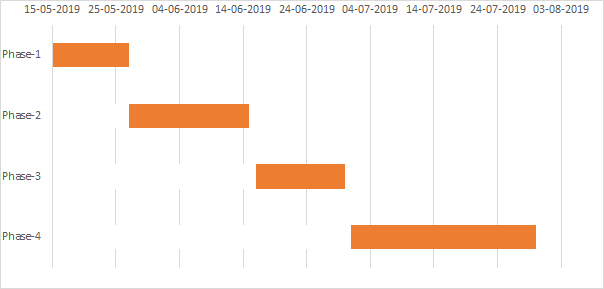
**Phase 3**

* Coding and Implementation of separate machine learning and deep learning models
* Integration of the models according to the required model
* Training, testing, and validation

**Phase 4**

* Result Analysis
* Conclusion
* Report Writing

**GANTT CHART**

****

**References:**

[1]G. C. Kessler, “Defenses against distributed denial of service attacks,” SANS Institute, vol. 2002, 2000.

[2]C. Guo, Y. Ping, N. Liu, S. S. Luo, "A two-level hybrid approach for intrusion detection", Neurocomputing, vol. 214, pp. 391-400, 2016.

[3]Bauer, E., & Kohavi, R. (1999). An empirical comparison of voting classification algorithms: Bagging, boosting, and variants. *Machine Learning*, 36(1/2), 105–139.

[4]Chen K, Xu L, Chi H (1999) Improved learning algorithms for the mixture of experts in multiclass classiﬁcation. Neural Netw 12(9):1229–1252

[5]A survey of intrusion detection systems based on ensemble and hybrid classifiers AA Aburomman, MBI ReazComputers & Security 65, 135-152

[6]Adaptive and online network intrusion detection system using clustering and Extreme Learning Machines. Roshan Kokabha, Setareh; Miche, Yoan; Akusok, Anton; Lendasse, Amaury.Vol. 355, No. 4, 2018, p. 1752-1779.