Network Intrusion detection system using artificial intelligence  
*Clementine Mamogale – 216025117*

**Abstract**

The widespread use of the internet and communication devices and the development of new technologies that can connect to one other has advanced, which increased the volume of data transfer over the internet. Simultaneously, this has opened many novel attacks which are beyond the human control capabilities, which also poses challenges to the current network securities. One tool that is used by the network securities to prevent possible network intrusion is an Intrusion Detection System (IDS), which works by monitoring the traffic over a network to ensure the availability, integrity, and confidentiality of the network. This tool used to be effective over the past years, but as the internet grows, the IDS has become less and less ineffective. Hence in this paper, I introduce a Network Intrusion detection system (NIDS) architecture that uses Artificial Intelligence as its backbone. This architecture will feature deep learning and machine learning techniques to develop a system that is adaptive and resilient to network intrusions, including zero-day intrusions. To demonstrate the effectiveness of this model, we use the old KDD+ and the new CICIDS 2017 datasets. The reason for these two datasets is because the KDD+ is widely used because it has well-known intrusions and can be used to create the baseline of the NIDS. Then the CICIDS is new and has new attacks that happened recently. Hence it can be used for training for zero-day attacks.

**Keywords:** Network Intrusion Detection System (NIDS), machine learning, deep learning, Network Security, Vector Machine, Naïve Bayes, Neural Networks.

**Introduction**

In this modern life, our daily activities are influenced by the widespread use of computer devices, which are connected to one another and share data and information. Using the information and communication technology (ICT) and its resilience, businesses and individuals were able to offer real-time global business continuity and a frontier solutions of interoperability [1]. The rise of this interoperability and data exchange among computers on the internet has opened vulnerabilities that are exploitable, and they can result in harmful effects on the end-users of the computers. Hence a resistant and resilient intrusion detection system (IDS) is needed, an IDS which will be able to maintain and provide availability, integrity, and confidentiality of the system. After all, an IDS is recognized as the first layer of defense among the defensive mechanisms that address all the attack vectors [1].

A Network Intrusion Detection System works by scanning a network traffic as it comes and identify any violations if they exist based on customized detection levels that are preconfigured on the network and then report them, then block them from going through the network before they cause any damage to the data that is being protected by the network. IDS use the idea of behavioral features to differentiate between a legitimate and non-legitimate traffic. Hence the development of Intelligent Intrusion Detection system is needed, which will help in learning about the behaviors of different traffic and be able to detect intrusion and differentiate between normal and abnormal traffic by using the features learned [1].

Refs

1. <https://reader.elsevier.com/reader/sd/pii/S1877050921011078?token=B9BD6FFE3C86E2DD74A456A01956CF6DA067E92A474645A6F1360558C7F127895C1D0E990B5C4E33630BC1CF08F91064&originRegion=eu-west-1&originCreation=20220612193324>
2. <https://reader.elsevier.com/reader/sd/pii/S1877050918321136?token=71A22DCD7E8606EF7E519D3A1E7939A5D7DCC70FB252A9610845A124066DE2BA46EEC85A07DD74A4E29468BC9D812487&originRegion=eu-west-1&originCreation=20220612193328>
3. <https://www.researchgate.net/journal/Transactions-on-Emerging-Telecommunications-Technologies-2161-3915/publication/344726867_Network_intrusion_detection_system_A_systematic_study_of_machine_learning_and_deep_learning_approaches/links/61a604c86864311d938a92c5/Network-intrusion-detection-system-A-systematic-study-of-machine-learning-and-deep-learning-approaches.pdf?_sg%5B0%5D=3jDD1L58VEnesSzxdTvYvwp0_61rq6ICOLKl2tjjxvTed3YAWsWX1Q2dcaSsqUPCQlbRSAcqxceJPxoDt5DdSg.JQJoBClZHuZcttTiLuMOW9UQnisaHqaJSDDs2oMBM9v1hKbmtPj0EtMlE5h3jY_ZGyqDu7T6anRV87RsntUh0w&_sg%5B1%5D=uQS6nkX6_GaKkhJD6vUMzkZKM7ySW_iU1XkoxouJsHKLnaCYA4zsKXdCEG3H_Y9BkeIFaegXckRbCvEEqs_9a0Sdvs6hd82ofvwu1AYxRSlH.JQJoBClZHuZcttTiLuMOW9UQnisaHqaJSDDs2oMBM9v1hKbmtPj0EtMlE5h3jY_ZGyqDu7T6anRV87RsntUh0w&_iepl=>