Intrusion detection system using Artificial Intelligence

Clementine Mamogale – 216025117

In this project, I will create a system that detects intrusion using artificial intelligence. This will help in the rise of intrusion that are happening worldwide. Hackers are gaining more knowledge and they are using most recent technologies which can bypass the currently available intrusion detection system. The mostly used intrusion detection system is a traditional one, whereby a human being analyses the traffic on the network by themselves and that can result in errors since humans are prone to errors, humans are also not fast enough to detect intrusion on a real time frame. One more reason why there is a high rate of intrusions in systems is because of how expensive this intrusion detection systems are, and only few big companies can afford them and leaves the middle or the startup companies at risks.

Using intrusion detection system that uses Artificial intelligence will make it possible for both big and small companies to afford this system because it will be running automatically and no hands on required. This will also decrease the false positive rate since computers are good at doing repetitive work, and they are accurate. Using AI will make it possible to the system to learn on its own and be up to date with the most recent intrusion out there and be able to detect them instantly.

My project will use AI as its backbone to make this system a full proof od intrusions. How it works is that it will analyze packets as they come though the network on every layer, it will check the header, the body, and the signature of the packet to see if it has changed somehow or not. In this project I will use python to build the whole system. I will use KDD+ and CICIDS 2017 as my datasets and use the Logistic regression and Naïve Buyes as my models to create the system.

KDD+ is old dataset and it has been used in many network intrusion detection, hence it make it a good dataset since it create a good baseline to be created. CICIDS 2017 is a new one compared to KDD+. This one is good because it has dataset that happened recent, it can run dataset that happened over the week and that is good. It is complicated but more accurate since it uses IPv4