Project - D3

Clementine Mamogale - 216025117

On my project titled Network Intrusion detection system using Artificial Intelligence will be using the Design Science methodology, using the DSR knowledge contribution framework, I will be doing the Improvement. Which means I will be doing a solution to an already known problem, which is that there is no enough network intrusion detection system that uses the intelligence of the computers to protect a network (Ahmad et al., 2020). The goal here is to create solution that is much better than what already is available in the industry in terms of efficiency and effectiveness using artificial intelligence techniques. The already available system tries to use the machine learning techniques, but they are still not as effective as they are supposed to, hence my solution will feature more functions that will make it more effective in terms of being able to work on its while being able to fight the zero-day attacks.

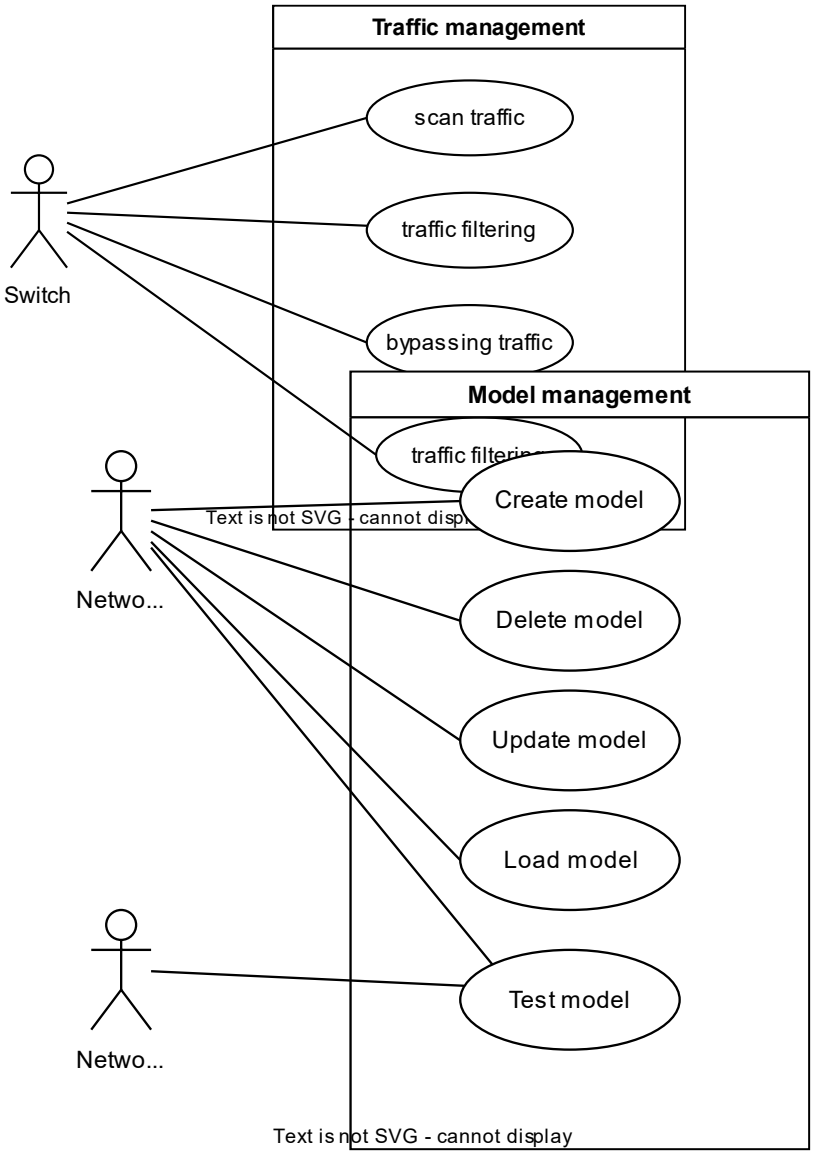
The project will make use of deep neural network that will be able to learn about both signature-based and anomaly-based attacks. The intrusion detection system will be placed on the gateways of all routes so that it can detect both internal and external attacks. The learning model will include Convolutional Neural Network, which will provide a multi-layered, unlike using a feed-forward neural network. The datasets that will be sued are the KDD+, is old and is used in many network intrusion detection system hence it can be used to create a good baseline system, and the second one is the CICIDS 2017, it is more recent is, it is good because it is modern and it uses the IPv4 standards (Ashiku and Dagli, 2021).

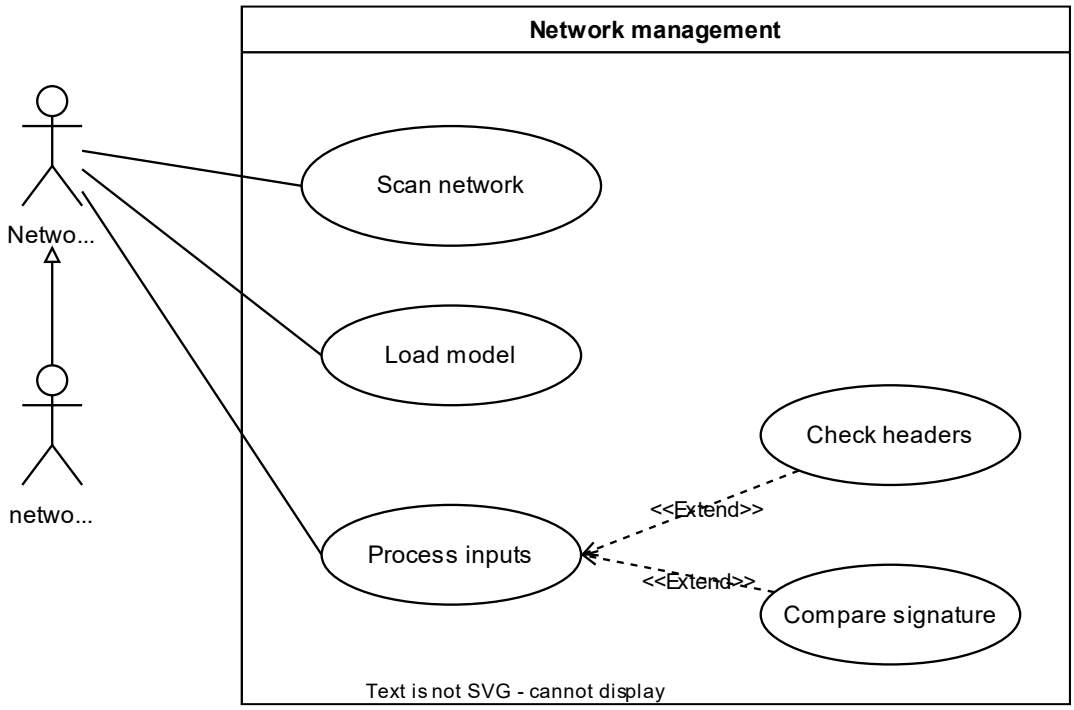
My functional requirements are the following: the network should be able to scan for network traffic as packets comes in though the network. Based on the type they get classified, they should be treated as malicious or normal then the normal they get approved to pass though, the malicious ones get blocked, and they get logged for future use. The system will be able to create a model and save it, then update it from time to time since it takes a quite computational time and power to create the models hence a saved model should be used an only get updated when there might be a new signatures of malicious packets to be registered on the model. Datasets that will be used to train the system, they might not be clean already hence the system should be able to clean the dataset beforehand.

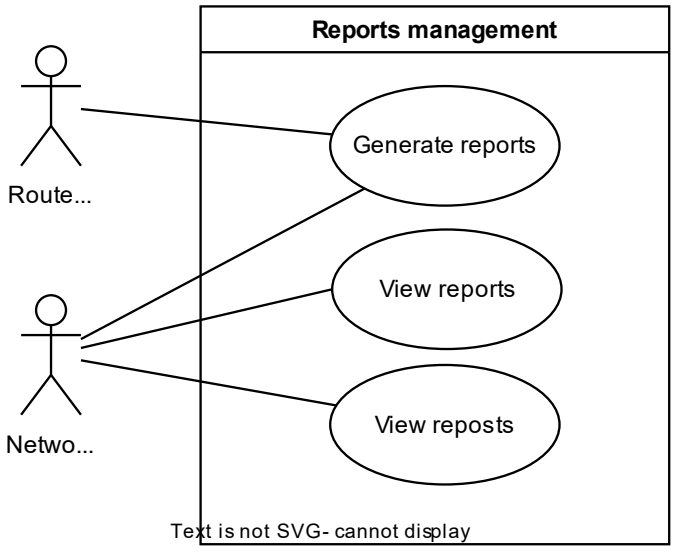
Use cases	**Functional requirements**
UC1 – Scan network traffic	The system must be able to scan the network traffic for any legit and non-legit traffic
UC2 – Load model	The system must be able to make use of a model and load it from where it is saved to save computational time
UC3 – Create model	The system should be able to create a model from time to time
UC4 – Delete model	The system should be able to delete the already existing model
UC5 – Update model	The system should be able to update the existing model with a model that is most recent that has recent attacks

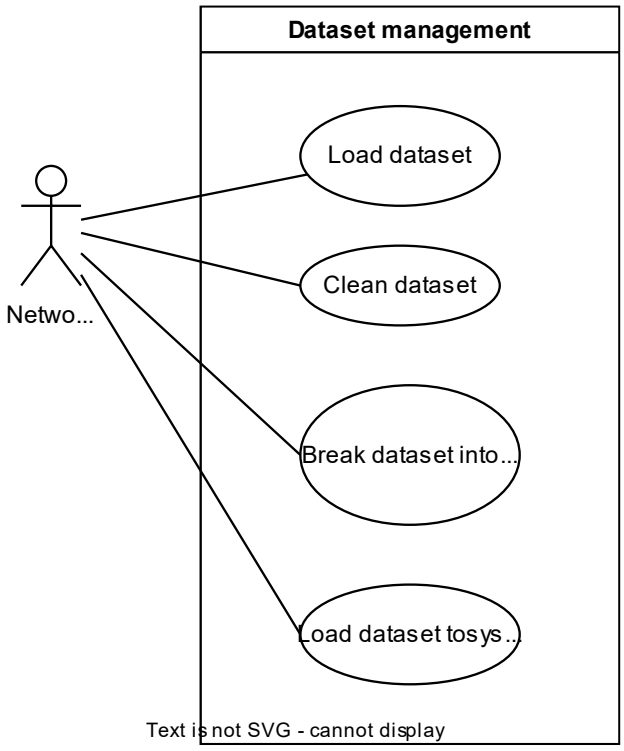
UC6 – Generate reports	The system should be able to generate reposts for administrators to be able to get insight of the system
UC7 – View reports	The system should be able to allow admins to be able to view reposts that have been generated
UC8 – Delete reports	The system should allow admins to be able to delete any report
UC9 – Load dataset	The system should be able to load an already existing dataset for testing and creating the model
UC10 – Clean dataset	The system should be able to clean the dataset to find and fix for errors that might be on the datset

Use cases




Network management
Netwo...
netwo...
Scan network
Load model
Check headers
<<Extend>>
Process inputs
<<Extend>>
Compare signature
Text is not SVG - cannot display


Reports management
Route...
Netwo...
Generate reports
View reports
View reposts
Text is not SVG- cannot display



Verification

Use cases	Verification	Validation
UC1 – Scan network traffic	Is the system able to scan the network that passes through it, all of it without any problems	Is the device the right one to scan a network or what, hence a right device for scanning network is need
UC2 – Load model	Is the system able to load the model that is saved and so that it will be used in scanning	Did we create the right model that will be suitable for scanning a network traffic or not, a great model will produce positive results
UC3 – Create model	Is the system able to create a model that can be used to scan network traffic	Is the model created the right model and can be saved for future used
UC4 – Delete model	Are we able to delete the model if we want to, it is important since we might want to replace it with a new one	Is the model the right one, if not, are we able to delete it and replace it with another model if we wish to
UC5 – Update model	Is the model dynamic in a way that allows for updates from time to time	A good model should be able to be updated so that it features new and recent signatures of attacks on it

UC6 – Generate reports	Is the device able to create reposts for admins to be able to see how the device is doing and how many attacks are there	A good system should be able to create reports for the system administrators to be able to see how the system is doing and how is risky they are
UC8 – Delete reports	As administrators, are we able to delete the reports if the reports become relevant or when the system us updated	A good system should be able to allow admins to be able to delete reports and log those actions
UC9 – Load dataset	Is the system able to load dataset from external parties?	A good system should be able to load datasets from external parties to save time on creating internal datasets and be able to work with all different kinds of attacks
UC10 – Clean dataset	A good system should be able to clean the datasets because most of the times the datasets from external parties will be having some faults here and there.	A good system should be able to clean the datasets before creating models and when doing the tests. Since most of the datasets are having some faults here and there

Project Management / Gantt Chart

A graphical representation of this is available on eve submission

D1	Find an industry related problem as a project, that is Intrusion detection system using artificial intelligence
D2	Research about the problem and find out, find out what is already been done and what is it that I will do different to solve the problem, already know that the system is already there but is not using artificial intelligence techniques that can solve the problem
D3	Create design on how the project is going to be solved, identify tools and how they going to be used to solve the problem
D4	Start coding by creating small, related codes that will be able to test on their own as stubs
D5	Connect the stubs created in the previous and test, see how they connect to each other
D6	Create models, test them, and make sure they can handle large data and they can be loaded into system to be able to detect intrusions
D7	Create a GUI to be used for the administrators
D8	Connect everything together and test once again to make sure everything is working well

D9	Presentation day for the whole project

Identification of Methods and Tools to be Utilized in Design & Implementation Phase

Tools and methods to be used are the following:

- Python
- Flask
- Numpy
- Metplotlab
- Sklearn
- Html
- Visual studio
- Jupyter notebook
- The 80% and 20% training and testing methods
- Logistic regression and naïve buyers methods are to be used

References

Ahmad, I., Ul Haq, Q., Imran, M., Alassafi, M. and AlGhamdi, R., 2022. An Efficient Network Intrusion Detection and Classification System. Mathematics, 10(3), p.530.

Ashiku, L. and Dagli, C., 2021. Network Intrusion Detection System using Deep Learning. Procedia Computer Science, 185, pp.239-247