American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-11, Issue-03, pp-99-106
www.ajer.org
Research Paper Open Access

Intrusion Detection aided by Artificial Intelligence (IDAI)

MELI TAMWA Jean
[1](ESIREM, Yaounde, Cameroon
TONYE Emmanuel
[1](University of Yaounde I , Yaounde, Cameroon
BINELE ABANA Alphonse
[1](University of Yaounde I ,Yaounde, Cameroon
MVEH Chantal
[1](CENADI , Yaounde, Cameroon

ABSTRACT : *Several techniques now make it possible to secure information systems. Increasingly complex techniques depending on the infrastructure to be protected. Without adequate methodology and appropriate knowledge, the poor application of these techniques for securing the information system can undermine the protection function of the system. The material and immaterial device that we propose makes it possible to improve the interaction between man and more or less complex security systems. This tool manages all the complexity of security architectures thanks to an artificial intelligence capable of communicating with humans and their environment to be protected. Our device is a connected object, a true conversational security agent that provides monitoring, detection and intrusion tests in a telematic network, hence the name IDAI (intrusion detection aided by artificial intelligence). It provides security monitoring through the continuous assessment of the level of vulnerability of the information system to attacks.*
KEYWORDS *information, intrusion, security, artificial intelligence.*

Date of Submission: 02-03-2022 Date of acceptance: 17-03-2022

I. INTRODUCTION

Any large, medium or small company whose activity is based in whole or in part on a computer system is exposed to a greater or lesser risk of suffering a cyberattack. The need for communication and development of business processes is the key factor pushing companies to anchor themselves to technology. The arrival of the Covid-19 health crisis was also a great catalyst during the second decade of the 21and century that pushed companies to equip themselves digitally (teleworking, collaborative platforms, etc.). This is to minimize the impact of this crisis on their business. But this was a turning point that made companies more open to the various vulnerabilities exploitable by cybercriminals. "Nearly three in five companies (58%) agree that due to more employees working from home, their business is more vulnerable to cyber attacks. » [1]

Network infrastructures all include a set of equipment (routers, switches, servers, user stations, hardware devices), the number of which depends on the type of network and the communication functions to be implemented. Internet, planetary network or networks of networks, is an effective channel for the connection Business-To-Business (B2B) and Business-To-Client (B2C). Unfortunately, the primary purpose (which is to ensure communication) of this network in particular and computer systems in general has been hijacked, exposing companies to a series of digital threats executed by cybercriminals with various motivations.

Computer security is based on several pillars and its application follows a set of standards. Depending on the computer system in place, the company can deploy an intrusion detection device to report and stop illicit actions in the system and having succeeded in circumventing the pre-established security device. A monitoring system to follow the operating mode of the resources of the computer system and avoid any stoppage of service that could negatively impact the activity. And also, the security watch through the continuous evaluation of the level of vulnerability of the system in the face of new attacks. The implementation of a good security plan as well as the follow-up require a qualified human resource who will have to continuously carry out a set of security tasks.

Smart devices provide tremendous help to man. Allowing him to achieve his objectives more quickly and more efficiently by providing him with several functions such as: interaction with his environment (actions on other network equipment), automation of actions, communication via a human channel (voice, text, …), abstraction of complex tasks. This is the key idea of this project, which aims to provide an intelligent device and a security stack to be integrated into any computer network to be protected. Our scope of research is the establishment of a system to solve the needs of companies and security engineers in particular to monitor, detect and conduct intrusion tests assisted by artificial intelligence. This is to achieve the objectives of productivity, quality of service and security of the information system.

II. GENERAL INFORMATION ON ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is defined as a set of theories and techniques implemented to produce machines capable of simulating human intelligence. It therefore corresponds to a set of concepts and technologies more than to a constituted autonomous discipline.

A Chatbot, bot, artificial agent, is basically an artificial intelligence driven software program that is used to engage in conversation with the user through texts or speech. Famous examples include Alexa, Siri, Google Assistant, etc. The key functions of the Chatbot that we are going to implement will be:

- Knowledge of the domain: being able to execute a sequence of actions linked to a security protocol;
- Recognition of intentions: knowing with a fairly high rate of precision what the user wants;
- Automatic speech recognition: Automatic speech recognition is a computer technique which makes it possible to analyze the human voice picked up by means of a microphone in order to transcribe it in the form of a text which can be read by a machine;
- Speech synthesis: It is a computer technique of sound synthesis which makes it possible to create artificial speech from any text;

III. ARTIFICIAL INTELLIGENCE MODEL

The conversational agent model we are building is a self-learning Chatbot. Self-learning robots are very effective because they are able to capture and self-identify user intent. They are built using advanced machine learning, deep learning and NLP (Natural Language Processing) tools and techniques. Companies such as Amazon (Alexa), Google (Google Assistant), Apple (Siri) have produced models of intelligent agents based on neural networks. They even go so far as to offer extensions of their system in the form of APIs for integration with applications. In our case, we train our own neural network built on the basis of deep learning. With as training dataset a dataset consisting of various communications between the user and the system. The different patterns are grouped by intents.

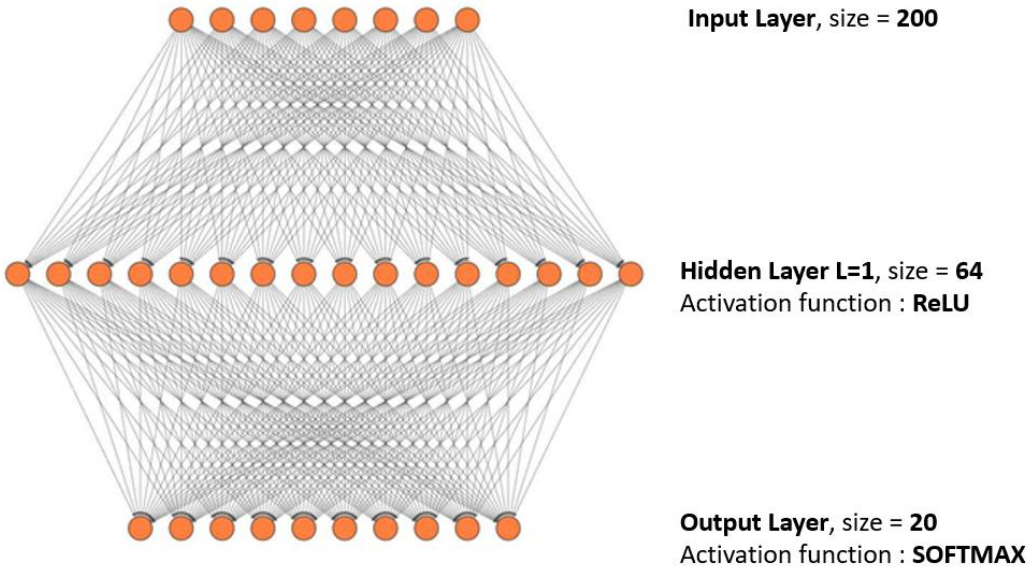

Figure 1 describes the architecture of our finally established neural network

As shown in Figure 1, we have about 200 features at the input layer, and 64 nodes at the first hidden layer. The activation function at this level is the function ReLU (Rectified Linear Unit) which is a function of rectifying the digital values [3]. Then we have the output layer, which has for the moment (current development)

20 intents (intents or classes which are the different possible predictions) with as an activation function softmax which is a probabilistic function intended to return the prediction with the strongest probability. The main purpose of an activation function is to introduce the properties of nonlinearity into the model. In artificial neural networks, the activation function of a node defines the output of that node given an input or a set of inputs.

The two activation functions that we will use for our Chatbot, which are also the most commonly used, are the Rectified Linear Unit function (ReLU: Rectified Linear Unit) and the Softmax function. The first will be used for the hidden layer while the second is used for the output layer. The softmax function is usually used as an output because it gives a probabilistic output. The ReLU function is defined in the follows:

$$f(x) = \begin{cases} 0, if\ x < 0 \\ x, if\ x \geq 0 \end{cases}$$

Next we have the definition of the softmax activation function given by the expression:

$$\sigma(\vec{z})_i = \frac{e^{z_i}}{\sum_{j=1}^{k} e^{z_j}}$$

The figure 2 presents the level of accuracy of the model after training it over 200 epochs: 97.70%.

```
Epoch 6/200
...
Epoch 197/200
3/3 [==============================] - 0s 4ms/step - loss: 0.1557 - accuracy: 0.9540
Epoch 198/200
3/3 [==============================] - 0s 7ms/step - loss: 0.0467 - accuracy: 0.9885
Epoch 199/200
3/3 [==============================] - 0s 8ms/step - loss: 0.0326 - accuracy: 0.9885
Epoch 200/200
3/3 [==============================] - 0s 8ms/step - loss: 0.0856 - accuracy: 0.9770
**************************************
"END OF MODEL TRAINING"
Number of classes : 12
Number of features : 110
Accuracy rate : 97.70 %
**************************************
```

Figure 2: Model training result

IV. MONITORING TOOLS

Network monitoring provides the information network administrators need to determine, in real time, if a network is performing optimally. With tools like network monitoring software, administrators can proactively identify gaps, optimize efficiency, and more. The engine responsible in our case for ensuring the monitoring function is ZABBIX [6] which is a multifunction open source platform.

V. NETWORK INTRUSION DETECTION ENGINE

The engine responsible for driving the detection of intrusions within the telematics network is a NIDS Network Intrusion Detection & Prevention System: SNORT. SNORT is a powerful intrusion detection system (IDS - Intrusion detection System) and an intrusion prevention system (IPS -Intrusion Prevention System) open source that provides real-time network traffic analysis and data packet logging. SNORT uses a rules-based language that combines anomaly, protocol, and signature inspection methods to detect potentially malicious activities such as denial of service (DoS) attacks, buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. As described in the logical architecture, it will interact with the Chatbot in order to monitor the flow of communication in the network in real time and prevent intrusions.

VI. WIZARD MODELING

VI.1 Software analysis

In this section, we will present two diagrams in the UML formalism which guided the design of the system. We first have in figure 3 the diagram of the use cases which presents the link of the actors of the system to the different functionalities:

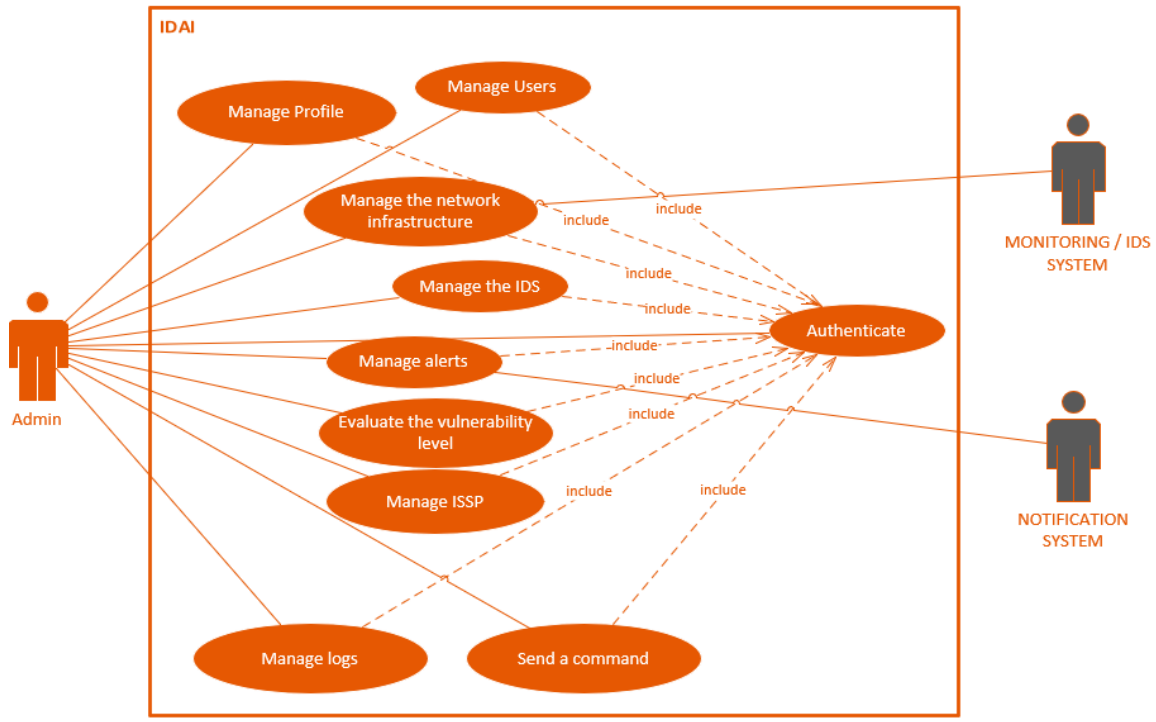

Figure 3: Use case diagram of IDAI system

Figure 4 presents the class diagram that will allow us to define the schema of the IDAI system database

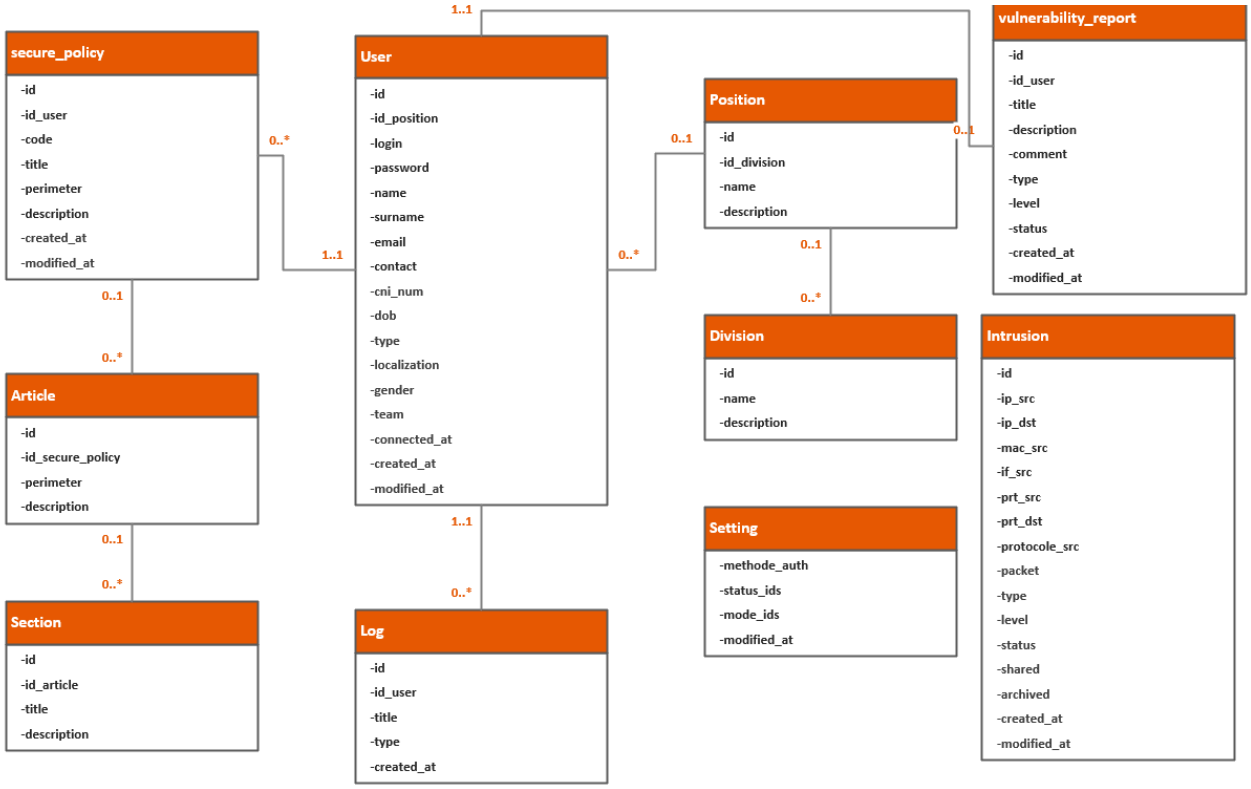

Figure 4: Class diagram of IDAI system

VI.2 Logical architecture of the Chatbot

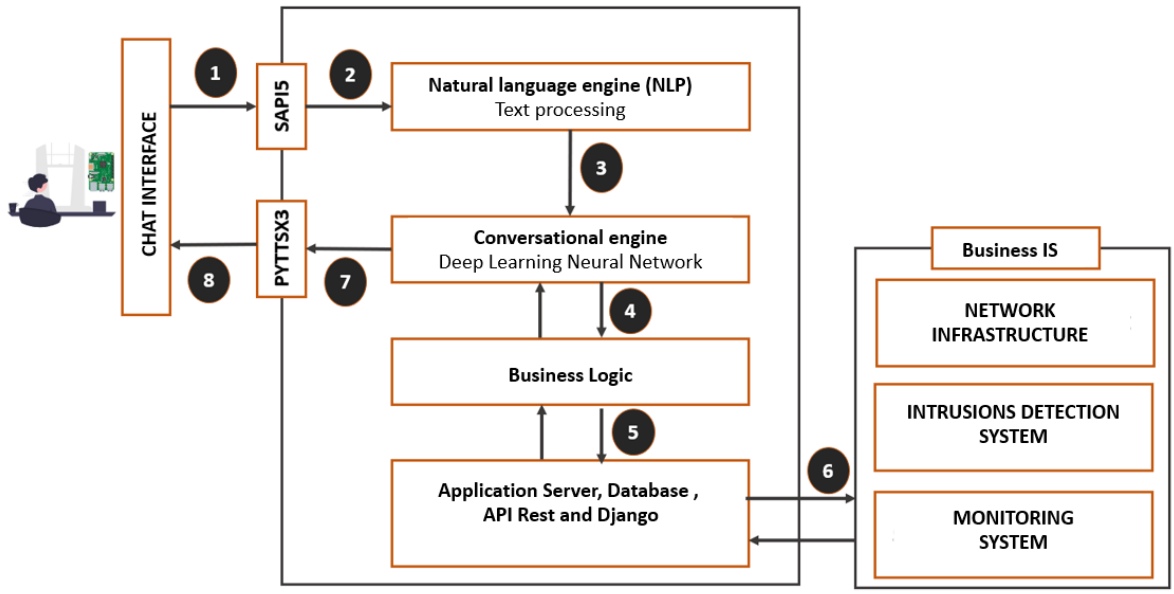

Figure 5: Logical system architecture

Figure 5 presented above presents the logical architecture of the system with a set of steps. Let's describe these different steps:
(1) Retrieving the user's voice command from the Raspberry PI board;
(2) Automatic voice recognition and sending the text command to the NLP engine;
(3) Sending the command in a new data format to the conversational engine (neural network);
(4) Mapping user intent to business functions;
(5) Sending the user's command to the application server via the REST API; (6) Interaction with network infrastructure and security stack;
(7) Sending the result of the execution of the command;
(8) Speech synthesis and sending of the final voice response (plus text) to the user.

VI.3 Wizard Sequence Diagram

Figure 6 presents the interaction sequence between a network administrator, the Chatbot and the network intrusion detection system.

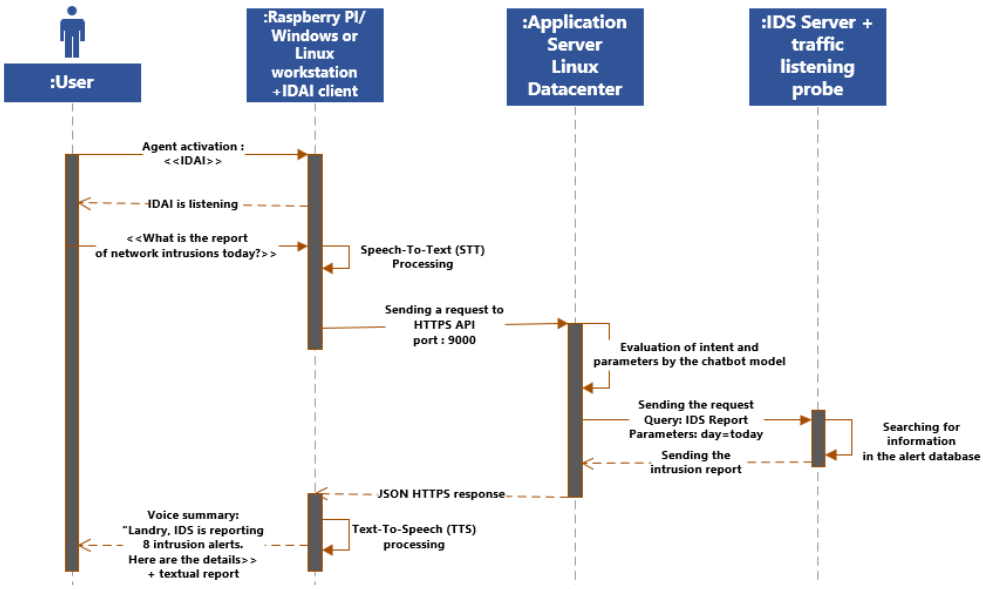

Figure 6: Interaction sequence between user, Chatbot and IDS

VI.4 System physical architecture

Figure 7 illustrates the physical architecture of the telematics network in which the security system we are designing will be deployed. Here is presented all the equipment and services to be monitored to be secured by the interface of the conversational agent.

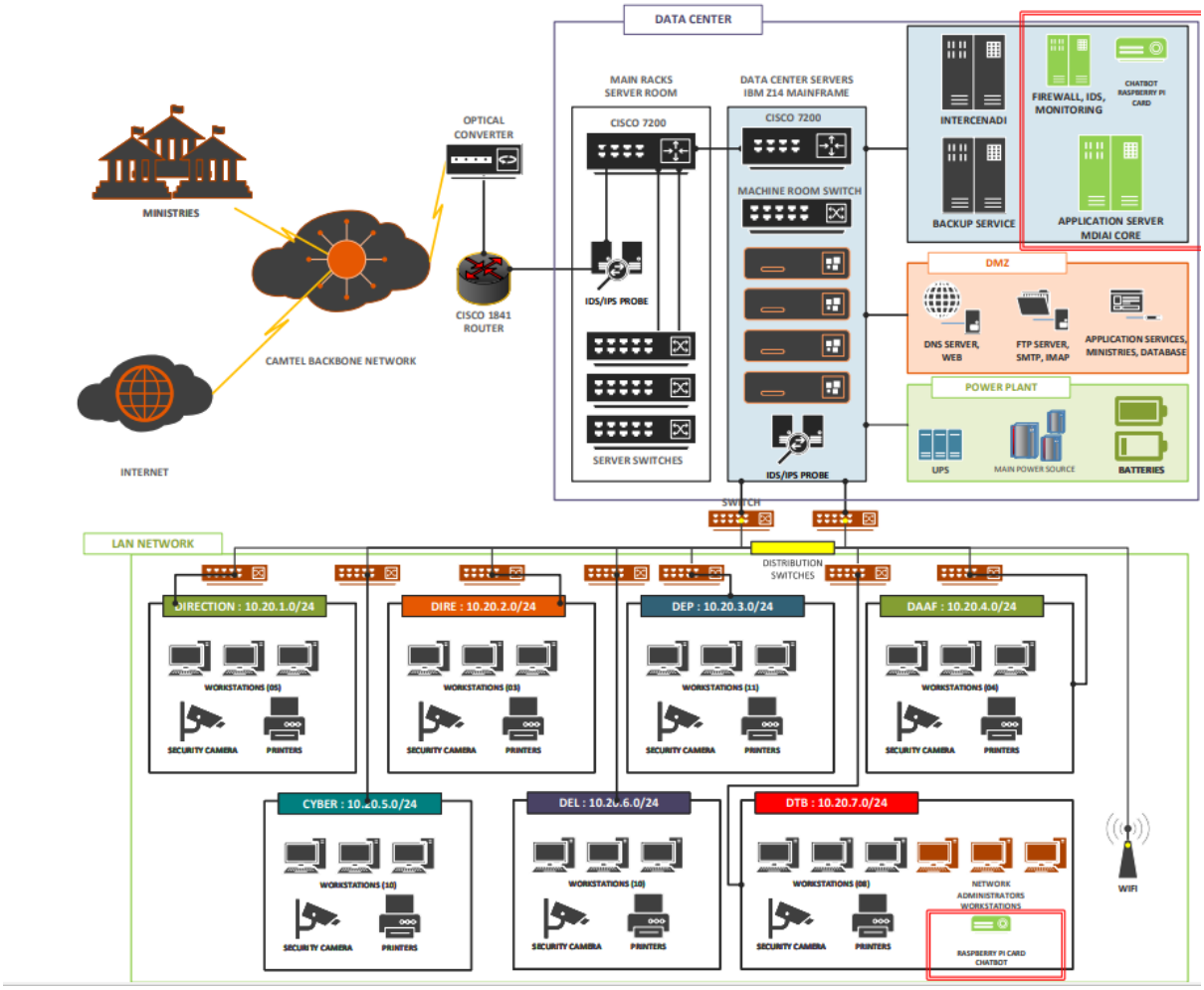

Figure 7: Physical architecture of the telematics network

VI.5 Assistant Achievement Flowchart

Figure 8 below shows the flowchart for setting up the system:

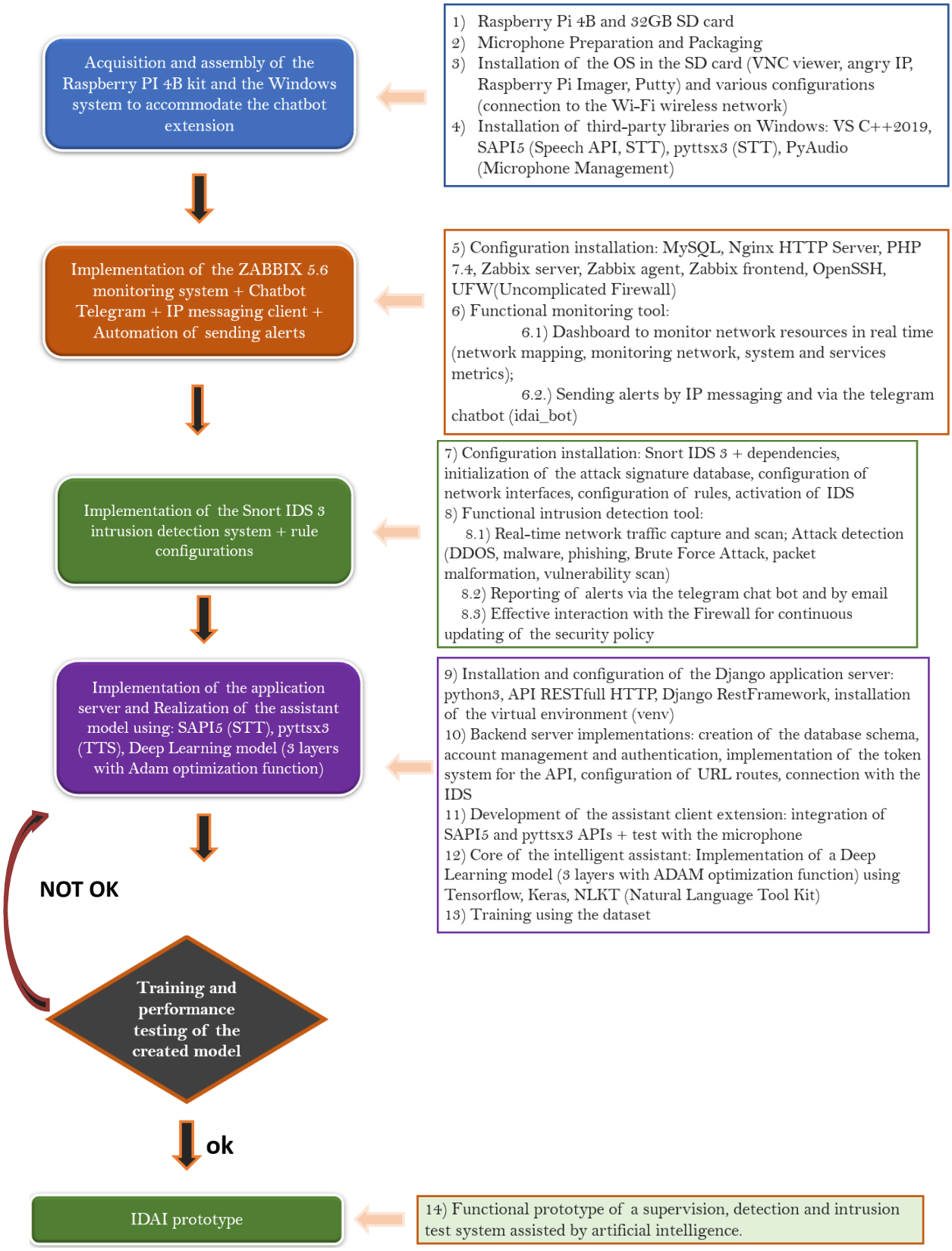

Figure 8: Intelligent Agent Realization Flowchart

VII. PROTOTYPING

The operational prototype is a set of tools including the conversational agent which will accompany the monitoring and intrusion detection solutions. It is composed as follows:

- A Raspberry PI 4 card in which runs the voice assistant shown in Figure 9;
- The application server (presented in the telematics network datacenter) which contains the trained neural network model and which acts as a conversational engine and NLP processing;
- A software client that can be installed on a Raspberry PI 4B nanocomputer or on Windows/Linux workstations to interact with the infrastructure via the conversation agent;

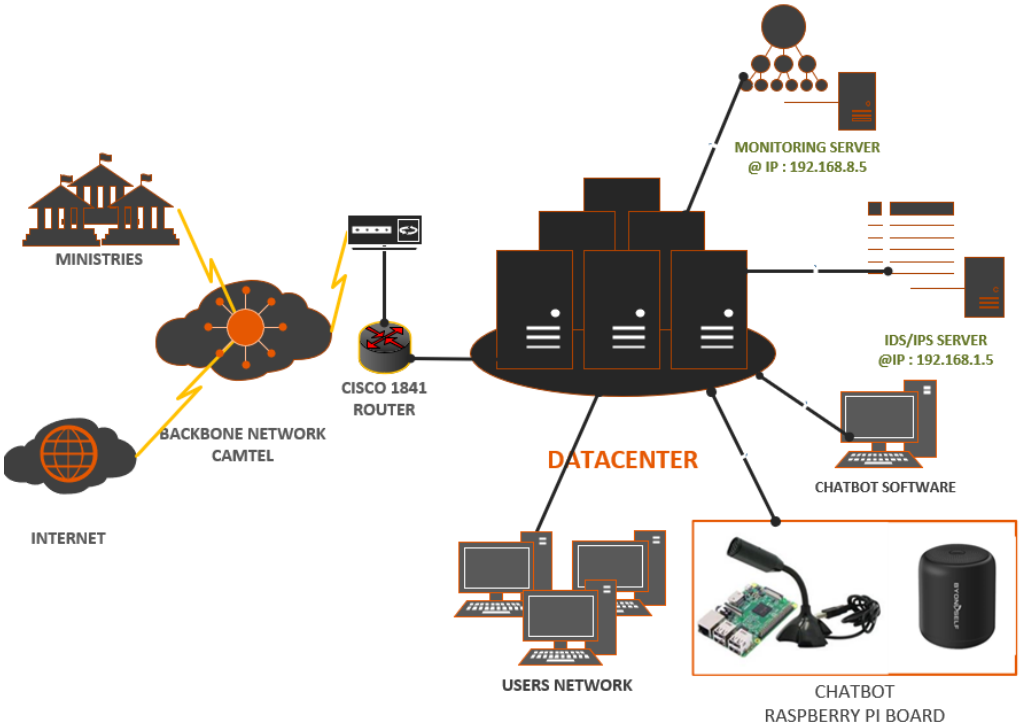

Figure 9: Chatbot Prototype

VIII. CONCLUSION

The integration of artificial intelligence, more precisely of the conversational agent, facilitates the interaction between humans and information systems. Throughout this project, we have shown how a perfect combination of different solutions could help secure a computer system by allowing real-time monitoring of network and system variables, intrusion detection to prevent illicit operations in the computer network. All this using an intelligent gateway, the Chatbot for interaction with administrators.

REFERENCES

[1]. L. Phanoukoun, « Rapport Hiscox 2021 sur la gestion des cyber-risques », HISCOX Assurance, 13 avril 2021
[2]. M. Stampar and K. Fertalj, Artificial Inteligence in Network Intrusion Detection, Faculty of Electrical Engineering and Computing, Zagred, Croatia, July 2015.
[3]. Akira Takewa, Masayui Kajiura, Hiroya Fukuda, Role of Layers and Neurons in Deep Learning With the Rectified Linear Unit, Cureus, October 2021.
[4]. Derar Abu Sheihka, Aref Khalil, Mohammed Adnan Moreb, Artificial Intelligence For Network Intrusion Detection And Cybercrimes, Derar Abu Sheihka's Lab, Arab American University.
[5]. Oleksandr Shmatko, German Zviertsev, A survey of Artificial Intelligence Methods in Intrusion Detection Tasks, Scientific Collection "INTERCONF", May 2021.
[6]. Nathan Liefting, Brian van Baekel, Zabbix 5 IT Infrastructure Monitoring Cookbook: Explore the new features of Zabbix 5 for designing, building, and maintaining your Zabbix setup [1 ed.], Packt Publishing, 2021.
[7]. Qingchuan Meng, Youzi Zhang, Fengzhi Wu, Xiaoming Chen, Network Intrusion Detection Model Based on Artificial Intelligence, Journal of Physics Conference Series, August 2020.
[8]. Anitha A, SV Revathi, S Jeevanantham, E Eliza Godwin, Intrusion Detection System based on Artificial Intelligence, International Journal of Technology, January 2017.