People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
University May 8, 1945 guelma
Faculty of Mathematics, Computer Science and Material Sciences

computer science department

Master's degree thesis

Branch : Computer Science
Option : Information and Communication Sciences and Technology

Theme

Deep Learning for Cybersecurity in the Industrial Internet of Things (IIoT)

---

supervised by :
Dr. Mohamed Amine Ferrag

Presented by :
Brahmia Abdelbacet

July 2022

Acknowledgements

FIRST of all, we thank God ALLAH who gave us the courage, the power,the strength and the patience to complete this modest work.

We would like to particularly thank Mohamed Amine FERRAG our supervisor for having followed us well during our work, and for making us benefit from her knowledge, as well as her advice, and for all her help, the constructive remarks which have enabled us to improve and achieve the objective of this work.

also thank Djallel Hamouda and Benrazek Alaeddine for the help he provided and the knowledge he was able to pass on to me. I also thank him for his availability and the quality of his advice.

Our precious thanks go to the members of the jury for their presence, their careful reading of my thesis as well as for the remarks they will contact me during the presentation in order to improve my work.

I thank my very dear family , who have always been there for me.Their unconditional support and encouragement has been of great help.

Nouar Ikram , I want to thank you for being in my life and tell you how much you mean to me in life, we all need someone we can count on and for me, that person is you. Thanks for being there and making me better my dear love.

and thanks to all of Nouar Nour, Nouar Farida, and Nouar Rim and my best friends yacine bechiri ,chaox , Tex , Satoru gojo ,A2 , Kento nanami ,TheSeeker and Rythme who have been my family as always supporting me. Without you, I wouldn't do anything

I extend my sincere thanks to all the teachers of the Computer Science Department who taught us during these five years of study. All the people who gave their words, their writings, their advice and their criticisms have guided my reflections. Many thanks to Dr. Kouahla Zineddine and Gabriela Kouahla, who helped me in many situations and gave me a lot of advice .

Anyone who has contributed directly or indirectly to the realization of this work our friends for their help . . . .

in 1er octobre 2022.

Résumé

Les systèmes de détection d'intrusion (IDS) font l'objet de nombreuses études et jouent un rôle important dans la sécurité des réseaux. Le but de cette étude est de modéliser un tel système pour aider les administrateurs système à détecter et identifier les failles de sécurité dans leur organisation afin qu'elles puissent être évitées avant qu'elles causent des dommages .

Pour cela, nous avons étudié les performances de méthodes d'apprentissage automatique (ML) appliquées à la détection d'intrusion pour la cybersécurité. Ensuite, nous avons appliqué deux techniques de détection basées sur des approches d'apprentissage en profondeur, un réseau de neurones profonds (DNN) et un réseau de neurones convolutifs (CNN) pour détecter les intrusions dans le réseau.

Nous avons évalué les méthodes proposées avec l'ensemble de données Edge_IIoT du trafic de cybersécurité réaliste des attaques IoT et IIoT sur les réseaux. Nous avons également présenté des projets réalistes d'apprentissage automatique, nous calculons et évaluons notre travail à l'aide de différentes métriques appliquées à l'évaluation des performances machine et apprentissage profond (précision, rappel,F1 score), et d'autres indicateurs de performance importants pour la détection d'intrusion (matrice de confusion). Les résultats expérimentaux ont montré que les performances des approches de le deep learning (DL) dépend de la base de données que vous utilisez et du modèle que vous avez choisi.

Mots clés : Cybersécurité, Système de détection d'intrusion (IDS), Deep Learning, Machine Learning , Edge_IIoT .

Abstract

Intrusion detection systems (IDS) are the subject of many studies and play an important role in network security. The purpose of this study is to model such a system to help system administrators detect and identify security breaches in their organization so that they can be prevented before they cause harm or damage.

For this, we studied the performance of the learning methods machine (ML) applied to intrusion detection for cybersecurity. Then, we applied two detection techniques based on deep learning approaches, a deep neural network (DNN), and a convolutional neural network (CNN) to detect intrusions into network connections.

We evaluated the proposed methods with the Edge_IIoT dataset of realistic cyber security traffic of IoT and IIoT attacks on networks. We also have presented realistic machine learning projects, we calculate and evaluate our work using different metrics applied for performance evaluation machine and deep learning (Precision, Recall, F1 score), and other important performance indicators for intrusion detection (confusion matrix). The experimental results showed that the performances of the approaches of deep learning (DL) is depend on the database that you use and on the model you chose.

Key words : Cybersecurity, Intrusion Detection System (IDS), Deep Learning, Machine Learning, Edge_IIoT .

Table des matières

Table des figures

Liste des tableaux

General introduction. . .

COMPUTING has revolutionized today's world in ways unlike anything seen before. Apps that can communicate with you, self-driving cars that are the future of transportation - computing has disrupted everything.
Due to the evolution and progress of computer science and network technology , life has become very easy due to the applications that have become in every field from medicine to accounting to literature . . .

With this development , the information and the data have become more valuable and in some cases are extremely confidential . Sometimes a small error in an information may lead to a disaster , that may put many lives in danger and more than you imagine , and despite the development and despite the fact that a lot of research exists in the field of security, still The risk of piracy and the risk of losing information is a big problem.But cyber-criminals continuously invent sophisticated new ways to steal sensitive data for identity theft, money laundering, drug trafficking, among other things, and they don't stop until humanity is gone .

The problem

In this century, we have seen a lot of inventions and a great development in technology, Where the internet being connects everything , from the car to the home Even the fridge and oven . . .With this development ,the information is being sent over the Internet in large quantities ,and the risk of losing it remains great , and as we said the information become more valuable even the Intrusion detection systems exist ,still has face major challenges in many forms, from the news intrusion to the time of the process and without forget the accuracy of the process .

The purpose of work

for this reasons we are trying to study the existing works and propose a new security method based on Deep Learning techniques to detect attacks in IIoT systems, We have use a new data-set, which represents traffic real network containing several types of attacks,in simple definition our work represent in making a security network that stops hackers in their tracks , additionally make an easy system that help the administration to detect the attacks and to defend their networks .

CHAPITRE 1 :
IOT and IIOT

IOT and IIOT

1.1 Introduction

With the invention of a large number of low-cost important sensors like flame sensors, RFIDs . . .coupled with a variety of communication mediums, the technology has gained tremendous fashionability in the last decade, where everything is measured by sensors and connected to the Internet.

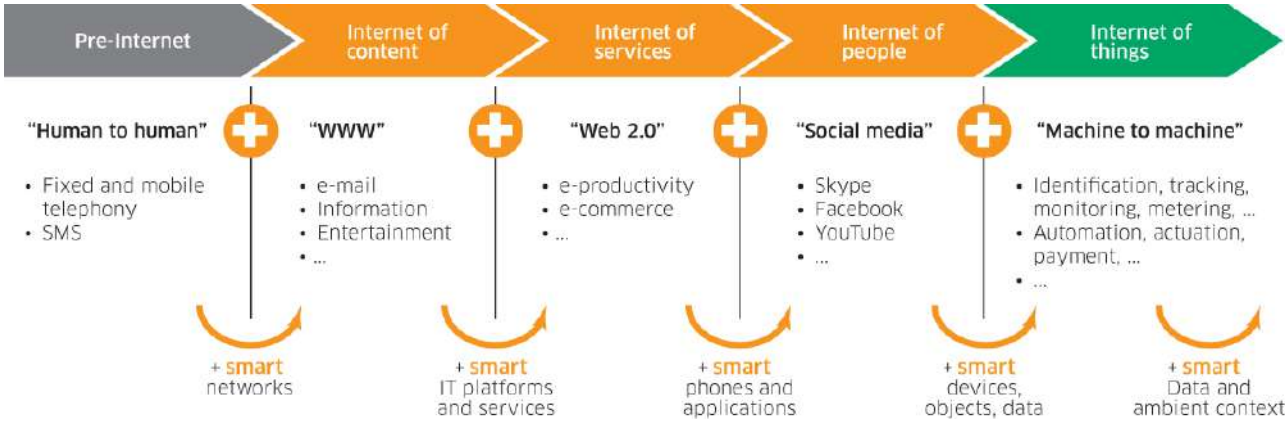


FIGURE 1.1 – The next step in internet evolution [6]

1.2 IoT

1.2.1 Definition

In the last few years, the Internet of Things has become one of the latest and high-level technologies of the 21st century. Having made it easy for us to connect everyday things : kitchen, cars, thermostats, baby monitors - to the Internet via various software, the connection between people, processes, and things has become possible [36].

In this world there are huge kinds and different objects, phones, sensors, software, and other technologies, all of those are connected over networks that leave them to

exchange, update, store, or use data and information with other devices and systems and more other operations, this is the IoT [36].

We can also definite it like this : The Internet of Things is a network of networks that allows, via identification systems standardized and unified electronic devices, and wireless mobile devices, to identify directly and unambiguously digital entities and physical objects and thus to be able to recover, store, transfer, and process, without discontinuity between the physical and virtual worlds, data attached to it [1].

There are also many areas of IoT application, among which we mention :

Smart city : By that we mean smart traffic and how to organize it using the technology of IoT, smart transportation, as it is now used in all developed countries, equipped with various sensors that facilitate the process of movement and more other applications

Smart environments : Earthquake prediction, fire detection, and other data that we can extract from the real world. A real example of this is meteorological technology.

Industrial control : Measuring various data and predicting faults without the need to check the health of machines, troubleshoot remotely, and even maintain them remotely.

Health : Remote monitoring of biological parameters and ensuring a person's health through programs designated for that and others.

Smart Agriculture : Measuring the various data related to agriculture and doing what is necessary automatically, and by that, we mean autonomous systems.
and more other domains

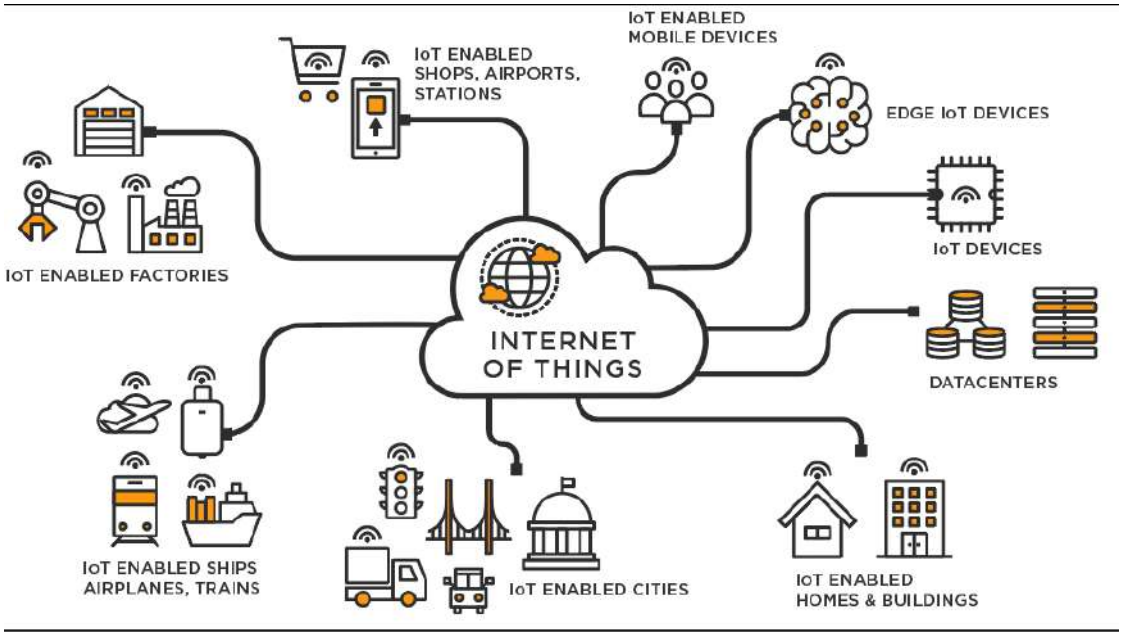


FIGURE 1.2 – Internet of Things[49]

1.2.2 Architecture of IoT

There is not only consensus on the architecture of the Internet of Things, which all the universe agrees on it. Different architectures have been proposed in different research : three, four, and five layers, and the basic one on those is a three-layer architecture. tee the figure below : [45]

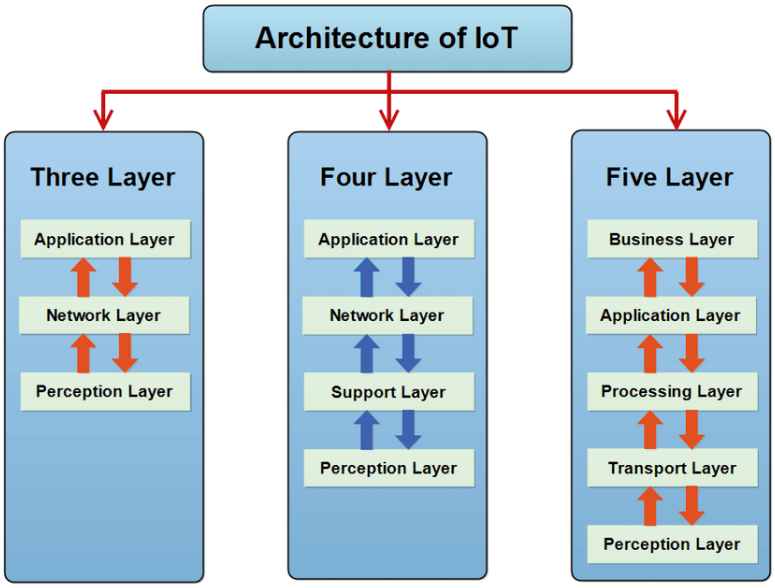


FIGURE 1.3 – The Different Architecture of IoT [42]

- **The perception layer :** Is the physical part, which has sensors for sensing and

gathering information and values from the environment. It senses some physical parameters or identifies other smart things in the environment [45].

- **The network layer :** Is responsible for connecting things to other smart things, servers, network devices ...Also it is used for transmitting and processing sensor data [45].
- **The application layer :** Is responsible for serving specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart cities, smart cities, and smart Agriculture ...[45]
- **The transport layer :** Transfers the data from the perception layer " sensors " to the processing layer and vice versa through networks such as WLAN, 5G, LAN, Bluetooth, RFID, and NFC [45] .
- **The processing layer :** Or the middleware stores, analyzes and processes a big size of information that comes from the transport layer. It can manage and gives a different set of services to the lower layers. It used many services similar as cloud computing and big data ...[45] .
- **The business layer :** Manages the entire IoT system, including applications, business and gain models ...[45]

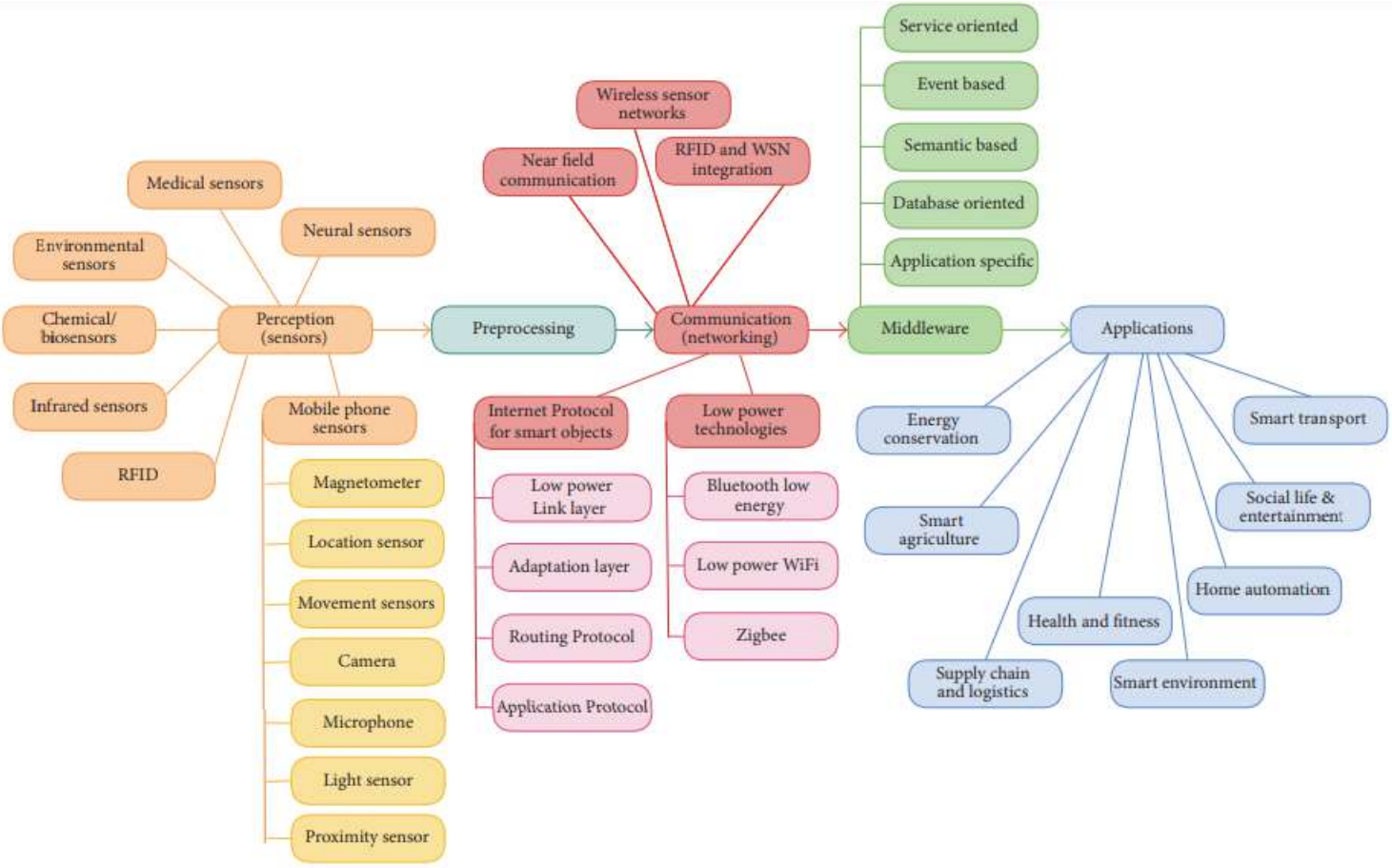


FIGURE 1.4 – Taxonomy and explanation of IoT technologie [45]

1.3 IIoT

1.3.1 Definition

The Industrial Internet of Things (IIoT) is the application of Internet and Internet of Things technologies in the industrial field to connect sensors and smart industrial equipment within industrial areas.

The goal of the Industrial Internet of Things is to develop highly automated production and business processes. Research also seeks to develop and disseminate industrial technologies based on the Internet of Things, in order to facilitate tasks for humans and reduce the risk they face [52].

1.3.2 Revolution

IIoT system is also known as Industry 4.0 or the Fourth Industrial Revolution. These terms have the same meaning and relate to the rise of automation, communication, and self-monitoring in traditional manufacturing and industrial activities [40].

When we talk about history, The industrial revolutions are coal, gas, electronics and nuclear, and the internet and renewable energy. Beginning from the 17th century through the present day, we've seen an amazing evolution. As we discovered different energy sources, and later when digital technologies were invented, the entire sense of technology has been changed [50] .
And from this the four industrial revolutions are :

The First Industrial Revolution : in 1765

Coal production The Industrial Revolution transformed our economy from agriculture to industry. The processes became mechanized which goes to the discovery of coal, Products were made for the first time. It also contributed to the development of the steam engine, which changed all concepts about production and transportation [50].

The Second Industrial Revolution : in 1870

Since the first industrial revolution was about coal, the second was about discovering other sources of energy which are electricity, gas, and oil. As well as the invention of the combustion engine that works with these fuel sources. Lots of new products entered the market during this time. With the intensity of developments in communication technology : the telegraph, then the telephone... and very quickly, they invented the plane and the car [50].

The third industrial revolution : electronics and nuclear 1969

This revolution took place around nuclear as the first commercial nuclear power plant was installed in the United States, Another hundred years later, nuclear power and electronics came out to the open world. Nuclear power began in Europe, then in Great Britain and the United States, and then in Asia [50].

The Fourth Industrial Revolution : Internet and Renewable Energy in 2000

with the industrial revolution in our time and the developments we witness every day, we see a displacement of renewable energy, solar energy, wind energy, and geothermal energy. Because of the acceleration of digital technology and the expansion of its use, all the world now uses the computer, and because of that, renewable energies must be used [50].

The Internet and the digital world have also changed a lot about production and industry, inside and outside the facility's walls. As the Industrial Internet of Things, cloud technology, and artificial intelligence continue to develop, the virtual world and the physical world merge. Predictive maintenance and real-time data will lead to smarter

decisions and now the IIOT become very interesting to countless companies around the world [50].

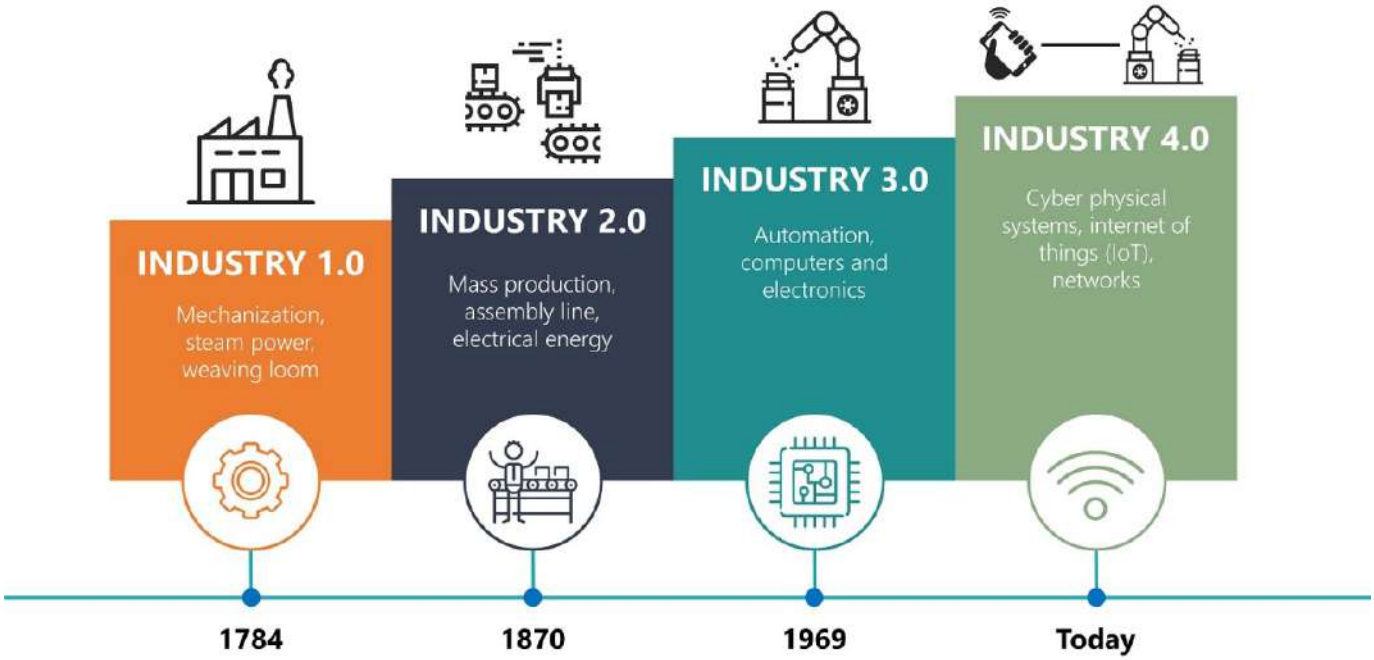


FIGURE 1.5 – The Fourth Industrial Revolution[32]

1.4 IIoT vs IoT

IoT, or the Internet of Things, is a general term, it describes objects connected over a network and sends or receive, or uses data on the internet. the IIoT is a subpart of IoT [40].

The IoT describes any equipment that sends or receives data over the networks. When this equipment is used in the industrial environment, we no longer speak of IoT, but we speak about IIoT [40].

For example, the IoT devices include connected light bulbs, locks, and thermostats ..., while IIoT devices include water meters, machines in factories, sensors for flame and humidity, sensors installed on pipelines, and many other pieces of equipment [40].

CHAPITRE 2 :
Intrusion detection system

Intrusion detection system

The security of information systems or more simply computer security is all the technical, organizational, legal, and human means necessary for the implementation of means aimed at preventing unauthorized use, misuse, modification, or misappropriation of the information system. Ensuring the security of the information system is an activity of the management of the information system.

Today, security is a major issue for companies as well as for all the players around them. It is no longer confined solely to the role of the IT specialist.

Its long-term purpose is to maintain the trust of users and customers. The medium-term goal is the consistency of the entire information system. In the short term, the goal is for everyone to have access to the information they need.

The standard dealing with information security management systems (ISMS) is ISO / IEC 27000 which emphasizes Confidentiality - Integrity - Availability [26].

2.1 Cybersecurity

Information Security is not only about authorized and unauthorized access. The practice of preventing unauthorized access is called Information Security, use, disclosure, disruption, modification, inspection, recording, or destruction of information. Information has many types physical or electronic ... Your details "your profile on social media, your data on your mobile phone, your biometrics, etc. " all of this considered as information This Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media, etc ...

Cybersecurity represents the development of technologies, processes, and controls to protect systems, networks, programs, devices, and data against potential digital attacks, to ensure three properties of information, services, and IT infrastructure : confidentiality, integrity, and availability.

When we talk about data security, it's all about securing data from malicious users and threats. So what is Data or Information and what is the big difference between them ? the important thing is that "not every data can be considered as information"

data can become a piece of information if it is interpreted in a context and given a sense. For example, some numbers are data and if we know that it's the age of a person then it is information because it has signification. So information means data that has some meaning [19, 17].

CYBER SECURITY	INFORMATION SECURITY
This is the practice of protecting data from external influences on Internet resources.	This is all to protect information from unauthorized users, access and data modification or deletion to ensure confidentiality, integrity and availability.
It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with protection of data from any form of threat.
Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Cybersecurity deals with danger against cyberspace.	Information security deals with the protection of data from any form of threat.
Cybersecurity strikes against Cyber crimes, cyber frauds and law enforcement.	Information security strives against unauthorised access, disclosure modification and disruption.
On the other side , cybersecurity professionals deal with cybersecurity using advanced persistent threats.	Information security professionals are the foundation of data security, and relevant security professionals prioritize resources before dealing with threats.
It deals with threats that may or may not exist in cyberspace, such as : B. Protecting your social media accounts, personal information, etc.	it deals with information, assets and integrity, confidentiality and availability.

Tableau 2.1 – Difference between Cyber Security and Information Security [17]

2.1.1 Concepts of Cybersecurity

The concept of cybersecurity is connected to the CIA security model. the picture below shows the triangular model with three components : confidentiality, integrity, and availability (CIA) [30].

CIA triad

These three letters are the first letters of the words : Confidentiality, Integrity, and Availability [13].

These principles constitute the basic security infrastructure for any organization, and they should act as goals and objectives for every security program [13].

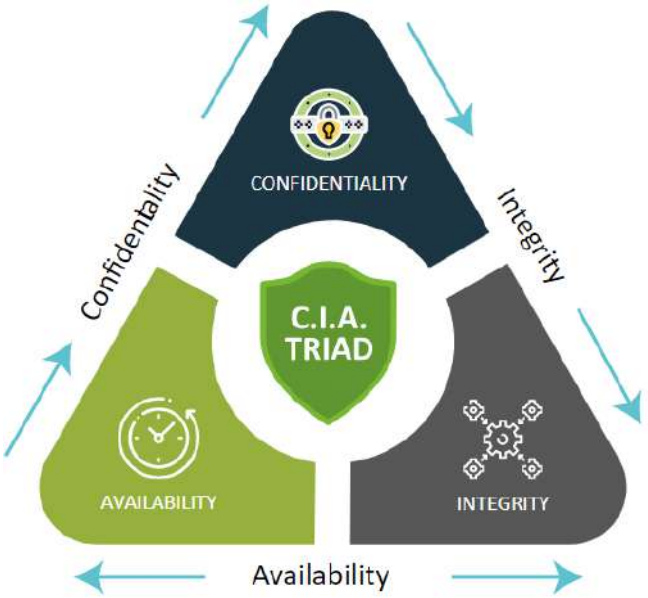


FIGURE 2.1 – CIA triad[51]

Confidentiality When forestalling the revelation of data to unapproved parties is required, the property of secrecy is also required. Cryptography is utilized to scramble data, to make it confused to everybody except the individuals who are approved to see it. The cryptographic calculation and method of activity should be planned and actualized so that an unapproved group will be not able to identify the keys that have been related to the encryption or infer the data without utilizing the right keys [30].

Integrity Information trustworthiness confirms that information has not been adjusted in an unapproved way after it was made, communicated, or put away. This implies that there has been no inclusion, erasure, or replacement carried out with the information. Advanced marks or message confirmation codes are cryptographic instruments that can be utilized to identify both inadvertent changes that may happen as a result of equipment disappointment or transmission issues and intentional adjustments that may be performed by an enemy. While non-cryptographic instruments can be utilized to identify coincidental adjustments, they are not solid for distinguishing conscious changes [30].

Availability A system must operate flawlessly during intended ranges of use and guarantee access to services or to the data or informations and resources installed over time expected response [30].

There are also other aspects that can be considered as information system security objectives, such as

Authorization An authorization needs an approval to play out a security capacity design for the same. This security administration is frequently supported by cryptographic help. Approval is commonly allowed after the effective execution of a source confirmation administration ...[30].

2.2 IDS

With the speed development of network technology and in particular wireless networks, the security of these networks as well as its connected terminals against various intentional or accidental threats, has become a crucial problem.

All information concerned with Internet technologies, information stored in databases and transmitted over the network must be protected. The intrusions are real threats that can be unauthorized activities or malicious uses of information resources that violate the policies of security.

Traditional intrusion prevention systems and techniques such as firewalls, encryption, and access control are mostly ineffective against to the evolution of new sophisticated threats.

How to overcome cybersecurity challenges, identify intrusions and protect our data is a key issue that should never be circumvented. A new concept of intrusion detection was proposed by James Anderson in 1980, with the aim of identifying any unauthorized activity in a network [16].

2.2.1 Definition of Intrusion detection system

Intrusion Detection System (IDS) is the system responsible for monitoring and searching for suspicious activities. Such a system is used to discover prohibited and malicious activities, and it also helps the person responsible for the information service to discover such activities [18].

In other definition : Intrusion detection is the process of monitoring events that occur in a network or on a computer system and analyzing them for signs of imminent threats of violation of computer system security policies or standard security practices. An intrusion detection system is a set of hardware and software components designed to automate the process intrusion detection ,In addition to this definition, Intrusion Detection Systems have the various definitions in literature such as ; they are designed to detect attacks on computer systems [44, 3].

Examples of these activities : hacking, hacking, malicious activity, safety violations, or anything illegal [18].

2.2.2 Architecture of intrusion detection systems

Since the first intrusion detection model was developed by "Dorothy Denning" of SRI International, many intrusion detection systems (IDS) have been proposed in both research and commercial fields [31].
Although these systems vary widely in the techniques used to collect and analyze data, most of them rely on a relatively common technique [31]. The architectural framework (diagram 2.2) consists of the following Element :

— Data acquisition devices (sensors) are responsible for a surveillance system.

— Detector (intrusion detection (ID) analysis engine) processes the data Collected by sensors to identify intrusion activity.

— Knowledge base (database) consists of sensors, but in a preprocessed format (e.g. attack knowledge base and their signatures, filtered data, data profiles, etc.). This information is Typically provided by network and security professionals.

— Configure the device to provide information about the current state Intrusion Detection System (IDS).

— The Response component initiates an action when an intrusion is detected. These responses can be automatic (proactive) or involve humans Interactive (inactive) [31] .

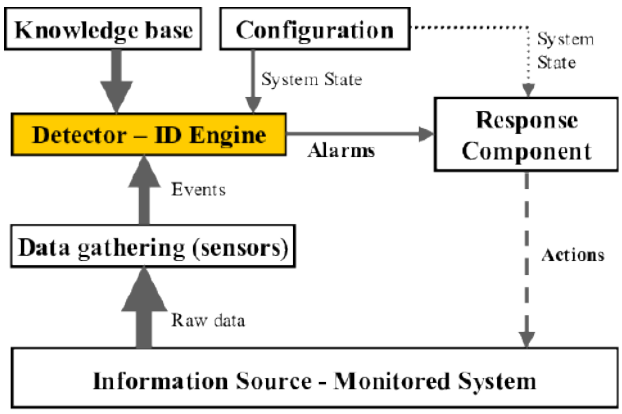


FIGURE 2.2 – Classification of IDS [31]

.

2.2.3 Classification of Intrusion Detection System

The intrusion detection system is classified into three main categories or classes : signature based detection systems , anomaly based detecstion systems , specification

based detection systems [4].

A signature-based detection system

Also called misuse based , This type of detection is very effective when we talk about the known attacks and the receiving of updates and it will not be able to detect unknown threats or new releases [4].

Anomaly based detection system

This type of detection depends on the classification of the network to the normal and anomalous, as this classification is based on rules or heuristics rather than patterns or signatures and to implement a system with this type we should have first a normal behavior of the network[4].

Specification based detection system

This type of detection system is responsible for monitoring the process and matching actual data with the program, alerting if there is abnormal behavior, and needs to be maintained and updated whenever any changes are made to the monitoring program to be able to detect unknown prior attacks, As well as the number of false positives, this can be less than the method of anomaly detection systems[4].

2.2.4 Method of IDS

According to the usage and the learning methods, Intrusion Detection Systems are classified to two main classes as bellow :

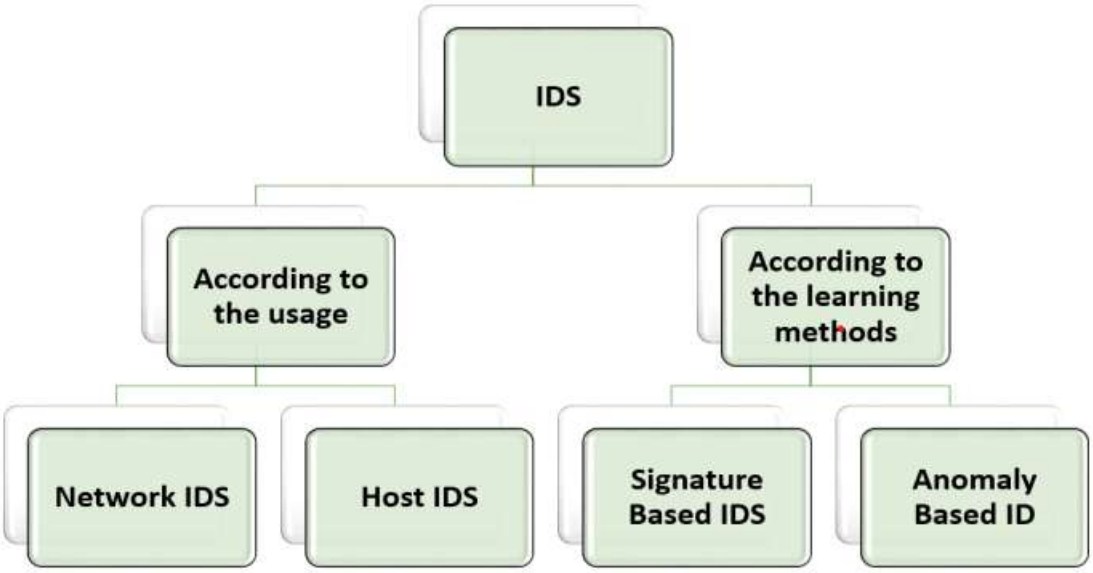


FIGURE 2.3 – Classification of IDS[3]

.

Network IDS

Network Intrusion Detection Systems (NIDS) monitor and analyze packet traffic on a network. Both Rule-based methods and Anomaly detection techniques can be used to detect intrusions. They usually work real time and when an intrusion is detected by NIDS, an alarm is generated. NIDS record all information about all intrusions as logs [3].

Host IDS

In spite of the fact that Network Intrusion Detection systems monitor all traffic on the network, Host-based Intrusion Detection systems only watch intrusions based on the system's configuration and application activity. Host-based IDS analyze abnormal behavior logs on a specific system. The term "host" is referred to a single computer, so a separate sensor for each machine will be required [3].

Signature-based Method

Signature-Base Detection , misuse detection , knowledge base detection ,they are all names for the same methods , it detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their

pattern (signature) is not known.
Also this method works as an antivirus technique that detects the intrusion's pattern or signature and compares it with the library database to decide if this traffic is legitimate or not and report it to the network administrator. Using this technique, it is very easy to detect known attacks, because information about the attack is available in the database in contracts. It's challenging to detect unknown attacks, however, because the database stele is not yet updated [30, 29].

Anomaly-based Method

Anomaly-based IDS is also known as behavior-based detection. It was introduced to detect unknown malware attacks when new malware was developed rapidly. Anomaly-based IDS uses machine learning to build a model of trusted activity, compares anything that comes up to that model, and flags it as suspicious if it's not found in the model. Compared to signature-based IDS, machine learning-based methods have more general properties, as these models can be trained according to the application and hardware configuration.
In other definition This method focuses on detecting both network traffic and computer intrusion or misuse by determining them to be normal or abnormal, using predefined rules created by the network administrator instead of using patterns or signatures. In these methods, the system can be used in several ways to detect positive traffic and report unwanted traffic to the network administrator [30, 29].

2.2.5 Evaluation of IDS

The parameter that allows us to know the percent of the efficacy of the intrusion detection systems are :

Accuracy

The IDS system is accurate when it detects attacks without raising false alarms. Non-precision arises when he declares as abnormal or instructive a legitimate action in the environment[10].

Processing performance

Is measured by the speed at which events are processed. When the IDS system is more efficient then real-time detection will be possible[10].

Completeness

This is the ability of an IDS to detect all attacks[10].

Fault tolerance

Most intrusion detection systems run on operating systems or hardware that are known to be vulnerable to attack. So an IDS should be resistant to these attacks especially denial of service attacks[10].

Speed

The IDS must be faster in analysis and execution to minimize the time to react, and also to prevent the attacker from altering the source of verification or interrupting the operation of the system [10].

2.2.6 The advantages and disadvantages of IDS methodology

Networks have been around for a very long time and it is already a blessing, that it is perhaps impossible to live without it, it has brought people and the world closer to each other, make commerce so easy, makes all things easier, and gives us a lot of other services. With networks, the risk of intrusion into these networks has become a reality. Because of this intrusion, the intrusion detection system has become a necessity.

The IPS is an advanced and very efficient technology but also has its disadvantages, the table below explains the advantages and disadvantages :

Methodology	Advantage	Disadvantage
Signature-based detection	-a very simple method	-unable to detect unknown attacks
	-powerful in detecting known attacks	-very difficult to keep signature pattern up to date
		-time-consuming to search in the database
Anomaly-based detection	-more powerful to detect new attacks and unexpected vulnerability	-due to constant changes, it has weak profiles accuracy
	-compatible with all operating system	-the service is not available in case of updating behavior profiles
	-easy to detect misuse of privileges	--not able to issue alerts in the right time
Stateful protocol analysis	-knowns and analyzes the protocol states	-consumes more resources to trace protocol state
	-able to detect unexpected commands	-unable to detect attacks that resemble protocol behavior
		-compatibility problem with some operating systems and applications

TABLEAU 2.2 – The advantages and disadvantages of IDS methodology [5]

.

CHAPITRE 3 :
The deep learning

The deep learning

Artificial Intelligence, Machine Learning, and Deep Learning have become the most recent technologies of the cycle, even in today's commercial world as companies are using these innovations to build intelligent machines and systems. And although these terms are dominating the research dialogues all over the world, many people have difficulty differentiating between them, they don't understand the concept of each one.

In this chapter, we are going to discuss the different technologies of deep learning and the here benefits of the IDS and security

3.1 neural network

A neural network is a set of algorithms inspired by the human brain. The purpose of this technology is to simulate the activity of the human brain, and more specifically the recognition of patterns and the transmission of information between the different layers of neural connections.

The basic unit of computation in the neural network is a Neuron. Neurons take input, process it through multiple Neurons in multiple hidden layers, and produce output through the output layer [48] .

3.1.1 Neurons

Biological neurons are the basic units of the brain and nervous system. These cells are responsible for receiving sensory input from the outside world through dendrites. They then process this sensory input and release output through axon terminals.

Biological neurons inspired the general model of neural networks in machine learning. This model is called a perceptron [48].

3.2 perceptron

A perceptron is a single layer neural network that gives a single output. The image below shows a model of Perceptron ,

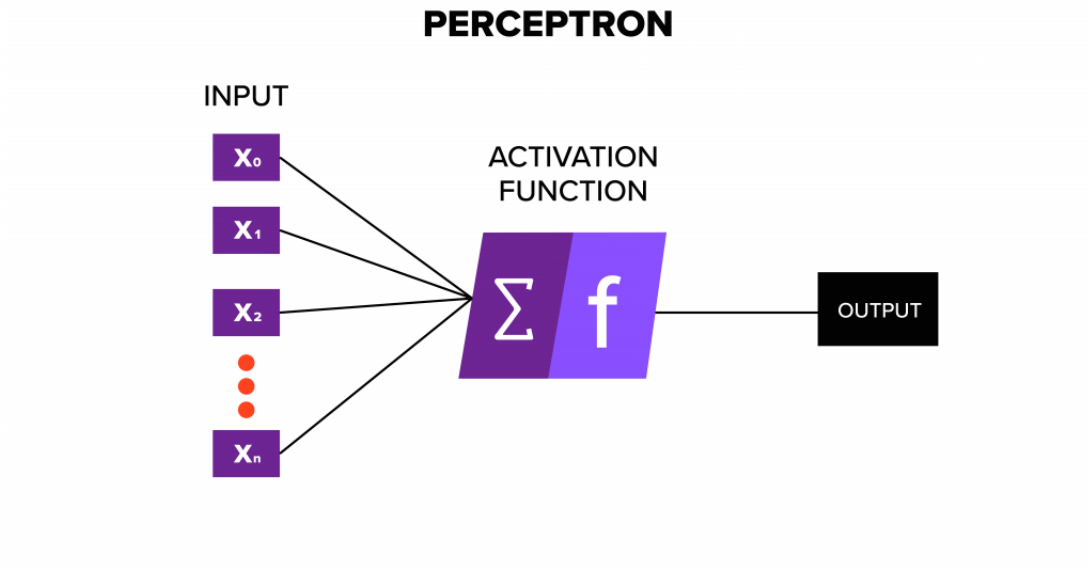


FIGURE 3.1 – Perceptron[48]

In this figure, x0, x1... xn represent various inputs (independent variables). Each of these inputs is multiplied by independent weights, which are represented as w0, w1...wn, These weights help determine the importance of any given variable. The products of inputs and weights are summed and fed to an activation function to generate an output, this is the concept of the perceptron [48].

3.2.1 The activation function

The activation function applies a step rule (convert the numerical output into +1 or -1) to check if the output of the weighting function is greater than zero or not [48, 47].

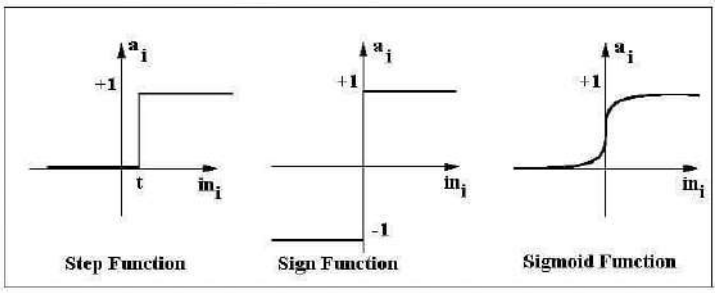


FIGURE 3.2 – activation function[47]

3.3 machine learning

Machine learning is a field of computer science that gives computers the ability to learn without being explicitly programmed, in another way it is the branch of artificial

intelligence and computer science that uses data and algorithms to mimic the way human beings learn. The aim is for machines to 'learn' autonomously. It should be noted that machine learning is different from 'deep learning', another field of artificial intelligence.

Neural network structures/arrange algorithms in layers of fashion, that can learn and make intelligent decisions on their own. Whereas in Machine learning the decisions are made based on what it has learned only [11, 24].

3.4 Deep learning

Deep learning is a machine learning technique that teaches computers to do what humans take for granted : learn by example. Deep learning is a key technology behind driverless cars, enabling them to recognize stop signs or differentiate between pedestrians and lampposts. It is the key to voice control in consumer devices such as cell phones, tablets, TVs and speakerphones. Deep learning has received a lot of attention lately, and for good reason. Achieved previously impossible results [24].

3.4.1 Deep Learning vs Neural Network

Parameters of Comparison	**Deep Learning**	**Neural Network**
Definition	Deep learning is a subset of machine learning that gives the system the capability to function like a human brain and imitate patterns that our brain does for making decisions	Neural networks are based on algorithms that are present in our brain and help in its functioning. A Neural network interprets Numerical patterns which may be present in the form of Vectors
Architectures	1. Convolutional Neural Network 2. Recurrent Neural Network 3. Unsupervised Pre Trained Network 4. Recursive Neural Network	1. Recurrent Neural Network 2. Symmetrically connected Neural Network 3. Single-Layer Feed-Forward Network
Interpretation Power	The deep learning network interprets your task with higher efficacy.	A Neural network interprets your task with poor efficacy.
Components Involved	Large PSU, GPU, Huge RAM	Neurons, learning rate, Connections, Propagation functions, weight
Time Taken	It may take a lot of time to train the network.	Since it is less complex, the time required to train the network is very less.
Performance	High Performance	Low performance

TABLEAU 3.1 – Comparison Table Between Deep learning and Neural Network [30]

3.5 The Intrusion Detection System based on deep learning

With the availability of large amounts of data from cyberinfrastructure, networks, operating systems, or information systems and to address cybersecurity challenges, methods and techniques such as machine learning, data mining, statistics, and other interdisciplinary capabilities have been exploited

Deep learning which is a subset of machine learning could be used for signature-based or anomaly detection-based IDSs. These classification and prediction methods can be used to detect unusual patterns and behaviors of various cyberattacks that enable real-time cyber response. They have the ability to detect attacks when they have occurred and also the ability to predict potential future attacks.

On the other hand, the collection of data and network traffic has led to a big-data problem security experts always want better performance IDS which have the highest detection rate and the highest false alarm rate low. Therefore, deep learning approaches adapt well to a very large amount of data.

The latter is introduced for the detection of network anomalies with the aim of differentiating between normal behavior and abnormal behavior in order to detect malicious or suspected malicious activity [14, 2].

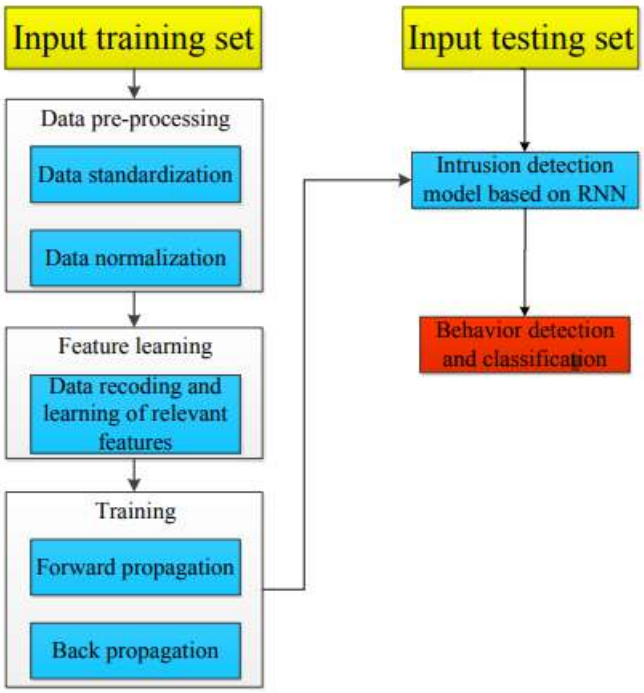


FIGURE 3.3 – Flow chart of the Intrusion Detection System based on deep learning example[14]

CHAPITRE 4 :
Intrusion detection based on deep learning

Intrusion detection based on deep learning

4.1 Related works :

Existed intrusion detection in different fields : Potluri et al [37]. Proposed a CNN-based detection method. They applied experiments on the NSL-KDD and the UNSW-NB 15 datasets. The data type in these datasets is a feature vector. The final result was that the feature vectors were transformed into images of 8*8 pixels. Finally, they constructed a three-layer CNN to classify the attacks. They compared their model with other deep networks (ResNet 50 and GoogLeNet), and the proposed CNN performed best, reaching accuracies of 91.14% on the NSL-KDD and 94.9% on the UNSW-NB 15.

Zhang et al [54]. Extracted features with a sparse autoencoder and detected attacks with an XGBoost model. They used data from the NSL-KDD dataset. Due to the imbalanced nature of this dataset, they used balance algorithms so they can make every class balanced. Finally, they classified the data using an XGBoost model. Their model achieved accuracies on the Normal, DOS, Probe, R2L, and U2R classes of 99.96%, 99.17%, 99.50%, 97.13%, and 89.00%, respectively.

Kang et al [28]. Proposed an intrusion detection system based on the deep neural network (DNN) to secure vehicle networks. The attack scenario was carried out on malicious data packets. These are injected into a network bus of vehicle controllers. The proposed system introduces the feature vector into the input nodes in order to classify the packets into two classes (a normal packet and an attack packet). The proposed system achieves a false positive rate (TPR) of less than 1 or 2%, and a detection rate (DR) of 99%.

Hajisalem et al [22]. Have creat a hybrid classification method using Artificial Bee Colony (ABC) and Artificial Fish Swarm (AFS) in their study. They use Fuzzy C-Means Clustering (FCM) for feature selection and Correlation-based Feature Selection (CFS) techniques. The last step was developing If-Then rules with the CART technique to

distinguish between normal and anomaly records. The data sets used in the application of those methods were NSL-KDD and UNSW-NB15 data sets with an accuracy rate of 99% were obtained.

Inayat et al [25]. Test the design parameters of the existing intrusion response system (IRS) in their study.in the line with this study, many comprehensive studies exist in this field, but in the studies conducted, attack semantics are missing and they use static response metrics instead of a dynamic approach. This causes the system to generate more false alarms.

Sharafaldin et al [46]. Realize the CSE-CIC-IDS-2017 dataset since the existing datasets did not satisfy today's intrusion detection needs. A test environment consisting of network attackers and attacks has been made, to create the data set. In the test environment, attacks such as Brute force, heartbleed attack, botnet, DoS, DDoS, Web attack, and Infiltration attack were organized. In addition, they used machine learning methods to evaluate system performance.

Sandee et al [20], A DNN for NIDS composed of a sparse auto-encoder used for unsupervised feature learning, and logistic regression for binary classification on the NSL-KDD dataset (normal/intrusion). The system takes 115 features as input, and the auto-encoder sparse was used for training and learning new features, so these features were reduced to 50, then to 10, then assigned to the regression classifier classification logistics. System performance was measured in terms of accuracy, precision, and recall. The overall accuracy of the model was 87.2%

Studies	Year	dataset	method	results
Potluri et al.	2018	NSL-KDD UNSW-NB 15	CNN	Accuracy : 91.14% 94.9%
Zhang et al.	2018	NSL-KDD	———	99.96%
Kang et al.	2016	———	DNN	99%
Hajisalem et al.	2018	NSL-KDD UNSW-NB 15	ABC/AFS	99%
Sharafaldin et al.	2018	CSE-CIC-IDS-2017	ML Methods	———
Sandee et al.	2019	NSL-KDD	DNN	87.2%

TABLEAU 4.1 – Some related works in IDS with different dataset and methods

Existed intrusion detection system in IIOT fields : Deep learning methods had been the main rock in intrusion detection systems for the last years, many works have

been developed recently in this field to take a brief idea about it we'll present to you some realizations :

Da Costa et al [9]. Presented some issues in IoT environments and their security and then reviewed some ML-based intrusion detection for IoT and network security. Only the detection approach alongside the target protocol, precision performance, and used data-set was considered in their study, which is not the only parameter that may identify the IDS efficiency. Zarpelao et al [53]. Reviewed some designed IDS systems schemes for IoT based on : detection method, placement strategy, security threat, and validation strategy. while the detection approach and performance metrics mainly used for IDS classification were out of the study.

Elrawy et al [12]. Discussed the typical IoT architecture, associated threat type, and emerging security vulnerabilities, then surveyed applied IDSs for the IoT paradigm. Their study was conducted based on : detection method, detection approach, placement, performance metrics, and some features. The IDS main standards were well-specified, and adequate requirements for IoT were brought out as well. On the other hand, the validation data were not considered.

Hajiheidari et al [21]. Showed a systemic review of proposed intrusion detection techniques for the IoT environment. Based on their literature research results, their study was focused on : detection methodology, detection approach, nine categories of target attacks, and related performance metrics. The benefits and disadvantages of the presented work are also highlighted. However, the data source was not considered. Santos et al [43]. Reviewed several selected IDSs for IoT networks, classifying the IDS based on only three levels : detection method, security thread, and placement strategy. Their selected works do not include a variety of IoT technologies and emerging attacks. Their study was also conducted on limited classification attributes, which does not reflect the nature of IDS-based security in IoT environments.

Pundir et al [38]. Discussed security problems and various attacks possible associated with Wireless Sensor Network (WSN) and IoT-based communication environments. They presented architectures, threat models, and security protocols applied in WSN and IoT. A comparative study of IDS methods based on performance metrics was also provided in their work. Cyber-Physical System (CPS) is part of IIoT that operates as a control system for the physical environment.

itchell and Chen[35] Reviewed IDSs design principal and detection techniques for CPS. They focused on two main dimensions : detection technique and audit material (data source). The functionality of IDS in CPS architecture and existing protocols are well explained. However, the used detection approaches are not discussed.

CHAPITRE 5 :
Conception and realization

Conception and realization

5.1 Introduction

Intrusion detection systems based on deep learning have become the subject of much research. So, we discussed in the chapter preceding the different deep learning methods that have been successfully applied in the intrusion detection task using different datasets dedicated to cybersecurity. The performance of IDS based on deep learning is highly dependent on the dataset used and no reference model for intrusion detection was found.

In this work, we chose a new cyber security dataset named Edge-IIoTset [15], the detection of cyberattacks in the industrial internet of things known as IIOT.

We offered 2 models of deep learning (DNN, CNN) (in cybersecurity allows the IDS to do against these types of network attacks to identify malicious activity in real network traffic. We first started with a DNN model. Then we implemented CNN. For classification of this type of network attack to remedy the problem of detecting various attacks possible with a very high detection rate and a negligible alarm rate.

The performances of the proposed detection approaches have been evaluated taking into account the different evaluation measures of deep learning algorithms namely, accuracy, recall, F1 score, detection rate, and false alarm rate.

5.2 Runtime environment

Deep Learning is a field with requirements for the availability of hardware resources (especially GPUs) capable of performing intense calculations. At first, we started by setting up a local Python development environment using the Anaconda platform, But not for long, we switch to using Google-Colab.

Anaconda : Is a free and open-source distribution of the Python and R programming languages. applied to the development of applications dedicated to machine learning and data science.

About the general analysis of the data and the conversation of type and other preparation of the data, This database has already been cleaned and made up also was converted to a CSV by several stages was done by researchers Mohammed Farag and djallel hamouda.

Afterward, to move towards deep learning of our work, we needed to go to the Cloud, the latter provides significant computing and memory resources that exceed our computers. Depending on the need, the Cloud can provide access to a free GPU graphics processor. Among the most widely used Cloud tools in the field of machine learning is **Google Colab**.

Colab Colaboratory, often shortened to "Colab", is a product of Google Research. Colab allows anyone to write and run Python code of their choice through the browser. It is an environment particularly suitable for machine learning, data analysis, and education. In more technical terms, Colab is a hosted Jupyter notebook service that requires no configuration and provides free access to computing resources, including GPUs.
In other definitions COLAB is a Cloud service based on Jupyter Notebooks that allows to development of Deep Learning applications in Python, it offers a free GPU processor, 12 GB of RAM, and more than 100 GB of storage. For access to this service, we simply need to have a Google account [41].

For the development language we chose Python, an interpreted, multi-paradigm, and multi-platform programming language, it is also a more common and popular language for machine learning and artificial intelligence thanks to its flexibility and also because there is a significant number of open-source software libraries available. Enables its libraries used in our project : pandas, Numpy TensorFlow,sklearn, google-Colab, matplotlib. . ., etc.

The TensorFlow and Keras frameworks were chosen for the implementation of the proposed deep learning methods.

TensorFlow Is an open-source deep-learning library developed by Google and used to perform complex numerical operations and several other tasks to model Deep Learning architectures. It can easily deploy calculations on multiple platforms like CPUs, and GPUs.

Keras Is a high-level API that aims to create and train python-based Deep Learning models. It was developed to allow rapid experimentation. Among these advantages,

— Was able to go from idea to result in the shortest time possible. And that is the key to effective research.

— Supports both convolutional networks (CNN) and recurrent networks (RNN) as well as the combination of the two items No separate model configuration files, everything is declared in the code.

— works on CPU and GPU.

Although Keras provides all the general functionality needed for building deep learning models, it does not provide as much as TensorFlow which offers more and more advanced operations to get good control to develop a particular type of model, it gives us also allows for better understanding what is happening inside a DL network. In order to benefit from the advantages of both, we used TensorFlow as a back-end with Keras. The experiment environment was google Colab with a GPU processor and 12 GB RAM.

Pandas and Numpy Are used for data manipulation (loading, rearranging, and processing data).
NumPy library provides objects for multi-dimensional arrays, whereas Pandas is capable of offering an in-memory 2d table object called DataFrame. NumPy consumes less memory as compared to Pandas. Indexing of the Series objects is quite slow as compared to NumPy arrays [27].

Scikit-Learn Allows us to experiment with different predefined machine learning and data analysis techniques and algorithms quickly and easily. used.

Matplotlib Matplotlib is the most famous library for data visualization with python. It allows the creation of literally every type of chart with a great level of customization. [39]

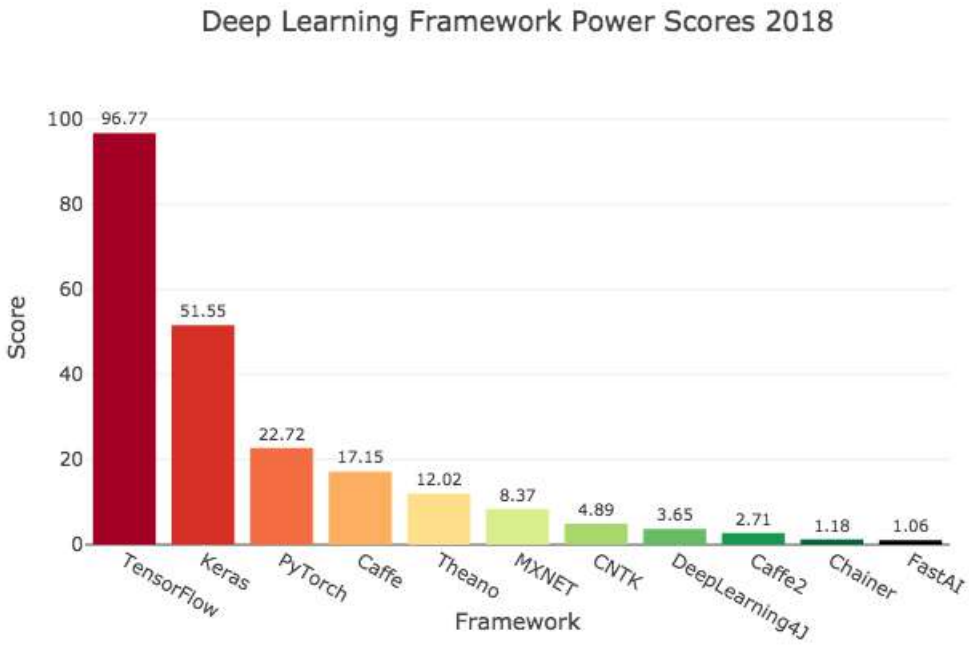


FIGURE 5.1 – The 10 Most Popular Deep Learning Frameworks[23]

5.3 Dataset

The dataset chosen for this study is Edge-IIoTset-2022 data-set, provided by the searcher MOHAMED AMINE FERRAG, it constitutes flow data real-world network with several of the latest and most prevalent cyber security attack types. These data are more condensed formats that contain mostly meta-information about network connections, or each data. Therefore, we decided to chose this new synthetic real-world cybersecurity dataset for IoT and IIoT applications, which can be used by deep learning-based intrusion detection systems in two different modes, centralized learning and federated learning. Specifically, the proposed test platform is divided into seven layers, including cloud computing layer, network function virtualization layer, blockchain network layer, fog computing layer, software-defined network layer, edge computing layer, and IoT and Industrial IoT perception layer. At every layer there are new technologies that meet the key needs of IoT and IIoT applications, such as : the ThingsBoard IoT platform, OPNFV platform, Hyperledger Sawtooth, Digital twin, ONOS SDN controller, Mosquitto MQTT brokers, Modbus TCP/IP, . . .etc [15].

IoT data is generated by various IoT devices (10+) such as B. Inexpensive digital sensors for temperature and humidity detection, ultrasonic sensors, sensors for water level detection, pH sensor meters and soil moisture sensors, heart rate sensors , flame sensor, etc.). However, they identified and analyzed 14 attacks related to IoT and

IIoT connectivity protocols, grouped into five threats, including DoS/DDoS attacks, intelligence gathering, man-in-the-middle attacks, injection attacks, and malware attacks [15].

The full of this dataset contains 2219201 instances, of which 603558 are attacks and 1615643 are instances of benign (legitimate/normal) network traffic, the number of instances for each type of cyber security attack is indicated in tables 5.1 and 5.2

This data-set also contains 61 Features choused between 1176 features found, where 6 of them are labeled and characterized by the stream itself, depending on **Source IP, Source Port, Destination IP, Destination Port, Protocol** and **Timestamp** (attack times), and over 55 network traffic flow characteristics.

Dataset has one disadvantage, this big disadvantage is that they are unbalanced. Instances of benign network traffic represent only 1.13% of the dataset. And also the percentages between attack classes are varied [15].

The classes of this database are : Normal, DDoS-UDP, DDoS-ICMP, SQL-injection , Password , Vulnerability-scanner , DDoS-TCP , DDoS-HTTP , Uploading , Backdoor , Port-Scanning , XSS , Ransomware , MITM , Fingerprinting [15].

1pt

Class Label	Number of Instances	percent
Backdoor	24862	1.120
DDoS_HTTP	49911	2.249
DDoS_ICMP	116436	5.246
DDoS_TCP	50062	2.255
DDoS_UDP	121568	5.478
Fingerprinting	1001	0.045
MITM	1214	0.054
Normal	1615643	72.802
Password	50153	2.259
Port_Scanning	22564	1.016
Ransomware	10925	0.492
SQL_injection	51203	2.307
Uploading	37634	1.695
Vulnerability_scanner	50110	2.258
XSS	15915	0.717
Total	2219201	100

TABLEAU 5.1 – Edge-IIoTset-2022 : The number of records for each category of cyber security attacks in the dataset

1pt

Class Label	Number of Instances	percent
normal	1615643	72.80
attack	603558	27.20
Total	2219201	100

TABLEAU 5.2 – Edge-IIoTset-2022 : The number of records for normal cases and cyber security attacks cases in the dataset

5.4 Taxonomy of attacks

In this dataset, they identified and analyzed fourteen attacks which are categorized into five threats, including, DoS/DDoS attacks, Information gathering, Man in the middle attacks, Injection attacks, and Malware attacks.

The DoS/DDoS attacks A denial of service or distributed denial of service (DDoS) attack aims to make a server inaccessible by sending multiple requests until it is saturated or by exploiting a security in order to cause a breakdown or a severely degraded operation of the service. This type of attack can be very serious for the organization that is the victim. During the attack, the site or service is no longer usable, at least temporarily, or with difficulty, which can lead to direct loss of income for merchant sites and loss of productivity. which include four attacks, namely, TCP SYN Flood DDoS attack, UDP flood DDoS attack, HTTP flood DDoS an ICMP flood DDoS attack [15, 8].

The Information gathering Consists of analyzing IoT data packets to spot the weakness of IoT devices as well as Edge servers, which include three attacks, namely, Port Scanning, OS Fingerprinting, and Vulnerability scanning attack [15].

Man-in-the-middle attacks Involve intercepting communications between IoT devices and edge servers, and include two types of attacks, ARP spoofing attacks and DNS spoofing attacks [15].

The injection attacks Consist of sending a malicious script to an unsuspecting user, which can access sensitive information, session tokens, cookies, ...etc [15].

Malware attacks Include installing backdoors to control vulnerable IoT network components, including three types of attacks, namely backdoor attacks, password

cracking attacks, and ransomware attacks. table 5.3 provides the list of attack scenarios included in Edge-IIoTset dataset [15].

Attack category	Attack type	IoT vulnerabilities
DoS/DDoS attacks	TCP SYN Flood DDoS attack	Make the victim's IoT edge server unavailable to legitimate requests
	UDP flood DDoS attack	Overwhelm the processing and response capabilities of IoT devices
	HTTP flood DDoS attack	Exploits seemingly-legitimate HTTP GET or POST requests to attack IoT application
	ICMP flood DDoS attack	tack The IoT edge servers become inaccessible to normal traffic By flooding them with request packets (i.e., with ICMP echo-requests (pings))
Information gathering	Port Scanning	Discover open doors or weak points in the edge-based IoT network
	OS Fingerprinting	Analyzing IoT data packets to spot the weakness of IoT devices as well as Edge servers
	Vulnerability scanning attack	Identifying IoT network security vulnerabilities
Man in the middle attack	DNS Spoofing attack	The interception of communications between IoT devices and a DNS server
	ARP Spoofing attack	Linking an attacker's MAC address with the IP address of an IoT device or Edge server
Injection attacks	Cross-site Scripting (XSS) attack	Send a malicious script to an unsuspecting user, which can access sensitive information, session tokens, cookies, ...etc.
	SQL Injection	(Read/Insert/Update/Delete) sensitive data from the IoT database by the injection of a SQL query
	Uploading attack	Uploading files that contain malwares' command and control data
Malware attacks	Backdoor attack	Install backdoors to take control of vulnerable IoT network components
	Password cracking attack	Identify an unknown or forgotten password to an IoT device in order to obtain unauthorized access to IoT resources
	Ransomware attack	Publish or blocks access to IoT data or an IoT device system by encrypting it, until the victim pays a ransom fee to the attacker

TABLEAU 5.3 – The list of attack scenarios included in Edge-IIoTset data-set [15]

5.5 Data preparation

The performance of deep learning methods depends heavily on the quantity and quality of learning data, more data with quality, more precision, and good results. And less data with the same information, less time in the process, and good evaluation of the result, In our case, we have a very sufficient mass of data. However, because of the data class imbalance. This data needs to be reduced. The preparation of the data is about 2 essential operations before processing them. which are : data reduction and resolution of labeling

5.5.1 Database Initialization

As we said previously, we must prepare the database before using it, in other sense, we need to get the important and relevant information and reduce the noise and prepare it for the next step.
This mass of data consists of 16 CSV files of sizes over 20GB and one file cleaned for almost 2 GB.

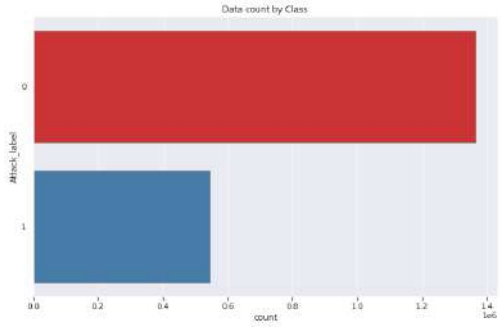
Reading and preparing data were not tasks easy with this huge amount of data, because of that we chose to work on Colab with Kaggle.
Kaggle and Colab give us a feature that we can use databases from Kagel directly through Colab, where we can download it directly in the cloud "memory of Colab", after this we unarchive it and read it directly.

We chose to use the cleaned file because it is better in terms of the originality and the importance of the information. This file contains all the database cleaned including both the normal case and cyber-criminal case, and we will also divide them into two data-set one for learning and the other one for testing.

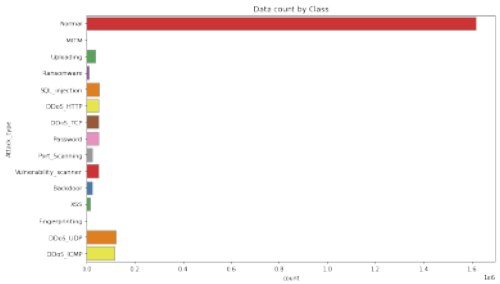
Images 5.2 and table 5.4show the distribution of these data sets.

the class	number of instance before preprocessing	instance before preprocessing %	number of instance after preprocessing	instance after preprocessing %	instance after preprocessing without normal case %
Normal	1615643	72.80	1363998	71.42	——-
DDoS UDP	121568	5.47	121567	6.36	22.30
DDoS ICMP	116436	5.24	67939	3.55	12.42
SQL injection	51203	2.30	50826	2.66	9.40
Password	50153	2.25	50062	2.62	9.24
Vulnerability	50110	2.25	50026	2.61	9.10
DDoS TCP	50062	2.25	49933	2.61	9.09
DDoS HTTP	49911	2.24	48544	2.54	8.83
Uploading	37634	1.69	36807	1.92	6.74
Backdoor	24862	1.12	24026	1.25	4.44
Port Scanning	22564	1.01	19977	1.04	3.65
XSS	15915	0.71	15066	0.78	2.75
Ransomware	10925	0.49	9689	0.50	1.77
MITM	1214	0.05	853	0.04	0.15
Fingerprinting	1001	0.04	358	0.02	0.06
total	**2219201**	**100**	**1909671**	**100**	**100**

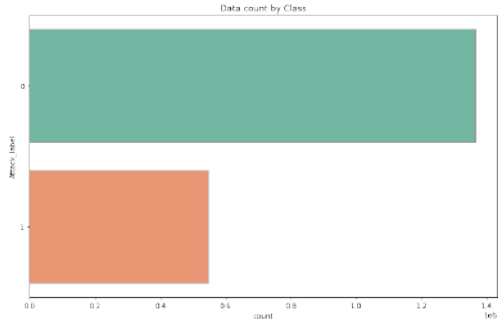
TABLEAU 5.4 – the distribution of data sets



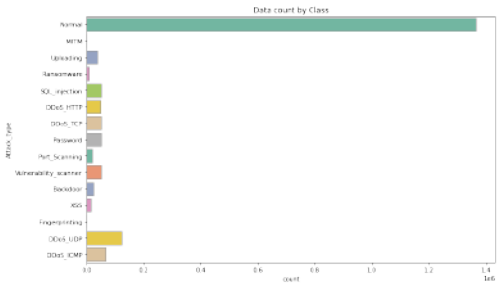
(a) the distribution of the database on 2 class before prepossessing



(b) the distribution of the database on 15 class before prepossessing



(c) the distribution of the database on 2 class after prepossessing



(d) the distribution of the database on 2 class after prepossessing

FIGURE 5.2 – the distribution of the database

5.5.2 Database pre-processing

In order to build a highly accurate model, it is important to perform exploratory analyzes of the data set and its characteristics. Pre-processing of the dataset is done before it is applied to the neural network. The pre-processing steps are as follows :

- First, the dataset was filtered to remove all redundant rows which represent class instances. Next, a scan was performed to detect any '**NAN**' value (Not A Number) or '**INF**' (Infinite Value), these values can be considered as missing values.
  Deep learning algorithms in general treat these values very badly which directly and negatively affects the performance of the final models.
  It appears that the data selected as the dataset concerned by this study have multiple values of 'NAN' for the **Flow Bytes** column, in order to keep this characteristic and as we have sufficient data, rows with NAN or INF values have been removed.
- There are several type characteristics categorical in the dataset that must be encoded. This column has been converted to a numeric column.
  However, other categorical columns like the IP Address and Timestamp columns have been removed. It has been considered that these characteristics are related to connection information and do not represent the properties attacks because the latter can be produced at any time by any machine against any which victim machine, for this reason, we delete other characteristics, so that only the network traffic characteristics remain .
  All the characteristics that we have deleted,converted and that we have left for this study are indicated in tables 5.5 , 5.6 and 5.7
- Also there is a problem of imbalanced data set, as know the data set and all classes in this data set must have an equal percentage for each class, in other since the number of examples in the training data-set for each class label must be balanced, so that the class distribution is equal or close to equal and not biased or skewed. And this to not face the problem of training the model with an imbalanced data-set that caused the model will be biased towards the majority class only. And it'll cause a problem when we are interested in the prediction of the minority class (in our case the detection of attack is important over the normal case).
  But after too much research, we found that it is too hard to make an oversampling to such a database with too many attributes as the one we work with it, also we found that its possible to simplify the data set to 2 or 3 attributes and make the oversampling but we ll lose too much information that ll be the reason to face a trouble detection [33, 7].

#	Column	Dtype	#	Column	Dtype
0	arp.opcode	float64	1	arp.hw.size	float64
2	icmp.checksum	float64	3	icmp.seq_le	float64
4	icmp.unused	float64	5	http.content_length	float64
6	http.request.method	object	7	http.referer	object
8	http.request.version	object	9	http.response	float64
10	http.tls_port	float64	11	tcp.ack	float64
12	tcp.ack_raw	float64	13	tcp.checksum	float64
14	tcp.connection.fin	float64	15	tcp.connection.rst	float64
16	tcp.connection.syn	float64	17	tcp.connection.synack	float64
18	tcp.flags	float64	19	tcp.flags.ack	float64
20	tcp.len	float64	21	tcp.seq	float64
22	udp.stream	float64	23	udp.time_delta	float64
24	dns.qry.name	float64	25	dns.qry.name.len	object
26	dns.qry.qu	float64	27	dns.qry.type	float64
28	dns.retransmission	float64	29	dns.retransmit_request	float64
30	dns.retransmit_request_in	float64	31	mqtt.conack.flags	object
32	mqtt.conflag.cleansess	float64	33	mqtt.conflags	float64
34	mqtt.hdrflags	float64	35	mqtt.len	float64
36	mqtt.msg_decoded_as	float64	37	mqtt.msgtype	float64
38	mqtt.proto_len	float64	39	mqtt.protoname	object
40	mqtt.topic	object	41	mqtt.topic_len	float64
42	mqtt.ver	float64	43	mbtcp.len	float64
44	mbtcp.trans_id	float64	45	mbtcp.unit_id	float64
46	Attack_label	int64	47	Attack_type	object

TABLEAU 5.5 – The set of features used for intrusion detection based neural network

#	Column	Dtype	#	Column	Dtype
01	frame.time	object	02	ip.src_host	object
03	ip.dst_host	object	04	arp.dst.proto_ipv4	object
05	arp.src.proto_ipv4	object	06	http.file_data	object
07	http.request.full_uri	object	08	icmp.transmit_timestamp	float64
09	http.request.uri.query	object	10	tcp.options	object
11	tcp.payload	object	12	tcp.srcport	object
13	tcp.dstport	float64	14	udp.port	float64
15	mqtt.msg	object			

TABLEAU 5.6 – The set of features deleted from the cyber security dataset

#	Column	Dtype	#	Column	Dtype
0	http.request.method	object	2	http.request.version	object
3	mqtt.protoname	object	4	mqtt.topic	object
5	dns.qry.name.len	object	6	mqtt.conack.flags	object

TABLEAU 5.7 – The set of features that we converted to a numeric columns

- For the Label column which represents the class of each instance, it has been encoded with a popular technique called "One-Hot-Encoding". The coding will convert rows containing categories to their column with a value 1 means true (this instance is of this class) or 0 means false (this instance is not of this class).
- When obtaining quality data, where each instance of the classes has information that well describes its class. The next step before moving on to learning is normalization. The input data must be normalized, this step has an effect on the model building by reducing the learning rate, and model training converges rapidly. She can also have a regularizing effect by reducing the generalization error.
- The training data is divided into 2, data for training and model validation. Then the model will be tested only on the test set of the Edge-IIoTset Data-set "using the library Scikit learn"

5.6 Intrusion detection system for detecting attacks in Networks

By using deep learning classification techniques ; we have implemented two types of models based on deep learning which are : the deep neural network (DNN), and the convolution neural network (CNN), These models were built and evaluated with Edge-IIoTset Data-set for 2 different experiments :

A binary classification (2 classes) on the data set illustrated in table 5.9 We have grouped both the training and Test data classes into 2 categories : the normal traffic class and the Attack class refers to malicious network traffic that contains all type of attacks from both data sets (Training/Test). We used the training data for model training and validation, then the model was evaluated on the test data from the Edge-IIoTset Data-set. The purpose of this experiment is to assess the effectiveness and anomaly detection rate of attacks.

A multi-classification (15-classes) with 14 different attack classes, on the data-set illustrated in table 5.8 . We used the training data from the Edge-IIoTset Data-set for training and model evaluation, this experimentation is to test the system detection efficiency against several types of attacks that have behaviors different and also to assess the ability to identify the type of attack. In this case, the system performance relies on the detection rate and the total classification accuracy.

The concerned Classes	**Number of instances for training**	**percent of instances for training**	**Number of instances for test**	**percent of instances for test**
Backdoor	19221	1.258136	4805	1.258067
DDoS_HTTP	38835	2.541997	9709	2.542056
DDoS_ICMP	54351	3.557617	13588	3.557673
DDoS_TCP	40050	2.621526	10012	2.621388
DDoS_UDP	97253	6.365825	24314	6.366005
Fingerprinting	682	0.044641	171	0.044772
MITM	286	0.018721	72	72 0.018851
Normal	1091198	71.425822	272800	71.425766
Password	39946	2.614719	9987	2.614843
Port_Scanning	15982	1.046123	3995	1.045990
Ransomware	7751	0.507352	1938	0.507416
SQL_injection	40661	2.661520	10165	2.661448
Uploading	29446	1.927427	7361	1.927291
Vulnerability_scanner	40021	2.619628	10005	2.619556
XSS	12053	0.788945	3013	0.788878
Total	1527736	100.000000	381935	100.000000

TABLEAU 5.8 – number of instances in each class after dividing the 15 different classes

The concerned Classes	**Number of instances for training**	**percent of instances for training**	**Number of instances for test**	**percent of instances for test**
Backdoor	1091198	71.425822	272800	71.425766
DDoS_HTTP	436538	28.574178	109135	28.574234
Total	1527736	100.000000	381935	100.000000

TABLEAU 5.9 – number of instances in each class after dividing the 2 different classes

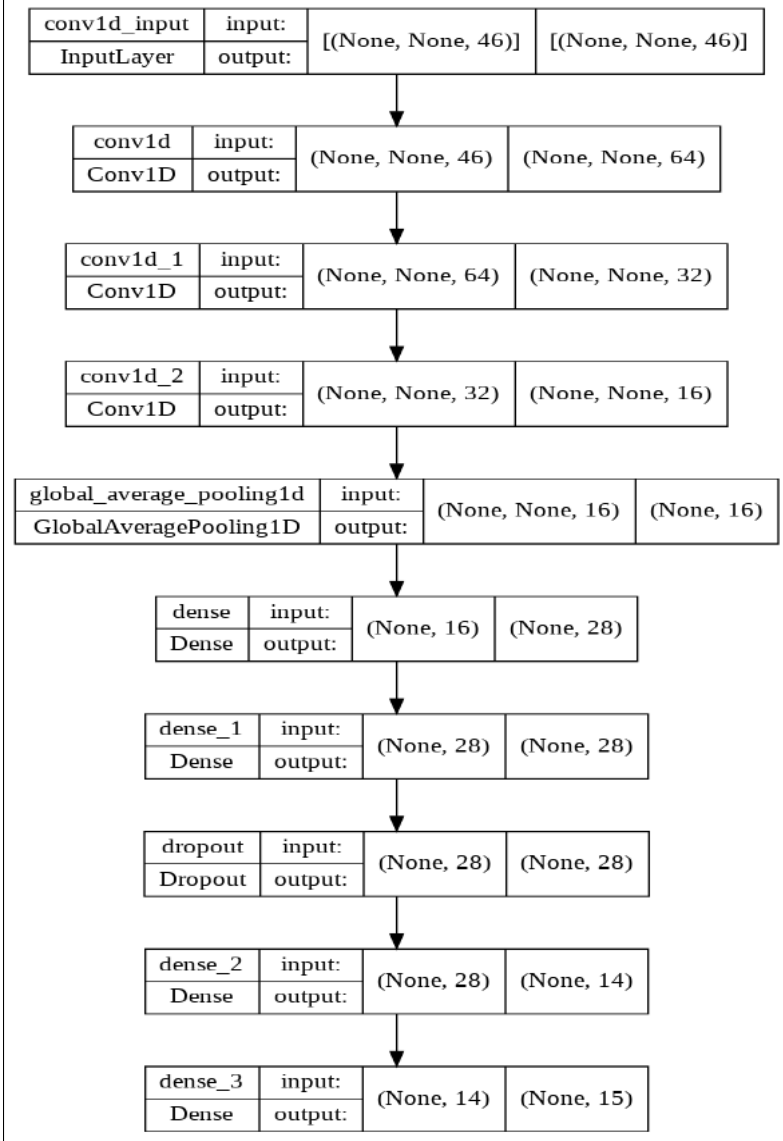
5.6.1 Deep Learning

We have implemented two types of deep network approaches (DNN, and CNN), the architecture of each of these approaches has been modified and improved by trying several combinations of several parameters for each experiment. Nevertheless, these proposed model architectures share some common properties and parameters :

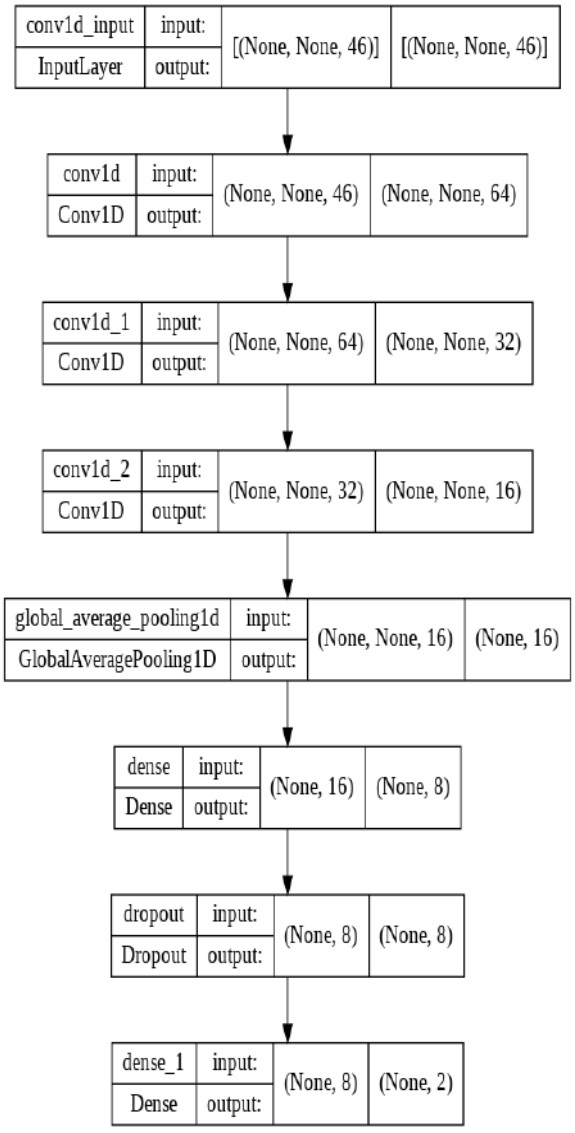
- The input layers have the same dimensions (number of neurons) as the number of features (Features) in the input vector for each model.
- The activation function used was ReLU, various other functions have been experimented with, but ReLU always has the best results.
- The output layers have the same dimensions as the number of classes, for the multi-class classification the “Softmax” activation function has been chosen. It

gives a probability (whose sum is 1) at the output of each neuron, the output neuron with the greatest probability is then allowed to decide that its associated class is the predicted class.

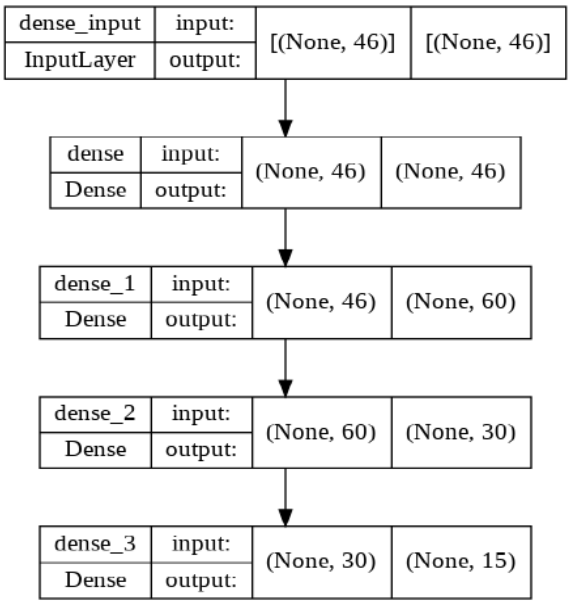
- In the CNN The dropout technique has also been used, when the overfitting problem is encountered. This technique involves randomly considering only a percentage of neurons in a layer to obtain a generalizable model.
- Loss function selected was “categorical-cross-entropy” for multi-class classification and “binary-cross-entropy” for binary (normal/attack) classification. and what concerns the optimizer we chose “Adam” because it is effective in our case



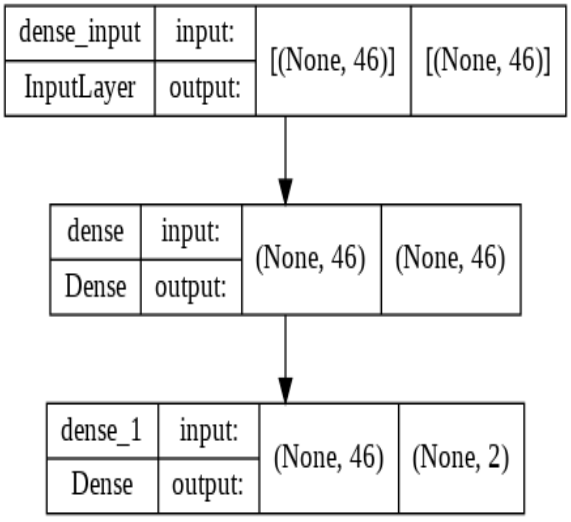
(a) the Cnn model used for 15-Class classification



(b) the Cnn model used for binary classification



(c) the Dnn model used for 15-Class classification



(d) the Dnn model used for binary classification

FIGURE 5.3 – The architecture of the models proposed for the "deep learning" classification

5.6.2 Intrusion detection model based on Deep Neural network (DNN)

The proposed architecture of the DNN model has multi hidden layers, with an input layer and an output layer (Figure5.3). Thanks to these hidden layers which contain a large number of parameters constituting the model,

The DNN network can perform automatic extraction of the corresponding complex characteristics from raw data. This is for the purpose of determining the underlying statistical properties of normal packets and packets of different attacks.

More hidden layers lead to a more complex model, the results can be better,, but they can lead to over-learning. After setting the activation functions, the number of samples per batch, and the optimization function. The model converges faster than the CNN model. This model was trained over 10 epochs.

5.6.3 An intrusion-detection model based on Convolution Neural Network CNN

1D CNNs was originally investigated for natural language processing using 1D convolution layers. In our study, network traffic events are represented as time series data in 1D form. Flow characteristics are captured in equivalent periods, but they have different behaviors from millions of benign connections and malicious DDoS attacks. Therefore, we tried to extract spatial discriminatory features by applying CNN 1d.

Initially, we started with a medium-sized CNN network using different numbers of convolutional layers, and different numbers of different filters with different lengths to find the right parameters and the best structure for the network.

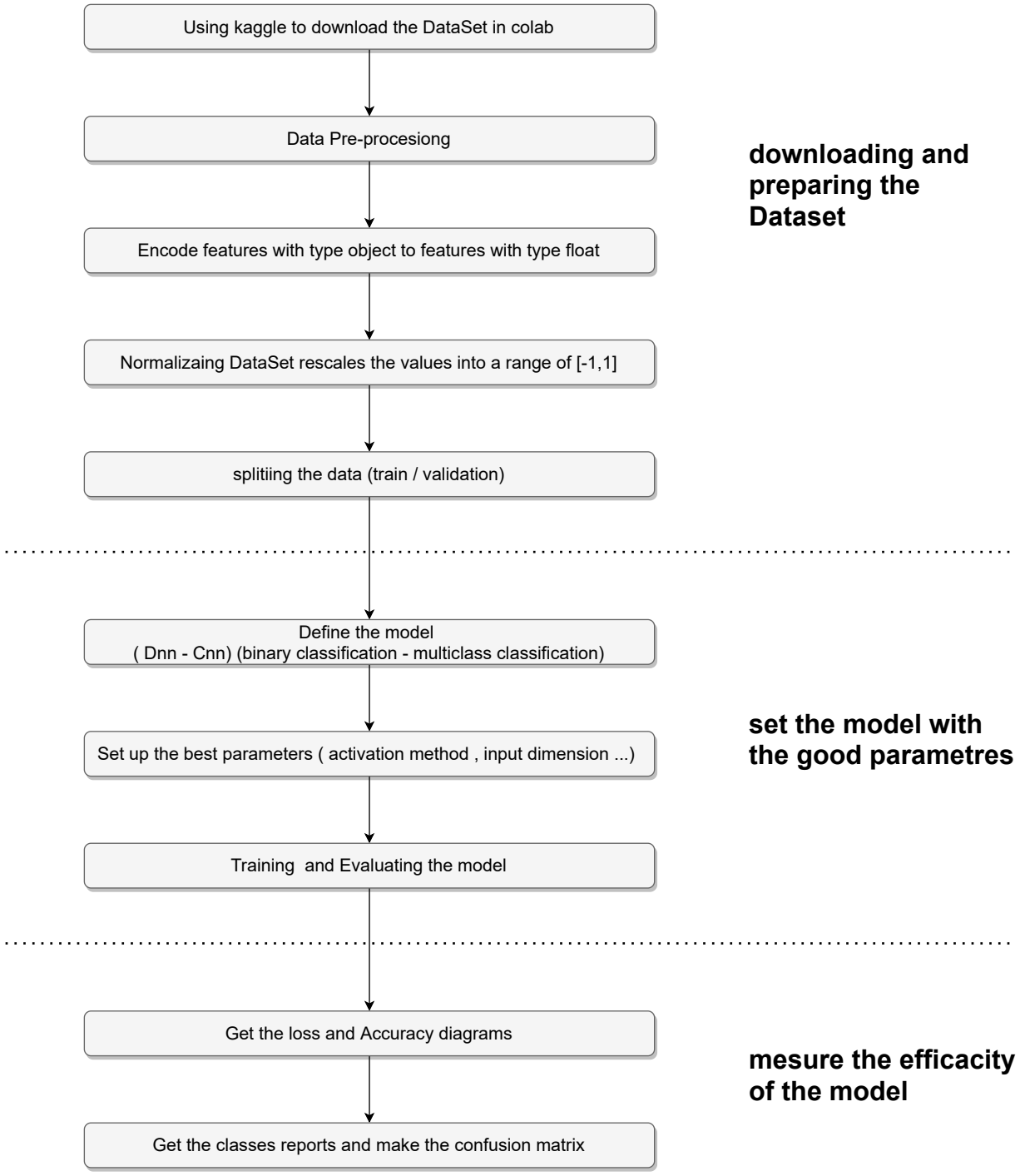


FIGURE 5.4 – Diagram of our method of implementing the proposed DL methods

5.6.4 Model evaluation measures

— Accuracy (ACC) : the percentage of DDoS attacks identified as TP attacks among all the examples predicted as an attack, it is given by :

$$Pr = \frac{TP_{Attack}}{TP_{Attack} + FP_{BENIGN}}$$

— Recall (Rc) : The percentage of DDoS attacks identified as TP attacks out of all attacks in the dataset :

$$Rc = \frac{TP_{Attack}}{TP_{Attack} + FN_{Attack}}$$

— F1-score ($F1$) : the weighted harmonic mean of precision and recall (Recall), it is given by :

$$F1 = \frac{2 * (Acc * Rc)}{(Acc + Rc)}$$

— Confusion Matrix : Is a specific array layout allowing to visualize the performance of an ML algorithm for a classification problem, it is known as the error matrix.

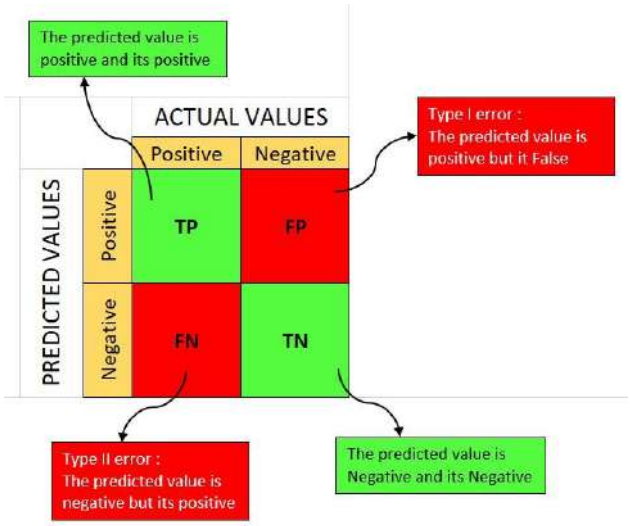


FIGURE 5.5 – Illustration of a matrix of confusion [34]

5.6.5 Result

We have implemented 2 Deep learning models, the DNN, and CNN. These models were trained and tested on DNN-EdgeIIoT-dataset.
Several tests were made to obtain the correct Hyperparameters for each model. These parameters cannot be adjusted during the training phase, yet they have a great impact on the performance of models during training. They include the variables that determine

the structure of the network (Nbr of neurons, Nbr of layers, activation function, . . .), the batch of samples (Batch Size) and the number of iterations . . .etc.

When we arrive at a good model with the minimum error rate and the maximum accuracy, we then test this model on the test subset. The results are presented in the figures above 5.6

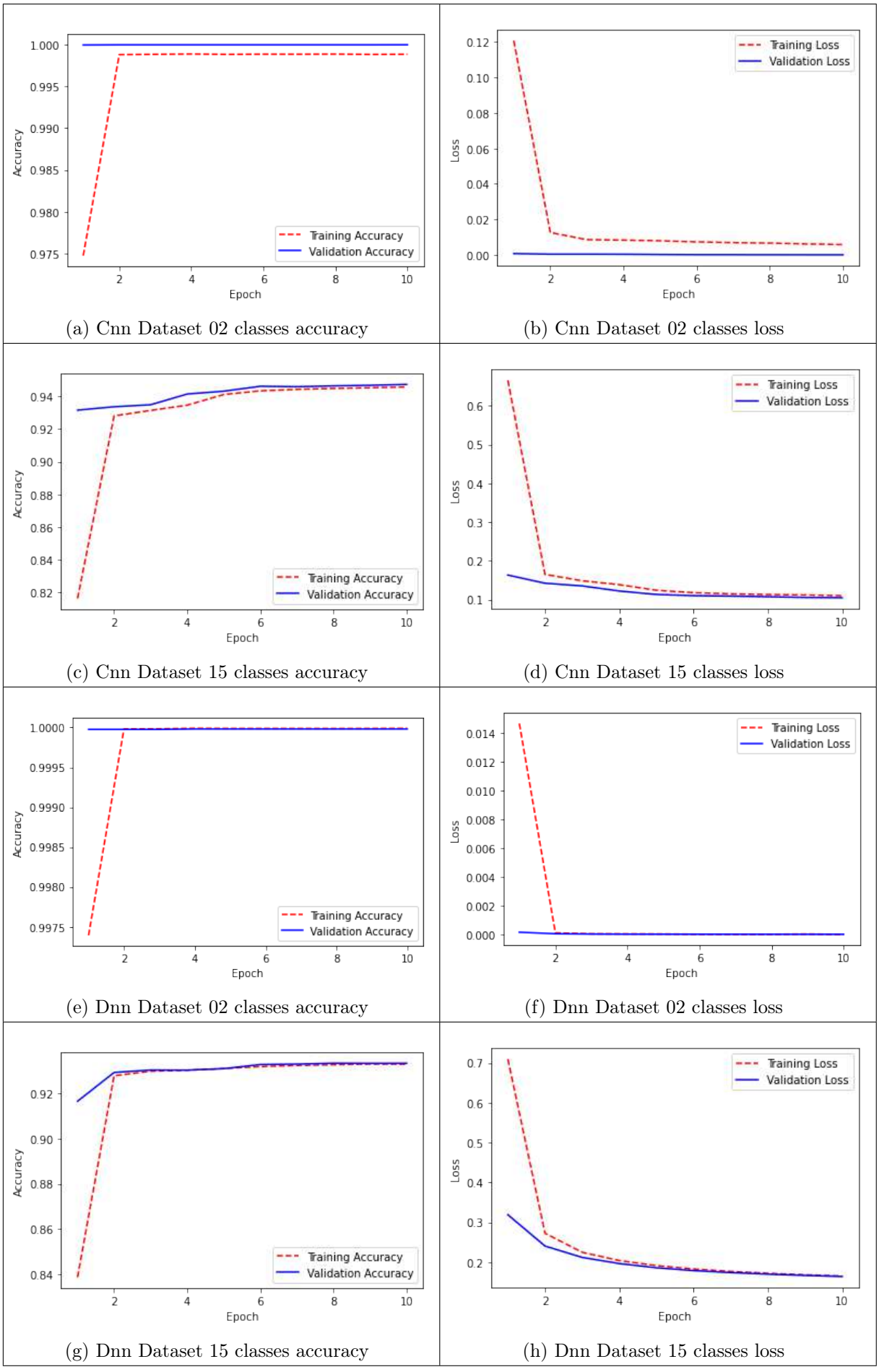
In the first experiment (15-class classification) which was made on the Edge-IIoTset Cyber Security Dataset subset of data indicated in tables 5.8. The training data was divided into 2 : 80% for learning and 20% for evaluation.
Learning does not take much time, models were trained in 10 epochs. They obtained a very good accuracy of 96% for the Cnn, and 93% for the Dnn .5.10
We note here that the 2 models converge to a minimum loss value, or they have almost the same learning and evaluation loss value. This indicates that these models will be generalized well beyond the training set. Then we tested these models on the test set. 5.10

The second experiment (binary classification) was made on the data subset of the same Data-set indicated in tables 5.9. Also in this experiment, the models were trained in 10 epochs. They obtained a very good accuracy of 99% for both DNN and CNN. 5.10

For all the models, we note that the training and validation accuracy constantly increases from the beginning to the end, it reaches a maximum value that tends toward 1. We also note that the value of loss decreases sharply during training and evaluation and reaches a minimum value that tends towards 0. This means that these models learn better and make better predictions after each optimization epoch.

	approach	Accuracy	Recall	F1-measure
binary experiment	DNN	0.99	0.99	0.99
	CNN	0.99	0.99	0.99
multi-class experiment	DNN	0.93	0.93	0.92
	CNN	0.96	0.95	0.94

Tableau 5.10 – The results of the proposed methods



(a) Cnn Dataset 02 classes accuracy

(b) Cnn Dataset 02 classes loss

(c) Cnn Dataset 15 classes accuracy

(d) Cnn Dataset 15 classes loss

(e) Dnn Dataset 02 classes accuracy

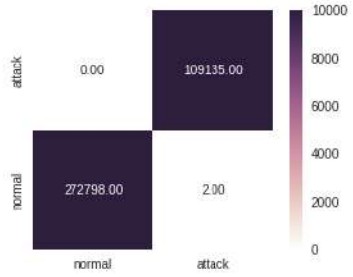
(f) Dnn Dataset 02 classes loss

(g) Dnn Dataset 15 classes accuracy

(h) Dnn Dataset 15 classes loss

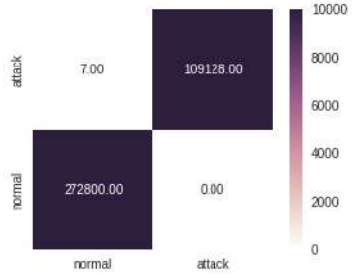
FIGURE 5.6 – Accuracy and loss curves of the proposed models with respect to the training and validation epochs

(a) confusion matrix CNN MUL



(b) confusion matrix CNN Binary

(c) confusion matrix DNN MUL



(d) confusion matrix DNN Binary

FIGURE 5.7 – confusion matrix

5.6.6 Conclusion

We implemented 2 discriminating deep learning models while using the Edge-IIoTset-2022 Data-set for the detection of cyber security attacks. The development had many problems that took us a long time to solve. The mass of data in the data-set, the imbalance and labeling data, and thus the limits of the hardware tools available (processor, memory). To overcome these issues, we reproduced 2 subsets of data using Random sampling for 2 different ratings. the first classification was a comparative study in binary classification. 2nd classification was to evaluate the proposed models in terms of detection type of attacks with the multi-classes model including different types of attacks. Different oversampling techniques with different percentages have been tried to overcome the data imbalance problem but We have not reached the goal we want to reach, then many experiments have been made to find the best architecture with the good hyper-parameters of the models for each type of classification. The results of the proposed DL models were very good, The proposed models have also obtained very satisfactory results with a very high detection accuracy of different types of attacks. And even though these attacks were not previously known during the learning phase. Those models can be considered the core of an IDS based on the detection of network traffic anomalies. And for the final result, we reached 99 % in binary classification and 96 % in multi-classes classification.

Conclusion générale

Cybersecurity is a set of practices that includes protecting vulnerable elements through information and communications technology (ICT). Intrusion detection systems are part of these monitoring practices to cover the deficiencies of various security modules such as antivirus software or firewalls. The software is largely ineffective against the development of new and more sophisticated threats. This research aims to demonstrate the effectiveness of deep learning in cybersecurity. Our goal is to implement a deep learning-based intrusion detection method and evaluate its performance.

We first choose the dataset, and we decided on a Very recent dataset called Edge-IIoTset to detect attacks in IIoT. These cyberattacks are the most common and widespread in the industrial field, some of them can be launched remotely and others not. It is difficult to identify and prevent them. Our goal is to examine the detection of these attacks, especially those that have occurred in recent years.

We then decided to implement two deep learning (supervised learning) discriminative models : Deep Neural Networks (DNN) and Convolutional Neural Networks (CNN) for classification. The choice of these methods is made When we saw the existing works.

The obtained results are satisfactory, considering only the real traffic characteristics of the public network, without any information on connected terminals, leading us to believe that if we apply these methods, the detection rate in a specific network will be higher. All you have to do is store the model weights and set up network sensors and analyzers where the stream can be read in real-time and fed into the model to make predictions. The response time of a single prediction depends on the model complexity (number of model parameters), which needs to be small enough to be used as a real-time alert detection system.

Perspective

In our future work, we will work on oversampling to calibrate the database, and also on the PCAP files of the Data-set using the different network traffic flow generators, then perform an exploratory analysis on the characteristics generated to extract additional information about the patterns of various attacks in the IIOT traffic and use it with

other unsupervised deep learning methods such as Recurrent Neural Network (RNN), Long Short Term Memory Networks (LSTMs) ...

...etc.

Bibliographie

[1] . *L'Internet des objets/The Internet of Things : Quels enjeux pour l'Europe ?/What Challenges for Europe ?* Les Editions de la MSH, 2015.

[2] . Un système de détection d'intrusion pour la cybersécurité. ., 78, 2020.

[3] Doğukan Aksu, Serpil Üstebay, Muhammed Ali Aydin, and Tülin Atmaca. Intrusion detection with comparative analysis of supervised learning techniques and fisher score feature selection algorithm. In *International symposium on computer and information sciences*, pages 141–149. Springer, 2018.

[4] Asmaa Shaker Ashoor and Sharad Gore. Importance of intrusion detection system (ids). *International Journal of Scientific and Engineering Research*, 2(1) :1–4, 2011.

[5] askanydifference. difference between deep learning and neural network. `https://askanydifference.com/difference-between-deep-learning-and-neural-network/`.

[6] blogspot. `https://1.bp.blogspot.com/-BUlBWn_LHG8/WdEP4COKKLI/AAAAAAAABX8/40GNrr5Nilo2mXnatYLnTqTj8Z-bQbYmgCLcBGAs/s1600/Figure-1.-The-next-step-in-internet-evolution.jpg`.

[7] Jason Brownlee. *Imbalanced classification with python : Better metrics, balance skewed classes, cost-sensitive learning.* Machine Learning Mastery, 2020.

[8] cybermalveillance. Dos/ddos. `https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/attaque-en-deni-de-service-ddos`.

[9] Kelton AP da Costa, João P Papa, Celso O Lisboa, Roberto Munoz, and Victor Hugo C de Albuquerque. Internet of things : A survey on machine learning-based intrusion detection approaches. *Computer Networks*, 151 :147–157, 2019.

[10] Hervé Debar, Marc Dacier, and Andreas Wespi. A revised taxonomy for intrusion-detection systems. In *Annales des télécommunications*, volume 55, pages 361–378. Springer, 2000.

[11] educba. machine learning vs neural network. `https://www.educba.com/machine-learning-vs-neural-network/`.

[12] Mohamed Faisal Elrawy, Ali Ismail Awad, and Hesham FA Hamed. Intrusion detection systems for iot-based smart environments : a survey. *Journal of Cloud Computing*, 7(1) :1–20, 2018.

[13] f5. the cia triad. https://www.f5.com/labs/articles/education/what-is-the-cia-triad.

[14] Li Fei, Zhang Jiayan, Song Jiaqi, and Edward Szczerbicki. Deep learning-based intrusion system for vehicular ad hoc networks. *CMC-Computers Materials & Continua*, 65 :653–681, 2020.

[15] Mohamed Amine Ferrag, Othmane Friha, Djallel Hamouda, Leandros Maglaras, and Helge Janicke. Edge-iiotset : A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning. *IEEE Access*, 10 :40281–40306, 2022.

[16] Ni Gao, Ling Gao, Quanli Gao, and Hai Wang. An intrusion detection model based on deep belief networks. In *2014 Second International Conference on Advanced Cloud and Big Data*, pages 247–252. IEEE, 2014.

[17] geeksforgeeks. difference-between-cyber-security-and-information-security. https://www.geeksforgeeks.org/difference-between-cyber-security-and-information-security/.

[18] geeksforgeeks. intrusion detection system ids. https://www.geeksforgeeks.org/intrusion-detection-system-ids/.

[19] geeksforgeeks. what-is-information-security. https://www.geeksforgeeks.org/what-is-information-security/.

[20] Sandeep Gurung, Mirnal Kanti Ghose, and Aroj Subedi. Deep learning approach on network intrusion detection system using nsl-kdd dataset. *International Journal of Computer Network and Information Security (IJCNIS)*, 11(3) :8–14, 2019.

[21] Somayye Hajiheidari, Karzan Wakil, Maryam Badri, and Nima Jafari Navimipour. Intrusion detection systems in the internet of things : A comprehensive investigation. *Computer Networks*, 160 :165–191, 2019.

[22] Vajiheh Hajisalem and Shahram Babaie. A hybrid intrusion detection system based on abc-afs algorithm for misuse and anomaly detection. *Computer Networks*, 136 :37–50, 2018.

[23] Jeff Hale. Deep learning framework. https://towardsdatascience.com/deep-learning-framework-power-scores-2018-23607ddf297a. [En ligne ; Consulté le 16/05/2020].

[24] ibm. deep learning. https://www.ibm.com/cloud/learn/deep-learning.

[25] Zakira Inayat, Abdullah Gani, Nor Badrul Anuar, Muhammad Khurram Khan, and Shahid Anwar. Intrusion response systems : Foundations, design, and challenges. *Journal of Network and Computer Applications*, 62 :53–74, 2016.

[26] iso. iso iec 27001 information security. https://www.iso.org/fr/isoiec-27001-information-security.html.

[27] javatpoint. pandas-vs-numpy. https://www.javatpoint.com/pandas-vs-numpy.

[28] Min-Joo Kang and Je-Won Kang. Intrusion detection system using deep neural network for in-vehicle network security. *PloS one*, 11(6), 2016.

[29] N Dimple Sai Keerthana. Intrusion detection system with machine learning algorithms and comparison analysis. ., 2020.

[30] Gautam Kumar, Om Prakash Singh, and Hemraj Saini. *Cybersecurity : Ambient Technologies, IoT, and Industry 4.0 Implications*. CRC Press, 2021.

[31] Aleksandar Lazarevic, Vipin Kumar, and Jaideep Srivastava. *Intrusion Detection : A Survey*, volume 5, pages 19–78. 01 2005.

[32] linkedin. www.linkedin.com/pulse/industry-40-fourth-industrial-revolution-ingersol-s

[33] linkedin. /what imbalanced dataset its impacts machine learning models cheruku. https://www.linkedin.com/pulse/what-imbalanced-dataset-its-impacts-machine-learning-models-cheruku/. [En ligne ; Consulté le 20/04/2022].

[34] medium. confusion-matrix. https://medium.com/analytics-vidhya/what-is-a-confusion-matrix-d1c0f8feda5.

[35] Robert Mitchell and Ing-Ray Chen. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys (CSUR)*, 46(4) :1–29, 2014.

[36] oracle internet of things. https://www.oracle.com/internet-of-things.

[37] Sasanka Potluri, Shamim Ahmed, and Christian Diedrich. Convolutional neural networks for multi-class intrusion detection system. In *International Conference on Mining Intelligence and Knowledge Exploration*, pages 225–238. Springer, 2018.

[38] Sumit Pundir, Mohammad Wazid, Devesh Pratap Singh, Ashok Kumar Das, Joel JPC Rodrigues, and Youngho Park. Intrusion detection protocols in wireless sensor networks integrated to internet of things deployment : survey and future challenges. *IEEE Access*, 8 :3343–3363, 2019.

[39] python-graph gallery. matplotlib. https://www.python-graph-gallery.com/matplotlib/.

[40] redhat / internet of things. https://www.redhat.com/fr/topics/internet-of-things/what-is-iiot.

[41] research google. What is colaboratory ? https://research.google.com/colaboratory/faq.html.

[42] researchgate. https://www.researchgate.net/figure/The-layered-architectures-of-IoT-three-four-and-five-layers_fig6_327272757.

[43] Leonel Santos, Carlos Rabadao, and Ramiro Gonçalves. Intrusion detection systems in internet of things : A literature review. In *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–7. IEEE, 2018.

[44] Karen Scarfone, Peter Mell, et al. Guide to intrusion detection and prevention systems (idps). *NIST special publication*, 800(2007) :94, 2007.

[45] Pallavi Sethi and Smruti R Sarangi. Internet of things : architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 2017, 2017.

[46] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A Ghorbani. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp*, 1 :108–116, 2018.

[47] simplilearn. perceptron. `https://www.simplilearn.com/tutorials/deep-learning-tutorial/perceptron`.

[48] smartboost. deep learning vs neural network. `https://smartboost.com/blog/deep-learning-vs-neural-network/`.

[49] tibco. `https://www.tibco.com/es/reference-center/what-is-the-internet-of-things-iot`.

[50] upkeep. four industrial revolutions. `https://www.upkeep.com/answers/maintenance-history/four-industrial-revolutions`.

[51] websitesecuritystore. `https://websitesecuritystore.com/wp-content/uploads/2021/08/cia-triad.svg`.

[52] wikipedia Industrial internet of things. `https://fr.wikipedia.org/wiki/Internet_industriel_des_objets`.

[53] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications*, 84 :25–37, 2017.

[54] Baoan Zhang, Yanhua Yu, and Jie Li. Network intrusion detection based on stacked sparse autoencoder and binary tree ensemble method. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE, 2018.