International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 66 No. 1 Apr. 2023, pp. 256-263

http://www.ijisr.issr-journals.org/

Implementation of an electronic system for the detection of non-technical losses in electrical power distribution systems

Nimi Malonda Gauthier[1], Meni Babakidi Narcisse[2], Lidinga Mobonda Flory[3], Cimbela Kabongo Joseph Gregorius[1], and Pasi Bengi Masata André[2]

[1]Université Pédagogique Nationale, Faculty of Sciences, Department of Physics and Applied Sciences, Kinshasa, RD Congo

[2]Institut Supérieur de Techniques Appliquées de Kinshasa, Electronic section, Kinshasa, RD Congo

[3]Institut Supérieur de Techniques Appliquées de Lukula, Boma, Electrical section, Kongo Central, RD Congo

ABSTRACT: In many countries, non-technical losses and theft of electricity are serious problems for electricity companies. The development of cost-effective algorithms to deal with these types of non-technical losses aims to reduce trading losses. This article presents a strategy for detecting non-technical losses using an arduino UNO control board that establishes a reliable region to monitor the measured variance and a practical scheme for determining and reducing non-technical losses in the electrical network by detecting the suspicious area where incorrect meter readings and electricity thefts occur. After the detection of the non-technical losses, a path finding procedure based on different algorithms is able to locate the consumption point with the non-technical loss. In addition, an information system application displays the targeted consumption point. The numerical results demonstrate the selectivity and efficiency of the proposed methodology applied for the monitoring of a real distribution network.

KEYWORDS: electrical energy, non-technical loss, Prepayment mode, algorithms, arduino UNO.

1 INTRODUCTION

Energy losses in an electricity distribution network are of two types: technical losses (TL) and rated non-technical losses (NTL). We speak of non-technical losses for unregistered energy consumption. They come from energy theft or metering and/or profiling errors. Technical losses are due to line losses, but also losses related to high voltage (HV) and low voltage (LV) transformation.

Although it seems easy to estimate the overall level by deducting the overall losses or the difference between the energy injected into the distribution network and the energy actually billed, the origins of these losses are not always obvious and they can be measured precisely. It is estimated that in some developing countries, losses of a non-technical nature can reach 50% of the total quantity of electricity injected into the grid.

Non-technical losses are the main cause of revenue loss in the smart grid. According to a recent study by [1], electric utilities lose $89.3 billion per year due to non-technical losses. Developing countries like India and Brazil respectively lose 42% and 8% of the total electricity produced annually due to energy theft [HX16, Smi04]. The NTL is still as important in developed countries as it is in developing countries. Generally, energy losses in developed countries represent between 0.5% and 3% of annual revenues. Although this amount seems to be minimal, the financial losses in the United States alone reach up to 6 billion [1].

Due to the growth of electricity fraud, several NTL detection techniques have been implemented to mitigate this problem. NTL detection solutions include contributions from various knowledge areas, ranging from hardware-based to data-based solutions. Several data-driven methods have been proposed for the detection of NTLs. These methods include statistical methods [2], [3], expert systems [4], [5], game theory [6], [7] and machine learning methods [8], [9]. These approaches are less complex to implement but expensive than hardware approaches.

Electricity theft is common, encompassing meter fraud, illegal connections to the distribution network and any other tactics aimed at consuming electricity without being billed. This action creates a loss in the revenue collection. It thus generates enormous losses in cash and malfunctions in the distribution of electricity.

This is how we propose in this chapter an electronic system based on Arduino using various algorithms capable of solving this problem of electrical energy theft case of the National Electricity Company in the Democratic Republic of Congo.

2 FOUNDATIONS

NTL represents electricity used but not billed. NTL is primarily associated with electricity theft/fraud, but can also be caused by faulty metering devices and reading and billing errors. NTL occurs when a consumer misreports energy consumption to the utility company. A common practice of NTL is to track the meter and alter the readings to conceal energy consumption and reduce bills. Figure 1 shows the different places where NTLs can occur within a power grid.

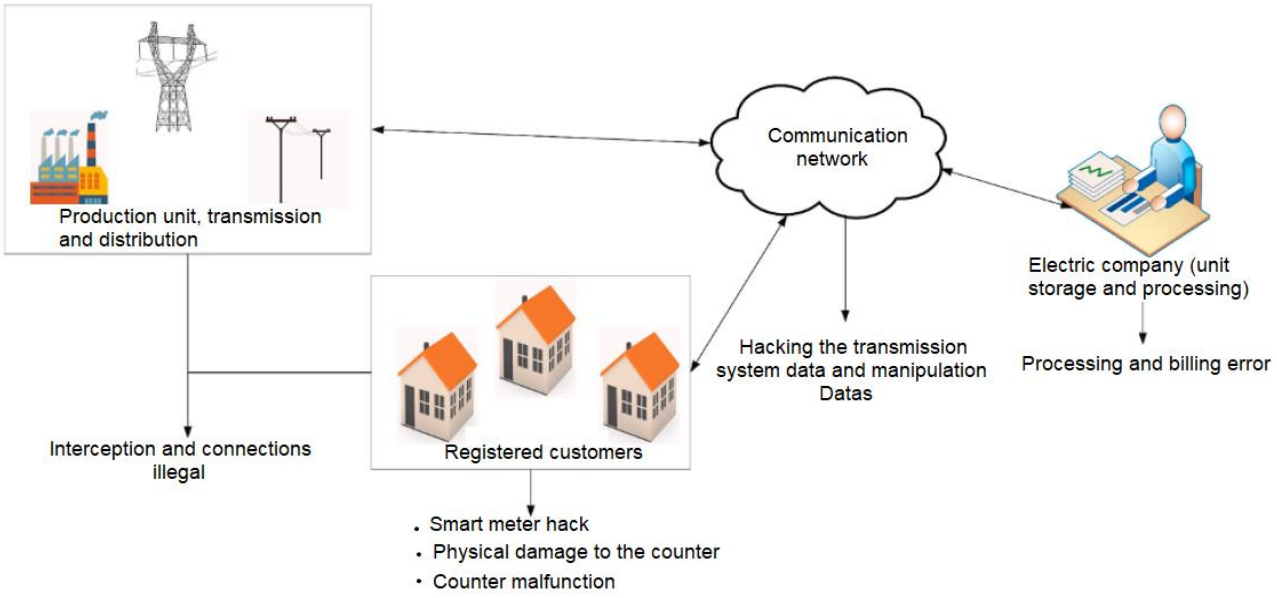

Fig. 1. Likely objectives for NTL in the field of electrical networks

There are two types of NTL attacks in smart grids: cyber-attacks and physical attacks. The attacks manifest themselves in distribution lines, in metering devices and in communication networks [MPM09a]. One of the main reasons for cyber-attacks and physical attacks is to manipulate data in order to reduce energy consumption and therefore energy bills. In this article the focus is on physical attacks.

2.1 PHYSICAL ATTACKS

Physical attacks require some physical manipulation of the meters to change the smart meter measurement. Methods of physical attack are: bypassing the meter by splicing pipes or using cables, illegal plugging, placing a strong magnet, reversing the meter and malfunctioning the meter [10].

It is important to understand the fundamentals of measuring electricity. There are two ways to supply electricity to consumers, namely single-phase and three-phase. A single-phase system is mainly used for residential consumers. For a single-phase electricity meter, the active power at time t is calculated by:

$$p(t) = v(t)\, i(t) \cos\Phi \quad (1)$$

Where:

v (t), i (t) and Φ are respectively the voltage measured at the input terminals, the current flowing between the load input terminals and the phase angle between current and voltage.

The three-phase system is used for industrial and commercial customers. For a three-phase system, the total power is calculated by adding the active power of the three phases. Thus, the active power for a three-phase system is given by the following equation:

$$P(t) = p_1(t) + p_2(t) + p_3(t) \quad (2)$$

Then the energy measured by a smart meter in each measurement interval δt is given by:

$$E_t = (p_1(t) + p_2(t) + p_3(t))\,\delta t \quad (3)$$

For a balanced three-phase meter, each phase has almost equal power so that the total power is:

$$P(t) = 3v(t)\,i(t) \quad (4)$$

2.2 DATA CYBER-ATTACKS

The heavy reliance of data transmission on a smart grid communication network increases its vulnerability to cyber-attacks. Cyber-attacks can occur during the data recording process, when data is transmitted over the power grid or stored on the meter or in the control center. There are many cyber-attacks targeting smart grids with specific objectives. These attacks include but are not limited to eavesdropping, denial of service, cloaking, malware injection, and fake data injection (FDIA) attacks [10].

3 MATERIALS AND METHODS

3.1 MATERIALS

A system is proposed which allows remote detection of cases of fraud in real time. This system uses the following hardware:

- The BC 547 B transistor is a small, versatile and identical transistor, ideal for making all kinds of electronic circuits. It serves as a controlled switch for powering the load through the relay
- The LEG-5 Relay from RELEX INC: is a small inexpensive relay that can support an AC load of around 7A/230V and a DC load of around 10A/24V. In our circuit, it is this which isolates the control part from the power part thanks to its two parts which have no physical contact. Also, it allows the microcontroller to control the system note power part
- The 1N4007 diode: is a diode that can withstand a voltage of 1000V and a peak current of 50A. In the circuit, it is mounted in freewheel to avoid the destruction of the transistor which may occur during an overvoltage due to the relay coil
- Base resistance: The value of 5.6K chosen for this resistance was not taken by chance. It is taken following the various calculations
- The Arduino UNO is a component consisting of an integrated microcontroller in a version called ATmega328. This card will play a very important role. Indeed, it is the card which will execute the instructions of the system allowing precisely to collect the information of the current sensor, and to send the information concerning the consumption of the current to the server via the GSM network
- Server: This is the large-capacity computer that will host a database to save information on subscribers, namely their identities, energy consumption, fraud, etc. and a web application to support all system instructions executed in the server, viz; database queries, display of information, reporting of fraud, etc
- The contactor is an electromagnetic switch which, thanks to power contacts (poles), ensures the operation of motors, resistors or other high-power receivers
- AC current sensor (SCT 013-100A maxi sensor): The main role of the sensor is to collect information relating to current consumption at the subscriber and then send it to the microcontroller so that it can transfer it to the server. SNEL
- GSM SIM 800A4 module: Information between subscribers and the SNEL server will circulate via the GSM network. Indeed, energy consumption and fraud, i.e. the information sent by the subscriber will be transmitted via the GSM network
- Communication module: In order to allow users to directly access their consumption information or activations, Bluetooth communication is then an ideal means

3.2 METHODS

This section describes the procedure to follow with the various diagrams allowing the implementation of the system of detection of the frauds including the electronic part and computer.

3.2.1 BLOCK DIAGRAM OF THE SAMPLING SYSTEM

Figure 2 shows the basic diagram of the sampling system made up of five blocks that are made and which will be placed in the electrical energy distribution system to signal possible fraud.

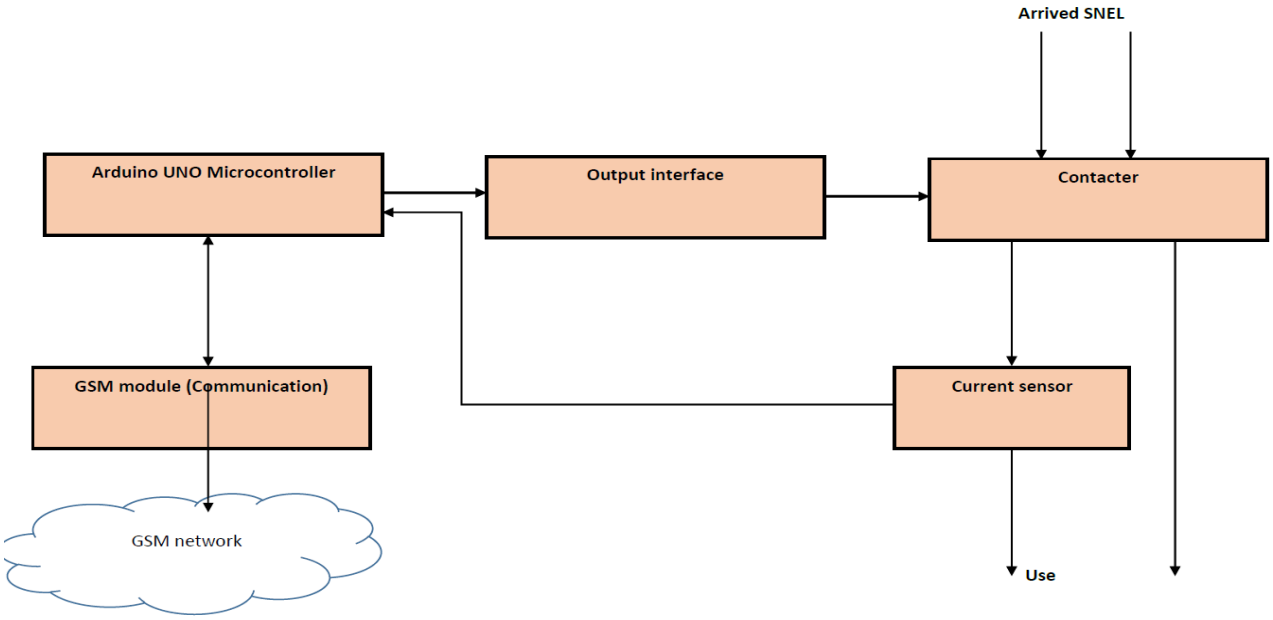

Fig. 2. Block diagram of the sampling system

Figure 3 shows the schematic of the computer system.

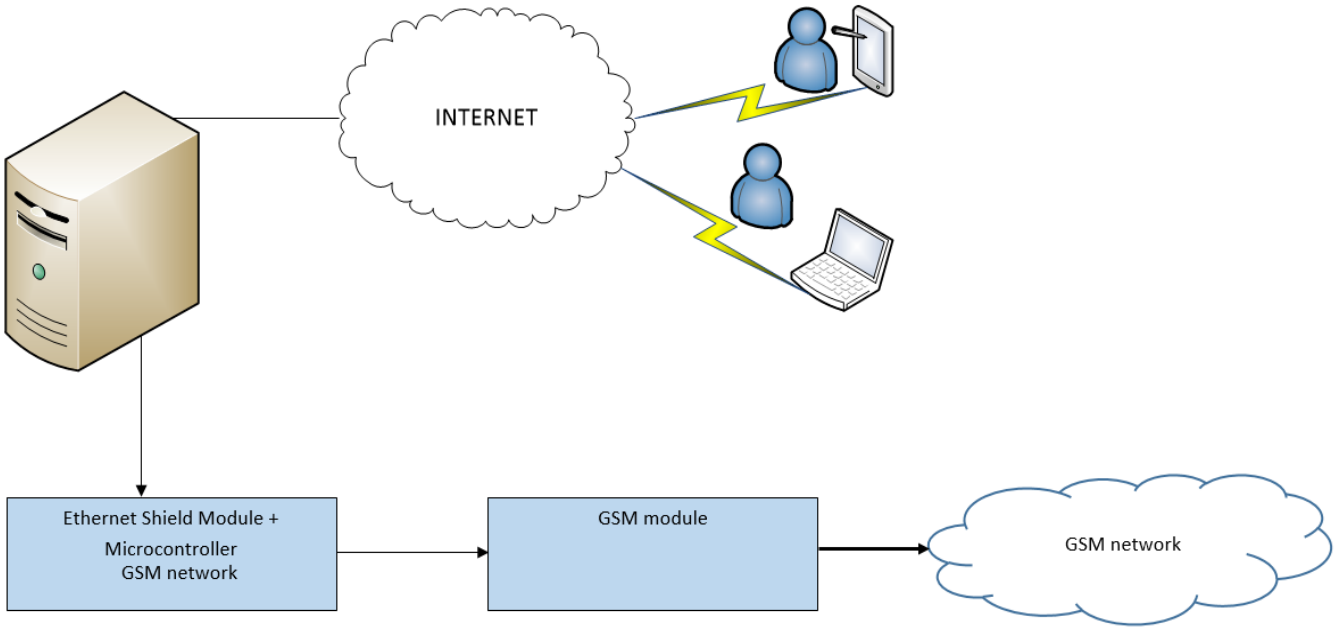

Fig. 3. Computer system diagram

3.2.2 EXPANDED SYSTEM DIAGRAM

The developed diagram of the system is shown in the following figure 4.

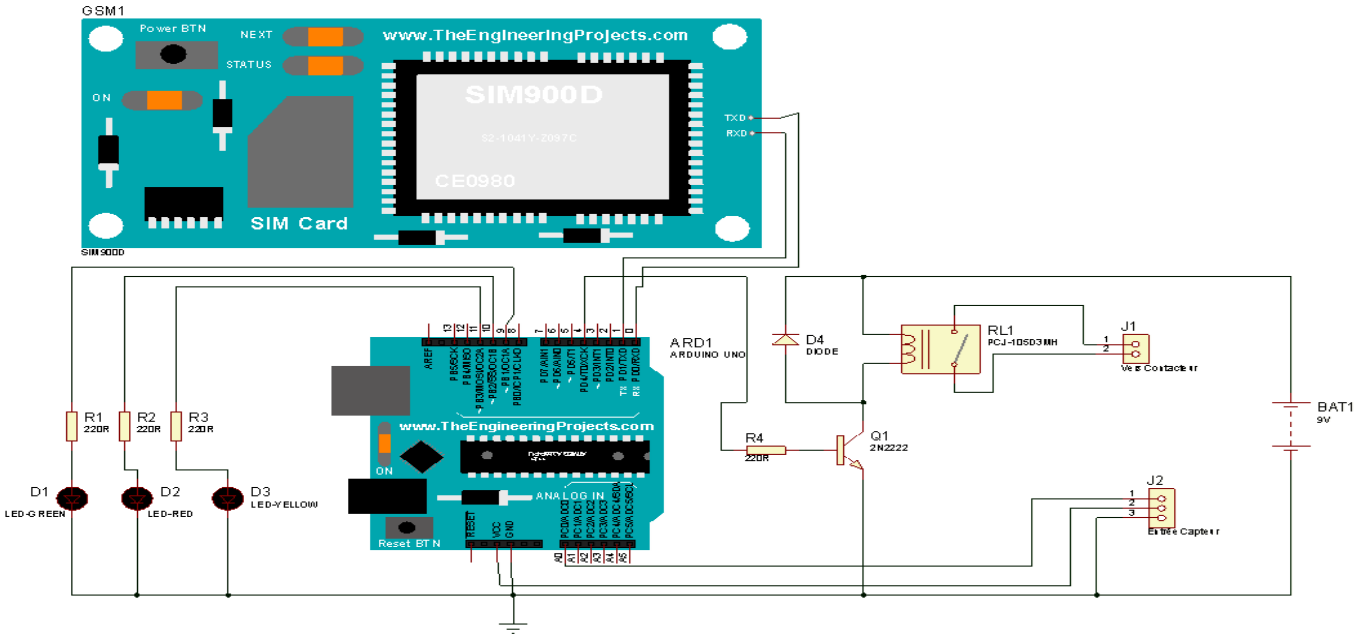

Fig. 4. Expanded diagram of the system

3.2.3 DATA STRUCTURE MODELING

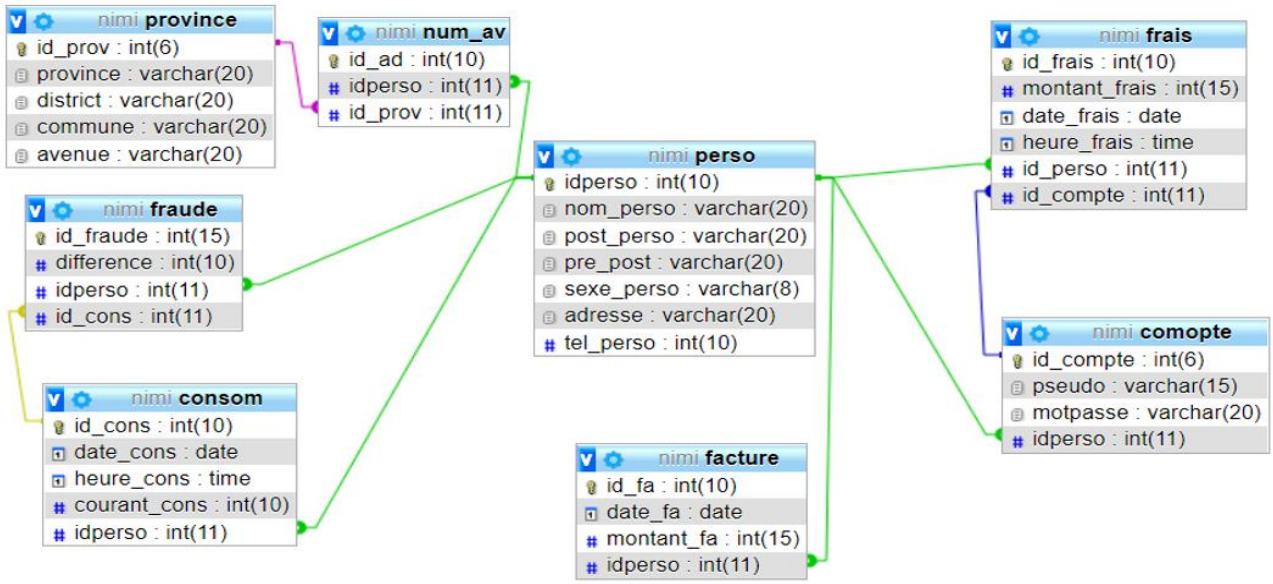

Fig. 5. Data structure modeling

4 RESULTS

It is important to emphasize that the results obtained essentially concern the contribution and the limits of the prepayment meter which seemed to solve the problem of fraud or fraudulent connection of electrical energy in the City of Kinshasa in the Democratic Republic of Congo.

4.1 INTERFACES

4.1.1 CONNECTION

The connection interface will allow customers and SNEL agents to access other sections of the site. It is illustrated in the following figure.

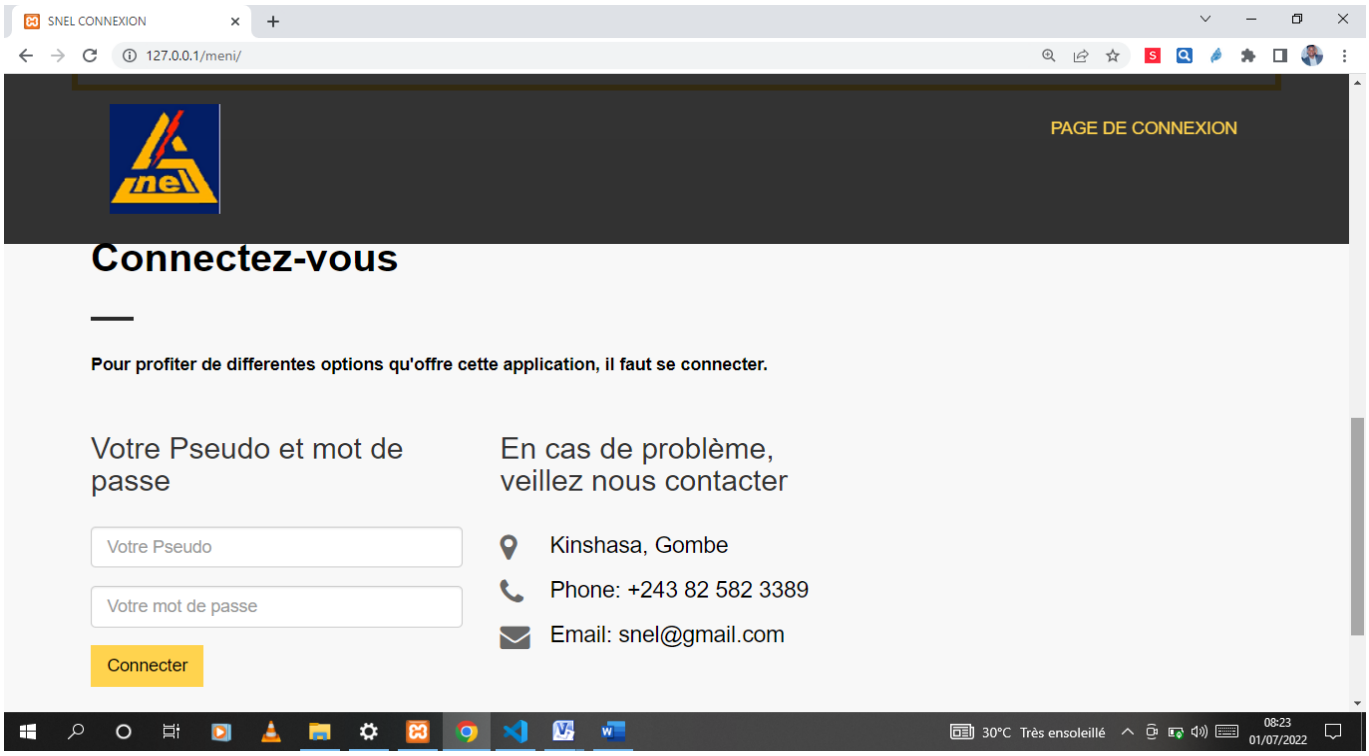

Fig. 6. Connection interface

4.1.2 INTERFACE FOR THE SUBSCRIBER (CLIENT)

The interface for the subscriber is shown in the following figure. It allows the subscriber to:

- Check daily consumption,
- Activate packages (activation),
- View consumption history.

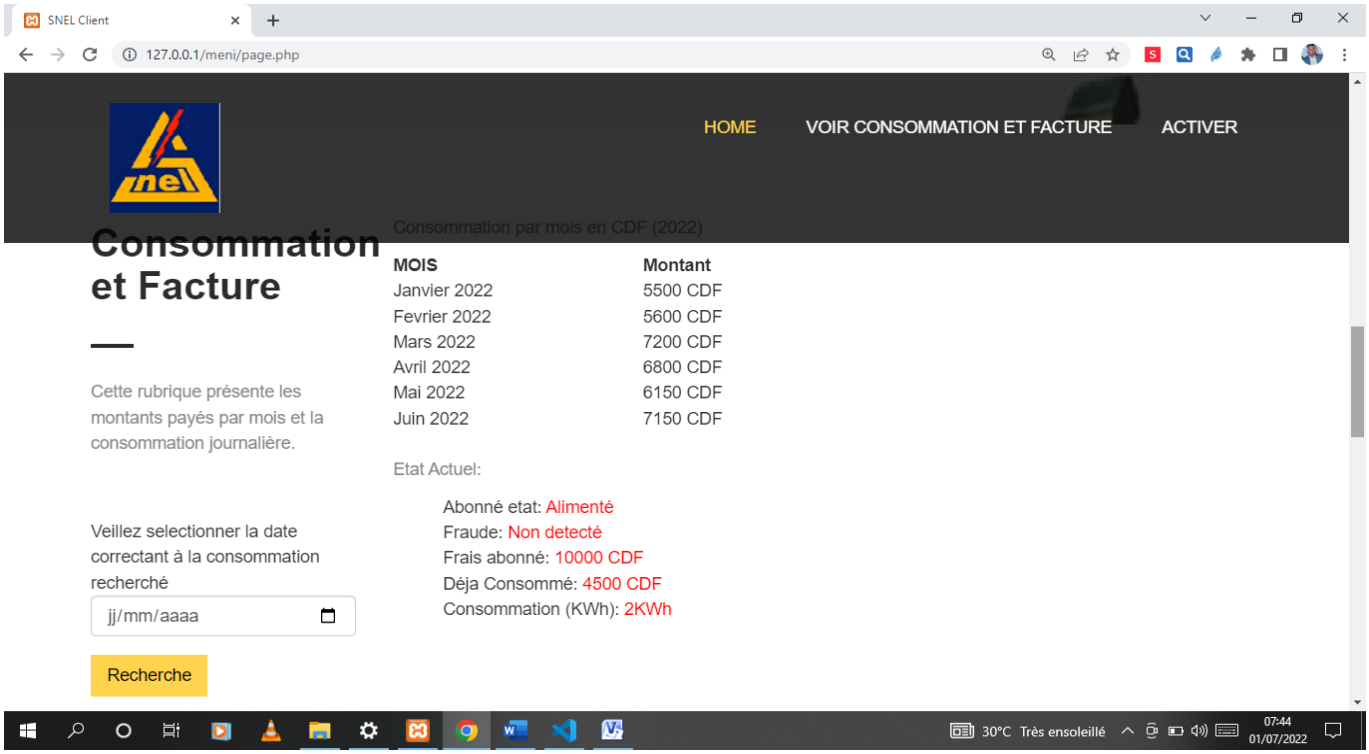

Fig. 7. Interface for the subscriber

4.1.3 INTERFACE FOR ADMINISTRATOR

The interface for the administrator, SNEL agents, is as follows:

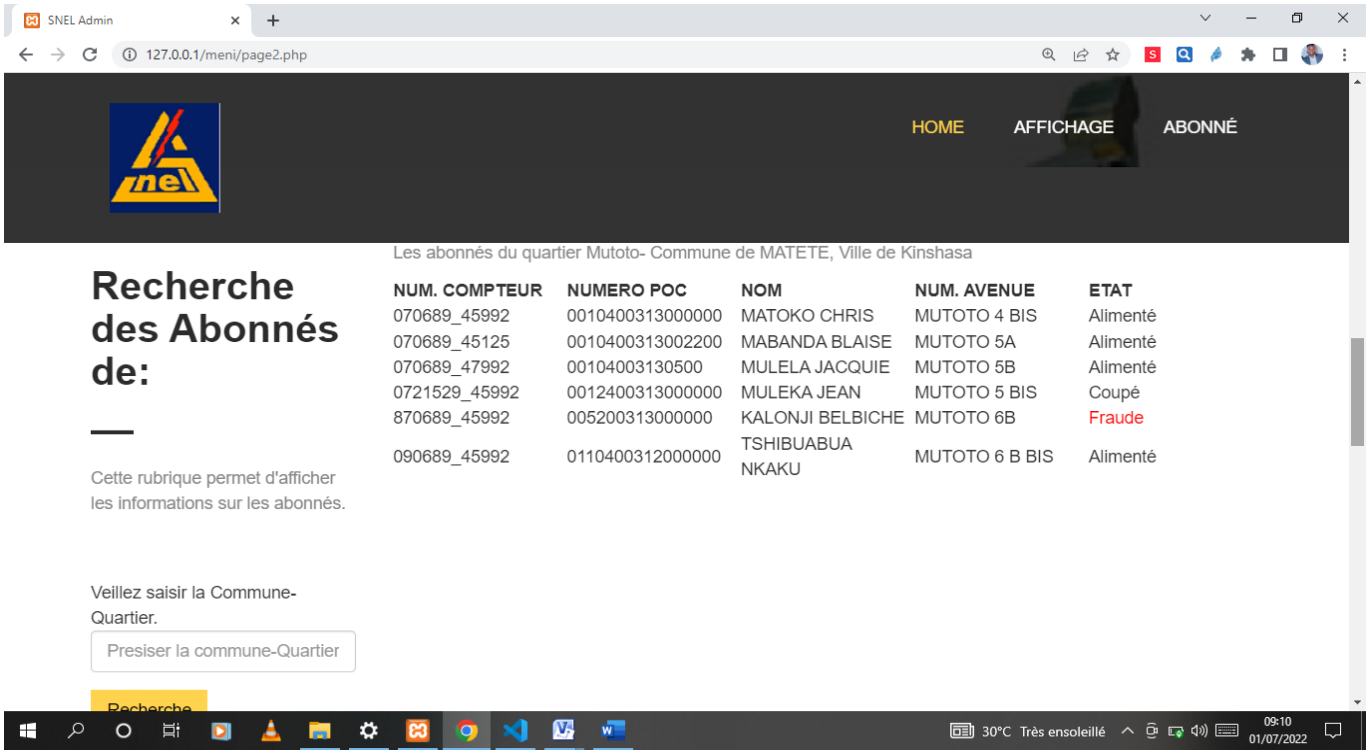

Fig. 8. Interface for administrator

5 ANALYSIS AND DISCUSSION

It happens that in the Democratic Republic of Congo, the use of the prepayment meter does not seem to solve the problem of the instability of the electrical networks caused by fraudulent connection, the burning of the cables and especially by the overload of the MV / LV cabins. In the case of the electromechanical meter, fraudulent connection is possible upstream as well as downstream, because it does not have an anti-fraud device. Even its manual disc adjustment device also allows consumers or subscribers of electrical energy to manipulate it as they wish, without the distributor being able to detect it. On the other hand, the prepayment or smart meter has an anti-fraud system. Simply disconnect a wire from a phase to the input terminal, the anti-fraud device reacts by disconnecting on the customer area and prevents the passage of current. To circumvent this device, the subscriber proceeds by the Bay-passage of the meter by connecting upstream, which is to say at the arrival of the National Electricity Company and goes straight to the distribution board (subscriber area) for the restoration of electrical energy. Therefore, the subscriber can defraud without being seen by the anti-fraud system if and only if there are no SNEL agents or inspectors who go down to the field for verification.

6 CONCLUSION

The use of the prepayment meter, which seemed to solve the difficulties of electrical energy management by consumers and the stabilization of the distribution network, has not sufficiently eliminated the cases of fraudulent connections. Thus our study set out to design a computer system for the remote and real-time detection of any case of electrical energy fraud. The system designed makes it possible to check whether there are credits or not and whether there is fraud or Bay-passage. Whether there are credits or not, a set value will determine the normal or abnormal operation of the prepayment meter. In the event of an abnormality, Bay-passage will be taken into account, because the set point value will be lower than the maximum value provided. This system is able to detect the case of fraud by the subscriber from the central CVS server.

ACKNOWLEDGMENTS

We have the obligation to fulfill a pleasant duty, that of thanking all the people who have contributed from far or near to the writing of this article.

REFERENCES

[1] Han, Wenlin, and Yang Xiao. «Big data security analytic for smart grid with fog nodes.» Security, Privacy, and Anonymity in Computation, Communication, and Storage: 9th International Conference, SpaCCS 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings 9. Springer International Publishing, 2016.

[2] Liu, Yang, and Shiyan Hu. «Cyberthreat analysis and detection for energy theft in social networking of smart homes.» IEEE Transactions on Computational Social Systems 2.4 (2015): 148-158.

[3] Yip, Sook-Chin, et al. «Detection of energy theft and defective smart meters in smart grids using linear regression.» International Journal of Electrical Power & Energy Systems 91 (2017): 230-240.

[4] Guerrero, Juan I., et al. «Improving knowledge-based systems with statistical techniques, text mining, and neural networks for non-technical loss detection.» Knowledge-Based Systems 71 (2014): 376-388.

[5] Glauner, Patrick, et al. «Is big data sufficient for a reliable detection of non-technical losses?» 2017 19th International Conference on Intelligent System Application to Power Systems (ISAP). IEEE, 2017.

[6] Lin, Chia-Hung, et al. «Non-cooperative game model applied to an advanced metering infrastructure for non-technical loss screening in micro-distribution systems.» IEEE Transactions on Smart Grid 5.5 (2014): 2468-2469.

[7] Wei, Longfei, et al. «A distributed intelligent framework for electricity theft detection using benford's law and stackelberg game.» 2017 Resilience Week (RWS). IEEE, 2017.

[8] Guarda, Fernando GK, et al. «Non-Hardware-Based Non-Technical Losses Detection Methods: A Review.» Energies 16.4 (2023): 2054.

[9] Guarda, Fernando GK, et al. «Non-Hardware-Based Non-Technical Losses Detection Methods: A Review.» Energies 16.4 (2022): 2054.

[10] Barros, Rafael MR, Edson G. da Costa, and Jalberth F. Araujo. «Evaluation of classifiers for non-technical loss identification in electric power systems.» International Journal of Electrical Power & Energy Systems 132 (2021): 107173.