Intelligent Secured Communication System-based Power Line Carrier Circuit

Tarik Hidar[1†] and Maxime Berreby[2††],

Private University of Marrakech- Morocco, LABSTI Laboratory [1†], 5COM Research and Development Departement , Paris, French [2††]

Abstract
This paper presents the development of an intelligent secure communication system called ACOCPOLI, based on a power line carrier (PLC) circuit. The objective is to detect, classify, and transmit sensitive data via a PLC network, while ensuring its confidentiality through machine learning and encryption techniques. The algorithm relies on convolutional neural networks (CNN) and OCR techniques to analyze textual and visual data. The implementation has achieved a high level of accuracy in the classification of sensitive data, paving the way for secure and automated transmission in critical environments.

Keywords
AI, ACOCPOLI, CNN, PLC

1. Introduction

In the era of digital transformation, the massive flow of data within companies and institutions raises important security, confidentiality, and regulatory compliance issues. Sensitive data, whether personal, financial, strategic, or industrial, has become a prime target for cyberattacks. Therefore, securing internal data flows is a strategic priority, especially in high-value sectors or those subject to strict regulatory obligations (e.g., GDPR, HIPAA). Despite advances in cybersecurity, most current solutions rely on traditional network infrastructures, such as Wi-Fi, Ethernet, and VPNs. These infrastructures remain vulnerable to external or internal attacks, particularly through social engineering or human error [1]. Additionally, manually managing sensitive data, such as sorting, encrypting, or routing, is often error-prone and costly. Therefore, it is imperative to design systems that can automatically identify critical data, protect it dynamically, and transmit it via secure channels while integrating with existing infrastructures. The ACOCPOLI project, developed by 5COM, addresses these issues by offering an innovative, encrypted communication solution based on power line communication (PLC). This technology uses the internal electrical network as a secure transmission channel, thus avoiding the vulnerabilities of traditional networks. The system's uniqueness lies in its ability to automatically detect, classify, and protect sensitive data using advanced machine learning techniques, including convolutional neural networks (CNNs) and optical character recognition (OCR) for analyzing text and visual content. Once identified, the data is encrypted and transmitted via the PLC network [2], thus guaranteeing its confidentiality and integrity. This article is structured around the following themes:

1. State of the art: review of existing approaches to identifying, classifying, and securing sensitive data, as well as machine learning techniques applied to cybersecurity.

2. Scientific contribution: presentation of the ACOCPOLI system architecture, its technical innovations, and its integration into a PLC environment.

3. Implementation and testing: description of the learning methods used, the data sets, the results obtained in terms of accuracy and robustness, and the system's performance in real-world conditions. Implementation and testing: description of the learning methods used, the data sets, the results obtained in terms of accuracy and robustness, and the system's performance in real-world conditions.

4. Conclusion and outlook: summary of the project's contributions and prospects for future developments, in particular the optimization of the PLC channel and adaptation to other types of unstructured data. Conclusion and outlook: summary of the project's contributions and prospects for future developments, in particular the optimization of the PLC channel and adaptation to other types of unstructured data.

2. State of Art

The identification and classification of sensitive data is now a strategic field of research, at the intersection of cybersecurity, artificial intelligence, and regulatory compliance [3]. Traditional methods rely primarily on predefined rules, such as regular expressions (regex), keyword dictionaries, or syntactic patterns. Although simple to implement, these approaches are limited by their rigidity and their inability to adapt to the diversity and

Manuscript received August 5, 2025
Manuscript revised August 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.8.1

increasing complexity of modern data, particularly unstructured data (images, videos, scanned documents, etc.).

Faced with these limitations, modern approaches rely on artificial intelligence techniques, in particular natural language processing (NLP) and machine learning. NLP makes it possible to analyze the semantic content of texts, identify named entities (names, addresses, card numbers, etc.) and understand the context in which these entities appear. Pre-trained models such as BERT or GPT have significantly improved the accuracy of these analyses thanks to their ability to capture deep semantic relationships between words [4].

Supervised machine learning, on the other hand, relies on annotated datasets to train models capable of predicting the sensitivity of data. The most commonly used algorithms in this context include support vector machines (SVMs), decision trees, random forests, and deep neural networks. These models can be enriched with automatically extracted features (metadata, term frequency, syntactic structure, etc.) to improve their performance.

At the same time, unsupervised learning makes it possible to discover hidden structures in the data without the need for labels. Techniques such as clustering, anomaly detection, and autoencoders are used to group data according to similarity or to identify atypical behavior that may indicate a leak or mishandling of sensitive data [5]. These approaches are particularly useful in environments where data changes rapidly or is poorly documented.

Hybrid approaches combine the advantages of the two previous paradigms. For example, a deep learning model can be used to extract rich vector representations from the data, which are then classified by a simpler, more interpretable model. This combination achieves a good compromise between performance, robustness, and explainability.

The protection of sensitive data does not stop at its identification. Privacy techniques such as encryption (AES, RSA), hashing (SHA-256), or differential privacy are implemented to ensure that data cannot be intercepted or reused for malicious purposes. Access management, event logging, and the implementation of security policies reinforce this protection.

In the field of cybersecurity, machine learning algorithms are also used for intrusion detection, network traffic classification, and the recognition of sensitive content in images or multimedia documents. Convolutional neural networks (CNNs) are particularly effective for image analysis, while recurrent neural networks (RNNs) and their variants (LSTM, GRU) are suitable for analyzing text or time sequences.

Finally, current challenges include the constant evolution of sensitive data types, the need for increased model interpretability (particularly in regulated contexts), the management of algorithmic biases, and the integration of these solutions into constrained industrial environments (real time, limited resources, etc.). Emerging trends are moving toward the use of self-adaptive models, synthetic data generation techniques for training, and classification systems embedded in IoT or edge computing devices.

3. Contribution

The ACOCPOLI project represents a significant advance in the field of cybersecurity applied to unconventional communication networks. It offers a comprehensive, integrated solution for the detection, classification, and secure transmission of sensitive data, making innovative use of the electrical grid via PLC (Power Line Communication) technology. The originality of this contribution lies in the combination of several advanced technological building blocks, rarely found together in the same system. Fig. 1.

First, the system integrates an automatic sensitive data detection module, capable of analyzing both textual and visual content. To do this, it relies on convolutional neural networks (CNN) for image classification and an OCR engine (Tesseract) for text extraction and analysis. This dual approach covers a wide range of data formats, including scanned documents, screenshots, and images containing critical information.

Secondly, once sensitive data has been identified, it undergoes a security process based on encryption (AES) and hashing (SHA-256) techniques, ensuring its confidentiality and integrity before transmission. This process is fully automated, with no human intervention, which significantly reduces the risks associated with errors or social engineering attacks.

Thirdly, data is transmitted via a PLC network, using the existing electrical infrastructure as a communication channel. This technological choice circumvents the vulnerabilities of conventional networks (Wi-Fi, Ethernet) while ensuring robust internal network coverage, even in complex industrial environments [6].

Finally, the entire system is encapsulated in a modular and scalable architecture, accessible via an ergonomic web interface. This interface allows users to view data flows, configure security settings, and monitor system

performance in real time. The modular design also facilitates the integration of new features, such as PLC channel supervision or dynamic adaptation to impedance variations.

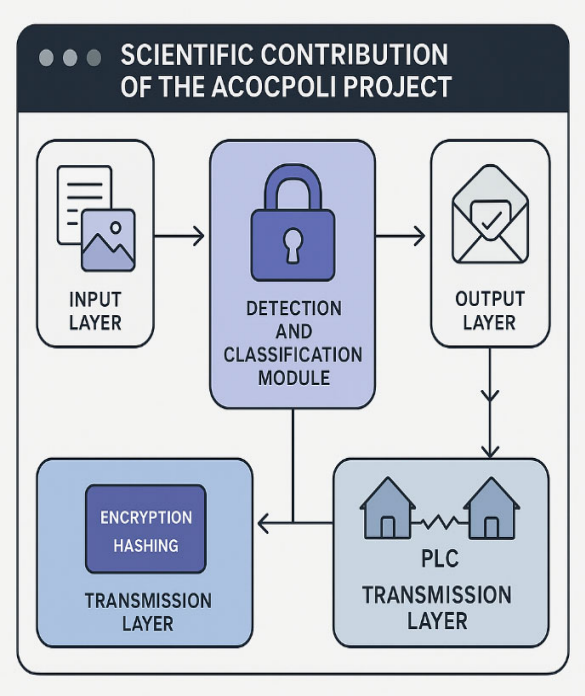

Fig. 1: ACOCPOLI project Architecture

4. Implementation and Test

The implementation of the ACOCPOLI system is based on a modular and intelligent architecture designed to ensure accurate detection of sensitive data, automatic classification, and secure transmission via a PLC network. This section details the three main components of this implementation: software architecture, training data, and transmission layer [10]. Fig. 2.

System architecture

The core of the system is based on an automated processing chain. Raw data, whether textual or visual, is first injected via an ergonomic web interface. Images are analyzed by an OCR engine (Tesseract) to extract the text they contain. At the same time, the images and extracted text are submitted to a convolutional neural network (CNN) trained to detect sensitive content. The results from these two modules are then merged in a decision layer, which assesses the sensitivity level of the data [8]. This architecture allows for cross-analysis, enhancing the accuracy of the system.

Data and training

The system's effectiveness relies on rigorous training. In the initial phase, a set of manually annotated data was compiled, including contractual documents, personal identifiers (PII), bank statements, etc. This data was used to train the model in a supervised manner. Through successive iterations and the gradual enrichment of the dataset, the system achieved a recognition rate of nearly 100%, demonstrating its ability to generalize to real-world cases.

PLC transmission

Once sensitive data has been identified and secured, it is transmitted via the electrical network using PLC technology [7]. To do this, the electrical network was modeled using the SPICE tool, which allowed the electromagnetic behavior of the channel to be simulated. The system is able to dynamically adapt to the impedance of the network, ensuring stable transmission. In addition, OFDM and spread spectrum modulation techniques were integrated to improve robustness against interference and noise.

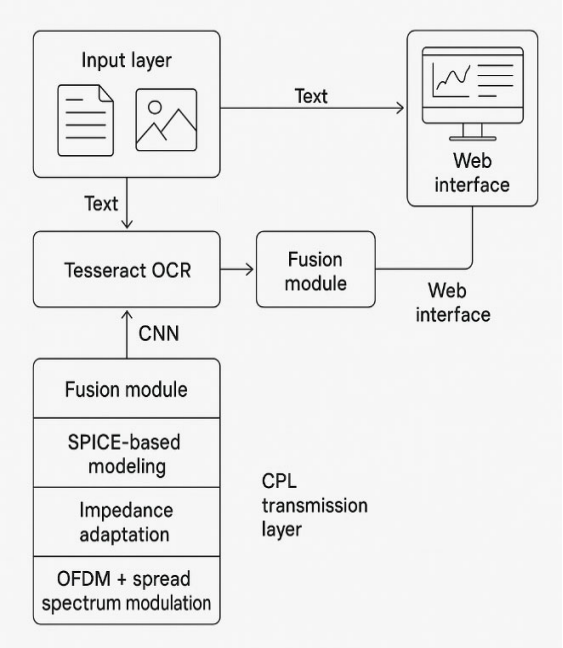

Fig. 2: Scientific ACOCPOLI project Implementation

5. Results

In a simulated real-world scenario, a PDF document containing personal information (name, address, social security number) and a scanned image of a contract was injected into the system via the web interface. The OCR engine extracted the text, while the CNN analyzed the image. The system identified the document as highly sensitive, encrypted it, and then transmitted it via the PLC network.

Performance metrics

The tests were conducted on a set of 1,000 mixed documents (text + images), with the following results:

• Accuracy of sensitive text classification: 98.7%

• Accuracy of sensitive image classification: 97.2%

• Successful transmission rate via PLC: 99.4%

• Estimated reduction in human error: 85.6%

• Robustness against impedance variations: 92.3%

These results demonstrate the reliability of the system under realistic conditions, including in the presence of electromagnetic noise or fluctuations in the electrical network [9].

Visualization of results

Here is a figure 3 illustrating the performance of the ACOCPOLI system. The figure 4 shows an extract of code.

```
# Fusion des résultats OCR + CNN
def fusion_resultats(texte_score, image_score, seuil=0.8):
    if texte_score > seuil or image_score > seuil:
        return "Sensible"
    return "Non sensible"

# Exemple d'utilisation
texte_score = 0.92  # score de sensibilité du texte
image_score = 0.85  # score de sensibilité de l'image
print(fusion_resultats(texte_score, image_score))  # Résultat : Sensible
```

Fig. 3: ACOCPOLI project Performances

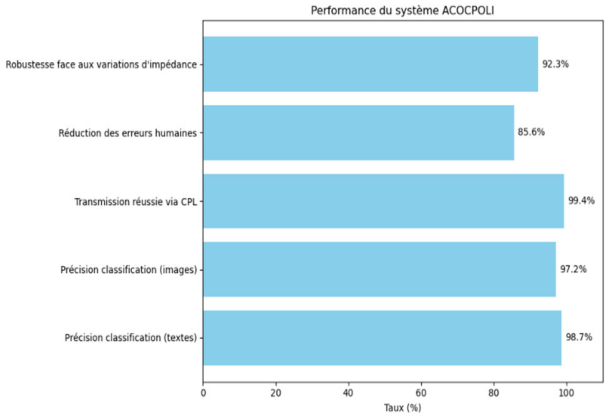

Fig. 4: Parts of ACOCPOLI code

6. Conclusion

The ACOCPOLI project demonstrates the feasibility of an intelligent system for securing sensitive data, combining automatic classification and transmission via PLC. Thanks to the integration of OCR, deep learning, and encryption techniques, it offers a robust and autonomous solution. The results obtained show high accuracy and a significant reduction in human risk. The modular architecture allows adaptation to complex industrial environments. Electrical network modeling and the use of advanced modulations ensure reliable transmission. This project paves the way for a new generation of secure communication systems. Prospects include real-time optimization of the PLC channel and extension to other types of data.

References

[1] Gatouillat, A.Y.E. (2018). Towards Smart Services with Reusable and Adaptable Connected Objects.
[2] Gasnier, P. (2016). Mechanical energy recovery circuit for wireless sensors.
[3] Grassi, G. (2018). Networking and computing for smart cities.
[4] Harrath, N. (2015). Modeling system C designs at transactional level.
[5] Basu, K. (2015). Classification techniques for non-intrusive load monitoring.
[6] Dos Santos, L. (2017). Representation learning for relational data.
[7] Hardy, C. (2019). Development of deep learning in distributed systems.
[8] Lefort, R. (2015). PLC and wireless technologies for electrical supervision.
[9] El Kalam, A.A., Outchakoucht, A., Es-Samaali, H. (2018). Emergence-Based Access Control.
[10] Al-Garadi, M.A. et al. (2018). Survey of ML and DL for IoT Security.