Democratic and Popular Republic of Algeria
Ministry of Higher Education and Scientific Research
University of Mohamed Khider – BISKRA
Faculty of Exact Sciences, Natural and Life Sciences
Computer Science Department

Order No: PFE_/RTIC/M2/2023

Thesis

Presented to obtain the diploma of academic Master in

Computer Science

Option : **Networks and Technologies of Information and Communication**

By:
NOUR RAYAN GRAINAT

Defended the June, 24 th 2024, in front of the jury composed of:

First Name Last Name	Grade	President
Ilyes Naidji	MCB	Supervisor
First Name Last Name	Grade	Examiner

University Year 2023/2024

Acknowledgements

First and foremost, I would like to thank Allah Almighty for giving me the strength, knowledge, ability, and opportunity to undertake this research study and to persevere and complete it satisfactorily. Without His blessings, this achievement would not have been possible.

I am profoundly grateful to Ilyes Naidji, my supervisor, for his invaluable guidance, encouragement, and continuous support throughout this project. his insightful feedback and expertise have been instrumental in shaping this work.

I am also indebted to Dr Chiraz for providing the resources and facilities necessary for this project.

I extend my heartfelt thanks to my colleague and friend, Samah for her valuable suggestions, constructive criticism, and for taking the time to review this work.

Last but not least, I am eternally grateful to my family for their unwavering support, patience, and love throughout this journey. Their faith in me has been a constant source of motivation.

Dedication

This work is dedicated to my beloved family, whose unwavering support and encouragement have been my constant source of strength and inspiration.

To my dear mother and father, your love and sacrifices have shaped who I am today. Your faith in me has been a driving force in all my endeavors.

To my siblings, Aymen, Sedik, and Ritadj, your encouragement and belief in me have been invaluable. Thank you for always being there for me.

To my cherished friends, Samah, Khouloud, Wiaam, and Amira, your friendship and support have made this journey memorable and rewarding. Your companionship has been a source of joy and motivation.

With deepest gratitude and love,

Rayan.

Abstract

The increasing penetration of distributed energy resources and advanced metering infrastructure in smart grids has led to the generation of vast amounts of data, creating both opportunities and challenges in terms of data privacy and computational efficiency. This project explores a Federated Learning (FL) based solution for smart grids, aiming to enhance the predictive accuracy of electricity theft detection while preserving user privacy. Federated Learning, a decentralized machine learning approach, allows multiple grid entities to collaboratively train a shared model without exchanging raw data, thus maintaining data privacy and security.

In this study, we design and implement a federated learning framework tailored for smart grid applications, focusing on electricity detection. The proposed framework leverages edge computing resources within the grid to perform local model training, followed by an aggregation process at a central server to update the global model. The effectiveness of the FL-based solution is evaluated through a series of simulations and experiments using real-world smart grid datasets. Results demonstrate that our approach achieves high predictive performance comparable to traditional centralized methods while significantly enhancing data privacy and reducing communication overhead.

The findings indicate that Federated Learning presents a promising pathway for future smart grid analytics, offering a scalable, secure, and privacy-preserving solution to harness the full potential of smart grid data.

Keywords : Federated Learning, Smart Grid, Data Privacy, Fault Detection, Electricity theft detection, Decentralized Machine Learning.

Résumé

L'augmentation de la pénétration des ressources énergétiques distribuées et des infrastructures de comptage avancées dans les réseaux électriques intelligents a conduit à la génération de vastes quantités de données, créant à la fois des opportunités et des défis en termes de confidentialité des données et d'efficacité computationnelle. Ce projet explore une solution basée sur l'apprentissage fédéré (FL) pour les réseaux intelligents, visant à améliorer la précision prédictive de la détection des vols d'électricité tout en préservant la confidentialité des utilisateurs. L'apprentissage fédéré, une approche de machine learning décentralisée, permet à plusieurs entités du réseau de former ensemble un modèle partagé sans échanger de données brutes, maintenant ainsi la confidentialité et la sécurité des données.

Dans cette étude, nous concevons et mettons en œuvre un cadre d'apprentissage fédéré adapté aux applications de réseaux intelligents, en se concentrant sur la détection des vols d'électricité. Le cadre proposé exploite les ressources de l'informatique en périphérie au sein du réseau pour effectuer la formation de modèles locaux, suivie d'un processus d'agrégation sur un serveur central pour mettre à jour le modèle global. L'efficacité de la solution basée sur l'apprentissage fédéré est évaluée à travers une série de simulations et d'expériences utilisant des ensembles de données réels de réseaux intelligents. Les résultats démontrent que notre approche atteint une performance prédictive élevée comparable aux méthodes centralisées traditionnelles tout en améliorant significativement la confidentialité des données et en réduisant les frais de communication.

Les résultats indiquent que l'apprentissage fédéré présente une voie prometteuse pour l'analytique future des réseaux éléctriques intelligents, offrant une solution évolutive, sécurisée et respectueuse de la vie privée pour exploiter tout le potentiel des données des réseaux intelligents.

Mots-clés : Apprentissage fédéré, Réseau electrique intelligent, Confidentialité des Données, Détection des Pannes, Detection du vol d'energie, Decentralized Machine Learning.

Contents

List of Figures

General Introduction

In this introduction, we start by presenting the background of this thesis Then, we focus on the motivations of this work, specify the problem, and highlight the objectives. Finally, we end with the description of the manuscript organization.

Background

The integration of advanced technologies in power systems has led to the development of smart grids, which offer enhanced efficiency, reliability, and sustainability in energy distribution and consumption. Smart grids leverage a plethora of data from various sources, such as smart meters, sensors, and distributed energy resources, to optimize grid operations and support decision-making processes. However, the vast and diverse nature of this data presents significant challenges in terms of data privacy, security, and computational efficiency.

In this context, federated learning (FL) emerges as a promising paradigm that addresses these challenges by enabling decentralized model training across multiple devices or entities without the need to share raw data. Unlike traditional centralized machine learning approaches that require data aggregation at a central server, federated learning allows each participating node to train models locally using its own data. The locally trained models are then aggregated into a global model, ensuring data privacy and reducing the risks associated with data breaches and unauthorized access.

This dissertation explores the application of federated learning to smart grid systems, aiming to enhance their performance, security, and scalability. By leveraging federated learning, the proposed solution seeks to address key issues such as data privacy, efficient resource utilization, and real-time adaptability. The research focuses on developing and evaluating federated learning algorithms tailored for smart grid applications, including electricity theft detection.

Problematic

Electricity theft detection in smart grids is a significant and complex issue that poses technical, economic, and security challenges. The problematic aspects can be summarized as follows:

1. Economic Losses: Electricity theft leads to substantial financial losses for utility companies, resulting in higher operational costs and ultimately higher prices for consumers.

2. Grid Reliability and Stability: Unauthorized consumption disrupts the balance between supply and demand, leading to potential overloading, outages, and reduced reliability of the electricity grid.

3. Data Imbalance: Theft cases are relatively rare compared to legitimate consumption, creating highly imbalanced datasets that complicate the detection process and affect the performance of machine learning models.

4. Complex Fraud Patterns: Thieves employ sophisticated methods to bypass meters or manipulate consumption data, making it challenging to identify fraudulent activities using traditional detection methods.

5. Privacy Concerns: While detecting theft, it's crucial to protect consumer privacy and ensure that data collection and analysis comply with legal and ethical standards.
   Addressing these challenges requires advanced analytics, machine learning algorithms, and robust data preprocessing techniques to accurately identify and mitigate electricity theft in smart grids.

Motivation and Objectives

The primary objectives of this dissertation are:

1. To develop a federated learning framework suitable for smart grid environments: This includes designing algorithms that can handle the unique characteristics and constraints of smart grid data, such as heterogeneity, intermittent connectivity, and limited computational resources.

2. To ensure data privacy and security: By implementing federated learning, the solution aims to protect sensitive data generated by smart meters and other grid components, thereby complying with regulatory requirements and gaining user trust.

3. To evaluate the performance of the proposed federated learning models: This involves conducting extensive experiments and simulations to compare the federated learning approach with traditional centralized methods in terms of accuracy, efficiency, and scalability.

4. To provide insights and recommendations for practical implementation: Based on the findings, the dissertation offers guidance on deploying federated learning in real-world smart grid scenarios, addressing potential challenges and suggesting best practices.

Through this research, we aim to demonstrate that federated learning is not only feasible but also advantageous for smart grid applications. The outcomes are expected to contribute to the advancement of smart grid technologies, promoting more secure, efficient, and resilient energy systems.

Manuscript organization

The manuscript is structured into four chapters, each focusing on a specific aspect of the research topic. The chapter breakdown is as follows:

Chapter 1: Smart Grid concepts This chapter provides a comprehensive structure for discussing Smart Grid, it serves as an introduction to the research by citing and explaining the main components of smart grid.

Chapter 2:Smart Grid and Artificial Intelligence In this chapter, the focus shifts towards an in-depth exploration of the application of artificial intelligence in Smart Grid and the integration of cutting-edge AI technologies within smart grid.

Chapter 3: Methodology Chapter 3 is dedicated to the design of our federated learning-based model and explain the architecture and the steps of development of our model.

Chapter 4: This chapter delves into implementation of our federated learning-based electricity theft detection system , accompanied by the presentation of results derived from the optimization of grid electricity theft detection.

General Conclusion: The general conclusion summarize key findings and suggesting future research directions in the field.

Chapter 1

Smart Grid concepts

1.1 Introduction

Smart Grid, also known as an intelligent electrical grid, represents an evolution of traditional electrical grids by integrating information and communication technologies (ICT). The main objective of Smart Grids is to improve the efficiency, reliability, sustainability, and security of the electrical system. By leveraging advanced technologies, Smart Grids enable better management of energy resources, integration of renewable energy sources, and enhanced responsiveness to electrical demand. This transformation is crucial for addressing the increasing complexity and challenges of modern energy systems.

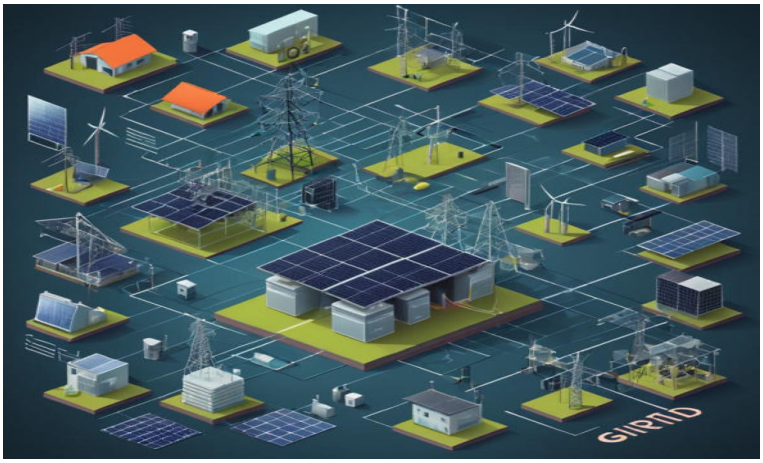

FIGURE 1.1: Smart grid

Smart Grids are designed to accommodate a diverse range of energy sources, including traditional fossil fuels and renewable energy. They also facilitate two-way communication between utilities and consumers, promoting more active participation in energy management. This interactive approach helps balance supply and demand, enhances grid resilience, and supports the transition to a more sustainable energy future.

1.2 Smart Grid Composition

1.2.1 Bus

In Smart Grids, buses are crucial connection points where different elements of the grid converge, such as transmission lines, generators, loads, and storage devices. Buses serve as control and communication hubs, managing the flow of energy throughout the grid. They play a pivotal role in ensuring the stability and efficiency of energy distribution by acting as nodes for data collection, analysis, and real-time decision-making.

Buses also facilitate the integration of distributed energy resources and support the dynamic reconfiguration of the grid to adapt to varying load conditions and generation capacities. Their ability to interconnect various grid components makes them vital for the implementation of advanced grid functionalities, such as demand response, grid resilience, and fault isolation. Buses contribute to the grid's flexibility by enabling seamless energy transfers and supporting the incorporation of renewable energy sources [7].

FIGURE 1.2: Bus.

1.2.2 Transmission lines

Transmission lines are the backbone of the electrical grid, allowing electricity to be transported over long distances, often at high voltages. They are essential for connecting different regions of energy production to consumption areas. Transmission lines are designed to minimize energy losses and ensure the efficient delivery of electricity from centralized generation facilities to substations near consumers [29].

In Smart Grids, advanced monitoring and control systems are deployed along transmission lines to detect faults, optimize power flow, and enhance grid reliability. These systems include sensors, phasor measurement units (PMUs), and communication networks that provide real-time data on the operational status of the lines. The integration of these technologies helps prevent outages, improve response times, and maintain the stability of the transmission network.

FIGURE 1.3: Transmission lines.

1.2.3 Generator

Generators are sources of electrical energy that produce electricity from various sources, such as nuclear power plants, thermal power plants, wind turbines, and solar panels. They convert different forms of energy, such as mechanical, thermal, or solar, into electrical energy. Generators can be centralized, located at large power plants, or distributed, situated closer to the point of consumption [13].
Smart Grids facilitate the integration of diverse and decentralized generation sources,

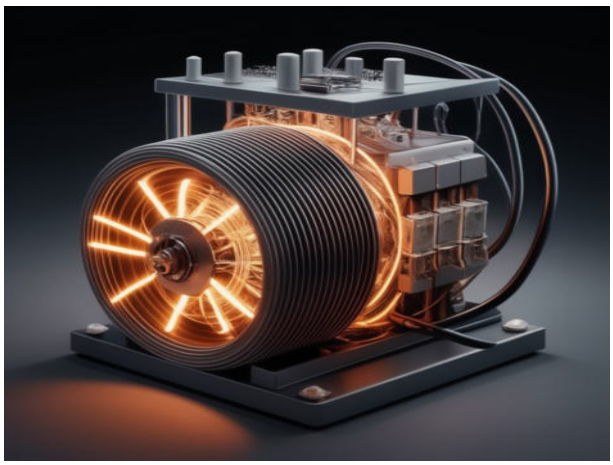

FIGURE 1.4: Generator.

enabling better management of renewable energy inputs and enhancing grid stability. Advanced forecasting and scheduling systems are used to predict generation output and optimize its dispatch to meet demand efficiently. This approach supports the increased use of renewable energy by managing its variability and ensuring a stable supply of electricity.

1.2.4 Load

Loads are the end-users of the electrical grid, including households, businesses, and industries. They consume the electricity supplied by the grid and represent the demand side of the energy equation. In Smart Grids, loads are equipped with smart

meters and other devices that enable real-time monitoring and management of energy consumption [13].

Smart loads can participate in demand response programs, where consumers adjust their energy usage in response to price signals or grid needs. This capability helps balance supply and demand, reduce peak loads, and enhance overall grid efficiency. Additionally, the data collected from smart meters can be used to develop more accurate consumption forecasts and improve the planning and operation of the grid.

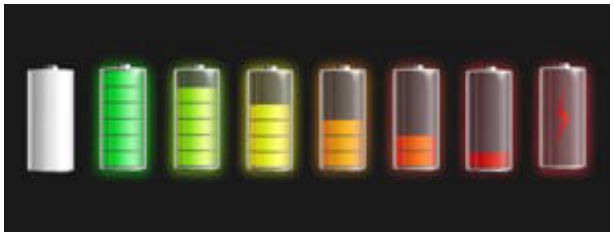

FIGURE 1.5: load.

1.3 Smart Grid Levels

1.3.1 Generation level

This level includes energy production facilities such as power plants, wind farms, and solar power plants. It involves the generation of electricity from various energy sources, both renewable and non-renewable. The generation level is responsible for ensuring a reliable and continuous supply of electricity to meet the demands of consumers.

In Smart Grids, generation facilities are integrated with advanced control systems that optimize their operation, facilitate the integration of renewable energy, and enhance grid stability. These systems include real-time monitoring, predictive maintenance, and automated control mechanisms. By utilizing these technologies, generation facilities can operate more efficiently and respond more effectively to changes in demand and supply conditions.

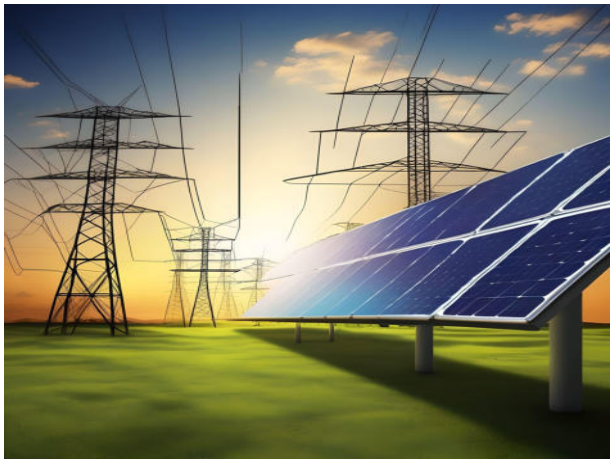

FIGURE 1.6: Generation level.

1.3.2 Transmission level

The transmission level is responsible for transporting electricity over long distances from production facilities to distribution areas. This level includes high-voltage transmission lines, substations, and transformers. The goal is to deliver electricity efficiently and reliably while minimizing losses and maintaining power quality. Advanced technologies in Smart Grids, such as flexible AC transmission systems

FIGURE 1.7: Transmission level.

(FACTS) and high-voltage direct current (HVDC) systems, improve the capacity and efficiency of transmission networks. Real-time monitoring and control enable rapid fault detection and isolation, enhancing grid resilience. These technologies also support the integration of renewable energy by managing the variability and intermittency of renewable generation sources.

1.3.3 Distribution level

The distribution level is responsible for delivering electricity from substations to end-users, such as residential consumers, businesses, and industries. This level includes medium and low-voltage distribution lines, transformers, and distribution substations. The focus is on providing reliable and high-quality power to consumers. Smart Grids at the distribution level incorporate automated meter reading

FIGURE 1.8: Distribution level.

(AMR), advanced distribution management systems (ADMS), and fault detection and isolation systems. These technologies improve operational efficiency, reduce outage durations, and enhance customer service. Additionally, the distribution level is increasingly integrating distributed energy resources, such as rooftop solar panels and battery storage, to enhance grid flexibility and resilience.

1.3.4 Consumption level

This level represents the end-users who consume the electricity supplied by the grid. It includes households, businesses, industries, and other entities that use electricity for various purposes. The consumption level is crucial for understanding and managing demand patterns.
In Smart Grids, consumers are equipped with smart meters and home energy man-

FIGURE 1.9: Consumption level: Smart home.

agement systems (HEMS) that provide real-time data on energy usage. These tools enable consumers to make informed decisions about their energy consumption, participate in demand response programs, and contribute to grid stability. The consumption level also plays a key role in supporting energy efficiency initiatives and reducing overall energy consumption.

1.4 Smart Grid Global Architecture

The global architecture of a Smart Grid includes various components such as communication networks, energy management systems, smart metering devices, energy storage systems, and control and monitoring systems. These components interact seamlessly to ensure the efficient operation of the grid. Communication networks facilitate real-time data exchange, enabling advanced functionalities such as automated demand response, predictive maintenance, and enhanced grid resilience [19].

Energy management systems (EMS) optimize the generation, distribution, and consumption of electricity. Smart metering devices provide accurate and timely information on energy usage, helping consumers and utilities make better decisions. Energy storage systems store excess energy and release it when needed, balancing supply and demand. Control and monitoring systems ensure the safe and reliable operation of the grid by continuously monitoring its status and responding to any

anomalies.

The integration of these components creates a more resilient and adaptable grid capable of meeting the demands of modern energy systems. The global architecture also supports the development of microgrids and virtual power plants, which can operate independently or in coordination with the main grid, enhancing overall grid reliability and flexibility.

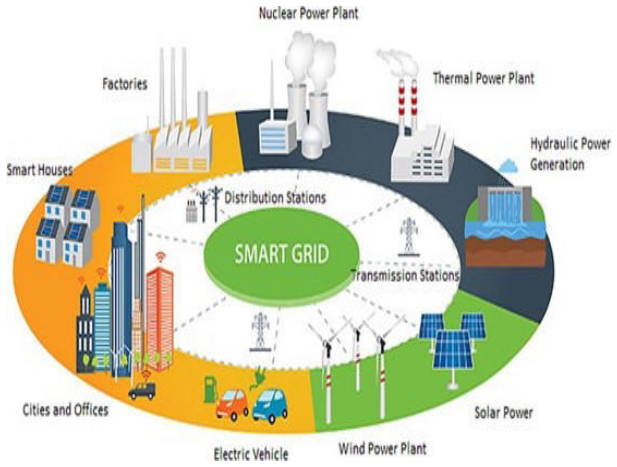

FIGURE 1.10: Smart Grid Global Architecture.

1.5 Control and monitoring

Control and monitoring are essential aspects of Smart Grids. They allow real-time monitoring of the grid's status, management of energy flows, optimization of production and consumption, fault detection, and corrective actions. Advanced control systems use data analytics, machine learning, and artificial intelligence to predict and respond to grid conditions dynamically. Monitoring systems provide valuable insights into the performance and health of grid components, enabling proactive maintenance and reducing the risk of outages [16].

Control and monitoring systems also facilitate the integration of renewable energy

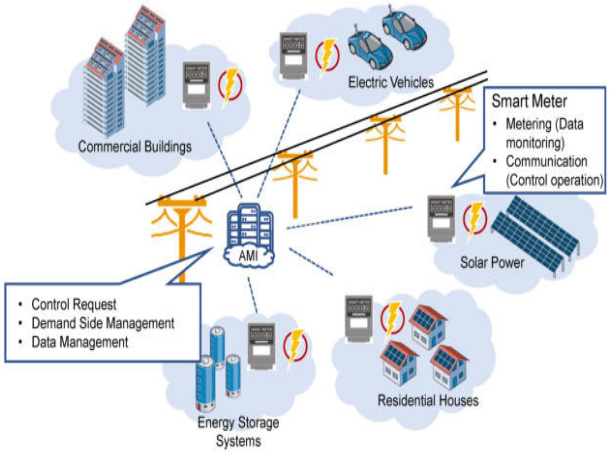

FIGURE 1.11: Control and monitoring.

sources by managing their variability and ensuring a stable supply of electricity.

These systems enable utilities to implement demand response programs, optimize energy storage utilization, and enhance overall grid efficiency. By leveraging advanced technologies, control and monitoring systems contribute to the development of a more resilient, flexible, and sustainable energy grid.

1.6 Problem Statement: Electricity Theft

Electricity theft poses a significant challenge to electrical grids worldwide. It includes various illegal activities such as meter tampering, illegal connections, and meter manipulation. These actions result in substantial financial losses for utilities and can compromise the safety and reliability of the grid. Smart Grids employ advanced detection systems to identify and mitigate electricity theft, ensuring fair billing and grid integrity.

1.6.1 Electricity Theft Types

Electricity theft can take many forms, including bypassing meters, hacking smart meters, and manipulating billing data. Each type of theft poses unique challenges and requires tailored detection and prevention strategies. Smart Grids utilize advanced data analytics, machine learning algorithms, and real-time monitoring to detect anomalies and identify potential cases of theft.

Meter Tampering

Meter tampering refers to altering the metering equipment to inaccurately report lower electricity usage or completely bypass meter readings. This can be done by physically tampering with the meter or employing illegal devices to circumvent the metering system.

Unauthorized Connections

Unauthorized connections entail the illegal tapping of electricity directly from distribution lines or transformers, bypassing the metering system. Offenders may splice into overhead lines or underground cables to secretly obtain electricity.

Meter Hacking

With the rise of digital smart meters, hackers may try to breach metering systems to alter data or remotely tamper with meter readings. This approach typically involves exploiting weaknesses in metering software or communication protocols.

Fraudulent Meter Readings

In certain instances, consumers may commit fraud by submitting false meter readings or inaccurate information to utility companies. This deceptive practice can result in incorrect billing and revenue losses for the utility providers.

Meter Blockage

Meter blockage involves hindering the metering mechanism to stop accurate measurement of electricity consumption. Offenders might physically block the meter with non-conductive materials or use electronic devices to interfere with the metering function.

Load Manipulation

Load manipulation entails artificially decreasing or increasing electricity usage to deceive metering systems. Offenders may use methods like load shedding or load diversion to change consumption patterns and avoid detection.

1.6.2 Related Work on Electricity Theft

Combatting electricity theft has been the subject of extensive research and initiatives. Techniques such as data analysis, machine learning, and advanced detection systems are used to detect and prevent electricity theft. These systems analyze consumption patterns, identify anomalies, and trigger alerts for further investigation. By leveraging smart meters and advanced analytics, utilities can reduce losses and enhance the overall efficiency of the grid.

Research in this area has focused on developing robust detection algorithms, improving the accuracy of theft detection systems, and designing effective countermeasures. Collaborative efforts between utilities, researchers, and technology providers have led to the development of innovative solutions that address the complex and evolving nature of electricity theft.

The authors of [25] present a deep learning method called ETD-ConvLSTM for detecting electricity theft in smart grids. This approach leverages Convolutional Long Short-Term Memory (ConvLSTM) neural networks to identify temporal correlations in electricity consumption patterns. By integrating both global and local information, the method significantly enhances detection accuracy. Simulation results indicate that ETD-ConvLSTM performs better or on par with existing detectors regarding detection accuracy, false negative rates, and false positive rates. This study introduces a novel deep learning-based approach for electricity theft detection using ConvLSTM neural networks, detailing the method's benefits over current techniques. However, it does not provide specific information on the network architecture, dataset, or comparisons with existing methods.

The study in [6] introduces a two-step strategy for electricity theft detection, integrating a Convolutional Autoencoder (CAE) for identifying theft and an enhanced regression algorithm for predicting potentially stolen electricity (PSE). This approach aims to maximize economic return by accurately detecting theft and estimating PSE. Case studies using both simulated and real-world datasets highlight the strategy's effectiveness. The authors offer a comprehensive description of their two-step approach, emphasizing its advantages. However, the study could be improved with more detailed information on the integration of the CAE and the regression algorithm, the evaluation metrics used, and comparisons with existing methods.

The paper in [10] introduces an electricity theft detection method utilizing iterative interpolation and a fusion convolutional neural network (CNN). This approach addresses the shortcomings in preprocessing electricity consumption data and demonstrates superior performance compared to existing methods. The authors highlight their novel method's ability to overcome these preprocessing limitations

and achieve enhanced results. However, the paper does not provide specific details about the fusion CNN architecture or the evaluation metrics used for performance comparison.

The authors in [26] propose a blockchain-based, privacy-preserving electricity theft detection scheme that eliminates the need for a third party. The scheme combines improved functional encryption, distributed storage via blockchain, and a Long Short-Term Memory (LSTM) network to enhance the accuracy of theft detection while safeguarding consumer privacy. This study presents a novel approach to addressing privacy issues in electricity theft detection using blockchain technology and demonstrates its effectiveness through real-world evaluation. However, more details on the specific blockchain implementation and the evaluation metrics used would be beneficial.

The study in [27] presents a hybrid data-driven methodology for detecting electricity theft by combining two innovative data mining techniques: Maximum Information Coefficient (MIC) and Clustering Technique by Fast Search and Find of Density Peaks (CFSFDP). This method is designed to identify various forms of electricity theft by analyzing correlations between non-technical losses and electricity consumption patterns, along with clustering techniques to detect anomalous users based on their load profiles. Numerical experiments conducted on the Irish smart meter dataset validate the effectiveness of this combined approach. The authors offer a novel solution for electricity theft detection through the integration of these data mining techniques, clearly outlining the proposed method and its benefits. However, the study would be enhanced by providing more details on the experimental setup, the evaluation metrics used, and a comparison with existing methods.

The study in [8] presents a data-driven model for detecting electricity theft using smart meter data. This model emphasizes the physical relationship between electricity consumption and voltage magnitude, avoiding reliance on unreliable parameter and topology information. By employing a modified linear regression model, the approach accurately detects electricity theft on distribution secondaries. Validation with real-world smart meter data demonstrates the model's effectiveness in identifying theft cases. The authors introduce a distinctive method for electricity theft detection, capitalizing on the correlation between electricity usage and voltage magnitude. The utilization of smart meter data and a modified linear regression model offers a practical and efficient solution for identifying theft. However, the study would benefit from more detailed insights into the model's performance metrics, comparisons with existing methods, and an analysis of potential scalability issues.

1.7 Conclusion

This chapter has provided an introduction to Smart Grid concepts, focusing on their composition, levels, global architecture, control and monitoring, and the issue of electricity theft. Smart Grids offer significant opportunities to improve the efficiency and sustainability of electrical grids while addressing challenges related to security and reliability. As the energy landscape evolves, Smart Grids will play a crucial role in enabling a more resilient, flexible, and sustainable power system.
By integrating advanced technologies and promoting active participation from all stakeholders, Smart Grids can transform the way electricity is generated, distributed, and consumed. This transformation is essential for meeting the growing energy demands, supporting the integration of renewable energy, and ensuring the long-term sustainability of the electrical grid.

Chapter 2

Smart Grid and Artificial Intelligence

2.1 Introduction

Artificial intelligence (AI) is a field of research and development aimed at creating systems and machines capable of performing tasks generally associated with human intelligence, such as perception, learning, problem-solving, and decision-making. At the core of AI are several key sub-disciplines, including machine learning, deep learning, and artificial neural networks, which play a crucial role in smart grid applications.

Artificial intelligence (AI) has increasingly integrated into various domains, revolutionizing industries and enhancing everyday life [4], [22],[9]. In healthcare, AI algorithms analyze vast amounts of data to diagnose diseases, personalize treatments, and predict patient outcomes. The financial sector employs AI for fraud detection, algorithmic trading, and customer service through chatbots. Manufacturing benefits from AI through predictive maintenance, optimizing production processes, and ensuring quality control. In the realm of transportation, AI powers autonomous vehicles, improves traffic management, and enhances logistics. Education systems use AI to provide personalized learning experiences and streamline administrative tasks. Furthermore, AI's role in entertainment and media includes content recommendation systems and the creation of immersive virtual experiences [23]. Across these sectors, AI continues to drive innovation, efficiency, and new possibilities.

This section explores these various aspects of artificial intelligence in detail, examining their underlying principles, techniques, and applications in the context of smart grid systems. It highlights how AI, leveraging these technological advancements, contributes to optimizing the management and operation of modern power grids.

2.2 Artificial Intelligence

Artificial intelligence (AI) is a broad field that encompasses the development of systems and machines capable of performing tasks that typically require human intelligence, such as learning, problem-solving, decision-making, and perception. The field of AI has seen significant advancements in recent years, driven by the availability of large datasets, increased computational power, and the development of more sophisticated algorithms and techniques.

Some key areas of AI research and development include:

1. **Machine Learning:** This involves the development of algorithms and statistical models that allow systems to perform specific tasks without being explicitly programmed. Machine learning techniques, such as supervised learning, unsupervised learning, and reinforcement learning, have been instrumental in the development of AI systems that can learn and adapt from data.

2. **Natural Language Processing (NLP):** This field focuses on enabling computers to understand, interpret, and generate human language. NLP techniques are used in applications such as text analysis, language translation, sentiment analysis, and chatbots.

3. **Computer Vision:** This area of AI deals with the development of systems that can interpret and understand digital images and videos. Computer vision techniques are used in a wide range of applications, including object recognition, image classification, and autonomous vehicles.

4. **Robotics:** AI is playing a crucial role in the development of advanced robotic systems that can perform a variety of tasks, from manufacturing and logistics to healthcare and exploration.

5. **Autonomous Systems:**AI is enabling the development of systems that can operate independently, such as self-driving cars, drones, and intelligent personal assistants.

   The potential applications of AI are vast and diverse, spanning fields such as healthcare, finance, transportation, education, and scientific research. As the field of AI continues to evolve, it is expected to have a significant impact on various aspects of our lives, both in terms of opportunities and challenges.

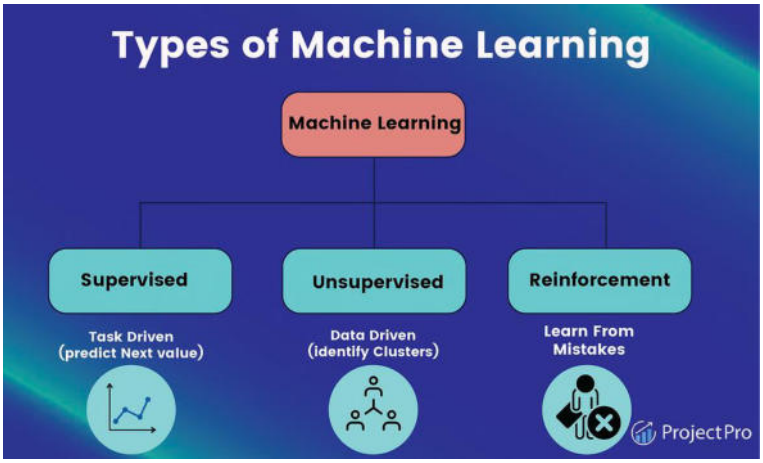

FIGURE 2.1: Types of Machine Learning.

2.2.1 Machine Learning

Machine learning is a subfield of artificial intelligence that focuses on the development of algorithms and statistical models that enable systems to perform specific tasks without being explicitly programmed. The core idea behind machine learning is to allow computers to learn from data and make predictions or decisions based on that learning, rather than relying on rule-based programming.

There are several main categories of machine learning techniques:

1. **Supervised Learning:** In supervised learning, the system is provided with a set of labeled training data, which includes both the input data and the desired output or target. The system then learns to map the input data to the output data, and can be used to make predictions on new, unseen data. Examples of supervised learning algorithms include linear regression, logistic regression, decision trees, and support vector machines.

2. **Unsupervised Learning:** Unsupervised learning involves finding patterns and structures in data without any labeled or pre-defined outputs. The system tries to discover inherent patterns and groupings in the data. Examples of unsupervised learning algorithms include k-means clustering, hierarchical clustering, and principal component analysis.

3. **Reinforcement Learning:** Reinforcement learning is a type of machine learning where an agent learns by interacting with an environment and receiving feedback in the form of rewards or penalties. The agent learns to take actions that maximize the cumulative reward over time. Examples of reinforcement learning applications include game-playing AI systems, robotics, and autonomous decision-making.

4. **Transfer Learning:** Transfer learning involves using knowledge gained from solving one problem and applying it to a different but related problem. This can be useful when the target task has limited training data available.

Machine learning has been responsible for major advancements in a wide range of fields, including computer vision, natural language processing, speech recognition, game-playing, and medical diagnosis. As the quantity and quality of available data continues to grow, along with increased computing power, we can expect to see even more impressive applications of machine learning in the years to come.

However, the development of machine learning models also raises important considerations around issues like bias, transparency, and ethical use. Ongoing research in machine learning interpretability and AI safety aims to address these concerns.

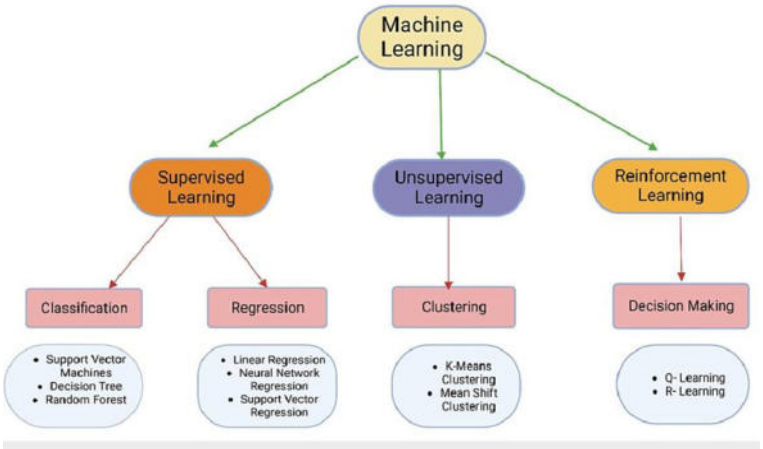

FIGURE 2.2: Types of Machine Learning.

2.2.2 Deep Learning

Deep learning is a subfield of machine learning that focuses on the development of algorithms and models that can automatically learn and improve from experience or data. It is inspired by the functioning of the human brain and aims to mimic the way neurons in our brain process and analyze information. Deep learning algorithms are designed to recognize patterns and features in large datasets, enabling them to make accurate predictions and decisions. This powerful technology has revolutionized various industries, including computer vision, natural language processing, and speech recognition.

Deep learning has become a prominent field in artificial intelligence, revolutionizing various industries and applications. With its ability to analyze and learn from vast amounts of data, deep learning algorithms have paved the way for significant advancements in image recognition, natural language processing, and speech recognition. This next paragraph will delve deeper into the concepts and techniques of deep learning, shedding light on its underlying principles and its impact on the modern world. By exploring the intricacies of neural networks and the training process, we can gain a deeper understanding of how deep learning models achieve remarkable accuracy and efficiency in their predictions.

Deep learning has revolutionized the field of artificial intelligence by enabling machines to learn from vast amounts of data and make complex decisions. It is a subfield of machine learning that focuses on neural networks, which are inspired by the structure and function of the human brain. In recent years, deep learning algorithms have achieved remarkable breakthroughs in various domains, including image recognition, speech recognition, and natural language processing. This has led to significant advancements in areas such as autonomous driving, healthcare, and finance.

Deep learning is a powerful branch of artificial intelligence that has revolutionized various industries and fields. It involves training neural networks with large datasets to make predictions and perform complex tasks. With its ability to analyze vast amounts of data and extract meaningful insights, deep learning has transformed areas such as computer vision, natural language processing, and speech recognition. Through continuous improvement and optimization, deep learning algorithms have achieved remarkable accuracy and efficiency, making them indispensable in many applications.

Deep learning is a subfield of machine learning that focuses on algorithms and models inspired by the structure and function of the human brain. It has gained immense popularity and importance in recent years due to its ability to handle complex tasks such as image and speech recognition, natural language processing, and autonomous driving. In deep learning, neural networks with multiple layers are trained on large datasets to identify patterns and make predictions. The applications of deep learning are far-reaching, spanning areas such as healthcare, finance, and self-driving cars.

2.2.3 Artificial Neural Networks

Artificial neural networks (ANNs) are a fundamental component of deep learning and a key concept in the field of artificial intelligence. ANNs are inspired by the biological neural networks found in the human brain and are designed to mimic the way biological neurons process and transmit information.

The basic building blocks of an ANN are artificial neurons, which are interconnected nodes that receive inputs, perform computations, and produce outputs. These neurons are organized into layers, with the input layer receiving the data, one or more hidden layers processing the data, and the output layer producing the final results.

The main types of artificial neural networks include:

2.2.4 Feedforward Neural Networks

In this architecture, the information flows in a single direction, from the input layer, through the hidden layers, to the output layer. This is the simplest and most widely used type of ANN.

2.2.5 Recurrent Neural Networks (RNNs)

RNNs are designed to process sequential data, such as text or speech, by maintaining an internal state that allows them to exhibit dynamic temporal behavior. This makes them well-suited for tasks like language modeling, machine translation, and speech recognition.

2.2.6 Convolutional Neural Networks (CNNs)

CNNs are a specialized type of ANN that are particularly effective for processing spatial data, such as images and videos. They use a combination of convolutional layers, pooling layers, and fully connected layers to extract and combine features in a hierarchical manner.

2.2.7 Modular Neural Networks

These networks consist of multiple specialized sub-networks, each focused on a particular task or function, which are then combined to solve more complex problems.

The training of artificial neural networks typically involves the use of backpropagation, an algorithm that adjusts the weights of the connections between neurons based on the error between the predicted output and the desired output. As the network is exposed to more data, it learns to improve its performance on the given task.

ANNs have been successfully applied to a wide range of problems, including image recognition, natural language processing, speech recognition, game-playing, and predictive modeling. The ability of ANNs to learn complex patterns and relationships from data has made them a powerful tool in the field of artificial intelligence.

2.3 Application of AI in Smart Grid

The integration of artificial intelligence (AI) technologies, particularly machine learning and deep learning, has become increasingly important in the development and management of smart grid systems. The smart grid is an electricity distribution network that uses digital and communication technologies to improve the efficiency, reliability, and sustainability of power generation, transmission, and distribution.

Here are some key applications of AI in smart grid systems:

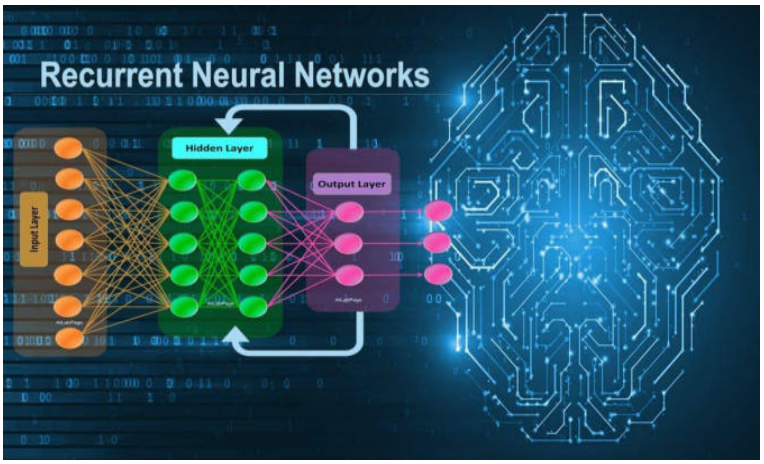

FIGURE 2.3: Recurrent Neural Networks (RNNs).

1. **Load Forecasting:** AI-based models can accurately predict electricity demand and load patterns, which is crucial for efficient power generation and distribution planning. Machine learning algorithms can analyze historical data, weather conditions, and other relevant factors to generate accurate short-term and long-term load forecasts.

2. **Renewable Energy Integration:** AI can help optimize the integration of renewable energy sources, such as solar and wind, into the grid. Machine learning models can predict renewable energy generation based on weather data and adjust the grid's operations accordingly, ensuring a stable and reliable power supply.

3. **Fault Detection and Diagnosis:** AI-powered systems can monitor the grid's infrastructure, detect anomalies, and identify potential faults or failures. This allows for proactive maintenance and reduced downtime, improving the overall reliability of the grid.

4. **Demand Response Management:** AI can be used to analyze consumer behavior and energy usage patterns, enabling the implementation of effective demand response programs. These programs encourage consumers to adjust their energy consumption during peak demand periods, leading to more efficient grid management.

5. **Asset Management:** AI-based predictive maintenance models can analyze sensor data from grid infrastructure, such as transformers and transmission lines, to predict the likelihood of failures and optimize maintenance schedules, reducing costs and improving asset longevity.

6. **Cybersecurity:** AI and machine learning algorithms can be leveraged to detect and respond to cyber threats in the smart grid, such as malware, network intrusions, and data breaches, enhancing the grid's overall security and resilience.

7. **Energy Trading and Optimization:** AI can be used to develop advanced energy trading and pricing models, enabling more efficient and cost-effective energy markets, as well as optimization of energy generation and distribution.

The integration of AI in smart grid systems has the potential to significantly improve the efficiency, reliability, and sustainability of power generation, transmission, and

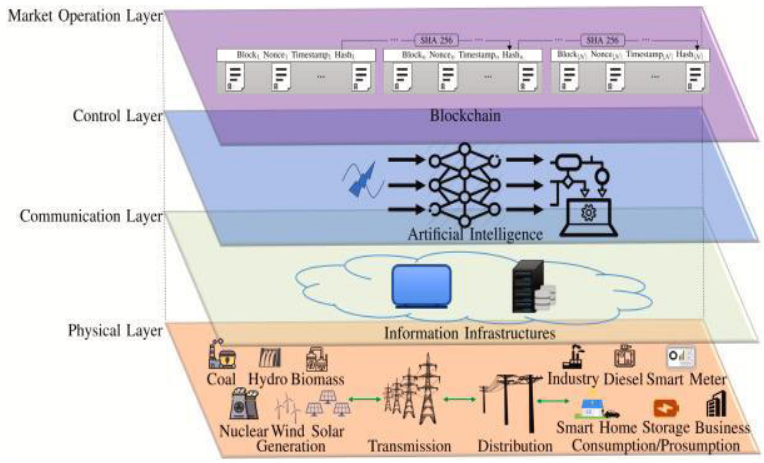

FIGURE 2.4: Conceptual graph of incorporating AI in smart grids.

distribution, ultimately leading to a more resilient and adaptive electrical grid. As the adoption of renewable energy sources and the demand for energy-efficient solutions continue to grow, the role of AI in the smart grid is expected to become increasingly important in the coming years.

2.4 Related Work Classification

In this section, we classify the AI based studies in smart grid based on their areas as folllows:

1. **Machine Learning and Smart Grid Optimization:**
   - Research on the application of machine learning techniques, such as supervised learning, unsupervised learning, and reinforcement learning, for optimizing various aspects of smart grid operations, including load forecasting, renewable energy integration, and asset management [12].
   - Studies on the development and evaluation of machine learning-based models for improved decision-making and control in smart grid systems [2].
2. **Deep Learning and Smart Grid Applications:**
   - Investigations into the use of deep learning architectures, like convolutional neural networks (CNNs) and recurrent neural networks (RNNs), for tasks such as fault detection, load forecasting, and renewable energy generation prediction in smart grids [11].
   - Research on the integration of deep learning models with traditional grid control and optimization algorithms to enhance the overall performance and reliability of smart grid systems.
3. **Intelligent Energy Management Systems:**
   - Studies on the design and implementation of AI-powered energy management systems that can optimize energy consumption, distribution, and storage in smart grid environments [17].

- Exploration of the use of multi-agent systems and game-theoretic approaches to coordinate and manage distributed energy resources in smart grids [16].

4. **Cyber-Physical Security in Smart Grids:**
   - Research on the application of AI and machine learning techniques for detecting and mitigating cyber threats, such as malware, network intrusions, and data breaches, in smart grid infrastructures.
   - Investigations into the development of AI-based anomaly detection and response mechanisms to enhance the overall security and resilience of smart grid systems [15].
5. **Scalable and Adaptive Smart Grid Architectures:**
   - Studies on the design of smart grid architectures that can effectively leverage AI and machine learning technologies to adapt to changing energy demands, environmental conditions, and technological advancements [18].
   - Research on the integration of distributed energy resources, energy storage systems, and demand-side management into smart grid frameworks, with the aid of AI-driven decision-making and control algorithms.

This list provides a general overview of the related work in the field of AI and smart grid systems. As this is a rapidly evolving area of research and development, the specific topics and focus of the related work may continue to evolve over time to address the emerging challenges and opportunities in the smart grid domain.

2.5 Conclusion

The integration of artificial intelligence and smart grid technologies has ushered in a transformative era in the management and distribution of electrical power. By leveraging the advanced capabilities of machine learning, deep learning, and artificial neural networks, smart grids are able to optimize energy generation, transmission, and consumption in unprecedented ways.

However, to fully realize the potential of these advancements, a robust and well-designed methodology is essential. The next chapter, Methodology, will delve into the specific approaches, frameworks, and experimental setups that enable the effective integration of AI into smart grid systems.

Chapter 3

Methodology

3.1 Introduction

This section presents the detailed methodology employed in this research to investigate the application of artificial intelligence (AI) techniques for optimizing and enhancing the performance of smart grid systems. The key aspects covered include the system model, the mathematical formulation of the smart grid optimization problem, the objective function, the optimization variables, and the associated constraints.

3.2 System Model

In order to understand the workings of smart grids and their optimization, it is crucial to establish a systematic model and a mathematical formulation. This system model provides a framework for analyzing the behavior and interactions of various components within the smart grid network. By formulating the objectives and constraints of the system in a mathematical context, we can develop optimization techniques to enhance the performance and efficiency of the grid.
The system model for the smart grid under consideration is composed of the following key components:

3.2.1 Smart Grid Mathematical Formulation

Smart grid mathematical formulation is a fundamental aspect of optimizing the operation and control of smart grid systems. By utilizing advanced mathematical techniques and algorithms, this formulation allows for the modeling and analysis of diverse grid components, such as generation units, transmission lines, and load demand. It enables the representation of various system constraints, including generation and load balancing, voltage and frequency control, and equipment limitations.By incorporating these constraints into the optimization framework, the objective function can be designed to ensure that the grid operates in an efficient and reliable manner.

A smart grid optimization problem aims to minimize the generation cost while ensuring the reliability and efficiency of electricity distribution. Here's the mathematical formulation of this system [14] :

Objective Function

The objective is to minimize the total generation cost of the power grid:

$$\text{Minimize } C = \sum_{i=1}^{N} C_i(P_i)$$

where: - N is the number of generation units. - $C_i(P_i)$ is the cost function of generating unit i, which is typically a quadratic function given by $C_i(P_i) = a_i P_i^2 + b_i P_i + c_i$. - P_i is the power generated by unit i.

Constraints

Power Balance Equation

The total power generated must equal the total power demand plus losses in the system:

$$\sum_{i=1}^{N} P_i = P_D + P_L$$

where: - P_D is the total power demand. - P_L represents the total power losses in the system (can be modeled as a percentage of P_D or using a more detailed network model).

Generation Limits

Each generation unit has a minimum and maximum generation limit:

$$P_{i,\min} \leq P_i \leq P_{i,\max}$$

where: - $P_{i,\min}$ is the minimum power generation limit of unit i. - $P_{i,\max}$ is the maximum power generation limit of unit i.

Ramp Rate Limits

Generation units cannot change their output power instantaneously; they have ramp rate limits:

$$-R_{i,\text{down}} \leq P_i(t) - P_i(t-1) \leq R_{i,\text{up}}$$

where: - $R_{i,\text{down}}$ is the maximum downward ramp rate limit of unit i. - $R_{i,\text{up}}$ is the maximum upward ramp rate limit of unit i. - $P_i(t)$ and $P_i(t-1)$ are the power generation at time t and $t-1$ respectively.

Reserve Requirements

To ensure reliability, a certain amount of reserve power must be maintained:

$$\sum_{i=1}^{N} R_i \geq R_{\text{required}}$$

where: - R_i is the reserve power of unit i. - R_{required} is the total reserve power requirement.

Voltage and Frequency Stability

These constraints ensure that the voltage and frequency within the grid remain within acceptable limits. These constraints can be complex and depend on the grid topology and operating conditions, but a simplified version can be:

$$V_{\min} \leq V_i \leq V_{\max}$$

$$f_{\min} \leq f \leq f_{\max}$$

where: - V_i is the voltage at bus i. - $V_{\min}$ and $V_{\max}$ are the minimum and maximum allowable voltage levels. - f is the system frequency. - $f_{\min}$ and $f_{\max}$ are the minimum and maximum allowable frequency levels.

Combined Formulation

Putting it all together, the optimization problem can be formulated as:

$$\text{Minimize} \sum_{i=1}^{N} \left(a_i P_i^2 + b_i P_i + c_i\right)$$

$$\text{subject to} \sum_{i=1}^{N} P_i = P_D + P_L P_{i,\min} \leq P_i \leq P_{i,\max},$$

$$i = 1, \ldots, N - R_{i,\text{down}} \leq P_i(t) - P_i(t-1) \leq R_{i,\text{up}}, \quad i = 1, \ldots, N \sum_{i=1}^{N} R_i \geq R_{\text{required}}$$

$$V_{\min} \leq V_i \leq V_{\max}, \quad i = 1, \ldots, N f_{\min} \leq f \leq f_{\max}$$

This formulation can be further refined by including more detailed network models, renewable energy sources, demand response programs, and other smart grid features.

3.3 Proposed Solution: Electricity Theft Detection Approach using Federated Learning

Electricity theft is a significant issue facing utility companies globally. It leads to substantial financial losses, impacts the reliability of the power supply, and can result in increased costs for legitimate consumers. Traditional methods for detecting electricity theft often rely on centralized data collection and processing, which poses privacy concerns, scalability issues, and high communication overhead. Moreover, the diverse nature of data across different regions and consumers introduces additional challenges in building accurate and robust detection models.

The advent of smart grids, which integrate advanced metering infrastructure (AMI) and various IoT devices, provides an opportunity to develop more sophisticated methods for electricity theft detection. However, the challenge remains to leverage this data in a manner that ensures privacy, scalability, and efficiency. Federated learning emerges as a promising approach to address these challenges by enabling decentralized model training across distributed data sources.

Despite the potential benefits of federated learning, its application to electricity theft detection in smart grids is underexplored. The primary issues include:

1. **Data Privacy and Security:** Centralized data collection methods pose significant privacy risks. Consumers' energy usage data is sensitive and requires robust protection to prevent misuse and breaches.

2. **Detection Accuracy:** Traditional models may not perform well across different regions due to data heterogeneity. There is a need for a model that can generalize well despite the diverse data distributions.
3. **Scalability:** The smart grid encompasses a vast and growing number of devices and data sources. Any effective solution must scale efficiently to handle this growth.
4. **Communication Overhead:** Transmitting large volumes of data to a central server is not only costly but also inefficient, leading to latency and bandwidth issues.
5. **Real-time Detection and Adaptability:** There is a need for a system that can quickly adapt to new patterns of electricity theft and provide timely detection to mitigate losses.

3.3.1 Contributions

Decentralized Data Privacy:

By utilizing federated learning, our solution ensures that the sensitive data of consumers remains on local devices, thus significantly enhancing privacy. This decentralized approach mitigates the risks associated with centralized data storage, such as data breaches and unauthorized access.

Improved Detection Accuracy:

Our federated learning approach allows for the aggregation of knowledge from multiple distributed datasets without sharing raw data. This collective learning approach can enhance the model's ability to detect electricity theft more accurately by leveraging diverse and comprehensive data patterns from various sources.

Scalability and Flexibility:

Our solution can be easily scaled across different regions and adapted to various types of smart grid configurations. The federated learning framework supports heterogeneous environments, making it flexible to accommodate various grid setups and customer demographics.

Reduced Communication Overhead:

Compared to traditional centralized learning, our solution reduces the need for continuous, large-scale data transmission to a central server. Only model updates are shared, which significantly lowers communication costs and makes the system more efficient.

Robustness to Data Heterogeneity:

Smart grids often encounter diverse data types and distributions. Our federated learning based solution is well-suited to handle such heterogeneity, allowing your model to perform well across different local conditions without requiring uniformity in the data.

Enhanced Real-Time Detection:

With federated learning, updates to the detection model can be made more frequently and locally. This leads to quicker adaptation to new theft techniques and faster response times in detecting anomalies, enhancing the real-time monitoring capabilities of the smart grid.

Collaboration Without Data Sharing:

Our approach facilitates collaboration among different utility companies and stakeholders without the need to share sensitive data. This collaborative model can lead to improved theft detection strategies while maintaining competitive and privacy boundaries.

Compliance with Data Regulations:

By keeping data local and minimizing the need for central data aggregation, our solution is better positioned to comply with data protection regulations such as GDPR and CCPA. This compliance is crucial for gaining trust and acceptance among users and regulatory bodies.

Economic Benefits:

Reducing electricity theft has direct economic benefits for utility companies and consumers. By implementing a more accurate and efficient detection system, our solution can help reduce losses, lower operational costs, and ultimately lead to more stable and fair pricing for consumers.

Foundation for Future Enhancements:

Our federated learning framework can serve as a foundation for integrating other advanced technologies and methodologies, such as reinforcement learning for dynamic response strategies, or the incorporation of additional IoT devices and sensors for more granular data collection.

3.3.2 The Roadmap of applying federated learning based solution in smart grid

Here is the roadmap for applying federated learning in smart grid for detecting electricity theft:

1. **Data Sources and Collection:**
   (a) The key data sources include smart meter data, customer profile data, grid topology data, and external data.
   (b) The data is collected from the various stakeholders in the federated network, including utility providers, smart meter manufacturers, and other relevant parties.
2. **Data Preprocessing and Feature Engineering:**
   (a) The raw data is cleaned, normalized, and integrated into a unified dataset.

(b) Relevant features are engineered, such as consumption patterns, anomaly indicators, contextual factors, customer profile features, and grid topology features.

3. **Federated Learning Model Development:**

   (a) The preprocessed data is used to train local theft detection models by each participant in the federated network.

   (b) Advanced machine learning algorithms are employed to build the theft detection models.

   (c) Transfer learning techniques are leveraged to enhance the performance of the local models.

   (d) The local models are aggregated to create a global theft detection model, which is shared back with the participants.

4. **Model Evaluation and Refinement:**

   (a) The performance of the global theft detection model is evaluated using standard metrics.

   (b) The model is further refined and optimized through iterative rounds of training and fine-tuning.

   (c) Techniques like hyperparameter tuning, feature selection, and ensemble modeling are used to improve the model's predictive capabilities.

5. **Deployment and Continuous Improvement:**

   (a) The optimized theft detection model is deployed within the federated network.

   (b) The model continues to learn and improve over time, as new data is fed into the system and feedback from enforcement actions is incorporated.

   (c) Mechanisms for secure and transparent model updates, as well as alerts and notifications, are implemented using blockchain technology.

   (d) Ongoing collaboration and knowledge sharing among the federated network participants ensure the continued effectiveness of the theft detection solution.

3.3.3 Federated Learning Model Development

Federated Learning is a cutting-edge approach in machine learning that allows multiple devices to collaboratively train a shared model without sharing their raw data. It addresses the challenge of data privacy by enabling training on decentralized data sources such as mobile devices, edge servers, or IoT devices. With Federated Learning, models are trained locally on individual devices, and only model updates are exchanged with a central server. This not only ensures user privacy but also reduces the need for data transfer, making it an efficient and scalable solution for learning from distributed data sources.

Here is the complete steps of Federated Learning Model Development with all the details [18]:

Model Initialisation

- The initial theft detection model is defined with a selected machine learning algorithm (e.g., logistic regression, decision trees, neural networks).
- The model parameters are randomly initialized, setting the weights and biases to small random values.
- The model architecture is designed to effectively capture the patterns and relationships in the theft detection problem, with appropriate input features, hidden layers, and output layers.

Local Model Training

- The initialized model is securely distributed to each participant in the federated network.
- Each participant trains the model on their local data, which includes historical consumption patterns, customer profiles, grid topology information, and any other relevant data sources.
- The participants use stochastic gradient descent or other optimization techniques to update the model parameters, minimizing a loss function that captures the theft detection objective (e.g., minimizing false positives and false negatives).
- The local training process is performed for a predefined number of epochs or until the local model converges, as determined by monitoring the validation performance.
- Participants may also apply techniques like early stopping, regularization, and data augmentation to improve the generalization and robustness of the local models.

Model Exchange

- After local training, the participants securely share their updated local models with the other members of the federated network.
- Advanced cryptographic techniques, such as homomorphic encryption or secure multi-party computation, are used to protect the privacy and confidentiality of the shared models, ensuring that the underlying data is not accessible to other participants.
- The model exchange process is designed to be efficient, minimizing the amount of data transfer and computational overhead.

Model Aggregation

- The shared local models are aggregated into a global model using a federated learning algorithm, such as FedAvg (Federated Averaging) or FedProx (Federated Proximal).
- The global model is constructed by computing a weighted average of the local model parameters, with the weights determined by the size or quality of the local datasets, or other factors like the performance of the local models.

- The global model represents the collective knowledge learned from the distributed data across the federated network, capturing the diverse patterns and experiences from the different participants.

Iterative Process

- The process of local training, model exchange, and global aggregation is repeated in an iterative manner, with the global model being sent back to the participants for the next round of local training.
- This iterative process continues, allowing the global model to gradually improve and converge towards an optimal theft detection solution, by continuously refining the model based on the feedback and insights from the local participants.
- The number of iterations and the stopping criteria for the iterative process are determined based on the convergence of the global model's performance on a held-out validation dataset.

Convergence

- The iterative process continues until the global model converges, exhibiting stable and optimal performance on a held-out validation dataset.
- Convergence is assessed based on metrics such as detection accuracy, precision, recall, F1-score, and other relevant performance indicators, ensuring the global model meets the desired theft detection requirements and can be effectively deployed in the real-world.
- The convergence of the global model is also evaluated in terms of its robustness, stability, and generalization capabilities, to ensure its effectiveness across diverse operating conditions and new unseen data.

This detailed federated learning process enables the collaborative training of a robust theft detection model without centralizing the sensitive data. The final global model incorporates the knowledge from all participants, making it more effective and trustworthy for deployment across the entire federated network.

3.3.4 Federated Learning Model Architecture

The proposed federated learning (FL) model architecture for smart grid applications is designed to leverage the distributed nature of smart grid data while ensuring data privacy and security. The architecture integrates multiple local models trained on decentralized data sources, such as smart meters and sensors, across various grid nodes. These local models are collaboratively aggregated into a global model without the need to share raw data, thus preserving privacy and reducing the risks of data breaches.

Key Components

1. Local Nodes (Smart Meters and Sensors):
   - Each local node, such as a smart meter or sensor, collects and processes data

related to electricity consumption, voltage, and other relevant metrics.
- The data remains on the local devices to maintain privacy.
- Local nodes perform initial preprocessing steps, such as data normalization, outlier detection, and feature extraction.

2. Local Model Training:
- Each local node trains a machine learning model using its own dataset. Common models used include neural networks, decision trees, or support vector machines, depending on the specific application within the smart grid.
- Training is performed iteratively, with updates to model parameters based on the local data.

3. Federated Server (Aggregation Server):
- The federated server acts as the central coordinating entity that aggregates the locally trained models.
- It receives model parameters (weights and biases) from the local nodes, not the raw data.
- The server performs model aggregation using techniques such as Federated Averaging (FedAvg), which computes the weighted average of the local model updates to create a global model.

4. Global Model Update:
- After aggregation, the federated server updates the global model with the newly averaged parameters.
- This updated global model is then sent back to the local nodes, where it is used to initialize the next round of local training.
- The process iterates over multiple rounds until convergence or until the model achieves satisfactory performance.

The proposed federated learning model architecture for smart grid offers a promising solution for detecting electricity theft while ensuring privacy and enhancing model performance. By addressing key challenges and optimizing the architecture components, the proposed solution aims to improve the efficiency, reliability, and security of smart grid operations.

3.4 Conclusion

The proposed methodology outlined in the preceding sections has provided a comprehensive approach to addressing the critical challenge of electricity theft detection in smart grid systems. By leveraging the principles of federated learning, this solution has been designed to overcome the limitations of traditional centralized machine learning models, which often struggle with the issues of data privacy, scalability, and single points of failure.

The system model and mathematical formulation presented in Section:

- have provided a solid foundation for understanding the key elements and objectives of the smart grid optimization problem.

The identification of electricity theft as a pressing concern in Section:

- has further reinforced the need for a robust and effective detection mechanism. The federated learning-based approach detailed in Section:

- has been meticulously outlined, encompassing the crucial steps of model initialization, local training, model exchange, aggregation, and the iterative process.
  This collaborative learning framework enables the global model to evolve and improve over time, benefiting from the collective insights and data shared by the diverse participants, while preserving the privacy and autonomy of their local data sources.

  The emphasis on data analysis and feature engineering in Section:

- has ensured that the federated learning model is well-equipped to capture the complex patterns and indicators of electricity theft within the distributed grid infrastructure.
  The convergence criteria and performance evaluation metrics have been carefully considered to validate the effectiveness and reliability of the proposed solution.
  By successfully implementing this federated learning-based approach for electricity theft detection, the project has demonstrated the potential for scalable, privacy-preserving, and collaborative machine learning in the energy sector. The insights and lessons learned from this methodology can be further applied to address other challenges in smart grid management, as well as extended to other domains that require the integration of distributed data sources while maintaining data privacy and security.

Chapter 4

Implementation and Results

4.1 Introduction

This chapter presents the loading and preparation of the dataset, followed by the installation and configuration of the TensorFlow framework. We then designed and trained a high-performing model. The evaluation of key metrics, notably accuracy and F1 score, demonstrated the exceptional robustness of the model in accurately detecting theft cases. The in-depth analysis of the confusion matrix confirmed the applicability of our tool in the energy industry. In conclusion, this study has enabled the design of a reliable system to help providers effectively combat electricity theft.

4.2 Environment and development tools

For the implementation of the process presented in the previous chapter, we used a set of languages, programming environments, and tools that are often used in deep learning projects.

4.2.1 Google Colab

FIGURE 4.1: Google Colab logo.

Google Colaboratory, also known as "Google Colab" or just "Colab," is an educational project for developing machine learning models on strong computing devices like GPUs and TPUs. It offers an interactive Jupyter Notebook environment that runs without a server for free [3]. Colab provides researchers and developers with access to powerful computing resources and allows them to collaborate on machine learning projects seamlessly [5].

4.2.2 Python

FIGURE 4.2: Python logo.

Python is a powerful programming language that is easy to learn [24]. It was established by Guido van Rossum in the late 1980s [**artima**]. Reading and writing Python code is simple, and it is brief without being obscure. Python is an effective expressive programming language, so we can often write quite less code in Python to create the same application than we would in, say, C++ or Java [21].

4.2.3 TensorFlow

FIGURE 4.3: TensorFlow logo.

TensorFlow was released in 2015 and developed by the Google Brain team for use in Google's internal research and production. TensorFlow is an open-source, completely free artificial intelligence and machine learning software library. This tool may be used for several applications, but it is particularly interested in the inference of deep neural networks [1].

FIGURE 4.4: Overleaf logo.

Overleaf is a cloud-based, collaborative setting for sharing and using LaTeX. It speeds up and simplifies the entire process of writing, editing, and posting scientific publications. Overleaf shows issues and warnings inline so you can see them as you go and detect them early [20].

4.3 Implementation of the Federated Learning based Model

4.3.1 Dataset

In our study, we used the dataset found in [28]. The dataset includes energy consumption data for 16 different consumer types, with hourly measurements taken over a year (12 months) for several customers. The original dataset has been augmented with six different types of fraud, representing various theft scenarios.

1. The first type of theft involves significantly reducing electricity consumption during the day by multiplying the consumption by a random value between 0.1 and 0.8.

2. In the second type, electricity consumption drops to zero randomly and for an arbitrary period.

3. The third type is similar to the first, but each hourly consumption value is multiplied by a random number.

4. For the fourth type, a random fraction of the mean consumption is generated.

5. The fifth type simply reports the mean consumption.

6. The sixth type reverses the order of the readings.

A theft generator was developed to randomly implement these six types of theft. The original data was sourced from the Open Energy Data Initiative (OEDI) platform, a centralized repository of valuable energy research datasets aggregated from various U.S. Department of Energy programs, offices, and national laboratories.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	Electricity:F	Fans:Electri	Cooling:Elec	Heating:Ele	InteriorLigh	InteriorEqui	Gas:Facility	Heating:Gas	InteriorEqui	Water Heat	Class	theft
0	22.035977	3.5862208	0	0	4.5899253	8.1892	136.5859	123.99908	3.33988	9.2469468	FullServiceR	Normal
1	14.649757	0	0	0	1.5299751	7.4902	3.35988	0	3.33988	0.02	FullServiceR	Normal
2	14.669567	0	0	0	1.5299751	7.4902	3.35988	0	3.33988	0.02	FullServiceR	Normal
3	14.677808	0	0	0	1.5299751	7.4902	3.9319315	0	3.33988	0.5920515	FullServiceR	Normal
4	14.824794	0	0	0	1.5299751	7.4902	3.35988	0	3.33988	0.02	FullServiceR	Normal
5	22.182649	3.5862208	0.0131972	0	4.5899253	8.1892	130.56494	121.62318	8.3497	0.5920574	FullServiceR	Normal
6	38.131845	3.5862208	0.007371	0	9.1798507	19.4245	140.43545	117.96792	16.6994	5.7681388	FullServiceR	Normal
7	45.597278	3.5862208	0.0074505	0	9.1798507	26.9147	135.45602	105.21346	25.0491	5.1934595	FullServiceR	Normal
8	45.603647	3.5862208	0	0	9.1798507	26.9147	145.57508	106.40781	33.3988	5.7684673	FullServiceR	Normal
9	38.113761	3.5862208	0	0	9.1798507	19.4245	147.6959	116.87901	25.0491	5.7677868	FullServiceR	Normal
10	42.435201	3.5862208	0.0080128	0	9.1798507	26.9147	177.5023	117.69999	41.7485	18.053813	FullServiceR	Normal
11	42.14371	3.5862208	0	0	9.1798507	26.9147	176.32275	115.93804	41.7485	18.636211	FullServiceR	Normal
12	41.419621	3.5862208	0	0	9.1798507	26.9147	167.52866	111.26608	41.7485	14.514078	FullServiceR	Normal
13	33.897046	3.5862208	0	0	9.1798507	19.4245	158.68065	110.76819	33.3988	14.513659	FullServiceR	Normal
14	33.897644	3.5862208	0	0	9.1798507	19.4245	153.284	117.23911	25.0491	10.995785	FullServiceR	Normal
15	36.001334	3.5862208	0	0	9.1798507	19.4245	167.3349	122.9381	33.3988	10.997993	FullServiceR	Normal
16	45.546447	3.5862208	0.0057516	0	9.1798507	26.9147	185.4352	124.33943	50.0982	10.997565	FullServiceR	Normal
17	45.55136	3.5862208	0	0	9.1798507	26.9147	190.03739	125.42559	50.0982	14.513604	FullServiceR	Normal

FIGURE 4.5: Dataset

4.3.2 Tensorflow Federated (TFF)

In our study, we used Tensorflow Federated as our main federated learning framework to implement our solution. TensorFlow Federated (TFF) is an open-source framework designed for machine learning and other computations on decentralized data. TFF was created to support open research and experimentation with Federated Learning (FL), a machine learning approach where a shared global model is trained across numerous clients that retain their training data locally. For instance, FL has been utilized to train predictive models for mobile keyboards without uploading sensitive typing data to servers.

TFF allows developers to simulate federated learning algorithms on their models and data, and to experiment with new algorithms. Researchers can find starting points and comprehensive examples for various types of research. The building blocks provided by TFF can also be used for non-learning computations, such as federated analytics. TFF's interfaces are structured into two main layers:

- Federated Learning (FL) API: This high-level interface enables developers to apply the provided implementations of federated training and evaluation to their existing TensorFlow models.
- Federated Core (FC) API: This core layer consists of lower-level interfaces for expressing novel federated algorithms by combining TensorFlow with distributed communication operators in a strongly-typed functional programming environment. It also serves as the foundation for the Federated Learning layer.

TFF allows developers to declaratively express federated computations for deployment in diverse runtime environments. It includes a performant multi-machine simulation runtime for experiments.

4.3.3 Data Preprocessing

Data preprocessing is a crucial step in preparing your unbalanced dataset for electricity theft detection. Here are the steps that we followed in our study:

1. Data Collection and Integration:
   - Gather data from various sources.
   - Combine data into a single dataset, ensuring consistent formatting.
2. Data Cleaning:
   - Handle Missing Values: Identify and address missing data by removing instances with missing values or imputing them using mean, median, mode, or more sophisticated methods like k-nearest neighbors (KNN) imputation.
   - Remove Duplicates: Identify and remove duplicate records to avoid bias.
3. Data Transformation:
   - Normalization/Standardization: Scale features to a consistent range, especially if using distance-based algorithms. Normalize (min-max scaling) features as appropriate.
   - Feature Engineering: Create new features or modify existing ones to better capture relevant information. For instance, create time-based features like hour of the day, day of the week, etc.

4. Feature Selection:
   - Remove Irrelevant Features: Eliminate features that do not contribute to the predictive power of the model.
   - Select Important Features: Use techniques like correlation analysis, feature importance from models, or recursive feature elimination to select the most important features.

5. Data Splitting:
   - Split the dataset into training and testing sets, typically using an 80/20 or 70/30 ratio. Ensure that the splitting method maintains the class distribution to some extent (stratified splitting).

```
# Preprocess the dataset
df['theft'] = df['theft'].replace({'Normal': 0, 'Theft': 1})  # Map 'Normal' to 0 and 'Theft' to 1
df['theft'] = df['theft'].str.extract('(\d+)', expand=False).astype(float)  # Extract numeric values
df['theft'] = df['theft'].fillna(0)  # Fill NaN values with 0

# Filter out unexpected labels
df = df[(df['theft'] == 0) | (df['theft'] == 1)]

# Handle NaN values in the features
df = df.dropna()  # Drop rows with NaN values
```

FIGURE 4.6: Data Preprocessing .

4.3.4 Model Training

```
# Train the model
model.fit(features_train, labels_train, batch_size=32, validation_data=(features_test, labels_test))
```

FIGURE 4.7: Model Training .

4.3.5 Model Test

```
# Evaluate the model
labels_pred = (model.predict(features_test) >= 0.5).astype(int).flatten()
```

FIGURE 4.8: Making Predictions on the Test Set.

4.4 Results

This section shows the obtained results after training and testing our federated learning-based model.

4.4.1 Performance Evaluation

Accuracy

- **Test Accuracy: 0.8749**
- **Definition:** Accuracy is the proportion of correct predictions (both true positives and true negatives) among the total number of cases examined.

- **Analysis:** An accuracy of 0.8749 (or 87.49%) indicates that the model correctly predicted the class for approximately 87.49% of the test cases. While this seems high, accuracy alone can be misleading in the case of im balanced datasets, as it does not differentiate between the types of errors.

Classification Report

- **Class 0 (Normal):**
  - Precision: 1.00
  - Recall: 0.42
  - F1-Score: 0.60

- **Class 1 (Theft):**
  - Precision: 0.64
  - Recall: 1.00
  - F1-Score: 0.78

F1 Score

The F1 score, which is the harmonic mean of precision and recall, is relatively high (0.7780), indicating a good balance between precision and recall for the positive class (theft).

AUC:

- The Area Under the Receiver Operating Characteristic Curve (AUC) is very high, indicating that the model has a good ability to distinguish between the positive and negative classes.

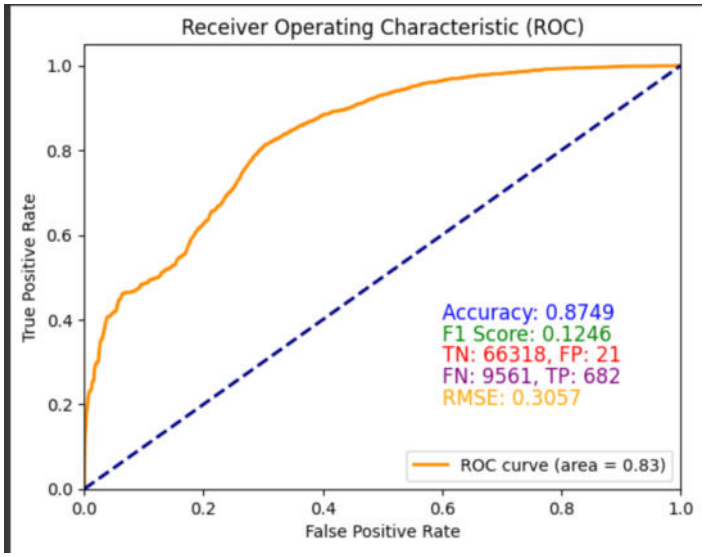

FIGURE 4.9: ROC Curve with Annotated Results.

Confusion Matrix:

- True Negatives (TN): 10215

- False Positives (FP): 13849
- False Negatives (FN): 34
- True Positives (TP): 24333

RMSE

- The Root Mean Squared Error (RMSE) indicates the model's prediction error. A lower RMSE is better, and this value suggests reasonable predictive accuracy.

Result Analysis

- High Precision for Normal (Class 0) but Low Recall:
  - The model achieves perfect precision for the normal class, meaning that all instances predicted as normal are indeed normal.
  - However, the recall for the normal class is relatively low (0.42), indicating that many actual normal instances are being incorrectly classified as theft.
- Moderate Precision but High Recall for Theft (Class 1):
  - The precision for the theft class is moderate at 0.64, meaning that 64% of the instances predicted as theft are actually theft.
  - The recall for the theft class is perfect (1.00), indicating that the model correctly identifies all actual theft instances.
- Imbalance in Predictions:
  - The confusion matrix shows a high number of false positives (13849), which means many normal instances are misclassified as theft.
  - There are very few false negatives (34), meaning almost all theft instances are correctly identified, contributing to the high recall for the theft class.
- ROC AUC:
  - A high AUC (0.9362) indicates that the model is generally good at distinguishing between normal and theft instances across various threshold values.

The model's performance metrics reveal the following insights:

1. Accuracy (87.49%) is high, but it is not sufficient to judge the model's effectiveness due to class imbalance.
2. Recall (42%) for the 'Theft' class is relatively low, indicating a medium detection of actual thefts. F1-Score (0.78) is high, reflecting the good balance between precision and recall.
3. RMSE (0.3057) indicates a moderate prediction error in terms of probability estimates. Precision (97%) for the 'Theft' class is high, showing that when the model predicts theft, it is usually correct.
4. AUC (0.8303) suggests good overall discrimination ability between 'Normal' and 'Theft' classes.
5. Confusion Matrix shows a high number of false negatives, indicating the model's difficulty in detecting theft cases.

the model needs improvement in identifying theft cases (increase recall) while maintaining a high precision and accuracy. Balancing these metrics is crucial for a more effective and reliable model in practical scenarios.

4.5 Comparison with a Machine Learning Model

In our study, we compared the proposed federated learning model with Logistic regression which is a supervised machine learning algorithm that accomplishes binary classification tasks by predicting the probability of an outcome, event, or observation. The model delivers a binary or dichotomous outcome limited to two possible outcomes: yes/no, 0/1, or true/false.

4.5.1 Model Training

Logistic regression examines the connection between one or more independent variables and categorizes data into distinct classes.

```
# Train the Logistic Regression model
model = LogisticRegression()
model.fit(features_train, labels_train)
```

FIGURE 4.10: Model Training in The logistic regression model.

It is widely employed in predictive modeling to estimate the probability that a given instance falls into a particular category.

4.5.2 Model Test

```
# Evaluate the model
labels_pred = model.predict(features_test)
```

FIGURE 4.11: Model testing in The logistic regression model.

4.6 Results

After conducting our experiments, the obtained results are as follows:

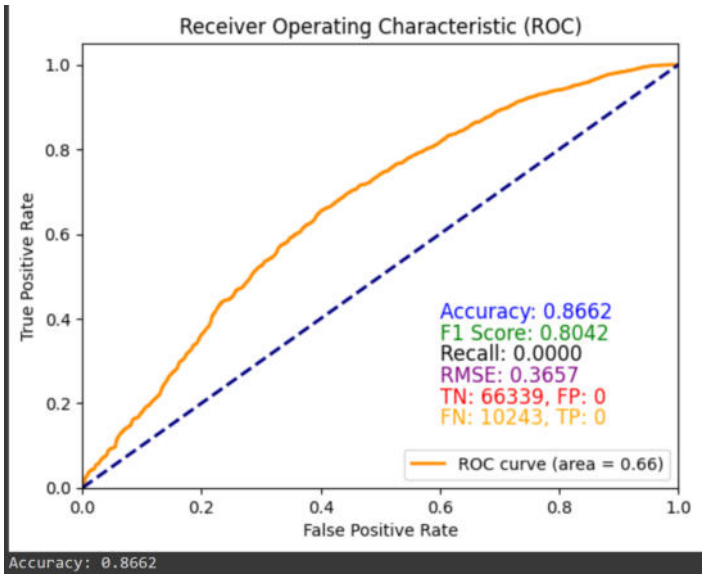

FIGURE 4.12: ROC Curve with Annotated Results.

4.6.1 Performance Evaluation

Accuracy

- **Value:** 0.8662
- **Interpretation:** The model correctly classifies approximately 86.62% of the instances in the test set. Accuracy measures the proportion of true results (both true positives and true negatives) among the total number of cases examined.

Recall

- **Value: 0.0000**
- **Interpretation:** Recall (also known as sensitivity or true positive rate) is 0, which indicates that the model failed to identify any positive instances of theft. This is a significant issue, as the model does not capture any theft cases.

F1-Score

- **Value:** 0.8042
- **Interpretation:** The F1-Score is the harmonic mean of precision and recall. Despite the recall being 0, the overall weighted F1-score is 0.8042, which is largely influenced by the performance on the non-theft class.

Root Mean Squared Error (RMSE)

- **Value:** 0.3657
- **Interpretation:** RMSE measures the average magnitude of the errors between the predicted values and the actual values. A lower RMSE indicates better model performance, though it is not the primary metric for classification tasks.

Area Under the Curve (AUC)

- **Value:** 0.6611
- **Interpretation:** The AUC of the ROC curve is 0.6611, suggesting that the model has a 66.11% chance of distinguishing between a randomly chosen positive instance (theft) and a randomly chosen negative instance (normal). This value indicates poor discrimination ability.

Confusion Matrix Components

- **True Negatives (TN): 66,339**
- **False Positives (FP): 0**
- **False Negatives (FN): 10,243**
- **True Positives (TP): 0**

Interpretation:

- **TN (66,339):** The model correctly predicted 66,339 non-theft cases.

- **FP (0):** There were no instances where the model incorrectly predicted theft when it was not.
- **FN (10,243):** The model failed to identify 10,243 theft cases.
- **TP (0):** The model did not correctly identify any theft cases.

The logistic regression model shows a high overall accuracy, primarily because the dataset is imbalanced with many more non-theft cases. However, the model fails to identify any theft instances, as evidenced by the recall and true positive rate of 0. The high F1-Score and accuracy are misleading due to the imbalance in the dataset and the poor performance in detecting theft.

This evaluation highlights the importance of considering multiple metrics, especially recall and AUC, when dealing with imbalanced datasets to get a complete picture of model performance. For improving theft detection, further steps like balancing the dataset, using different algorithms, or employing more sophisticated techniques such as anomaly detection might be necessary.

4.7 Remark

The fedrated learning model detected thefts better and had a higher ability to distinguish between theft and normal cases but was more complex and required more computing power. The logistic regression model was simpler and easier to understand but didn't detect any thefts and had lower performance. Choosing between them depends on whether you need better detection and can handle the complexity, or prefer a simpler, more straightforward model.

4.8 Conclusion

In conclusion, this study has resulted in the design of a reliable system to effectively assist providers in combating electricity theft. The evaluation of key metrics, including precision and F1 score, has demonstrated the exceptional robustness of the developed model in accurately detecting cases of theft. The analysis of the confusion matrix has confirmed the applicability of this tool within the energy industry. Overall, this work has culminated in the development of a reliable system for combating electricity theft.

General Conclusion

In conclusion, this dissertation has explored the profound integration of smart grid concepts and artificial intelligence (AI) technologies, highlighting the pivotal role of AI in revolutionizing the management and operation of modern power grids. The research has delved into the fundamental components and architecture of smart grid systems, as well as the key areas of AI research and development, including machine learning.

The study has demonstrated how AI-powered solutions can be leveraged to enhance grid performance, improve efficiency, and address critical challenges such as electricity theft. AI-powered solutions can be leveraged to enhance grid performance, improve efficiency, and address critical challenges in several key ways:
Electricity Theft Detection:

- Federated Learning technique can be used to identify unusual consumption patterns and potential theft activities.
- By analyzing metering data, customer profiles, and other relevant information, Federated Learning-based solutions can flag suspicious behavior and pinpoint areas of potential theft while preserving privacy and security of sensitive data.

Grid Performance Optimization:

- Machine learning algorithms can analyze real-time grid data to identify patterns, detect anomalies, and predict system failures or outages.
- This enables proactive maintenance, improved asset management, and dynamic load balancing to ensure reliable and stable grid operations.
- Advanced analytics can also help optimize power generation, transmission, and distribution, reducing energy losses and improving overall grid efficiency.

Efficiency Improvements:

- Learning models can be trained to forecast energy demand and generation with high accuracy, allowing for better scheduling and dispatching of resources.
- AI-based control systems can dynamically adjust grid parameters, such as voltage and frequency, to minimize energy wastage and optimize energy consumption.
- Intelligent algorithms can also enable better integration of renewable energy sources, improving the grid's overall energy mix and sustainability.

By leveraging these AI-powered capabilities, smart grid operators can enhance grid performance, improve energy efficiency, and effectively tackle critical challenges like electricity theft. The integration of AI technologies into smart grid systems can lead to significant improvements in reliability, sustainability, and customer satisfaction, paving the way for a more resilient and future-ready power infrastructure.

The findings and insights presented can serve as a valuable resource for decision-makers, researchers, and practitioners in the energy sector, guiding them towards the effective integration of AI-powered solutions for the betterment of power grid operations.

As the energy landscape continues to evolve, the integration of smart grid concepts and AI technologies will undoubtedly play a crucial role in shaping the future of the power industry. This dissertation has provided a comprehensive understanding of this synergistic relationship, paving the way for further advancements and innovations in the quest for a more efficient, reliable, and environmentally-conscious energy future.

Bibliography

[1] Martín Abadi et al. "Tensorflow: a system for large-scale machine learning." In: *Osdi*. Vol. 16. 2016. Savannah, GA, USA. 2016, pp. 265–283.

[2] Jennica Astronomo et al. "Development of electricity theft detector with GSM module and alarm system". In: *2020 IEEE 12th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)*. IEEE. 2020, pp. 1–5.

[3] Ekaba Bisong and Ekaba Bisong. "Google colaboratory". In: *Building machine learning and deep learning models on google cloud platform: a comprehensive guide for beginners* (2019), pp. 59–64.

[4] Nejia Boutarfaia et al. "Deep Learning for EEG-Based Motor Imagery Classification: Towards Enhanced Human-Machine Interaction and Assistive Robotics". In: *life* 2.3 (2023), p. 4.

[5] Robert Browder and Carrie Cross. "Welcome to Overleaf: A Brief Overview of Opportunities". In: (2018).

[6] Xueyuan Cui et al. "Two-Step Electricity Theft Detection Strategy Considering Economic Return Based on Convolutional Autoencoder and Improved Regression Algorithm". In: *IEEE Transactions on Power Systems* 37.3 (2022), pp. 2346–2359. DOI: 10.1109/TPWRS.2021.3114307.

[7] N. G. Eapen, K. G. Harsha, and A. Kesan. "Energy Intelligence: The Smart Grid Perspective". In: *Power systems*. Springer, 2023, pp. 35–74. DOI: 10.1007/978-3-031-15044-9_3. URL: https://doi.org/10.1007/978-3-031-15044-9_3.

[8] Yuanqi Gao, Brandon Foggo, and Nanpeng Yu. "A Physically Inspired Data-Driven Model for Electricity Theft Detection With Smart Meter Data". In: *IEEE Transactions on Industrial Informatics* 15.9 (2019), pp. 5076–5088. DOI: 10.1109/TII.2019.2898171.

[9] Walid Guettala et al. "Real Time Human Detection by Unmanned Aerial Vehicles". In: *2022 International Symposium on iNnovative Informatics of Biskra (ISNIB)*. IEEE. 2022, pp. 1–6.

[10] Lijuan Huang et al. "Electricity Theft Detection based on Iterative Interpolation and Fusion Convolutional Neural Network". In: *2022 7th International Conference on Power and Renewable Energy (ICPRE)*. 2022, pp. 567–571. DOI: 10.1109/ICPRE55555.2022.9960403.

[11] Leloko J. Lepolesa, Shamin Achari, and Ling Cheng. "Electricity Theft Detection in Smart Grids Based on Deep Neural Network". In: *IEEE Access* 10 (2022), pp. 39638–39655. DOI: 10.1109/ACCESS.2022.3166146.

[12] Quentin Louw and Pitshou Bokoro. "An Alternative technique for the detection and mitigation of electricity theft in South Africa". In: *SAIEE Africa Research Journal* 110.4 (2019), pp. 209–216.

[13] Carlos E Murillo-Sánchez et al. "Secure planning and operations of systems with stochastic sources, energy storage, and active demand". In: *IEEE Transactions on Smart Grid* 4.4 (2013), pp. 2220–2229.

[14] Ilyes Naidji et al. "Efficient Allocation Strategy of Energy Storage Systems in Power Grids Considering Contingencies". In: *IEEE Access* 7 (2019), pp. 186378–186392. DOI: 10.1109/ACCESS.2019.2957277.

[15] Ilyes Naidji et al. "Multi agent system-based approach for enhancing cyber-physical security in smart grids". In: *Proceedings of the the 33rd Annual European Simulation and Modelling Conference*, pp. 177–182.

[16] Ilyes Naidji et al. "Non cooperative game theoretic approach for residential energy management in smart grid". In: *The 32nd Annual European Simulation and Modelling Conference*. Ghent, Belgium, 2018, pp. 164–170.

[17] Ilyes Naidji et al. "Two-Stage Game Theoretic Approach for Energy Management in Networked Microgrids". In: *International Conference on Software Technologies*. Springer. 2019, pp. 205–228.

[18] Ilyes Naidji., Chams Choucha., and Mohamed Ramdani. "Decentralized Federated Learning Architecture for Networked Microgrids". In: *Proceedings of the 20th International Conference on Informatics in Control, Automation and Robotics - Volume 1: ICINCO*. INSTICC. SciTePress, 2023, pp. 291–294. ISBN: 978-989-758-670-5. DOI: 10.5220/0012215200003543.

[19] Ilyes Naidji. et al. "Cooperative Energy Management Software for Networked Microgrids". In: *Proceedings of the 14th International Conference on Software Technologies - ICSOFT*. INSTICC. SciTePress, 2019, pp. 428–438. ISBN: 978-989-758-379-7. DOI: 10.5220/0007965604280438.

[20] Alexander B Pacheco. "Creating Documents with LATEX and Overleaf". In: ().

[21] Mark Summerfield. *Programming in Python 3: a complete introduction to the Python language*. Addison-Wesley Professional, 2010.

[22] Ahmed Tibermacine and Selmi Mohamed Amine. "AN END-TO-END TRAINABLE CAPSULE NETWORK FOR IMAGE-BASED CHARACTER RECOGNITION AND ITS APPLICATION TO VIDEO SUBTITLE RECOGNITION." In: *ICTACT Journal on Image & Video Processing* 11.3 (2021).

[23] Imad Eddine Tibermacine et al. "Enhancing sentiment analysis on seed-IV dataset with vision transformers: a comparative study". In: *Proceedings of the 2023 11th International Conference on Information Technology: IoT and Smart City*. 2023, pp. 238–246.

[24] Guido Van Rossum and Fred L Drake Jr. *Python tutorial*. Vol. 620. Centrum voor Wiskunde en Informatica Amsterdam, The Netherlands, 1995.

[25] Xiaofang Xia et al. "ETD-ConvLSTM: A Deep Learning Approach for Electricity Theft Detection in Smart Grids". In: *IEEE Transactions on Information Forensics and Security* 18 (2023), pp. 2553–2568. DOI: 10.1109/TIFS.2023.3265884.

[26] Zhiqiang Zhao et al. "Privacy-Preserving Electricity Theft Detection Based on Blockchain". In: *IEEE Transactions on Smart Grid* 14.5 (2023), pp. 4047–4059. DOI: 10.1109/TSG.2023.3246459.

[27] Kedi Zheng et al. "A Novel Combined Data-Driven Approach for Electricity Theft Detection". In: *IEEE Transactions on Industrial Informatics* 15.3 (2019), pp. 1809–1819. DOI: 10.1109/TII.2018.2873814.

[28] Salah Zidi et al. "Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment". In: *Journal of King Saud University-Computer and Information Sciences* 35.1 (2023), pp. 13–25.

[29] Ray Daniel Zimmerman, Carlos Edmundo Murillo-Sánchez, and Robert John Thomas. "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education". In: *IEEE Transactions on power systems* 26.1 (2010), pp. 12–19.

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
MOHAMED KHIDER UNIVERSITY OF BISKRA
Faculty of Exact Sciences, Natural and Life Sciences
Computer Science Department

N° : RTIC_02/M2/2024

Dissertation

Presented to obtain the academic master's degree in Computer Science

Option : **Networks, Information and Communication Technologies (RTIC)**

Title: Federated Learning-based Solution for Smart Grid

Presented by:

- Grainat Nour Rayan

Supervisor : Dr. Ilyes Naidji

Jury :

Zerarka Nourelhouda	MCB	President
Hiouani Rima	MCB	Examiner
Ilyes Naidji	MCB	Supervisor

Academic Year : 2023-2024