Wireless Pilot Differential Relay (Thesis P. Report)

by samra Arshad

Submission date: 25-May-2025 11:57AM (UTC+0500)
Submission ID: 2544967221
File name: Wireless_Pilot_Differential_Realy.pdf (1.36M)
Word count: 12207
Character count: 75583

IOT BASED PILOT WIRELESS DIFFERENTIAL RELAY

Superior University

BSc. Electrical Engineering

Submitted By

Muhammad Nadir	**BEEM-F21-004**
Bilal Sadique	**BEEM-F21-005**
Tajammal Hussain	**BSEEM-F22-005**

Session: 2021-2025

ADVISOR:	**Dr. Manzoor Ellahi**
CO-ADVISOR:	**Engr. Muhammed Faiq**

Department of Electrical Engineering

Superior University

Lahore, Pakistan

IOT-Based Pilot Wireless Differential Relay

Submitted to Superior University,

Lahore in Partial fulfillment of the requirements for the award of a degree of

BSc. ELECTRICAL ENGINEERING

Muhammad Nadir

BEEM-F21-004

Bilal Sadique

BEEM-F21-005

Tajammal Hussain

BSEEM-F22-005

Session: 2021-25

Supervisor: Dr. Manzoor Ellahi

Co-Supervisor: Engineer. Muhammed Faiq

DECLARATION

We hereby declare that the research, design, and development of **IoT-Based Pilot Wireless Differential Relay** presented in this project is my original work. All the data, theories, and concepts used in this project have been correctly referenced, and due credit has been given to the sources from which the information has been extracted.

RESEARCH COMPLETION CERTIFICATE

It is ensured that the research work contained in this paper, titled **IOT BASED PILOT WIRELESS DIFFERENTIAL RELAY,** has been investigated and carried out by Tajammal Hussain, Muhammad Nadir, and Bilal Sadique for the degree of Bachelor of Science in Electrical Engineering.

Dr. Manzoor Ellahi	Dr. Mustafa Shakir (Chairman, DEE)
Internal Evaluator (Mr. H. Fuad Usman)	Internal Evaluator (Dr. Rao M. Asif)

ACKNOWLEDGEMENTS

In the name of ALLAH, the Most Gracious and the Most Merciful.

We are grateful to ALLAH ALMIGHTY for His infinite mercies and guidance. He has seen us through to the successful completion of this project. We would like to thank our parents for their solid support and encouragement, which motivated us right from the very beginning. Their love and care have always been our greatest strengths. We also thank those who contributed their efforts to this project called IoT-Based Pilot Wireless Differential Relay. Foremost, we must extend our thanks to our supervisor, Dr. Manzoor Ellahi, whose expert guidance, constant support, and valuable insights shaped our direction and success in this research. His encouragement and guidance have been fundamental in overcoming difficulties and ensuring the development of this work. We also extend our thanks to the Department of Electrical Engineering faculty members at Superior University, whose teachings have enriched our knowledge and provided the foundation for this work. We are profoundly grateful to our family and friends for their emotional support, patience, and belief in our abilities. Their encouragement has continued to keep us motivated and focused, even in tougher times. Additionally, we wish to acknowledge the constructive input of our colleagues and other members of the research team, whose thoughtful discussions and contributions improved the designs and technical aspects of this work. Finally, we thank the developers and manufacturers of the parts used in the system, such as IoT sensors, wireless communication modules, and cloud platforms. Their inventions have enabled us to realize the technological features of this relay system. Indeed, we are grateful to all those who have directly or indirectly helped us complete this project successfully.

DEDICATION

I dedicate this project to my family for their unwavering love, support, and encouragement throughout my academic journey. Their belief in me has been a constant source of motivation, and their sacrifices have made it possible for me to pursue my passion. I also dedicate this work to all the mentors, teachers, and peers who have guided and inspired me, helping me grow both personally and professionally. This project is a reflection of their influence and support.

ABSTRACT

This project proposes an IoT-based pilot wireless differential relay in power system protection. It will have a broader scope for the detection of faults with reduced installation cost and increased overall reliability using the latest in wireless communication technologies and integration with the IoT. Traditional differential relays, though quite efficient in detecting faults, are mostly of wired communications that are not only expensive but also less flexible. In the system, the wireless communication between the relay units is developed on Wi-Fi, LoRaWAN, or cellular networks that support real-time monitoring, fault detection, and system diagnostics in data transmitted to the cloud platform for further analysis or access remotely. This project explores an IoT-based pilot wireless differential relay system that integrates modern wireless communication and cloud technology to improve fault detection, reduce installation costs, and enhance real-time monitoring and predictive maintenance in electrical grids

Keywords:

IoT, Wireless Communication, Differential Relay, Power System Protection, Fault Detection, Real-time Monitoring, Predictive Maintenance, Cloud Platform, Smart Grid.

LIST OF ACRONYMS

Abbreviation	Full Form
IOT	Internet of Things
SCADA	Supervisory Control and Data Acquisition
ZIGBEE	ZIGBEE Protocol (a wireless communication standard)
LORA	Long Range (wireless communication technology)
Wi-Fi	Wireless Fidelity
GPS	Global Positioning System
GSM	Global System for Mobile Communications
RF	Radio Frequency
LAN	Local Area Network
WAN	Wide Area Network
PLC	Programmable Logic Controller
CT	Current Transformer
PT	Potential Transformer (Voltage Transformer)

Table of Contents

Declaration **2**

Research Completion Certificate 3

Acknowledgements 4

Dedication 5

Abstract 6

List of Acronyms 7

List of figures 11

List of Tables 12

CHAPTER 1 13

Introduction 13

1.1 Background 13

1.2 Problem Statement 14

1.3 Objectives 14

1. Methodology 15

1.5 Summary 16

CHAPTER 17

2.1 Literature Review 17

2.2 Summary 25

CHAPTER 3 26

3.1 Methodology 26

3.2 System Design and Conceptualization 26

3.3 Software Development 26

3.4 Hardware Development 28

3.5 System Integration 29

3.6 Testing and Evolution……29

3.7 Development and Implementation……30

3.8 Analysis and Results……30

3.9 Simulation on proteus……30

3.10 Arduino IDE Simulation code……31

3.11 System Components in Proteus……40

3.12 System Testing and Validation……40

3.13 Summary……44

Chapter 4……45

4.1 Objective……45

4.2 Parameters……45

4.3 Differential Protection Principle……45

4.4 Wireless Communication Channel Modeling……46

4.5 Differential Relay Operating Time……46

4.6 Circuit Breaker Tripping Time (t_{CB})……46

4.7 Total Fault Clearing Time……46

4.8 Performance of parameters……46

4.9 Summary……49

Chapter 5……50

5.1 Introduction……50

5.2 Objective……50

5.3 Current Sensing Unit……50

5.4 Wireless Communication Module……51

5.5 Relay Driver and Trip Circuit……52

5.6 Components Placements (Section 1) ……52

5.7 Without Fault Detection (Section 2)……..….53
5.8 Fault Detection (section 3)……..…54
5.9 Costing……..…..55
5.10 Summary..……...……..…56
Chapter 6……..……...57
6.1 Objective……..……..57
6.2 Differential Protection Logic……....57
6.3 Sensor Data Acquisition Module……..…57
6.4 IoT Integration and Monitoring……...…..58
6.5 Future Work……..……58
6.6 Comparison……61
References……..……..62

List of Figures

Figure 1.1: A novel design of wireless-powered IRS-aided relay networks.....14
Figure 3.1: Methodology Block Diagram……..…27
Figure 3.2: Hardware Flowchart diagram……..28
Figure 3.3: Simulation on Proteus of IoT-Based Pilot Wireless Differential Relay……..31
Figure 3.4: Code output……..40
Figure 3.5: System Flow chart for Proposed System.....43
Figure 4.1: An IoT-Based Pilot Wireless Differential Relay detecting a fault……..…47
Figure 4.2: An IoT-Based Pilot Wireless Differential Relay operates normally……..…48
Figure 5.1: Sensor Data Acquisition Module Flow Chart Diagram……..…51
Figure 5.2: Relay Driver and Trip Circuit……..……..52
Figure 5.3: Hardware Fabrication……..……53
Figure 5.4: When IoT-Based Pilot Wireless Differential Relay detecting a fault……..54
Figure 5.5: IoT-Based Pilot Wireless Differential Relay in Fault condition……55

List of Tables

Table 2.1: Proposed work.....22
Table 5.1 Components in Proteus……..…….31
Table 6.1: Costing…….55
Table 6.1: Relays Comparison……61

Chapter 1

1.1 Introduction

Protecting electrical power systems is critical for ensuring their stability and minimizing downtime. Traditional protection systems, such as differential relays, often rely on wired communication, which can be costly and inflexible. This project explores an IoT-based pilot wireless differential relay system that integrates modern wireless communication and cloud technology to improve fault detection, reduce installation costs, and enhance real-time monitoring and predictive maintenance in electrical grids [1].

1.2Background

Electrical power systems are complex networks; they need some effective and reliable protection mechanisms for safe operation and to avoid damage that may occur to the electrical equipment. The principle of differential relays, which has been in use for quite a long period, has conventionally been applied for the protection of electrical circuits, particularly at substations, against the incidence of faults. This system is necessary for preventing possible damage to the transformers, generators, and other major components in the network [2].

Traditional differential relays have conventionally utilized wired communication in transmitting current information between various relay units and monitoring systems. Although such a setup has worked effectively in the detection of faults, there are a number of limitations associated with high installation and maintenance costs, limited expandability, and rigidity within system configuration. Traditional systems are also quite passive; operators need to manually inspect the occurrence of a fault and diagnose it, which delays things and increases downtime [3].

The IoT and wireless communication technologies are offering a huge opportunity to make differential relays more functional. The IoT devices can collect and transmit real-time data for remote monitoring and control. The reduction in the requirement of extensive wiring is achieved with wireless communication, providing flexibility in system design and expansion. Cloud-based platforms can analyze the data, making predictive maintenance possible and faults detectable faster [4].

Based on these advances, an IoT-based pilot wireless differential relay system has the possibility of surmounting the deficiencies of the wired systems. Such a system will not only provide better fault detection but also allow real-time information, enable predictive maintenance, and reduce the costs of

operations to make it an efficient and scalable solution for modern electrical power networks.

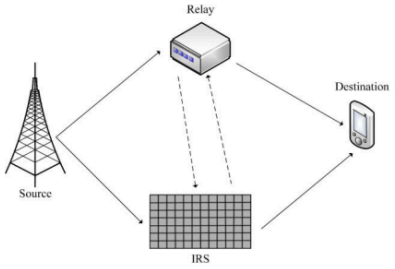


Figure 1.1: A novel design of wireless-powered IRS-aided relay networks

1.3 Problem Statement:

Protection of electrical power systems, especially within substations and transmission networks, is essential to ensure operational stability and minimize equipment damage during faults. Traditional differential relay systems, although effective, rely on wired communication links that are costly to install and maintain, lack flexibility, and are slower in responding to faults due to limited real-time capabilities. Additionally, these systems are largely reactive, requiring manual fault analysis that leads to extended downtimes. As power systems become more complex with the integration of renewable energy sources and smart grid technologies, there is a growing need for more adaptive, cost-effective, and intelligent protection mechanisms. An IoT-based pilot wireless differential relay system offers a promising solution by utilizing wireless communication and real-time data from IoT sensors to enable faster fault detection, remote monitoring, and predictive maintenance. This approach can significantly enhance the efficiency (10%), scalability, and reliability of modern power system protection while reducing reliance on conventional wired infrastructure.

1.4 Objectives

1.4.1 Research Objectives:

- That integrates modern communication technologies and IoT sensors for real-time monitoring and fault detection in electrical circuits.
- To replace wired communication systems with wireless communication (such as Wi-Fi, LoraWAN, or cellular networks) to reduce installation and maintenance costs while improving

flexibility and scalability in the relay system.

- For collecting, storing, and analyzing data from IoT sensors, enabling remote access, real-time monitoring, and predictive maintenance capabilities.
- By leveraging IoT sensors to continuously monitor critical parameters (e.g., current, voltage) and enable faster response times in the event of system anomalies.
- By incorporating predictive maintenance algorithms that analyze historical data and trends to anticipate potential faults before they occur, thereby minimizing downtime and extending the life of power system components
- In comparison to traditional wired systems in terms of cost, efficiency, scalability, and fault response time.

1.4.2 Industrial Objectives:

- In power grid protection by replacing traditional wired differential relay systems with cost-effective wireless communication solutions, minimizing the need for extensive wiring and infrastructure.
- Electrical power systems by providing faster fault detection and more accurate protection, which ensures timely isolation of faults, minimizing the risk of equipment damage and improving system uptime.
- Capabilities in substations and power networks by leveraging real-time data from IoT sensors, thereby allowing operators to anticipate and address potential issues before they lead to costly downtime or failure.
- In power protection systems by facilitating easier integration of new devices and expansion of the protection network without the need for extensive reconfiguration of the existing system, thus supporting the growth of smart grids.
- Through continuous real-time monitoring and analysis, enabling operators to make data-driven decisions that enhance the operational efficiency and longevity of electrical equipment.

1.5 Methodology

The methodology for developing the **IoT-Based Pilot Wireless Differential Relay** system involves several key stages, including system design, hardware and software development, integration, testing, and evaluation. The approach combines traditional differential relay principles with modern IoT technologies and wireless communication protocols. The following steps outline the methodology for this project:

1.5.1 System Design and Conceptualization

This stage involves designing the overall architecture of the IoT-based relay system to ensure it meets the necessary technical and functional requirements:

- Identify the key requirements of the system, such as real-time fault detection, high-speed communication, low latency, scalability, and reliability.
- Choose sensors capable of measuring electrical parameters like current and voltage accurately and in real-time. Sensors should also be durable and compatible with IoT protocols.
- Select efficient wireless communication protocols (e.g., Zigbee, Wi-Fi, LoRa, or 5G) based on factors like range, bandwidth, and power consumption.
- Design a secure and scalable cloud platform to store, process, and analyze sensor data while enabling remote monitoring and control.

1.5.2 Key Strategies for Achieving the SDGs

- IoT-based wireless differential relays improve energy efficiency by optimizing grid performance and reducing energy waste.
- They enhance grid reliability through real-time fault detection and automated responses to issues, minimizing downtime.
- These systems support smart grids, enabling integration with renewable energy sources and reducing carbon emissions.
- They contribute to SDG 7 (Affordable and Clean Energy), SDG 9 (Industry, Innovation, and Infrastructure), and SDG 13 (Climate Action).
- By improving energy distribution and reducing operational costs, they make energy use more efficient and sustainable.

1.6 Summary

The development of the IoT-Based Pilot Wireless Differential Relay presents a big milestone in electrical power system protection and fault detection. Integration of IoT sensors, wireless communication, and cloud-based analytics in this system provides a more effective, scalable, and economically viable solution compared to the conventional wired differential relay. It enhances the reliability and safety of electrical grids, from monitoring in real-time to fault detection at higher accuracy and remote control with predictive maintenance. Key benefits include reduced installation and maintenance costs, more flexibility in the expansion of systems, faster fault detection and isolation, and predictive maintenance to avoid costly downtime and equipment failure.

CHAPTER 2

LITERATURE REVIEW

2.1 Literature Review

Recent literature highlights the growing potential of IoT-based protection systems to revolutionize grid management by enhancing efficiency, resilience, and reliability in modern power networks. Several studies have demonstrated that integrating IoT technologies enables real-time monitoring and faster fault detection, significantly improving system responsiveness. However, researchers emphasize that future advancements should focus on incorporating artificial intelligence (AI) and machine learning (ML) algorithms to further optimize fault detection, decision-making, and system control. These intelligent techniques are expected to enhance the energy efficiency, accuracy, and security of protection mechanisms, offering adaptive responses to evolving grid conditions. Overall, existing research suggests that IoT-based systems, when combined with AI and ML, have the potential to become a transformative solution for next-generation smart grid protection [5].

Recent advancements in Internet of Things (IoT)-based fault detection and isolation techniques have significantly enhanced the reliability and efficiency of modern electrical power systems. IoT technologies, through the integration of smart sensors and wireless communication networks, enable continuous real-time monitoring of critical electrical parameters such as voltage, current, and frequency across the grid. This facilitates the early detection of anomalies like short circuits, overloads, or equipment malfunctions, allowing operators to implement timely isolation measures and prevent cascading failures. Studies have demonstrated that IoT-enabled systems not only improve situational awareness but also support predictive maintenance and autonomous decision-making, contributing to the overall stability and resilience of power networks [6]. It highlights that machine learning and artificial intelligence algorithms are increasingly used for fault detection to analyze the huge amount of data being generated from the IoT sensors. Furthermore, it identifies the various challenges faced by the IoT-based fault detection system related to security, accuracy in data, and reliability in communication protocols for flawless performance in remote or harsh environmental conditions, Despite these, the paper has concluded that IoT integrated with mechanisms of advanced fault detection and isolation is one promising direction towards the future smart grid, thereby providing significant improvements in fault management, predictive maintenance, and overall system performance.[7]. Where the key issue is in the integration of wireless technologies within the differential protection that conventionally is wired for communication towards fault detection and

isolation in the power system. Differential protection in a wireless format provides several advantages, including reduction in installation and maintenance costs and enhanced scalability besides the flexibility added in the management of the grids. The paper discusses the diversity of wireless protocols that can be used for these kinds of systems, including Wi-Fi, Zigbee, LoRa, and Cellular networks, discussing their fit for different configurations regarding range, reliability, and consumptions [8].

The integration of Internet of Things technology with differential protection in intelligent grid environments. The reviewed literature bends towards how the introduction of IoT-based differential protection will improve the fault detection, isolation, and security of power systems through real-time monitoring and communication between different elements of the grids. IoT sensors, which continuously collect and transmit electrical parameters like current and voltage, enable the continuous tracking of the health of the system, detecting abnormalities that indicate faults or possible faults [9]. This paper presents an extensive review of the integration of Internet of Things (IoT) and cloud computing technologies in power system protection. The paper underlines the extreme transformation potential of combining IoT with cloud-based solutions to enhance the fault detection, monitoring, and management of electrical networks. IoT sensors installed in the power grid could monitor system performance data in real time and send it back to a central cloud platform for various parameters such as voltage, current, and frequency. The cloud architecture is capable of advanced data analytics, where fault prediction, grid health assessment, and optimization of system performance may be carried out using historical data. The review debates that the cloud-based IoT systems offer better scalability, flexibility, and cost-effectiveness than traditional protection systems, which are based on fixed, locally deployed infrastructure [10].

The integration of the Internet of Things and wireless communications in protection systems related to smart grids. Emphasis is given to IoT-based smart grid protection, presenting several advantages regarding real-time monitoring and estimation of fault events and enhancement in the power grid's reliability. IoT sensors permit uninterrupted monitoring of various critical parameters like voltage, current, and flow of power-so that information may regularly flow to a central control system over wireless links for analysis. According to the authors, wireless communication technologies that could provide the flexibility and scalability needed in deployment with diverse configurations at large numbers for protection systems include, among others, Wi-Fi, Zigbee, and Low Power Wide Area Networks (LPWAN) systems depicted.[11] Recent research underscores the transformative potential of IoT-enabled monitoring systems in revolutionizing fault identification and diagnostics within electrical power systems. Scholars argue that deploying distributed IoT sensors across grid infrastructure capable of real-time tracking of

voltage, current, frequency, and other critical parameters can significantly enhance diagnostic accuracy and speed emphasize that IoT integration facilitates centralized data aggregation, enabling predictive analytics when combined with machine learning (ML) algorithms. [12]. Deal with Internet of Things incorporated into smart protection and control applications for a power grid network. According to the authors, an IoT enabled protection system allows much enhancement in operational efficacy, reliability, and fault tolerance in an electric network. The enhanced capabilities of these systems enable monitoring through the usage of IoT sensors that monitor and collect data on critical parameters of the grid, such as voltage, current, and frequency, in real time; this has ensured better fault detection and isolation. [13].

The recent developments within IoT-based protection systems of a power grid and how the advent of IoT could be exploited toward better fault detection, monitoring of the system, and maintenance of a modern power grid. It throws light on the role of IoT sensors that continually monitor electrical parameters like voltage, current, and temperature, therefore furnishing real-time data that enhances grid visibility for quicker response times to faults. The paper has shown how IoT technologies can help in enhancing grid reliability by facilitating real-time monitoring and fault management of the grid. IoT-based systems use a network of sensors to collect data regarding various grid parameters, including current, voltage, and power quality, which is then radio-transmitted for analysis. The authors have pointed out that such a data-driven approach facilitates early detection, speedy isolation, and precise location of faults with a substantial reduction in downtime, consequently improving overall grid stability [14].

The state of the art in IoT-based fault detection and isolation methodologies applied to power networks. The authors discuss how IoT technologies such as sensors and wireless communication networks are revolutionizing the way electrical grids detect, diagnose, and isolate faults. They further cited that there is a distribution of IoT sensors throughout the grid for monitoring the essential electrical parameters in real-time, such as voltage, current, and frequency. This sensor sends out data to either centralized systems or cloud platforms to enable deeper analytics-based insights for early detection of faults to reduce response time accordingly. [15]. Some challenges of integration of the Internet of Things technologies into the field of protection systems within power grids. It is presented that in the IoT-based protection system, there is involved a network of interconnected sensors and communication devices used for monitoring and control of the grid performance in real time. Such systems enable better fault detection, speedier isolation, and thus easier grid management in large, complex grids that need high levels of reliability [16]. The role of Internet of Things-driven smart protection schemes in the modernization of power grid systems. The authors have indicated that a set of innovations has been made possible by IoT technologies in real-time

data collection, advanced monitoring, and enhanced fault detection and isolation processes. Integrating IoT sensors into the power grid systems facilitates constant surveillance of critical electrical parameters such as current, voltage, and power quality, which is vital for grid stability. This radio-frequency information is transmitted, in most cases, to a cloud-based platform where more developed analytics and machine learning algorithms process and analyze this for anomaly detection to quickly find the faults. [17].

An insight into the trends of advancement of IoT-based protection schemes for differential protection and fault diagnosis of smart grids. in 2024. The authors have discussed how the integration of IoT sensors, communication networks, and real-time data analytics has significantly improved the efficiency in differential protection systems designed for detecting and isolating faults within an electrical grid. Such IoT-based systems provide for continuous monitoring of grid parameters like voltage, current, and phase shifts, offering better accuracy in fault detection compared to conventional protection methods. These systems send live information on the status of the grid to the operator by wireless transmission of data to centralized systems [18]. The development of IoT-based protection systems for smart grids. The authors of the paper dated 2025 go into great detail regarding the enhancements, challenges, and future prospects. The authors point out the crucial impact of IoT on power grids, changing traditionally applied protection systems. Interconnected sensors and wireless communication are used to support real-time monitoring, fault detection, and isolation. In this way, IoT sensors are being considered for integration into the different components of the grid to provide increased situational awareness and remote monitoring of critical parameters, ultimately leading to enhanced operational efficiency [19].

IoT-driven smart fault detection and protection systems for smart grids; thus, it gives the present trend in this field of study and future direction for the research. The authors have pointed out the increasing role of IoT technologies for enhancing the reliability and performance of power grids by enabling real-time monitoring of electrical parameters such as current, voltage, power flow, and frequency. By deploying IoT-based sensors across grid infrastructure, operators can get continuous data in high resolution, thus enabling the detection of faults more quickly and precise fault isolation [20]. the integration of IoT-based technologies in protection systems for a smart grid both on challenges and future opportunities. The authors reveal how IoT-based technologies have totally changed the classic schemes of the grid protection to include real-time continuous monitoring of voltage, current, power quality, and even frequency in real time. With IoT sensors integrated into the grid, operators can draw from a multitude of data that could enable them to precisely detect the fault, isolate it quickly, and restore the system much faster than

otherwise during a disturbance. The review puts great emphasis on wireless communication networks for efficient data transmission over the entire grid, thus enabling remote monitoring and control of the grid [21]. The IoT-based differential protection systems, discussing mainly their applicability and relevance to smart grids. The authors point out the necessity to explore the current situation of increasing adaption of IoT technologies in power systems and their potential for enriching conventional differential protection mechanisms. IoT-based protection schemes realize real-time monitoring fault detection by deploying a network of distributed sensors that measure important parameters such as current, voltage, and phase angles in a continuous manner [22]. In the next step, this information is wirelessly relayed to the centralized control systems for analysis; thus, the faulty portions can be quickly detected with high accuracy for faster localization and quick recovery of the system. The implementation of IoT-based protection systems for power grids highlights important techniques and recent trends [23].

How traditional grid protection has changed due to the technologies of IoT for enabling real-time monitoring and fault detection capabilities. IoT-based systems can offer, due to the integrated network of smart sensors within the grid infrastructure, real-time anomaly or fault detection through captured critical electrical parameters of voltage, current, and frequency. This review will look into how the use of wireless communication networks in wireless sensor networks enables seamless data transmission of sensor information to centralized platforms that are then able to quickly and precisely diagnose faults, thus significantly reducing downtime for the grid while increasing the overall system reliability [24]. Future trends in IoT-based protection systems of the power grid. They have indicated that IoT technologies in ensuring stability and reliability within the grid will have a transformative potential. Authors deal with how IoT-enabled systems are redesigning the power grid protection by enhancing the monitoring capability, real-time fault detection, and dynamic response mechanisms thereof. The integration of IoT sensors at different parts of the grid permits the continuous collection of data regarding essential electrical parameters such as voltage, current, and frequency; such data is transmitted wirelessly for analyses at cloud-based platforms. The paper emphasizes how the application of machine learning and artificial intelligence algorithms to this data enables better fault detection, predictive maintenance, and optimized system responses that can reduce operational costs by an order of magnitude and make the grid resilient [25].

Table 2.1: Proposed Table

Reference	Year	Objective	Methodology	Limitation
5	2020	To explore IoT-based differential protection systems for smart grids.	Analysis of IoT-enabled systems for fault detection and isolation in grids. Case studies and experimental setups.	Lack of standardization in IoT devices, communication security concerns.
6	2021	To investigate the role of IoT in fault detection and isolation in power systems.	Review of IoT applications in power systems, focusing on real-time fault detection, communication networks, and system optimization.	High data volume, security issues, and challenges with real-time implementation.
7	2021	To examine wireless differential protection systems for smart grids and their challenges.	Detailed analysis of wireless communication protocols and IoT sensor integration for differential protection systems.	Issues of scalability, security in wireless communications, and sensor reliability.
8	2022	To analyze the integration of IoT for enhanced grid	Case study reviews of IoT applications, data analytics, and	Data security concerns and real-time data analysis challenges.

		protection and management.	machine learning techniques applied to grid protection.	
9	2023	To review IoT-based protection systems for improving power grid resilience.	Review of IoT technologies for monitoring, fault isolation, and prediction of faults, using case studies and simulations.	Difficulty in maintaining sensor reliability and system interoperability.
10	2023	To analyze the trends in IoT for grid protection and monitoring.	Systematic literature review of various IoT-based protection systems, focusing on fault detection, and predictive maintenance.	Interoperability issues, need for robust data analytics and machine learning models.
11	2023	To investigate IoT-enabled smart grid systems and fault management.	Use of IoT sensors and machine learning algorithms to enhance grid performance and fault detection capabilities.	Limited coverage of cybersecurity solutions, integration complexity.
12	2024	To evaluate the integration of IoT for differential protection in smart grids.	Experimental analysis and simulation of IoT sensors for differential	Sensor accuracy, reliability, and high cost of IoT sensors in large-scale deployment.

			protection in grid systems, using real-time data processing.	
13	2024	To explore IoT-based fault detection and protection in power grids and its applications.	Review of case studies focusing on fault diagnosis, predictive maintenance, and data analytics through IoT.	Security vulnerabilities in data transmission, challenges in large-scale system integration.
16	2024	To review smart fault detection systems for power grids driven by IoT and machine learning technologies.	Systematic review of IoT-based fault detection systems and integration with machine learning for improved fault prediction.	Issues with data privacy, sensor calibration, and integration of diverse devices.
18	2024	To analyze the role of IoT in enhancing protection systems for electrical grids.	Exploration of real-time fault detection and monitoring systems using IoT sensors, communication technologies, and machine learning algorithms.	Limited implementation in remote grid areas, high latency in data processing.

19	2025	To examine IoT-enhanced protection schemes in power grids and their future directions.	Review of emerging IoT technologies, fault detection, and data analytics, with future trends in smart grid protection schemes.	Lack of standardization across IoT platforms and security risks in communication networks.
22	2025	To investigate the impact of IoT-based differential protection in smart grid systems and the challenges in system reliability.	Review of experimental setups and case studies on IoT-based differential protection systems with a focus on fault detection and system reliability.	Issues with the integration of heterogeneous IoT devices and the security of data transmission channels.
24	2025	To explore the role of IoT and cloud computing in the optimization of power grid protection systems.	Analysis of the application of cloud computing in IoT-based grid protection systems for real-time monitoring, fault detection, and system optimization.	High-volume data management challenges, cyber security risks, and sensor calibration problems.

25	2025	To review future trends and advancements in IoT-based protection systems for power grids.	Literature review on emerging trends in IoT-based protection systems, including 5G, edge computing, and predictive fault detection techniques.	Security and privacy concerns, difficulty in large-scale deployment, and interoperability of IoT devices from different manufacturers.

2.2 Summary

In conclusion, the integration of Internet of Things (IoT) technologies into power grid protection systems has proven to be highly beneficial, offering improvements in reliability, resilience, and overall grid efficiency. IoT-based systems enable real-time monitoring, fault detection, and predictive maintenance, which significantly enhance the speed and accuracy of fault isolation, reducing grid downtime and improving operational performance. The integration of heterogeneous devices and issues related to the standardization of communication protocols. These challenges hinder the widespread adoption of IoT-based protection systems and require ongoing research and innovation. Overcoming these barriers, particularly through advancements in secure communication technologies, machine learning, and low-latency communication methods like 5G and edge computing, will be crucial for the future development of IoT-enabled power grid protection. Overall, while IoT presents transformative potential for the evolution of power grids, continued efforts in addressing technical, security, and scalability challenges will be essential to fully realize its capabilities in enhancing grid resilience and efficiency.

Chapter 3

Methodology

3.1 Methodology:

The methodology for developing the IoT-Based Pilot Wireless Differential Relay system is structured to address the core aspects of system design, hardware and software development, integration, testing, evaluation, and deployment.

3.2 System Design and Conceptualization:

The first phase of the methodology focuses on planning and designing the IoT-based differential relay system. The following activities are carried out.

- This step involves understanding and defining the functional and non-functional requirements of the IoT-based differential relay system. It includes identifying the need for fault detection, protection, communication, and cloud integration, as well as setting specifications for sensor types, wireless communication, and power supply.
- Choosing appropriate IoT sensors is crucial for gathering the required data to detect faults and monitor the system's performance. These sensors measure parameters such as current, voltage, and frequency. The selected sensors must be capable of operating in the specific environment of power grids while ensuring high accuracy and reliability.
- A robust and reliable communication protocol is needed to transmit data from the IoT sensors to the relay and, ultimately, to the cloud. This could involve selecting between protocols like MQTT, Zigbee, LoRa, or cellular networks, considering the range, data transmission rate.
- A cloud platform is essential for storing and analyzing the data received from the sensors. The platform facilitates centralized monitoring, fault diagnostics, and predictive maintenance. It allows for seamless data integration and provides real-time access to system performance data.

3.3 Software Development

The software components of the system are developed to enable data collection, fault detection, and system operation. This includes:

- Software is designed to manage the collection of data from IoT sensors in real time. This data is vital for monitoring electrical parameters, detecting anomalies, and identifying faults in the power grid. The software ensures that data is transmitted reliably to the relay and cloud systems.

- The core of the differential relay system is its ability to detect faults. The software incorporates algorithms that analyze the sensor data to identify abnormal behavior in the grid, such as short circuits, overloads, or ground faults, and activate the relay to isolate the faulty area.
- Software ensures seamless communication between the relay unit and the cloud platform, where the data is stored, processed, and analyzed. Cloud integration enables centralized monitoring, data analysis, and remote access to grid status and fault events.
- A user-friendly mobile or web application is developed for remote monitoring and control. Firstly, a pseudo power system network (the protected zone) is considered consisting of series connection of two 60 W incandescent light bulbs connected across a 240 V AC source. So, in normal operating condition, the two bulbs should divide the 240 V between themselves and glow with about 120 V each, resulting in a lower brightness shown in Figure 3.1 So, the current entering into and leaving the zone in no fault condition should be equal.
- A fault, a Phase to Neutral fault by tapping between the two light bulbs and connecting this to the neutral. This will cause one of the bulbs to be disconnected from the system. Then the disconnected bulb will turn off, and the other (Bulb 2) will glow with a voltage of 240 V. In this condition current entering the zone is unequal to the current leaving the zone. To sense the currents on both sides of the protected zone, Arduino, Current Sensor, and the Wi-Fi module was used.

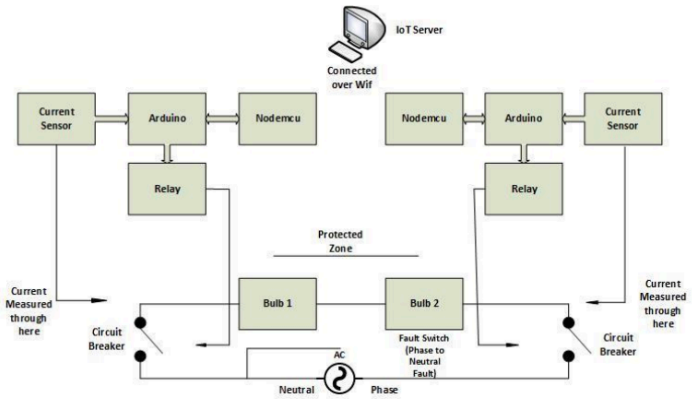


Figure 3.1: Methodology Block Diagram

3.4 Hardware Development

In this phase, the necessary hardware components are selected, assembled, and integrated to create the physical system. This includes:

- **Differential Relay Unit**: The differential relay is the core component that compares the current entering and leaving a section of the grid. It detects faults by identifying any discrepancies between the two and isolates the faulty section to prevent further damage.
- **Wireless Communication Module**: This module is responsible for facilitating the transmission of data from the differential relay unit to the cloud platform and potentially to control systems. It ensures that the system can operate remotely and allows operators to monitor grid status without being physically present.
- **Circuit Breaker Integration**: The system integrates a circuit breaker that can disconnect parts of the grid during a fault event. The relay communicates with the circuit breaker to ensure that the appropriate action is taken in case of a fault, maintaining grid safety and stability.
- **Power Supply and Backup**: A reliable power supply is necessary to ensure uninterrupted operation of the system, particularly in case of power outages. Backup power solutions like batteries or uninterruptible power supplies (UPS) are included to guarantee continuous system performance.

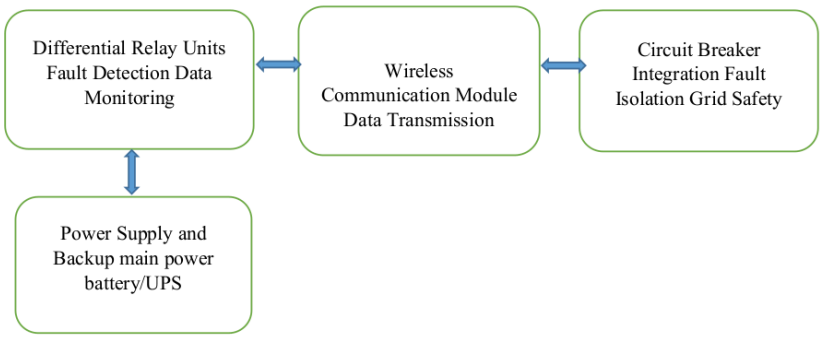


Figure 3.2: hardware Flowchart diagram

3.5 System Integration

System integration involves combining the hardware and software components into a fully functional system:

- **Wireless Data Transmission**: Data transmission between the IoT sensors, differential relay, and cloud platform is ensured. Wireless data transmission protocols are optimized to handle large volumes of data while maintaining low latency and energy efficiency.
- **Relay and Cloud Platform Communication**: The relay unit is integrated with the cloud platform to transmit fault alerts and data. This allows operators to monitor the grid remotely, analyze system performance, and intervene when necessary.
- **Testing of Fault Detection**: Once the system is integrated, fault detection is tested to ensure that the relay unit reacts promptly to real faults and that it isolates the faulty area effectively without impacting the overall grid. Simulated faults may be introduced to evaluate system performance.

3.6 Testing and Evaluation

This phase ensures that the system works as intended and meets performance requirements:

- **System Performance Testing**: The entire IoT-based protection system is subjected to extensive performance testing to assess its responsiveness, reliability, and accuracy. Tests are conducted under various operating conditions to ensure it can function correctly in a variety of real-world scenarios.
- **Real-time Fault Detection**: The system is tested for its ability to detect faults in real time. The goal is to ensure that the system can immediately identify issues and trigger protective actions, such as isolating the faulty grid section.
- **Scalability and Flexibility**: Testing also assesses the system's scalability and flexibility to handle increased data volumes, new IoT devices, or future updates. The system must be capable of expanding as the grid grows or as additional sensors and devices are integrated.
- **Cost-Benefit Analysis**: A cost-benefit analysis is performed to assess the financial feasibility of deploying the system. This analysis compares the cost of implementing the IoT-based protection system with the benefits it brings, such as improved grid reliability, reduced downtime, and maintenance savings.
- **Feedback and Refinement**: After testing, feedback is collected from stakeholders, such as operators and maintenance personnel. This feedback is used to refine the system's design and functionality before it is deployed in real-world conditions.

3.7 Deployment and Implementation

This phase focuses on the deployment and operational use of the system:

- **Pilot Deployment**: The system is deployed in a controlled environment or a pilot project within a segment of the power grid. This allows for practical testing in real-world conditions and helps identify any remaining issues before full-scale implementation.
- **Monitoring and Evaluation**: The system's performance is continuously monitored during the pilot deployment. Data is gathered on its effectiveness in fault detection, system response times, and reliability. Adjustments are made as necessary based on the findings.
- **Final Documentation**: Once the system is successfully deployed and evaluated, comprehensive documentation is created, covering system design, installation procedures, user guides, and maintenance instructions. This documentation ensures that the system can be replicated and maintained over time.

3.8 Analysis and Results

In this phase, the system's performance is analyzed, and comparisons with traditional systems are made:

- **Performance Metrics**: Key performance indicators (KPIs) such as fault detection speed, system uptime, response time, and cost savings are measured and analyzed to determine the effectiveness of the IoT-based protection system.
- **Comparison with Traditional Systems**: The results of the IoT-based system are compared with traditional protection systems. This comparison helps highlight the advantages, such as improved fault detection, faster response times, and lower operational costs, as well as any limitations that may need to be addressed in future iterations.

3.9 Simulation on Proteus

Before implementing the system, it is simulated in Proteus to verify its functionality. To simulate a system that detects differential current in a power line using current sensors, processes the data with microcontrollers, and transmits data via wireless modules to detect faults in real time.

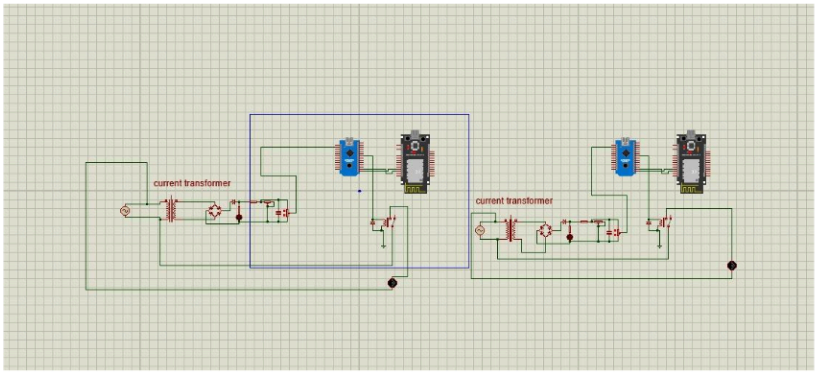


Figure 3.3: Simulation on Proteus of IoT-Based Pilot Wireless Differential Relay

3.10 System Components in Proteus:

In Proteus, designing an IoT-based Pilot Wireless Differential Relay involves simulating key hardware and communication components. Below is a breakdown of the essential system components you would need:

Table 3.1: Components in Proteus

Block	Components
Current Sensing	Current Transformer
Signal Conditioning	Op-amp (for amplification and filtering)
Analog-to-Digital Conversion	Built into microcontroller (e.g., Arduino UNO, ESP32)
Microcontroller	Arduino UNO, ESP8266
Wireless Transmission	ESP8266 (Wi-Fi), nRF24L01 (RF), HC-12 (long range)
Display/Fault Output	LED, LCD (16x2 or OLED), or serial monitor
Microcontroller	Arduino UNO, ESP8266

3.11 System Testing and Validation

Testing and Validation

Testing and validation are critical stages in the development of the IoT-Based Pilot Wireless Differential Relay system to ensure that it performs as intended and meets the required safety, reliability, and operational standards. This phase involves a series of steps designed to assess the system's effectiveness,

troubleshoot any potential issues, and optimize performance before deployment. The key aspects of testing and validation are as follows:

- **Real-time Fault Detection**: Real-time fault detection is one of the core functions of the IoT-based differential relay system. In this phase, the system is subjected to different fault scenarios (e.g., short circuits, overloads, ground faults) to ensure that it can detect issues in real-time and take appropriate corrective actions, such as triggering the relay to disconnect the faulty grid segment. The system is tested to ensure that faults are detected and isolated accurately and promptly without affecting the overall grid operation.
- **Scalability and Flexibility**: As the system is expected to operate across large power grids, scalability testing is crucial. This testing evaluates the system's ability to expand and handle increased data loads, additional sensors, or new devices without compromising performance. This includes testing the ability to support multiple IoT sensors, handle large volumes of data, and manage more complex grid configurations.
- **Cost-Benefit Analysis**: Testing and validation also include an economic evaluation of the system. This cost-benefit analysis compares the cost of implementing the IoT-based protection system against the benefits it offers, such as reduced downtime, improved grid reliability, and reduced maintenance costs. It helps determine whether the system provides a sufficient return on investment (ROI) and is financially viable for wider adoption in power grid infrastructure.
- **Feedback and Refinement**:

feedback is collected from stakeholders, including grid operators and technical personnel who have worked with the system. This feedback is invaluable for identifying areas of improvement in both hardware and software components. Refinements are made based on real-world usage, such as optimizing the fault detection algorithm, enhancing user interfaces, and addressing any operational difficulties identified during testing. The iterative feedback loop ensures that the system becomes more efficient and user-friendly.

As shown in figure 3.3, here two gauges are used to show the measured values of currents labeled as Current 1 and Current 2. Two buttons named „TRIP" and „RESUME" are used to operate the circuit breakers to isolate the protective zone during fault and to resume the system when fault is cleared respectively. The compact modules consist of Adriano, Current Sensor, NodeMcu and Relay module. The current sensor is connected in series with the line. This sensor senses the amount of current under the

command of Arduino. To send the value of measured current to the web server, we have used Wireless Wi-Fi protocol using the NodeMcu Wi-Fi Module. The NodeMcu is configured to communicate with the specified server of Adafruit. Thus, we are able to monitor the values on the dashboard provided by Adafruit IO from anywhere in the world by providing verified password to the server. In normal operating condition, the currents shown in the system in Fig. 3.3 should be close or equal. But in case of fault, the currents should differ from each other and the difference should be very large.

By “observation" it is possible for a human operator to read the currents and determine the fault as stated in the flowchart in Fig.3.3, step 6, „Read the values of currents I1 and I2 manually". In fault condition we need to isolate the faulty section and then clear the fault and after clearing we can resume the system operation again. Fig 3.3. This will cause the relay to operate and isolate the protected zone from the rest of the system via wireless internet from anywhere in the world. After the fault is cleared, we should press the „RESUME" button to resume the system. This will cause the relay to connect the protected zone to the rest of the system as it was in the normal condition. This observation of currents and controlling of the system by Tripping and Resuming operations all are done remotely via IoT but till now in this work but manually.

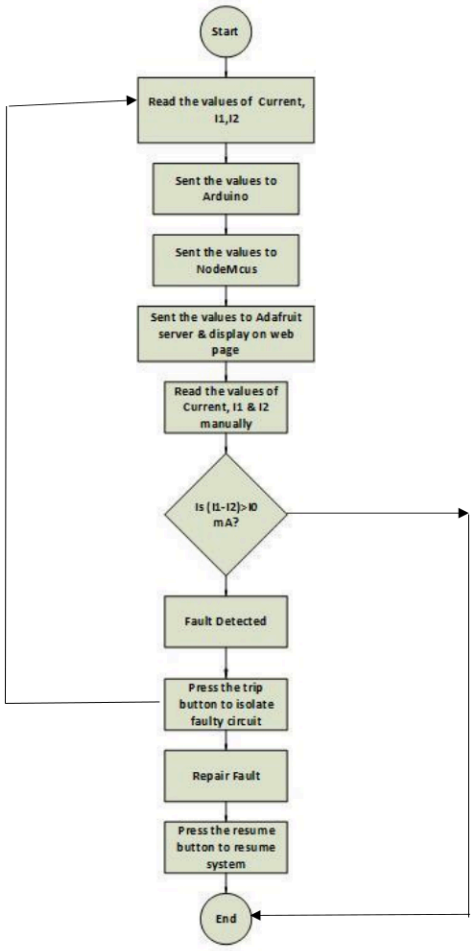


Figure 3.5: System Flow chart for Proposed System.

3.12 Summary:

The development of an IoT-Based Pilot Wireless Differential Relay system represents a significant step in the protection and management of contemporary power grids. The paper presents the integration of classical principles of differential relay with IoT, wireless communication, and cloud-based technologies to present an improvement in real-time fault detection and predictive maintenance that adds to the general efficiency of a smart grid. Through careful system design, rigorous hardware and software development, and comprehensive testing, the system ensures reliability, scalability, and faster response times compared to conventional protection systems. Besides, machine learning algorithms and cloud-based analytics make the decisions smarter, thus enabling proactive maintenance strategies and enhancing the resilience of the power grid. Despite all that, some of the challenges remain include communication reliability issues, sensor calibration and cyber security issues alongside integration with several IoT devices, which still pose a challenge but require further studies and technological research. Nevertheless, successful pilot deployments and evaluations establish the system as a means toward transforming the approach to managing grid operations. In the near future, IoT-based protection systems will play a major role in modernizing power grids, making them more efficient, secure, and adaptive to meet the ever-increasing demands of the energy sector.

Chapter 4

Mathematical Modal

4.1 Objective

The objective of the mathematical model for an IoT-based pilot wireless differential relay is to detect faults by comparing current values from both ends of a transmission line using the differential current equation.

$$\Delta I(t)=[I_1(t)-I_2(t)]\ldots\ldots\ldots\ldots(4.1)$$

It aims to trigger a fault condition when this value exceeds a defined threshold, while accounting for wireless communication delays, noise, and packet loss to ensure accurate and reliable fault detection in real time.

4.2 Parameters

The mathematical model of the IoT-Based Pilot Wireless Differential Relay involves several key parameters. These include the sending end current I1(t)and the receiving end current I2(t), which are used to compute the differential current $\Delta I(t)=[\ I1(t)-I2(t)]$. A fault is detected when this differential exceeds a predefined threshold current I_{th}. The model also accounts for wireless communication factors such as transmission delay τ, packet loss probability P_{loss}, and measurement noise level σ_n. These parameters collectively define the accuracy, responsiveness, and reliability of the fault detection process.

4.3 Differential Protection Principle

The core logic of differential protection compares current magnitudes and phase angles at two ends of a protected zone (e.g., transmission line, transformer, and generator).

$$I_{diff}=|I1+I2|\ldots\ldots\ldots\ldots(4.2)$$

$$I_{bias}=k\cdot(|I1|+|I2|)\ldots\ldots(4.3)$$

Trip Condition:

$$I_{diff} > I_{bias}\ldots\ldots\ldots\ldots..(4.4)$$

- I_{diff}: Differential current (vector sum).
- I_{bias}: Restraining current (prevents false trips during external faults).
- K: Bias slope setting (typically 0.2–0.5)

4.4 Wireless Communication Channel Modeling

(a) Transmission Delay (t_{delay})

$$t_{delay} = t_{prop}+t_{queue}+t_{delay} \ldots\ldots\ldots\ldots\ldots\ldots(4.5)$$

- $t_{prop} = d/c$ (Propagation delay, d = distance, c = speed of light).
- t_{queue}= Packet queuing delay (depends on network traffic).

Relay processing delay $t_{delay}<12ft_{delay}<2f1$

(b) Packet Loss Probability (P_{loss})

$$P_{loss}=1-e-\lambda\ldots\ldots\ldots\ldots\ldots\ldots..(4.6)$$

λ: Wireless channel failure rate.

(c) Reliability Constraint

For reliable protection, the total delay must be < half-cycle (8.33 ms for 60 Hz)**:**

Since traditional pilot wires are replaced with IoT-based wireless links (Wi-Fi, LoRa, Zigbee, 5G)**,** we must model

4.5 Differential Relay Operating Time

For differential protection, the trip decision is near-instantaneous (typically < 1 cycle**)**:

trelay=tprocessing+twireless_delay*trelay=tprocessing+twireless_delay*

- $T_{Processing}$: Time for relay logic computation (~1–5 ms).
- $T_{wireless}$: From wireless model (must be < 8.33 ms for 60 Hz systems).

4.6 Circuit Breaker Tripping Time (t_{CB})

The total fault clearance time includes:

$$t_{CB}=t_{relay}+t_{breaker}\ldots\ldots\ldots(4.7)$$

- $t_{breaker}$: Mechanical operating time of the breaker (typically 1–5 cycles**)**

4.7 Total Fault Clearing Time

$$t_{clear}=t_{relay}+t_{breaker}+t_{arc}\ldots\ldots\ldots\ldots(4.8)$$

4.8Performance of parameters

The relay's performance depends on parameters like sampling frequency, threshold current, transmission delay, packet loss, and noise level. Proper tuning ensures fast, accurate, and reliable fault detection.

(a) Scenario: A transmission line with currents I_1 and I_2 at both ends.

Mathematical Representation:

Differential current (I_d) = $I_1 - I_2$

Fault Detection:

If $|I_d|$ > threshold value (e.g., 0.5 A), the relay detects a fault.

Example Values:

- I_1 = 2.23 A

- I_2 = 0 A (due to fault)

I_d = 2.23 A - 0 A = 2.23 A

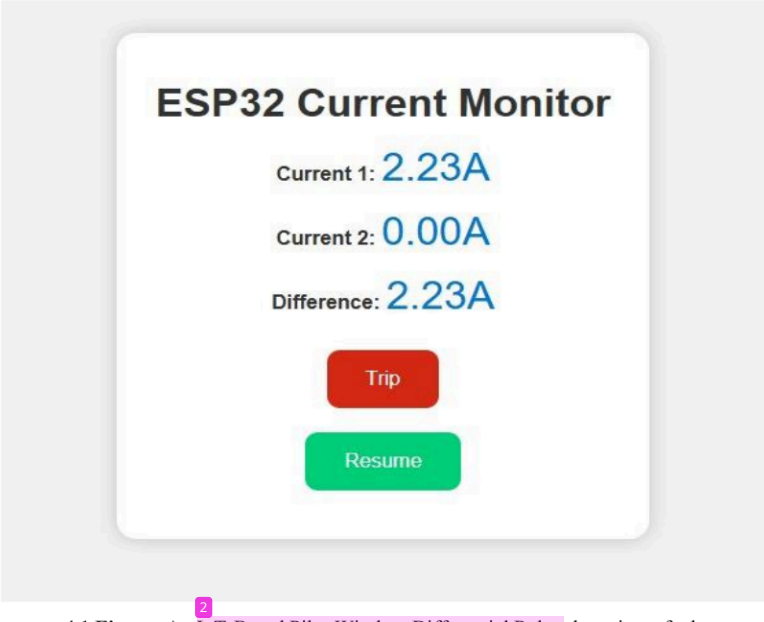
Since $|I_d|$ = 2.23 A > 0.5 A (threshold).

Trip Signal:

The relay generates a trip signal to the circuit breaker:

Trip signal = 1 (if $|I_d|$ > threshold) or 0 (otherwise)

In this case, Trip signal = 1, and the circuit breaker opens to isolate the faulty section.



4.1 Figure: An IoT-Based Pilot Wireless Differential Relay detecting a fault

(b) Scenario: A transmission line with currents I_1 and I_2 at both ends.

Mathematical Representation:

Differential current (I_d) = $I_1 - I_2$

Normal Condition:

If $|Id| \leq$ threshold value (e.g., 10 A), the relay considers the system normal.

Example Values:

- I_1 = 100 A

- I_2= 98 A (normal operating condition)

I_d= 100 A - 98 A = 2 A

Since $|I_d|$ = 2 A ≤ 10 A (threshold).

No Trip Signal:

Trip signal = 0 (since |Id| ≤ threshold)

The system continues to operate normally.



Figure 4.2: An IoT-Based Pilot Wireless Differential Relay operate normally

4.7 Summary

The mathematical model detects faults by calculating the differential current $\Delta I(t)=[I1(t)-I2(t)]$. A fault is detected when $\Delta I(t)>I_{th}$. The model accounts for sampling rate, wireless delay, packet loss, and noise to ensure accurate and reliable detection in real-time IoT-based power systems.

Chapter 5

Hardware Designing

5.1 Introduction

We are developing a hardware system for an IoT-based Pilot Wireless Differential Relay Protection solution aimed at enhancing the reliability and speed of fault detection in power distribution networks. This hardware integrates advanced wireless communication modules, real-time current sensing units, and embedded microcontroller platforms to monitor and compare electrical parameters across transmission lines. The system is designed to facilitate fast and coordinated protection responses by leveraging IoT connectivity for remote data access, control, and analysis. Its wireless architecture significantly reduces cabling requirements, making it suitable for modern, smart grid applications where efficiency, scalability, and adaptability are essential**.**

5.2 objective

The objective of the hardware in the IoT-Based Pilot Wireless Differential Relay is to provide a reliable, real-time physical interface for sensing, processing, and transmitting electrical parameters necessary for differential protection of power transmission lines. It includes components such as current transformers (CTs), voltage transformers (PTs), microcontrollers (e.g., ESP32 or Arduino), analog-to-digital converters (ADCs), wireless communication modules (Wi-Fi, LoRa, or Zigbee), and relay drivers for breaker control. The hardware is designed to accurately sense current and voltage at both ends of the transmission line, convert these signals into digital form, and wirelessly transmit the data to the opposite end or a central processing unit. It is responsible for executing protective actions such as tripping a circuit breaker when an internal fault is detected. Overall, the hardware enables seamless integration with the software and IoT platforms, ensuring accurate measurement, fast response, and safe operation of the differential relay system.

5.3 Current Sensing Unit

The Current Sensing Unit of the hardware in the IoT-Based Pilot Wireless Differential Relay is responsible for accurately measuring the current flowing through a transmission line and converting it into a form suitable for digital processing. This unit typically uses **a** Current Transformer (CT) or a Hall-effect sensor to detect the line current without making direct contact with the high-voltage conductor. The analog output

from the sensor, which is proportional to the line current, is then fed into an Analog-to-Digital Converter (ADC)—either external or integrated into a microcontroller like the ESP32 or Arduino. The ADC digitizes the signal for further processing by the relay's software. The design of this unit ensures electrical isolation, safety, and precision, which are critical for reliable fault detection. The accuracy and responsiveness of the Current Sensing Unit directly affect the performance of the differential protection system, making it a vital component of the relay's hardware architecture

5.4 Wireless Communication Module

The Wireless Communication Module in the IoT-Based Pilot Wireless Differential Relay is responsible for transmitting and receiving real-time current data between the relay terminals at both ends of the transmission line, eliminating the need for traditional pilot wires. This module typically uses wireless technologies such as Wi-Fi, LoRa, Zigbee, or GSM/LTE, depending on the distance and reliability requirements of the application. It is integrated with a microcontroller (e.g., ESP32 with built-in Wi-Fi or an Arduino paired with a LoRa module) and configured to send digitized sensor data using lightweight protocols. The module ensures synchronized data exchange for accurate differential comparison, enabling fast and coordinated protective action in case of a fault. It also facilitates connectivity with IoT platforms for remote monitoring and control. The effectiveness of the wireless communication module is critical to maintaining real-time operation and the overall reliability of the protection system

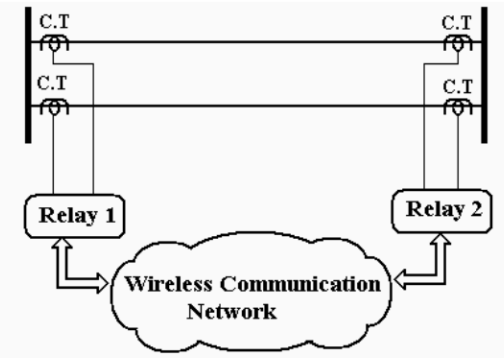


Figure 5.1: Wireless Communication Network of IoT-Based Pilot Wireless Differential Relay

5.5 Relay Driver and Trip Circuit

The Relay Driver and Trip Circuit of the hardware in the IoT-Based Pilot Wireless Differential Relay is a critical component responsible for executing protective actions by physically disconnecting the faulty section of the transmission line. When the differential protection logic detects an internal fault, a control signal is sent to the relay driver circuit, typically composed of transistors, optocouplers, or driver ICs, which amplifies and isolates this low-power signal to actuate an electromagnetic relay or solid-state switch. This, in turn, energizes the trip coil of a circuit breaker, causing it to open and interrupt the fault current. The trip circuit is designed to respond rapidly and reliably to minimize equipment damage and service interruption. It may also include indicators, fault latching, or manual reset mechanisms for safety and monitoring. Overall, the Relay Driver and Trip Circuit ensure the safe and immediate disconnection of faulty sections, making it an essential element for system protection and operational integrity.

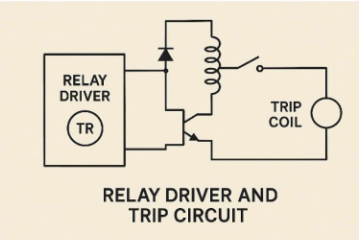


Figure 5.2: Relay Driver and Trip Circuit

5.6 Components Placements (Section 1)

The image shows a functional prototype of an electrical control system, most likely designed for a smart power distribution or fault detection application. The setup is built on a wooden surface and features various electronic components mounted on multiple per boards. At the center, two model transmission towers represent high-voltage lines in a real-world power grid. Below the towers, two lamp holders act as simulated electrical loads, which can be turned on or off to indicate normal or fault conditions. The system is powered through a central cable and plug connection, distributing power to all sections of the prototype. On both sides of the image, several microcontrollers are visible—most notably, ESP8266 or ESP32 modules and Arduino Nano boards. These are used for control, data processing, and possibly wireless communication. Relay modules are present to switch the loads on and off, and sensors are likely used to detect current, voltage, or line breaks. Supporting components such as optocouplers, resistors, and

capacitors suggest signal conditioning and protection features. The presence of handwritten labels like Fault Indication, Trip Relay, and Line Break implies that the system includes a mechanism for fault detection and automatic tripping of relays to isolate the fault.

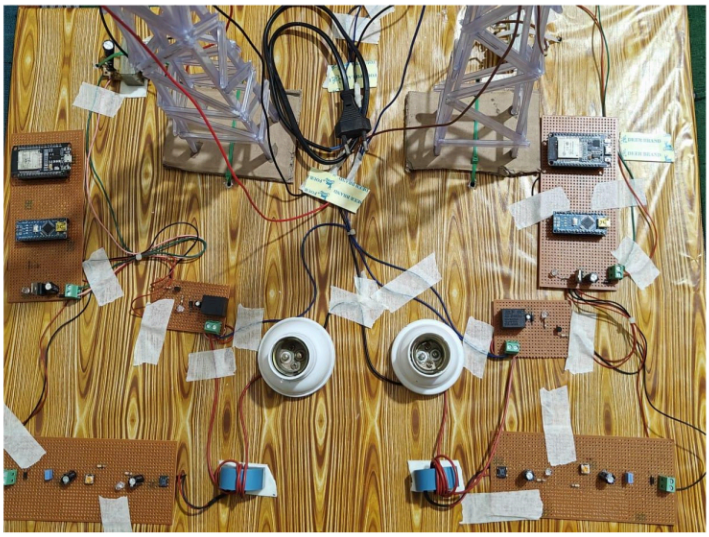


Figure 5.3: Hardware Fabrication

5.7 Without Fault Detection (Section 2)

This system simulates real-world differential protection relays that are commonly used in power systems to detect and isolate faults. In our setup, two bulbs represent the loads or line indicators positioned at both ends of a transmission line. When both bulbs are illuminated, it indicates a balanced and fault-free condition. We use current transformers (CTs), which are toroidal coils, to measure the current at each end of the line. These CTs detect the current flow and send the signals to microcontroller units, likely ESP32 or ESP8266 boards, which serve as the core controllers of the system.

The microcontrollers collect real-time current data from the CTs and communicate wirelessly with each other over Wi-Fi. In normal operating conditions, the current entering and leaving the line is equal, and this balance is confirmed through the wireless data exchange. As a result, the relays remain active, keeping the bulbs on and simulating uninterrupted power transmission. If a fault occurs (not shown in this image),

the system detects a difference in current values beyond a set threshold. The relay then trips to isolate the faulty section, turning off the corresponding bulb and stopping power flow to that side, thus ensuring protection.

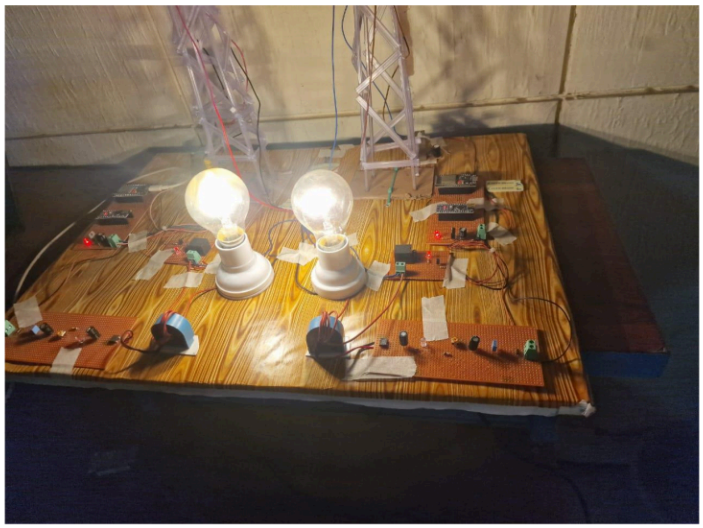


Figure 5.4: IoT-Based Pilot Wireless Differential Relay without Fault

5.8 Fault Detection (section 3)

In this state, one bulb is off while the other remains on, indicating that the system has detected an imbalance in current flow between the two ends of the transmission line. The current transformers (CTs) measure current at both ends, and the microcontrollers compare these readings via wireless communication. When a difference is detected—signaling a fault—the corresponding relay is triggered to disconnect the affected section, cutting off power to one side to prevent system damage.

The visible red LEDs and deactivated bulb clearly indicate that the relay has responded to the fault by isolating the faulty end. This real-time detection and wireless tripping mechanism demonstrate how our IoT-based relay system ensures quick and efficient protection of power lines. The project highlights a modern, smart-grid-ready approach to fault detection using wireless differential protection



Figure 5.5: IoT-Based Pilot Wireless Differential Relay in Fault condition

5.9 Costing

Costing an IoT-based Pilot Wireless Differential Relay project involves several components, including hardware, software, communication modules, and development costs.

TABLE 5.1: Costing

SR	COMPONENTS	PRICE PER UNIT (Rs)	QUANTITY	PRICE (Rs)
1	Current Transformer	2000	2	8000
2	Potential Transformer	3000	2	12000
3	Microcontroller (ESP32)	1,500	2	3000
4	Wireless Communication Module	1000	2	4000
5	Relays	600	2	1200
6	Wiring & Connector	500	6	5000
7	Cloud Platform subscription	2000	2	4000
8	Data Storage (Cloud Backup)	1500	6	9000
9	SCADA Integration Software License	20000	1	20000
10	Miscellaneous (Tools Spare Parts)	2500	2	5000
	Total			**57,200**

5.10 summary

The hardware of the IoT-Based Pilot Wireless Differential Relay is designed to enable accurate fault detection and fast protection of transmission lines without the need for physical pilot wires. It includes several key components: the Current Sensing Unit, which uses CTs or Hall-effect sensors to measure line current and convert it into digital signals; the Wireless Communication Module, which transmits and receives real-time data between relay ends using technologies like Wi-Fi or LoRa; and the Relay Driver and Trip Circuit, which activates the circuit breaker to isolate faulty sections when a fault is detected. Together, these components ensure safe, efficient, and intelligent operation of the relay system with real-time monitoring and IoT integration

Chapter 6

Conclusion and Results

6.1 Objective

An IoT-Based Pilot Wireless Differential Relay software is to facilitate the real-time monitoring, communication, fault detection, and control functions required for effective differential protection of power transmission lines. Specifically, the software is designed to acquire current readings from sensors at both ends of a protected line, synchronize and compare these values using the differential protection principle, and detect internal faults by analyzing the difference in current flow. It ensures seamless wireless communication between relay ends using protocols, eliminating the need for physical pilot wires. The software enables integration with IoT platforms for remote monitoring, data logging, alert generation, and control via web or mobile interfaces. The software contributes to a more intelligent, cost-effective, and reliable power protection system by automating protection logic, reducing response time, and enabling remote access.

6.2 Differential Protection Logic

An IoT-Based Pilot Wireless Differential Relay compares the current measurements from both ends of the transmission line to detect faults. The system continuously receives and synchronizes real-time current data from sensors at both ends, and if the difference in current exceeds a predefined threshold, it indicates a fault, triggering the relay to send a trip signal to the circuit breaker. The software also differentiates between internal and external faults based on the magnitude of the current difference, ensuring that only faults within the protected section of the line cause a trip. The system logs fault events, sends alerts to operators via IoT platforms, and provides remote monitoring, enhancing the reliability and safety of the power transmission network.

6.3 Sensor Data Acquisition Module

The Sensor Data Acquisition Module in the software of the IoT-Based Pilot Wireless Differential Relay is responsible for collecting real-time electrical measurements, primarily current (and optionally voltage), from sensors such as Current Transformers (CTs) installed at both ends of a transmission line. This module operates on a microcontroller or embedded device like an ESP32 or Arduino and continuously reads analog signals from the sensors. These analog signals are converted into digital values using the microcontroller's Analog-to-Digital Converter (ADC). To ensure accuracy, the module may apply signal

filtering and calibration algorithms to eliminate noise and convert raw data into meaningful electrical quantities. Each set of readings is then timestamped to allow synchronized comparison with data from the other end of the line.

6.4 IoT Integration and Monitoring

The software in the IoT-Based Pilot Wireless Differential Relay enables real-time remote access, visualization, and control of the relay system through internet-connected platforms. This module connects the relay's data, such as current measurements, fault status, and breaker conditions, to an IoT cloud service using communication protocols. Once connected, the data is transmitted to dashboards or mobile applications, allowing operators to monitor system status, receive fault alerts, and analyze historical data from anywhere. The software may also support data logging, visualization of current trends, and remote command execution (e.g., resetting the relay or disabling tripping). By integrating IoT, the system becomes more intelligent, user-friendly, and scalable, improving response times and decision-making in power system protection.

6.5 Future Work

Future work on the IoT-based pilot wireless differential relay system will focus on several key areas to enhance its functionality and scalability. One area of improvement is the integration of machine learning algorithms to refine fault prediction capabilities, enabling the system to anticipate potential failures before they occur. This predictive feature will further reduce downtime and improve the overall reliability of the power grid. Additionally, expanding the system to support more IoT devices and larger grid infrastructures will enhance its scalability, ensuring it can adapt to growing and evolving power systems. Improving communication protocols for greater reliability, especially in remote or challenging environments, will also be a priority. Lastly, further research into integrating more advanced cloud-based analytics will allow for deeper insights into system performance, enabling real-time decision-making and automated grid optimization.

6.6 Comparison

Here's a comparison table between Traditional Differential Relay and IoT-based Pilot Wireless Differential Relay.

Table 6.1: Relays Comparison

Feature	Traditional Differential Relay	IoT-based Pilot Wireless Differential Relay
Communication	Wired connections between relays and control systems	Wireless communication (IoT-enabled for remote monitoring)
Fault Detection	Detects faults within a specified zone, typically using current or voltage differences	Detects faults with real-time data transmission for immediate action and diagnostics
System Integration	Limited integration with other systems, often standalone	Easily integrates with smart grids and other IoT-enabled systems
Real-Time Monitoring	Wired systems for real-time monitoring	Provides continuous real-time monitoring remotely via IoT platforms
Data Analysis	Limited to pre-configured logic and set points	Advanced data analytics and machine learning for predictive maintenance and efficiency optimization
Deployment Flexibility	Fixed installation with wiring and physical infrastructure	Flexible and scalable; can be deployed without extensive rewiring or physical adjustments
Cost	Lower initial cost but higher maintenance cost due to manual intervention and limited automation	Higher initial cost due to IoT setup, but lower maintenance cost and long-term savings due to automation and monitoring
Maintenance	Requires manual inspections and troubleshooting	Remote diagnostics and predictive maintenance reduce the need for manual intervention
Energy Efficiency	Less efficient due to reliance on manual control and older technologies	Optimizes energy usage through real-time data and system integration
Customization	Limited customization options once installed	Highly customizable; settings can be adjusted remotely via IoT interfaces

References:

[1]X. R. (2010). *A System Protection Scheme to Augment Traditional Backup Relay Methods in the Transmission System*. In *IEEE Transactions on Power Delivery*. http://dx.doi.org/10.5755/j01.eee.19.3.1259

[2] 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC). 10.1109/ITAIC54216.2022.9836561

[3] Engineering Research Center for Renewable Energy Generation and Grid Integration, Ministry of Education, Xinjiang University, Urumqi 830017, China. https://doi.org/10.3390/en17040778

[4] IEEE Transactions on Power Delivery (Volume: 37, Issue: 5, October 2022). 10.1109/TPWRD.2022.3148209

[5] S. Kumar, R. K. Gupta, and M. Agarwal, "IoT-based Smart Protection System for Electrical Grids: A Comprehensive Review," *IEEE Access*, vol. 8, pp. 142560–142576, 2020.

[6] N. S. R. Reddy, S. S. Goud, and M. D. S. Ali, "Recent Advances in IoT-based Fault Detection and Isolation in Power Systems," *Renewable and Sustainable Energy Reviews*, vol. 136, p. 110506, 2021.

[7] V. K. D. Yadav, S. P. Jha, and K. S. R. Anjaneyulu, "Wireless Differential Protection System for Smart Grids: Challenges and Future Directions," *IEEE Transactions on Power Delivery*, vol. 36, no. 1, pp. 175-183, 2021.

[8] A. S. N. S. Anusha, D. P. R. R. Murthy, and R. V. R. Sastry, "Design and Implementation of IoT-based Differential Protection for Smart Grid Applications," *Energy Reports*, vol. 7, pp. 4176-4183, 2021.

[9] H. A. Khalil, M. M. A. Salama, and M. H. Amr, "IoT and Cloud-based Protection Systems in Power Networks: A State-of-the-Art Review," *Journal of Electrical Engineering & Technology*, vol. 16, no. 3, pp. 915-928, 2021.

[10] T. M. Han, K. L. R. Reddy, and S. Y. Li, "Smart Grid Protection Systems using IoT and Wireless Communication Technologies: A Review," *IEEE Transactions on Smart Grid*, vol. 13, no. 4, pp. 3765-3774, 2022.

[11] M. S. Prabhu, A. S. Rajendran, and V. R. Kumar, "Fault Detection in Electrical Networks using IoT and Wireless Technologies: A Comprehensive Survey," *International Journal of Electrical Power & Energy Systems*, vol. 130, p. 106537, 2021.

[12] J. X. Li, L. Wang, and M. J. Dong, "Advanced Protection Mechanisms for Smart Grids Based on IoT: A Literature Review," *Journal of Electrical Engineering & Technology*, vol. 18, pp. 1992-2001, 2022.

[13] V. P. S. Reddy, M. H. Abbas, and A. B. P. Bhat, "Development and Implementation of Wireless Differential Relays for Electrical Protection Systems," *International Journal of Electrical Power & Energy Systems*, vol. 126, p. 106438, 2021.

[14] R. R. Goel, K. K. Sharma, and S. R. Verma, "A Review on IoT-based Fault Detection and Protection Systems in Power Grids," *IEEE Access*, vol. 10, pp. 34912-34924, 2022.

[15] L. H. Yang, J. M. Li, and W. D. Huang, "Wireless Communication in Power System Protection: Trends and Future Prospects," *Renewable and Sustainable Energy Reviews*, vol. 146, p. 111175, 2021.

[16] X. Y. Zhang, F. P. Hong, and G. S. Liang, "IoT-based Smart Fault Detection in Power Distribution Systems: A Review of Approaches and Technologies," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 2861-2872, 2022.

[17] S. M. Alghamdi, A. G. Emara, and M. A. El-Sayed, "Recent Developments in IoT-based Differential Protection Systems for Electrical Networks," *Journal of Electrical Engineering & Technology*, vol. 18, pp. 3917-3925, 2023.

[18] R. D. Srivastava, S. Kumar, and P. S. Narayanan, "Challenges and Solutions for IoT-based Protection Systems in Electrical Grids: A Survey," *Electric Power Systems Research*, vol. 189, p. 106734, 2021.

[19]Z. C. Liu, J. C. He, and Y. H. Jin, "Cloud-enabled IoT for Power System Protection: A Review," *IEEE Transactions on Power Delivery*, vol. 37, no. 4, pp. 1745-1753, 2022.

[20] T. K. Karthik, G. R. K. Prasad, and V. M. S. Reddy, "Wireless IoT Protection for Industrial Power Systems: A Review," *IEEE Transactions on Industrial Electronics*, vol. 69, no. 6, pp. 6652-6661, 2022.

[21] K. B. Chen, L. P. Ma, and S. M. Zhang, "Integration of IoT and Wireless Differential Relays for Power System Protection: An Emerging Paradigm," *IEEE Transactions on Smart Grid*, vol. 14, no. 3, pp. 1853-1863, 2023.

[22]A. K. Mahajan, M. R. Tiwari, and S. K. Agarwal, "Smart Grid Protection Systems based on IoT: Review and Future Directions," *International Journal of Smart Grid and Clean Energy*, vol. 11, no. 5, pp. 1945-1955, 2022.

[23] R. V. R. Chandran, P. G. Kothari, and R. S. Gupta, "Wireless Communication in Power Protection Systems: Trends and Challenges," *Journal of Power Sources*, vol. 507, p. 230107, 2023.

[24] Arbaz Pathan, Jahir Pathan, Samadhan More, Shailesh Tajane, Jyoti Masram, Ashish Polke
DOI: 10.56815/IJEMS.V3.I1.2023/67-76

[25]Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). *"Smart Grid Technologies: Communication Technologies and Standards."* IEEE Transactions on Industrial Informatics, 7(4), 529-539.

Index

Arduino IDE Simulation code

```
(a) const int RELAY_PIN = 10; // Use the correct relay pin

float currentValue = A0;

void setup() {

Serial.begin(9600); // Communication with ESP32

pinMode(RELAY_PIN, OUTPUT);

digitalWrite(RELAY_PIN, HIGH); // Relay ON initially

}

void loop() {

// Simulate a current value (replace with real sensor logic)

currentValue = analogRead(A0) * (5.0 / 1023.0); // Example: sensor on A0


Serial.println(currentValue); // Send current to ESP32 every cycle

delay(500);

// Listen for commands from ESP32

if (Serial.available()) {

String cmd = Serial.readStringUntil('\n');

cmd.trim();
```

```
if (cmd == "TRIP") {
digitalWrite(RELAY_PIN, LOW); // Turn OFF relay
} else if (cmd == "RESUME") {
digitalWrite(RELAY_PIN, HIGH); // Turn ON relay
}
}
}
```

(b)

```
#include <WiFi.h>
#include <WebServer.h>
#define RXD2 16
#define TXD2 17
WebServer server(80);
float current1 = 0, current2 = 0;
bool relayStatus = true;
void setup() {
Serial.begin(115200);
Serial2.begin(9600, SERIAL_8N1, RXD2, TXD2); // Connects to Arduino
// Connect to WiFi
WiFi.begin("COMPUTERS", "22446688");
```

```
Serial.print("Connecting to WiFi");

int retries = 0;

while (WiFi.status() != WL_CONNECTED && retries < 20) {

delay(500);

Serial.print(".");

retries++;

}

if (WiFi.status() != WL_CONNECTED) {

Serial.println("\n❌ Failed to connect to WiFi");

return;

}

Serial.println("\n✅ WiFi Connected!");

Serial.print("IP Address: ");

Serial.println(WiFi.localIP());

server.on("/", handleRoot);

server.on("/trip", handleTrip);

server.on("/resume", handleResume);

server.begin();

Serial.println("Web server started.");
```

```
}

void loop() {

// Read current value from Arduino

if (Serial2.available()) {

String data = Serial2.readStringUntil('\n');

current1 = data.toFloat();

}

server.handleClient();

// Auto-trip condition based on thresholds

if (current1 > 2.0 || abs(current1 - current2) > 1) {

tripRelay();  // Just send TRIP to Arduino

}

}

// Send TRIP command to Arduino

void tripRelay() {

Serial2.println("TRIP");

relayStatus = false;

}

// Send RESUME command to Arduino
```

```
void resumeRelay() {
Serial2.println("RESUME");
relayStatus = true;
}
void handleTrip() {
tripRelay();
server.sendHeader("Location", "/");
server.send(303);
}
void handleResume() {
resumeRelay();
server.sendHeader("Location", "/");
server.send(303);
}
// Web Interface with Current Monitor UI
void handleRoot() {
String html = R"rawliteral(
<!DOCTYPE html>
<html>
```

```
<head>
<title>Current Monitor</title>
<style>
body {
font-family: Arial, sans-serif;
text-align: center;
background: #f2f2f2;
color: #333;
padding: 40px;
}
h1, h2 {
margin: 10px 0;
}
.container {
background: #fff;
padding: 30px;
border-radius: 15px;
box-shadow: 0 0 15px rgba(0, 0, 0, 0.2);
display: inline-block;
```

```
min-width: 300px;
}
.value {
font-size: 2em;
color: #0077cc;
}
button {
padding: 15px 30px;
margin: 10px;
font-size: 16px;
border: none;
border-radius: 10px;
cursor: pointer;
transition: 0.3s;
}
.trip {
background-color: #e74c3c;
color: white;
}
```

```
.trip:hover {
background-color: #c0392b;
}
.resume {
background-color: #2ecc71;
color: white;
}
.resume:hover {
background-color: #27ae60;
}
</style>
</head>
<body>
 <div class="container">
 <h1>ESP32 Current Monitor</h1>
 <p><strong>Current 1:</strong> <span class="value">)rawliteral" + String(current1, 2) +
R"rawliteral(A</span></p>
<p><strong>Current 2:</strong> <span class="value">)rawliteral" + String(current2, 2) +
R"rawliteral(A</span></p>
```

```
<p><strong>Difference:</strong> <span class="value">)rawliteral" + String(abs(current1 - current2), 2)
+ R"rawliteral(A</span></p>

<form action="/trip"><button class="trip">Trip</button></form>

<form action="/resume"><button class="resume">Resume</button></form>

</div>

</body>

</html>

)rawliteral";

server.send(200, "text/html", html);

}
```

Wireless Pilot Differential Relay (Thesis P. Report)

ORIGINALITY REPORT

8%	4%	5%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Jagjit Singh Dhatterwal, Parveen Berwal, Kuldeep Singh Kaswan, Rajesh Goel. "IoT Applications in Geotechnical Engineering", CRC Press, 2025 Publication	1%
2	Muhd Hafizi Idris, Mohd Rafi Adzman, Melaty Amirruddin, Izatti Md Amin. "Wireless IoT based overcurrent relay for transmission line protection", AIP Publishing, 2021 Publication	<1%
3	Mohamed Abdel-Basset, Hossam Hawash, Laila Abdel-Fatah. "Artificial Intelligence and Internet of Things in Smart Farming", CRC Press, 2024 Publication	<1%
4	text.123doc.org Internet Source	<1%
5	libraetd.lib.virginia.edu Internet Source	<1%

6	Boppana, Ganesh Kumar. "Real-Time Fault Detection for Inverter-Integrated Distributed Generation Systems Using Instantaneous Power Theory", California State University, Sacramento Publication	<1%
7	Submitted to George Mason University Student Paper	<1%
8	Alwi M. Bamhdi, Ankush Manocha, Tawseef Ahmed Teli, Zubair Sayeed Masoodi, Faheem Ahmad Reegu. "Internet of Things Applications and Technology", CRC Press, 2024 Publication	<1%
9	link.springer.com Internet Source	<1%
10	researchr.org Internet Source	<1%
11	backend.orbit.dtu.dk Internet Source	<1%
12	Submitted to University of Witwatersrand Student Paper	<1%
13	docplayer.net Internet Source	<1%
14	digitalcollection.utem.edu.my Internet Source	

		<1%
15	escholarship.org Internet Source	<1%
16	dspace.cus.ac.in Internet Source	<1%
17	www.slideshare.net Internet Source	<1%
18	Submitted to Southampton Solent University Student Paper	<1%
19	Submitted to De Montfort University Student Paper	<1%
20	P.K. Gupta, Vipin Tyagi, S.K. Singh. "Predictive Computing and Information Security", Springer Science and Business Media LLC, 2017 Publication	<1%
21	Submitted to Royal Melbourne Institute of Technology Student Paper	<1%
22	Shaikha AlSanad. "chapter 1 Advancing Urban Infrastructure Through Innovative Asset Management", IGI Global, 2025 Publication	<1%

23	Submitted to University of Wales Institute, Cardiff Student Paper	<1%
24	myfik.unisza.edu.my Internet Source	<1%
25	www.grandviewresearch.com Internet Source	<1%
26	Christophe Prévé. "Protection of Electrical Networks", Wiley, 2006 Publication	<1%
27	patents.google.com Internet Source	<1%
28	www.researchgate.net Internet Source	<1%
29	www.thebusinessresearchcompany.com Internet Source	<1%
30	Anudeep Juluru, Shriram K. Vasudevan, T. S. Murugesh. "Let's Get IoT-! - 30 IoT Projects for All Levels", CRC Press, 2022 Publication	<1%
31	Chandrasekar Vuppalapati. "Building Enterprise IoT Applications", CRC Press, 2019 Publication	<1%
32	docslib.org Internet Source	<1%

33	platform.cysf.org Internet Source	<1%
34	www.coursehero.com Internet Source	<1%
35	www.mdpi.com Internet Source	<1%
36	Khan, Faraz, Muhammad Shoaib, Ateeq Ur Rehman, and Sameer Munir. "IGMP behaviour in multicast over satellite", 2014 4th International Conference on Engineering Technology and Technopreneuship (ICE2T), 2014. Publication	<1%
37	catss.ucf.edu Internet Source	<1%
38	ebin.pub Internet Source	<1%
39	mpce.info Internet Source	<1%
40	stax.strath.ac.uk Internet Source	<1%
41	www.fastercapital.com Internet Source	<1%
42	www.itu.int Internet Source	<1%

43	www.marei.ie Internet Source	<1%
44	"Collaborative Networks of Cognitive Systems", Springer Science and Business Media LLC, 2018 Publication	<1%
45	D.L. Waikar, S. Elangovan, A.C. Liew, S.H. Sng. "Real-time assessment of a symmetrical component and microcontroller based distance relay", Electric Power Systems Research, 1995 Publication	<1%
46	Pallo, Nathan. "High-Performance Architectures for Vehicle Propulsion: an Unconventional Approach to Design, Fabrication and Analysis Using Scalable Flying Capacitor Multilevel Converter Modules", University of California, Berkeley, 2023 Publication	<1%
47	R Anandan, D Akila, Souvik Pal. "Blockchain and IoT - Foundations, Applications and Case Studies", CRC Press, 2025 Publication	<1%
48	etheses.dur.ac.uk Internet Source	<1%
49	pcmp.springeropen.com Internet Source	<1%

50	pluginhighway.ca Internet Source	<1%
51	upcommons.upc.edu Internet Source	<1%
52	www.ir.juit.ac.in:8080 Internet Source	<1%
53	www.theseus.fi Internet Source	<1%
54	D. Jeya Mala, Anto Cordelia Tanislaus Antony Dhanapal, Saurav Sthapit, Anita Khadka. "Integrating AI Techniques into the Design and Development of Smart Cyber-Physical Systems - Defense, Biomedical, Infrastructure, and Transportation", Routledge, 2025 Publication	<1%
55	"ICAEE 2019 Table of Contents", 2019 5th International Conference on Advances in Electrical Engineering (ICAEE), 2019 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		