Electricity Theft Detection System

Ram Siddharth R R, Santhosh N, Prakash M, Savio Godric Jesupal, Kalaiselvi C

Abstract

Electricity theft is a major challenge in modern power distribution systems, leading to significant financial losses, reduced power quality, and instability in the electrical grid. Traditional metering systems lack the capability to detect unauthorized usage, meter tampering, and illegal connections in real time. With the advancement of smart grid technology, Advanced Metering Infrastructure (AMI) has emerged as an effective solution to enable two-way communication, remote monitoring, and intelligent energy management. However, existing AMI systems still require improved mechanisms for fast and accurate theft detection.

This project proposes a **Change-and-Transmit based Electricity Theft Detection System** integrated into Advanced Metering Infrastructure. The system continuously monitors electrical parameters such as voltage, current, power consumption, and load variations using smart sensors connected to a microcontroller-based smart meter. Whenever a significant change in consumption pattern or abnormal condition is detected, the system automatically transmits the updated data to a central utility server using IoT communication technologies such as GSM, Wi-Fi, or LoRa. The system also incorporates tamper detection features to identify unauthorized activities such as meter bypassing, magnetic interference, neutral disturbance, and illegal load tapping.

In addition, machine learning techniques can be applied to analyze historical consumption data and identify suspicious patterns that indicate potential electricity theft. Real-time alerts are generated and sent to utility authorities through SMS or a web-based monitoring dashboard, enabling quick response and preventive action. The proposed system improves billing accuracy, enhances grid security, reduces technical and commercial losses, and supports efficient energy management in smart grid environments. Overall, the Change-and-Transmit AMI model provides a reliable, scalable, and cost-effective solution for modern electricity theft detection and prevention.

Introduction

Electricity is one of the most fundamental resources for economic growth, industrial development, and improvement in the quality of life. Modern societies depend heavily on reliable and uninterrupted electricity supply for domestic, commercial, agricultural, and industrial applications. As electricity demand continues to increase due to population growth, urbanization, and technological advancements, power distribution systems are becoming more complex and challenging to manage. One of the major issues affecting the efficiency and sustainability of power distribution networks is electricity theft, which results in significant financial losses for utility companies and negatively impacts service reliability.

Electricity theft refers to the unauthorized consumption of electrical energy by bypassing meters, tampering with meter readings, or illegally tapping into power lines. It is considered a major component of non-technical losses in the electrical distribution system. These losses not only reduce the revenue of electricity providers but also increase operational costs and lead to unfair billing for honest consumers. In many developing and densely populated regions, electricity theft remains a serious concern due to inadequate monitoring systems, outdated metering infrastructure, and lack of real-time detection mechanisms. Traditional methods of detecting electricity theft rely on manual inspections, periodic meter readings, and customer complaints, which are time-consuming, inefficient, and often inaccurate.

With the advancement of smart grid technologies, the electrical power system is gradually evolving into a more intelligent and automated network capable of monitoring, controlling, and optimizing energy distribution. One of the key components of the smart grid is the Advanced Metering Infrastructure (AMI), which enables two-way communication between consumers and utility providers. AMI systems consist of smart meters,

communication networks, and data management systems that collect and transmit energy consumption data in real time. This technology allows utilities to monitor usage patterns, perform remote meter reading, detect faults, and improve overall grid efficiency.

Despite the advantages of AMI, existing systems still face challenges in accurately identifying electricity theft in real time. Many conventional smart meter systems transmit data at fixed intervals regardless of whether significant changes occur in energy consumption. This continuous transmission increases communication overhead, network congestion, and power consumption. Additionally, some theft detection techniques rely solely on analyzing historical data, which may delay the identification of illegal activities. Therefore, there is a need for a more efficient and intelligent system capable of detecting theft events immediately while minimizing communication and operational costs.

The concept of **Change-and-Transmit Advanced Metering Infrastructure** addresses these challenges by enabling smart meters to transmit data only when a significant change or abnormal condition is detected in the system. Instead of sending continuous data, the meter monitors electrical parameters such as voltage, current, power consumption, and load behavior. When the system identifies unusual patterns or potential tampering events, it triggers an automatic transmission of updated data to the central utility server. This approach reduces unnecessary data communication, conserves energy, and improves system responsiveness.

In addition to monitoring electrical parameters, modern electricity theft detection systems incorporate tamper detection mechanisms that identify physical and electrical abnormalities in the meter. These mechanisms include detection of magnetic interference, neutral disturbance, meter opening, reverse current flow, and sudden load variations. By integrating multiple sensing technologies, the system can accurately determine whether abnormal behavior is caused by legitimate usage changes or unauthorized manipulation. This multi-layer detection strategy improves the reliability and effectiveness of theft detection compared to traditional methods.

Another important advancement in electricity theft detection is the application of machine learning and data analytics techniques. Machine learning algorithms analyze historical and real-time energy consumption data to identify patterns associated with normal and abnormal behavior. These algorithms can automatically learn from previous data and improve detection accuracy over time. For example, sudden spikes in energy usage during unusual hours or irregular consumption patterns may indicate unauthorized connections or meter bypassing. By combining machine learning with sensor-based monitoring, the system can provide intelligent and automated theft detection without human intervention.

The integration of Internet of Things (IoT) technology further enhances the capabilities of modern electricity theft detection systems. IoT-enabled smart meters can communicate with remote servers through wireless communication technologies such as Wi-Fi, GSM, LoRa, or NB-IoT. This connectivity allows real-time monitoring of energy consumption data, remote diagnostics, and instant alert notifications. When theft is detected, the system can automatically send alerts to utility personnel through SMS, email, or a web-based dashboard. This rapid response mechanism helps prevent further energy loss and improves operational efficiency.

Security is another critical aspect of Advanced Metering Infrastructure. Since smart meters transmit sensitive consumption data over communication networks, it is essential to protect this information from unauthorized access and cyber threats. Modern AMI systems incorporate encryption, authentication, and secure communication protocols to ensure data integrity and confidentiality. These security measures prevent data tampering, unauthorized meter control, and malicious attacks on the power distribution system.

The proposed **Electricity Theft Detection using Change-and-Transmit AMI** system aims to provide a reliable, efficient, and scalable solution for modern smart grid applications. The system combines sensor-based monitoring, tamper detection mechanisms, machine learning algorithms, and IoT communication to detect electricity theft in real time. By transmitting data only when significant changes occur, the system reduces communication overhead and improves energy efficiency. Furthermore, the use of automated alerts and remote monitoring enhances the ability of utility companies to respond quickly to theft incidents and maintain system reliability.

1.2 PROBLEM STATEMENT

Electricity theft has become a significant challenge in modern power distribution systems, leading to substantial financial losses, reduced operational efficiency, and unreliable electricity supply. Unauthorized consumption of electrical energy through illegal connections, meter bypassing, tampering, and manipulation of meter readings contributes to non-technical losses in the distribution network. These losses not only affect the revenue of utility companies but also increase electricity tariffs for legitimate consumers and place additional stress on power generation and distribution infrastructure.

Traditional electricity metering systems lack the capability to detect theft activities in real time. Most existing methods depend on manual inspection, periodic meter reading, and delayed analysis of consumption data. Such approaches are time-consuming, labor-intensive, and often fail to identify theft incidents promptly. Additionally, conventional systems transmit energy consumption data at regular intervals regardless of whether significant changes occur, resulting in unnecessary communication overhead and increased operational costs.

Although Advanced Metering Infrastructure (AMI) has improved monitoring and communication capabilities, many current implementations still rely primarily on data analysis rather than direct detection of tampering or abnormal conditions. These systems may experience delays in identifying suspicious behavior and may generate false alarms due to limited detection mechanisms. Furthermore, continuous data transmission in traditional AMI systems can lead to network congestion, increased power consumption, and reduced system efficiency.

Therefore, there is a critical need for an intelligent, reliable, and energy-efficient electricity theft detection system capable of identifying unauthorized activities immediately while minimizing communication and operational costs. The system should be able to monitor electrical parameters continuously, detect tampering events accurately, and transmit data only when significant changes occur. Implementing a **Change-and-Transmit Advanced Metering Infrastructure** integrated with smart sensing and communication technologies can address these challenges by enabling real-time detection, efficient data transmission, and improved security in modern power distribution networks.

1.3 OBJECTIVE

The main objective of this project is to develop an efficient and reliable electricity theft detection system using **Change-and-Transmit Advanced Metering Infrastructure (AMI)** technology. The system is designed to continuously monitor electrical parameters such as voltage, current, power consumption, and load variations in real time to ensure accurate energy measurement and prevent unauthorized usage. By integrating smart sensing devices and communication technologies, the proposed system aims to detect electricity theft activities such as meter bypassing, illegal connections, magnetic tampering, and neutral disturbances at an early stage. Another important objective of the project is to implement a **Change-and-Transmit communication mechanism**, which allows the smart meter to transmit data to the utility server only when significant changes or abnormal conditions are detected. This approach helps reduce communication overhead, save energy, and improve system efficiency compared to conventional systems that transmit data continuously. The project also aims to integrate Internet of Things (IoT) technologies such as GSM, Wi-Fi, or LoRa to enable remote monitoring and real-time data transmission between the consumer and the utility provider.

Furthermore, the system is intended to provide instant alerts and notifications to utility authorities through SMS, email, or a web-based monitoring dashboard whenever suspicious activity or electricity theft is detected. By improving the speed and accuracy of detection, the proposed system helps reduce non-technical losses, enhance billing transparency, and ensure fair usage of electrical energy. Ultimately, the objective of this project is to create a scalable, secure, and cost-effective solution that supports modern smart grid infrastructure and contributes to efficient energy management in residential, commercial, and industrial applications.

1.4 **Problem Identification**

Electricity theft is one of the major challenges faced by power distribution utilities worldwide, resulting in significant financial losses and reduced system efficiency. Unauthorized consumption of electricity through illegal connections, meter tampering, and bypassing of energy meters contributes to non-technical losses in the distribution network. These losses not only affect the revenue of utility companies but also lead to higher electricity tariffs for genuine consumers and increased operational costs for maintaining the power system. In many regions, especially in rapidly developing areas, the demand for electricity is increasing continuously, making it more difficult to monitor and control unauthorized usage using traditional methods.

Existing electricity metering systems and monitoring mechanisms are often unable to detect theft activities immediately. Conventional meters generally record energy consumption without identifying the cause of abnormal usage patterns or physical tampering. Detection of electricity theft usually depends on manual inspections, periodic meter readings, and customer complaints, which are time-consuming, labor-intensive, and prone to human error. Additionally, the lack of real-time monitoring and automated detection mechanisms delays the identification of illegal activities, allowing theft to continue for extended periods before corrective actions are taken.

Another significant issue is the continuous transmission of energy consumption data in many traditional Advanced Metering Infrastructure (AMI) systems. These systems transmit data at fixed intervals regardless of whether significant changes occur in energy usage. This constant communication increases network traffic, consumes more power, and raises operational costs without improving detection efficiency. Furthermore, many existing systems rely solely on software-based analysis of historical consumption data, which may produce false alarms or fail to detect sudden tampering events.

Therefore, there is a clear need for an intelligent and efficient electricity monitoring system capable of detecting theft and tampering activities in real time while minimizing communication overhead and energy consumption. The system should be able to monitor electrical parameters continuously, identify abnormal usage patterns accurately, and transmit data only when significant changes occur. Implementing a **Change-and-Transmit Advanced Metering Infrastructure** integrated with smart sensors and communication technologies can effectively address these problems by improving detection speed, reducing operational costs, and enhancing the reliability and security of modern power distribution systems.

1.5 HARDWARE REQUIREMENTS

1. Microcontroller Atmega328p
2. Voltage Sensor
3. Current Sensor
4. Gps
5. Temperature Sensor
6. GSM
7. Esp32
8. Transformer with rectifier board of 12V and 5V
9. Pzem 004t

1.7 SOFTWARE REQUIREMENT

1. Arduino IDE for programing Atmega 328p
2. Atmel Studio 7
3. HTML Coding C++
4. Flasher

Chapter 2

Literature Review

2.1.1 Review 1: Real-Time Power Theft Monitoring and Detection System with Double Connected Data Capture System -- Celimpilo Lindani Zulu, Oliver Dzobo- Electrical Engineering (Springer)- 2023

Power utilities worldwide are facing enormous challenges when it comes to the distribution of electricity. With these challenges, electricity theft is regarded as the most common challenge in the electrical distribution system. Electricity theft can be meter tampering done in consumer houses and illegal connections done using hook-ups from the distribution pole grids. These electricity theft challenges have caused power utilities to reconsider customer engagements focusing on feedback, putting loss detection systems in their distribution system networks, using artificial intelligence to schedule maintenance and other asset management activities, etc. The main focus of this paper is to design a real-time power theft monitoring and detection system that is able to detect power theft in distribution systems. This proposed system utilizes smart meters consisting of an Arduino ATMega328P microcontrollers with GSM modules (Global System for Mobile Communication) used for system communication. Cloud storage is created to store the smart meter data. Simulations of the proposed system were done using Proteus Design Suite v.8.10 SP3 software. The proposed system is practically constructed for prototype measurement results. Should power imbalances be measured by the system, the authority office will receive an SMS notification as an alert for power theft detected by a specific smart metering system. The authority office will analyse the power measurements sent to the cloud storage (MATLAB Online, ThingSpeak IoT channels display), and further action will be taken.

2.1.2 Review 2 Review of the Data-Driven Methods for Electricity Fraud Detection in Smart Metering Systems – Mahmoud M. Badr, Mohamed I. Ibrahem, Hisham A. Kholidy- Energies- 2023

In smart grids, homes are equipped with smart meters (SMs) to monitor electricity consumption and report fine-grained readings to electric utility companies for billing and energy management. However, malicious consumers tamper with their SMs to report low readings to reduce their bills. This problem, known as electricity fraud, causes tremendous financial losses to electric utility companies worldwide and threatens the power grid's stability. To detect electricity fraud, several methods have been proposed in the literature. Among the existing methods, the data-driven methods achieve state-of-art performance. Therefore, in this paper, we study the main existing data-driven electricity fraud detection methods, with emphasis on their pros and cons. We study supervised methods, including wide and deep neural networks and multi-data-source deep learning models, and unsupervised methods, including clustering. Then, we investigate how to preserve the consumers' privacy, using encryption and federated learning, while enabling electricity fraud detection because it has been shown that fine-grained readings can reveal sensitive information about the consumers' activities. After that, we investigate how to design robust electricity fraud detectors against adversarial attacks using ensemble learning and model distillation because they enable malicious consumers to evade detection while stealing electricity. Finally, we provide a comprehensive comparison of the existing works, followed by our recommendations for future research directions to enhance electricity fraud detection.

2.1.3 Review 3: Smart Grid Security: An Effective Hybrid CNN-Based Approach for Detecting Energy Theft Using Consumption Patterns – Muhammed Zekeriya Gunduz, Resul Das- Sensors- 2024

In Internet of Things-based smart grids, smart meters record and report a massive number of power consumption data at certain intervals to the data center of the utility for load monitoring and energy management. Energy theft is a big problem for smart meters and causes non-technical losses. Energy theft attacks can be launched by malicious consumers by compromising the smart meters to report manipulated consumption data for less billing. It is a global issue causing technical and financial damage to governments and operators. Deep learning-based techniques can effectively identify consumers involved in energy theft through power consumption data. In this study, a hybrid convolutional neural network (CNN)-based energy-theft-detection system is proposed to detect data-tampering cyber-attack vectors. CNN is a commonly employed method that automates the extraction of features and the classification process. We employed CNN for feature extraction and traditional machine learning algorithms for classification. In this work, honest data were obtained from a real dataset. Six attack vectors causing data tampering were utilized. Tampered data were synthetically generated through these attack vectors. Six separate datasets were created for each attack vector to design a specialized detector tailored for that specific attack. Additionally, a dataset containing all attack vectors was also generated for the purpose of designing a general detector. Furthermore, the imbalanced dataset problem was addressed through the application of the generative adversarial network (GAN) method. GAN was chosen due to its ability to generate new data closely resembling real data, and its application in this field has not been extensively explored. The data generated with GAN ensured better training for the hybrid CNN-based detector on honest and malicious consumption patterns. Finally, the results indicate that the proposed general detector could classify both honest and malicious users with satisfactory accuracy.

2.1.4 Review 4: Electricity Theft Detection and Prevention Using Technology-Based Models: A Systematic Literature Review – Potego Maboe Kgaphola, Senyeki Milton Marebane- Sensors MDP-2024

Electricity theft comes with various disadvantages for power utilities, governments, businesses, and the general public. This continues despite the various solutions employed to detect and prevent it. Some of the disadvantages of electricity theft include revenue loss and load shedding, leading to a disruption in business operations. This study aimed to conduct a systematic literature review to identify what technology solutions have been offered to solve electricity theft and the effectiveness of those solutions by considering peer-reviewed empirical studies. The systematic literature review was undertaken following the guidelines for conducting a literature review in computer science to assess potential bias. A total of 11 journal articles published from 2012 to 2022 in SCOPUS, Science Direct, and Web of Science were analysed to reveal solutions, the type of theft addressed, and the success and limitations of the solutions. The findings show that the focus in research is channelled towards solving electricity theft in Smart Grids (SGs) and Advanced Metering Infrastructure (AMI); moreover, there is a neglect in the recent literature on finding solutions that can prevent electricity theft in countries that do not have SG and AMI installed. Although the results reported in this study are confined to the analysed research papers, the leading limitation in the selected studies, lack of real-life data for dishonest users. This study's contribution is to show what technology solutions are prevalent in solving electricity theft in recent years and the effectiveness of such solutions.

2.1.5 Review 5 : Research on Blockchain-Enabled Smart Grid for Anti-Theft Electricity Securing Peer-to-Peer Transactions in Modern Grids - Jalalud Din, Hongsheng Su, Sajad Ali - Sensors MDP – 2024

Electricity theft presents a significant financial burden to utility companies globally, amounting to trillions of dollars annually. This pressing issue underscores the need for transformative measures within the electrical grid. Accordingly, our study explores the integration of block chain technology into smart grids to combat electricity theft, improve grid efficiency, and facilitate renewable energy integration. Block chain's core principles of

decentralization, transparency, and immutability align seamlessly with the objectives of modernizing power systems and securing transactions within the electricity grid. However, as smart grids advance, they also become more vulnerable to attacks, particularly from smart meters, compared to traditional mechanical meters. Our research aims to introduce an advanced approach to identifying energy theft while prioritizing user privacy, a critical aspect often neglected in existing methodologies that mandate the disclosure of sensitive user data. To achieve this goal, we introduce three distributed algorithms: lower–upper decomposition (LUD), lower–upper decomposition with partial pivoting (LUDP), and optimized LUD composition (OLUD), tailored specifically for peer-to-peer (P2P) computing in smart grids. These algorithms are meticulously crafted to solve linear systems of equations and calculate users' "honesty coefficients," providing a robust mechanism for detecting fraudulent activities. Through extensive simulations, we showcase the efficiency and accuracy of our algorithms in identifying deceitful users while safeguarding data confidentiality. This innovative approach not only bolsters the security of smart grids against energy theft, but also addresses privacy and security concerns inherent in conventional energy-theft detection methods.

2.1.6 Review 6: Robust Resampling and Stacked Learning Models for Electricity Theft Detection in Smart Grid - Angelos Figueroa, Yao et al. - Energy Reports

Electricity theft (ET) is a critical contributor to non-technical losses (NTLs) that significantly threaten the efficiency and reliability of power grids, leading to increased power wastage and financial losses. Despite the development of various artificial intelligence (AI)-based machine learning (ML) and deep learning (DL) approaches for electricity theft detection (ETD), existing methods often exhibit limitations in memorization and generalization, mainly when applied to large-scale electricity consumption datasets characterized by high variance, missing values, and complex nonlinear relationships. These challenges can result in models needing high variance and bias, reducing their effectiveness in accurately predicting electricity theft cases. To address these limitations, we propose a three-layer framework that employs a stacking ensemble model to combine the benefits of both ML and DL algorithms. During the first stage of data preprocessing, missing data is imputed through data interpolation, while the normalization is done through min–max scaling. To solve the high-class imbalance problem prevalent in most real-world datasets, we combine borderline synthetic minority oversampling techniques and near-miss under sampling strategies. In the final layer of our proposed ETD framework, we employ four ML base and five meta-classifiers. The outputs of base classifiers are aggregated and passed to a meta-classifier, where we evaluate recurrent neural networks (RNN) and convolutional neural network (CNN) as potential meta-classifiers. The RNN are long short-term memory (LSTM), gated recurrent unit (GRU), Bi-directional LSTM (Bi-LSTM) and Bi-directional GRU (Bi-GRU), respectively. Experimental outcomes show that the proposed Bi-GRU better achieves accuracy enhancement of detection in general than meta-classifiers and other state-of-the-art models used for ETD.

2.1.7 Efficient and Accurate Zero-Day Electricity Theft Detection from Smart Meter Sensor Data Using Prototype and Ensemble Learning - Alyaman H. Massarani, Mahmoud M. Badr - Sensors - 2025 Electricity theft remains a pressing challenge in modern smart grid systems, leading to significant economic losses and compromised grid stability. This paper presents a sensor-driven framework for electricity theft detection that leverages data collected from smart meter sensors, key components in smart grid monitoring infrastructure. The proposed approach combines prototype learning and meta-level ensemble learning to develop a scalable and accurate detection model, capable of identifying zero-day attacks that are not present in the training data. Smart meter data is compressed using Principal Component Analysis (PCA) and K-means clustering to extract representative consumption patterns, i.e., prototypes, achieving a 92% reduction in dataset size while preserving critical anomaly-relevant features. These prototypes are then used to train base-level one-class classifiers, specifically the One-Class Support Vector Machine (OCSVM) and the Gaussian Mixture

Model (GMM). The outputs of these classifiers are normalized and fused in a meta-OCSVM layer, which learns decision boundaries in the transformed score space. Experimental results using the Irish CER Smart Metering Project (SMP) dataset show that the proposed sensor-based detection framework achieves superior performance, with an accuracy of 88.45% and a false alarm rate of just 13.85%, while reducing training time by over 75%. By efficiently processing high-frequency smart meter sensor data, this model contributes to developing real-time and energy-efficient anomaly detection systems in smart grid environments.

2.1.8 Advanced Deep Learning-Based Electricity Theft Detection in Smart Grids Using Multi-Dimensional Analysis with Convolutional Autoencoder and Transformer-Jian Shan, Cheng Zeng, Yan Wang-Engineering Applications of Artificial Intelligence-2025

Machine learning (ML) techniques utilizing electricity consumption (EC) data from smart meters have shown potential, traditional methods often rely on single-dimensional analysis, lacking the granularity to capture complex, periodic EC patterns, which results in suboptimal detection performance. To address these shortcomings, we propose a novel ETD system that utilizes deep learning (DL) through a combination of Convolutional Autoencoder (CAE) and Transformer models for advanced multi-dimensional analysis of EC data. We further tackle EC data imbalance with the K-means-based Synthetic Minority Oversampling Technique (K-means SMOTE). Our approach preprocesses EC data, employing the CAE to extract detailed features from 28-day consumption intervals, followed by the Transformer to analyze sequences and capture comprehensive patterns. The proposed model achieves an impressive F1 score of 0.9918, surpassing existing benchmarks. Notably, its lightweight design ensures scalability and efficiency, broadening its applicability to other smart grid anomaly detection tasks, such as identifying equipment failures or cyber threats, thus reinforcing modern power grid security.

Chapter 3

3.1 Existing System

In traditional power distribution systems, electricity consumption is measured using electromechanical or basic digital energy meters. These conventional metering systems are primarily designed to record the total amount of energy consumed by a consumer over a specific period. The collected data is typically read manually by utility personnel during scheduled visits, and the billing process is performed based on the recorded meter readings. While this method has been widely used for many years, it has several limitations in terms of efficiency, accuracy, and security. One of the major drawbacks of the existing system is its inability to detect electricity theft in real time.

Electricity theft in traditional systems commonly occurs through methods such as meter bypassing, illegal connections to distribution lines, meter tampering, and manipulation of meter readings. Since conventional meters lack advanced sensing and monitoring capabilities, these unauthorized activities often remain undetected for long periods. Utility companies typically identify theft only after significant discrepancies appear between the generated electricity and the billed consumption. This delayed detection results in substantial financial losses and operational challenges for power distribution companies.

Another limitation of the existing system is the dependence on manual inspection and monitoring processes. Utility staff are required to physically visit consumer locations to check meter readings and inspect connections for signs of tampering. This manual approach is time-consuming, labor-intensive, and prone to human error. In large distribution networks with thousands of consumers, it becomes extremely difficult to monitor each connection regularly. As a result, many theft incidents go unnoticed, and the overall efficiency of the electricity distribution system is reduced.

With the development of smart grid technology, Advanced Metering Infrastructure (AMI) systems have been introduced to improve energy monitoring and management. These systems use smart meters capable of measuring electricity consumption digitally and transmitting data to utility servers through communication networks. AMI systems enable features such as remote meter reading, automated billing, and load monitoring. However, many existing AMI implementations still rely on periodic data transmission at fixed intervals, regardless of whether significant changes occur in energy consumption. This continuous communication increases network traffic, consumes more power, and may lead to communication delays or system congestion.

In addition, existing smart meter systems often focus mainly on recording consumption data rather than detecting physical tampering or abnormal electrical conditions. Most theft detection methods in current systems are based on analyzing historical consumption patterns using statistical or machine learning techniques. While these methods can identify suspicious behavior, they may not detect sudden tampering events immediately. For example, if a consumer bypasses the meter or connects an illegal load, the system may take several hours or days to recognize the abnormal pattern, allowing theft to continue during that time.

Security is another critical concern in existing electricity monitoring systems. Many conventional systems lack strong data encryption and authentication mechanisms, making them vulnerable to cyberattacks and unauthorized access. Hackers or malicious users may attempt to manipulate meter data, disrupt communication networks, or disable monitoring systems. Such vulnerabilities can compromise the reliability and safety of the entire power distribution infrastructure.

Furthermore, existing systems generally do not include integrated tamper detection mechanisms such as magnetic sensors, neutral disturbance detection, or meter enclosure opening detection. Without these features, it is difficult to determine whether abnormal energy consumption is caused by legitimate usage changes or intentional manipulation. This limitation reduces the accuracy of theft detection and increases the likelihood of false alarms.

Another significant issue in traditional systems is the lack of real-time alert mechanisms. When electricity theft occurs, utility authorities may not receive immediate notification, resulting in delayed response and prolonged energy loss. In many cases, corrective actions are taken only after customers report issues or after periodic audits reveal discrepancies in energy usage data. This reactive approach is inefficient and costly, particularly in large-scale distribution networks.

In summary, the existing electricity monitoring and theft detection systems suffer from several limitations, including delayed detection of theft, dependence on manual inspection, continuous data transmission, lack of real-time alerts, limited tamper detection capabilities, and vulnerability to security threats. These challenges highlight the need for an advanced and intelligent monitoring system capable of detecting unauthorized electricity usage immediately while improving communication efficiency and system reliability. The development of a **Change-and-Transmit Advanced Metering Infrastructure** system addresses these limitations by enabling real-time monitoring, event-based communication, and enhanced security features for modern smart grid applications.

3.2 Limitations of Existing System

The existing electricity monitoring and theft detection systems, including traditional energy meters and basic smart metering infrastructure, face several technical and operational limitations. These limitations reduce the effectiveness of detecting unauthorized electricity usage and increase the financial losses experienced by utility companies. Although modern metering technologies have improved data collection and communication capabilities, many current systems still lack the intelligence and responsiveness required for real-time theft detection and prevention.

One of the primary limitations of existing systems is the **lack of real-time theft detection**. Traditional meters record energy consumption but do not actively monitor abnormal behavior or tampering events as they occur. As a result, electricity theft may continue for extended periods before being identified during routine inspections or data analysis. This delay in detection leads to significant energy loss and increased operational costs for utility providers.

Another major limitation is the **dependence on manual inspection and monitoring**. In many power distribution networks, utility personnel must physically visit consumer locations to read meters and check for signs of tampering or illegal connections. This process is time-consuming, labor-intensive, and inefficient, particularly in large urban or rural areas with thousands of consumers. Human error during manual inspections can also result in inaccurate readings and delayed detection of theft activities.

Existing systems also suffer from **continuous data transmission**, which increases communication overhead and power consumption. Many Advanced Metering Infrastructure (AMI) systems transmit data at fixed time intervals regardless of whether significant changes occur in electricity usage. This constant communication can lead to network congestion, reduced system performance, and higher operational costs. Additionally, continuous data transmission consumes more energy, reducing the overall efficiency of the system.

Another limitation is the **limited capability to detect physical tampering and abnormal electrical conditions**. Conventional meters often lack integrated sensors to identify unauthorized activities such as magnetic interference, meter bypassing, neutral disturbance, or reverse current flow. Without these detection mechanisms, the system may fail to recognize theft attempts or may generate false alarms due to normal variations in electricity usage.

Security vulnerabilities are also a significant concern in existing electricity monitoring systems. Many traditional systems do not implement strong encryption, authentication, or secure communication protocols. This makes them susceptible to cyberattacks, data manipulation, and unauthorized access to meter information. Such security weaknesses can compromise the reliability and integrity of the electricity distribution network.

Furthermore, existing systems typically rely on historical data analysis to identify suspicious consumption patterns. While data analytics can be useful, it may not detect sudden theft incidents immediately. The delay between data collection and analysis reduces the effectiveness of the system in preventing ongoing electricity theft. In addition, these systems may produce inaccurate results when the data is incomplete or when consumption patterns vary due to legitimate reasons.

Finally, the **lack of automated alert mechanisms** in many traditional systems limits the ability of utility authorities to respond quickly to theft incidents. Without instant notifications, corrective actions are delayed, and energy losses continue to accumulate. This reactive approach highlights the need for a more intelligent and proactive electricity monitoring system capable of detecting and reporting theft events in real time.

In summary, the limitations of existing electricity theft detection systems include delayed detection, dependence on manual inspection, continuous data transmission, limited tamper detection capability, security vulnerabilities, reliance on historical data analysis, and absence of real-time alert mechanisms. These challenges emphasize the need for an advanced and efficient monitoring system that can provide accurate, secure, and real-time detection of electricity theft in modern power distribution networks.

3.3 Proposed System

The proposed system introduces an intelligent electricity theft detection mechanism based on **Change-and-Transmit Advanced Metering Infrastructure (AMI)** technology. The system is designed to monitor electrical parameters continuously, detect abnormal conditions in real time, and transmit data to the utility server only when significant changes occur. This event-based communication approach improves efficiency, reduces network congestion, and enhances the responsiveness of electricity monitoring systems. By integrating advanced sensing technologies, communication modules, and intelligent detection algorithms, the proposed system provides a reliable and scalable solution for modern smart grid applications.

In the proposed system, a smart energy meter equipped with a microcontroller is used to measure important electrical parameters such as voltage, current, power consumption, and load variations. Sensors connected to the microcontroller continuously collect real-time data from the electrical supply line. The system analyzes this data to identify irregular patterns or abnormal conditions that may indicate electricity theft or system faults. For example, sudden changes in load consumption, reverse current flow, or imbalance between measured parameters can signal unauthorized usage or tampering activities.

One of the key features of the proposed system is the **Change-and-Transmit communication mechanism**. Unlike traditional systems that transmit data at fixed intervals, the proposed system sends information only when a significant change in electrical parameters or a tamper event is detected. This method reduces unnecessary communication traffic, conserves energy, and improves the overall performance of the communication network. The change detection algorithm compares the current sensor readings with predefined threshold values to determine whether data transmission is required.

The system also incorporates multiple **tamper detection mechanisms** to identify various forms of electricity theft. These mechanisms include detection of magnetic interference, meter enclosure opening, neutral disturbance, and reverse current flow. Magnetic sensors can identify the presence of strong external magnetic fields used to manipulate meter readings. Switch sensors detect unauthorized opening of the meter enclosure. Current sensors monitor the direction of current flow to detect reverse connections, while voltage and current comparison techniques help identify neutral disturbances or bypass conditions. By combining multiple detection methods, the system improves the accuracy and reliability of theft identification.

To enable remote monitoring and real-time communication, the proposed system integrates an **Internet of Things (IoT) communication module**, such as GSM, Wi-Fi, LoRa, or NB-IoT. This module allows the smart meter to transmit data to a central utility server or cloud platform. The transmitted information includes electrical parameters, tamper status, and system alerts. Utility personnel can access this data through a web-based dashboard or mobile application, enabling them to monitor energy usage and identify theft incidents from any location. The communication system also supports secure data transmission using encryption and authentication protocols to protect sensitive information.

Another important component of the proposed system is the **real-time alert mechanism**. When the system detects abnormal behavior or theft activity, it automatically generates an alert message and sends it to the utility authority. The alert may include details such as meter identification number, location, type of tamper event, and time of occurrence. Notifications can be delivered through SMS, email, or a monitoring dashboard. This immediate notification capability allows utility personnel to respond quickly to theft incidents and take corrective action before significant energy loss occurs.

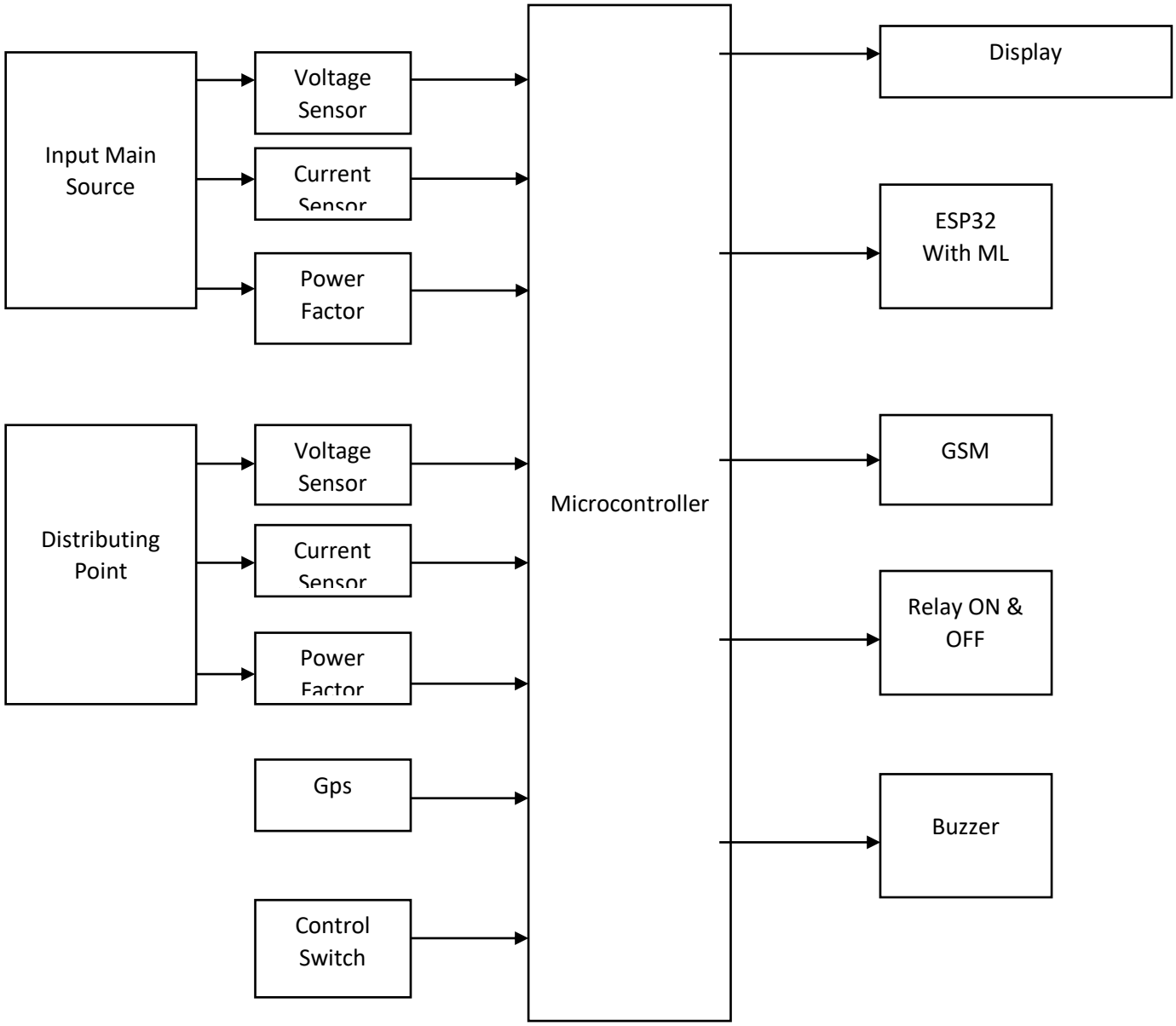
The proposed system can also incorporate **machine learning algorithms** to enhance the detection of complex theft patterns. By analyzing historical consumption data, machine learning models can learn the normal behavior of electricity usage and identify unusual patterns that may indicate fraudulent activity. These algorithms can adapt to changing usage patterns over time, improving detection accuracy and reducing false alarms. The integration of machine learning with sensor-based monitoring creates a hybrid detection system capable of identifying both physical tampering and abnormal consumption behavior.

In addition to theft detection, the proposed system improves overall energy management and system reliability. Continuous monitoring of electrical parameters helps identify faults such as overloading, voltage fluctuations, and equipment failure. Early detection of these issues allows preventive maintenance and reduces the risk of power outages. The system also supports automated data logging, enabling utilities to maintain accurate records of energy consumption and system performance.

The proposed Change-and-Transmit AMI system is designed to be **scalable and cost-effective**, making it suitable for deployment in residential, commercial, and industrial environments. The modular architecture allows additional sensors and communication modules to be integrated as needed. Furthermore, the system can be easily upgraded to support advanced features such as predictive maintenance, demand response, and smart grid automation.

In summary, the proposed system provides a comprehensive solution for real-time electricity theft detection and efficient energy monitoring. By combining continuous parameter monitoring, event-based data transmission, tamper detection mechanisms, secure communication, and intelligent analysis, the system addresses the limitations of existing electricity monitoring systems. The implementation of this advanced monitoring framework contributes to improved billing accuracy, reduced financial losses, enhanced grid security, and reliable power distribution in modern smart grid environments.

3.4 Block Diagram



The proposed electricity theft detection system is designed to monitor electrical parameters at both the **input main source** and the **distribution point** to identify any abnormal conditions that may indicate electricity theft. The system uses multiple sensors, a microcontroller, communication modules, and alert devices to ensure accurate monitoring and real-time detection. The block diagram represents the flow of electrical data and control signals within the system.

1. Input Main Source

The **Input Main Source** represents the primary electrical supply entering the system from the utility grid. This is the point where electricity is initially measured before distribution to consumers. Monitoring the input source is essential to establish a reference for comparing energy usage at different points in the distribution network. Any mismatch between the input and distributed power values can indicate possible electricity theft or system faults.

At the input main source, electrical parameters such as voltage, current, and power factor are measured using dedicated sensors. These measurements provide accurate information about the total power entering the system and help detect abnormal conditions such as overloading, voltage fluctuations, or unauthorized connections.

2. Voltage Sensor

The **Voltage Sensor** is used to measure the supply voltage at both the input main source and the distribution point. It converts the high voltage from the electrical line into a safe, low-level signal that can be processed by the microcontroller. Continuous monitoring of voltage helps detect irregularities such as sudden voltage drops or spikes, which may occur due to illegal connections or tampering activities.

3. Current Sensor

The **Current Sensor** measures the flow of electrical current in the circuit. It plays a critical role in calculating power consumption and detecting abnormal current variations. By comparing the current values at the input source and distribution point, the system can identify discrepancies that may indicate electricity theft or energy leakage.

4. Power Factor Sensor

The **Power Factor Sensor** measures the efficiency of electrical power usage in the system. Power factor is the ratio of real power to apparent power and is an important parameter in power quality analysis. A sudden change in power factor may indicate unauthorized load connections or abnormal operating conditions. Monitoring the power factor helps improve system efficiency and supports accurate detection of suspicious activity.

5. Distributing Point

The **Distributing Point** represents the location where electricity is delivered to consumers or load points. Similar to the input source, voltage, current, and power factor are measured at this point. The system compares the values from the input source and the distribution point to determine whether energy is being lost or diverted illegally. If the difference between the measured values exceeds a predefined threshold, the system identifies a potential theft condition.

6. GPS Module

The **GPS (Global Positioning System) Module** is used to determine the geographical location of the distribution point or meter. This feature is particularly useful for identifying the exact location of theft incidents in large distribution networks. When theft is detected, the GPS coordinates can be transmitted to the utility authority to enable quick response and corrective action.

7. Control Switch

The **Control Switch** allows manual or automatic control of the electrical supply. It can be used by authorized personnel to disconnect or reconnect power during maintenance, emergency situations, or confirmed theft conditions. The control switch enhances system safety and provides flexibility in managing the power distribution process.

8. Microcontroller

The **Microcontroller** is the central processing unit of the system. It receives input signals from all sensors, processes the data, and performs calculations to determine power consumption and system status. The microcontroller continuously compares electrical parameters from the input source and distribution point to detect abnormal conditions. If the system identifies a significant difference in energy measurements or detects tampering, it triggers an alert and initiates communication with external devices.

The microcontroller also controls the operation of output devices such as relays, buzzer, and display units. It ensures that all system components operate in coordination and respond appropriately to changing conditions.

9. ESP32 with Machine Learning

The **ESP32 with Machine Learning (ML)** module is responsible for advanced data analysis and intelligent decision-making. It analyzes historical and real-time data to identify patterns associated with normal and abnormal electricity usage. Machine learning algorithms improve detection accuracy by learning from previous data and adapting to changes in consumption behavior. The ESP32 also enables wireless communication and supports integration with IoT-based monitoring systems.

10. GSM Module

The **GSM Module** provides wireless communication between the system and the utility authority. It is used to send real-time notifications, alerts, and status updates through SMS or mobile networks. When electricity theft or abnormal conditions are detected, the GSM module automatically transmits an alert message containing relevant information such as system status and location details.

11. Display Unit

The **Display Unit** is used to show real-time system information such as voltage, current, power factor, and system status. It allows users and technicians to monitor system performance directly at the installation site. The display also indicates warning messages or fault conditions when abnormal activity is detected.

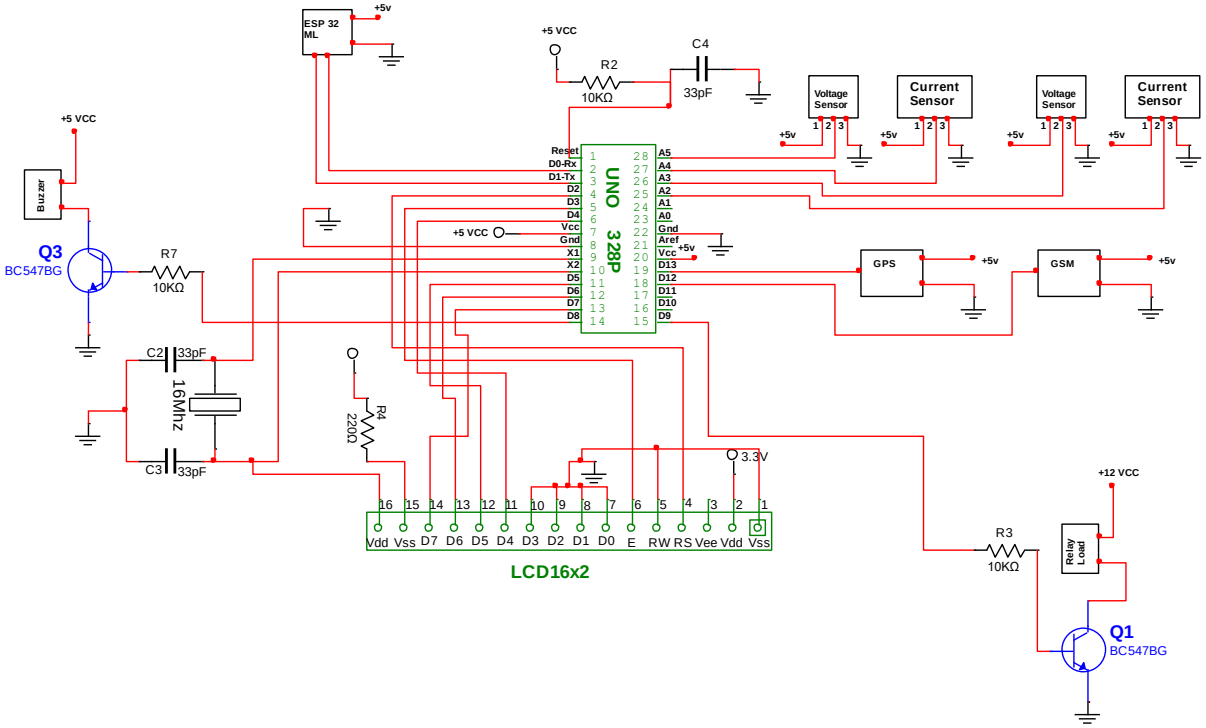
12. Relay ON and OFF

The **Relay ON and OFF** module controls the electrical supply to the load. When theft or dangerous conditions are detected, the microcontroller can automatically deactivate the relay to disconnect the power supply. This protective action helps prevent further energy loss and ensures system safety.

13. Buzzer

The **Buzzer** serves as an audible alert device. It is activated when the system detects electricity theft, system faults, or abnormal electrical conditions. The buzzer provides immediate notification to nearby personnel, enabling quick response and corrective action.

Circuit Diagram



The proposed electricity theft detection system operates on the principle of continuous monitoring and comparison of electrical parameters at two different points in the power distribution system: the **input main source** and the **distribution point**. By measuring and analyzing voltage, current, and power factor values at these locations, the system can identify discrepancies that may indicate electricity theft, system faults, or abnormal operating conditions. The system integrates sensors, a microcontroller, communication modules, and intelligent data analysis techniques to ensure accurate detection and timely response.

Initially, the electrical power from the utility grid enters the system through the **input main source**. At this point, voltage, current, and power factor sensors continuously measure the electrical parameters of the incoming supply. These sensors convert high-voltage and high-current signals into low-level analog signals suitable for processing by the microcontroller. The measured values represent the total electrical energy entering the distribution system and serve as a reference for comparison with downstream measurements.

The electricity is then distributed to consumers through the **distribution point**, where a second set of voltage, current, and power factor sensors is installed. These sensors measure the electrical parameters of the power delivered to the load. The system continuously compares the readings from the input main source and the distribution point to determine whether any energy loss or unauthorized consumption has occurred. Under normal operating conditions, the measured values at both points should be approximately equal, allowing for minor losses due to transmission and distribution.

If the difference between the input and distribution measurements exceeds a predefined threshold value, the system identifies a potential electricity theft or abnormal condition. For example, if the current measured at the distribution point is significantly lower than the current measured at the input source, it may indicate illegal tapping or meter bypassing. Similarly, sudden changes in power factor or voltage levels may signal tampering, equipment malfunction, or unauthorized load connections.

The **microcontroller** plays a central role in the system's operation. It receives input signals from all sensors, processes the data using programmed algorithms, and performs real-time calculations to determine system status. The microcontroller continuously monitors the difference between input and output electrical parameters and determines whether the system is operating normally or experiencing abnormal conditions. If the system detects a significant discrepancy, it triggers an alert and initiates further actions.

To enhance detection accuracy, the system incorporates an **ESP32 module with machine learning capability**. The ESP32 collects historical and real-time data from the microcontroller and analyzes consumption patterns

using machine learning algorithms. These algorithms learn the normal behavior of electricity usage over time and can identify unusual patterns that may indicate electricity theft. For instance, repeated sudden increases or decreases in current consumption during unusual hours may suggest unauthorized usage. The machine learning model improves system reliability by reducing false alarms and enabling intelligent decision-making.

The system also includes a **Global Positioning System (GPS) module**, which provides the geographical location of the distribution point or meter installation. When electricity theft is detected, the GPS module supplies location coordinates that are transmitted along with the alert message. This feature enables utility authorities to quickly identify the exact location of the theft incident and take immediate corrective action.

Communication between the system and the utility authority is established using a **GSM communication module**. When the microcontroller detects an abnormal condition or theft event, it sends a signal to the GSM module to transmit an alert message. The message may include details such as voltage, current, power factor, system status, and location information. This real-time communication capability ensures that utility personnel are informed immediately and can respond promptly to theft incidents.

The system also features a **Change-and-Transmit communication mechanism**, which improves efficiency by sending data only when significant changes occur in the system. Instead of continuously transmitting data at fixed intervals, the system monitors sensor readings and transmits information only when abnormal conditions are detected. This approach reduces communication overhead, conserves energy, and enhances network performance.

To provide local monitoring, the system includes a **display unit** that shows real-time information such as voltage, current, power factor, and system status. The display allows technicians and users to observe system performance directly at the installation site. When an abnormal condition is detected, the display indicates a warning message to alert nearby personnel.

The **relay ON and OFF module** is used to control the electrical supply to the load. When electricity theft or a dangerous condition is detected, the microcontroller can automatically deactivate the relay to disconnect the power supply. This protective measure prevents further energy loss and ensures safety in the distribution system. The relay can also be controlled manually using the **control switch**, allowing authorized personnel to manage the power supply during maintenance or emergency situations.

In addition to visual alerts, the system uses a **buzzer** to provide an audible warning when abnormal conditions are detected. The buzzer immediately alerts nearby personnel, ensuring quick awareness and response to potential theft or system faults.

Overall, the working principle of the proposed system is based on real-time monitoring, intelligent data analysis, and event-based communication. By continuously comparing electrical parameters at different points in the distribution network, the system can accurately detect electricity theft and abnormal conditions. The integration of machine learning, GPS location tracking, and wireless communication enhances system reliability, improves response time, and supports efficient energy management. This advanced monitoring framework ensures secure, reliable, and efficient operation of modern power distribution systems.

Merits of proposed System

The proposed electricity theft detection system using **Change-and-Transmit Advanced Metering Infrastructure (AMI)** provides several important advantages over traditional electricity monitoring systems. One of the major benefits of the system is its ability to detect electricity theft in real time by continuously monitoring electrical parameters such as voltage, current, and power factor. This real-time monitoring helps utility authorities identify unauthorized electricity usage immediately and take prompt corrective action, thereby reducing energy losses and improving system reliability.

Another significant advantage of the proposed system is its improved detection accuracy. By measuring electrical parameters at both the input main source and the distribution point, the system can accurately compare the values and identify discrepancies caused by illegal connections or tampering activities. The integration of machine learning techniques further enhances the system's capability to recognize abnormal consumption patterns and reduce false alarms. This intelligent detection mechanism ensures reliable operation and efficient monitoring of the power distribution network.

The system also improves communication efficiency through the implementation of the **Change-and-Transmit mechanism**, which transmits data only when significant changes or abnormal conditions occur. This approach reduces unnecessary data transmission, lowers communication costs, and conserves energy, making the system more efficient compared to conventional systems that continuously transmit data. In addition, the system supports remote monitoring and control through GSM or IoT communication technologies, allowing utility personnel to monitor system performance from any location without the need for frequent manual inspections.

Furthermore, the proposed system enhances safety and security in the power distribution network. The automatic alert system sends notifications through SMS, display messages, and buzzer alarms whenever theft or abnormal conditions are detected. The relay control mechanism can disconnect the power supply during dangerous situations, preventing further energy loss and protecting electrical equipment. Overall, the proposed system offers a scalable, reliable, and cost-effective solution for modern smart grid applications by improving billing accuracy, reducing non-technical losses, and ensuring efficient energy management.

Chapter 4

4.1 HARDWARE MODULE

4.1.1 BASIC OF IOT

The Internet of Things is simply "A network of Internet connected objects able to collect and exchange data." It is commonly abbreviated as IoT. The word "Internet of Things" has two main parts; Internet being the backbone of connectivity, and Things meaning objects / devices The Internet of Things (IoT), also sometimes referred to as the Internet of Everything (IoE), consists of all the web-enabled devices that collect, send and act on data they acquire from their surrounding environments using embedded sensors, processors and communication hardware. The Internet of Things (IoT) refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems. The IoT platform is a suite of components that enable: Deployment of applications that monitor, manage, and control connected devices. Remote data collection from connected devices. Independent and secure connectivity between devices. Device/sensor management.

The Internet of Everything (IoE) is a concept that extends the Internet of Things (IoT) emphasis on machine-to-machine (M2M) communications to describe a more complex system that also encompasses people and processes. The Internet of things (stylized Internet of Things or IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect information The processing of data on web-connected servers in large data centers, what we refer to as the cloud, has also contributed greatly to the ability of everyday gadgets to become part of the IoT.

These devices may connect to the Internet by sending data to your phone or some other dedicated hardware in your home that acts as a hub over a local communication method, such as:

Bluetooth

Bluetooth LE (low energy)

6LowPan

IEEE 802.15.4

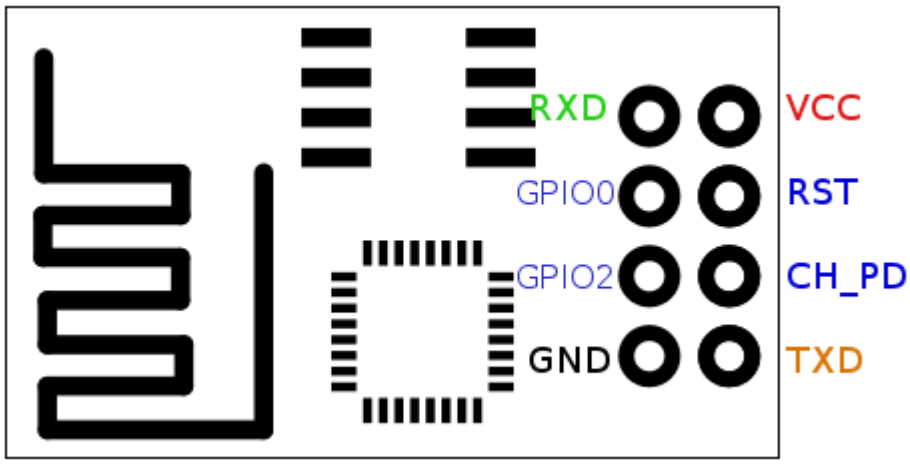
NFC (near-field communication)

ZigBee

Z-wave

The connected gadgets of the IoT contain computing hardware, including processors with embedded programming telling them what to do, sensors that gather various sorts of readings (such as temperature, moisture, light, motion, chemical levels, heart rate and body movement) and communication hardware that can send and receive signals.

5.2 ESP 8266 IOT Module



The ESP8266 is a very low-cost module that comes pre-programmed with an AT command set firmware, meaning, it can simply hook this up to the Arduino device and get about as much WiFi-ability. This module has a powerful on-board processing and storage capability that allows it to be integrated with the sensors and other application through its GPIOs. The ESP8266 communicates with the Arduino through a serial interface. That is, it uses the Arduino's Rx and Tx pins (digital pins 0 and 1) hooked up to the module for receiving commands and communicates back. The module features a full TCP/UDP stack support and can be configured as a web server.

The ESP8266 module has three operational modes:

1. Access Point (AP)

In AP, the Wi-Fi module acts as a Wi-Fi network, or access point (hence the name). It allows other devices to connect to it. And establishes a two-way communication between the ESP8266 and the device that is connected to it via Wi-Fi.

2. Station (STA)

In STA mode, the ESP-01 can connect to an AP(access point) such as the Wi-Fi network from your house. This allows any device connected to that network to communicate with the module.

3. Both

In this mode ESP-01 act as both an AP as well as in STA mode.

ESP8266EX can be used in sensor products, using the I2C interface. The I2C works in the master mode and can connect to multiple sensors. The slave devices is identified through addressing mode (each slave device has a unique address identity). The sensor products send the real-time data to SP8266EX via I2C interface, and ESP8266EX uploads the data to server wirelessly. Users can acquire information from server through applications when the mobile phone connects to internet.

Some connected systems may be able to use other nearby devices to gather data, like city road systems that signal smart phones to help monitor traffic conditions. Smart devices can work in conjunction with tagging technology including RFID tags, QR codes, barcodes and the like to obtain data about items. The devices also need a power source, which can include a connection to a power outlet, a solar panel, or even replaceable or rechargeable batteries, provided the embedded hardware is of the low-power variety. Companies are also working on wireless power for a possible future power source.

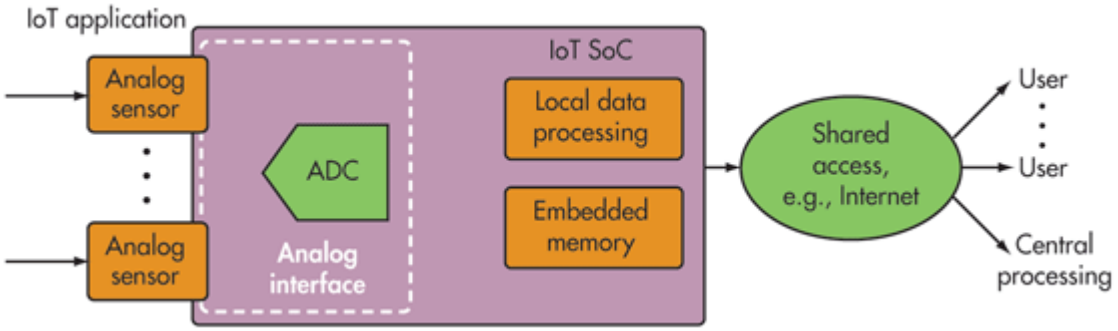


Fig: 2.1 IoT Access

The devices may be run mostly via their own embedded software or firmware, but they can also offload a lot of the processing to cloud-based software via the Internet, where they can crunch more data. Some use advanced algorithms that let them learn from and adjust to various stimuli and patterns (letting them program themselves, to an extent). This sending and processing of the sensor data is often nearly instantaneous (thanks to the usually lightning-fast speeds of Internet communication), allowing the devices to react in real-time.

Internet, things, Internet of things, Internet of Everything! These are some of the buzzwords you may have been hearing, reading & very likely talking about endlessly. These are more than just keywords; IoT (Internet of Things) is a technology concept and/or an architecture which is an aggregation of already available technologies. Similar to the way in which Internet has changed the way we work & communicate by connecting us (humans) through World Wide Web, IoT aims to take this connectivity to next level by connecting various devices to the internet – facilitating human-machine, machine-machine interactions also.

The visionaries have also realized that this IoT ecosystem has business applications in areas of Home Automation, Automotive, Factory/assembly line automation, Retail, Medical/Preventive healthcare and more.

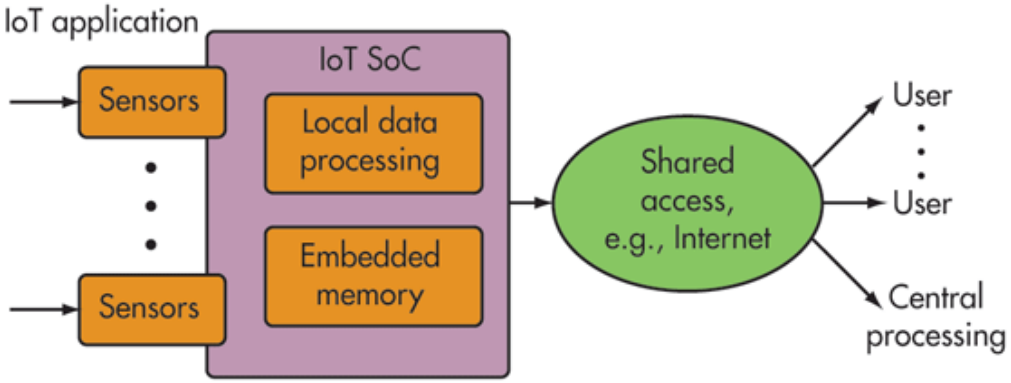


Fig: 2.2 IoT with Sensor module

The digital sensor outputs data in a digital format. It may already take care of some of the data processing, like calibration and other functions. Also, it may implement sensor fusion techniques by including several different sensors and combining them to derive meaningful information, as in motion detection. The analog sensor outputs raw data in analog format. There is a significant range of analog sensors such as temperature whose output is delivered in the analog domain. The application SoC needs to collect the output in raw format and convert it to digital for processing. When connecting with a digital sensor device, the IoTSoC needs to include a digital interface that complies with the one the sensor chip is using to drive the sensor signals into the processor in the SoC. When connecting with an analog sensor, the IoTSoC needs to convert the sensor signal into the digital domain by means of an analog-to-digital converter (ADC).Now that we all understand the IoT concept, it would be worthwhile to deep dive in order to get familiar with the building blocks of IoT:

Sensors & Sensor technology – They will sniff a wide variety of information ranging from Location, Weather/Environment conditions, Grid parameters, Movement on assembly lines, Jet engine maintenance data to Health essentials of a patient

IoT Gateways – IoT Gateways, as the name rightly suggests, are the gateways to internet for all the things/devices that we want to interact with. Gateways help to bridge the internal network of sensor nodes with the external Internet or World Wide Web. They do this by collecting the data from sensor nodes & transmitting it to the internet infrastructure.

Cloud/server infrastructure & Big Data – The data transmitted through gateway is stored & processed securely within the cloud infrastructure using Big Data analytics engine. This processed data is then used to perform intelligent actions that make all our devices 'Smart Devices'!

End-user Mobile apps – The intuitive mobile apps will help end users to control & monitor their devices (ranging from room thermostat to jet engines & assembly lines) from remote locations. These apps push the important information on your hand-held devices & help to send commands to your Smart Devices!

IPv6 – IP addresses are the backbone to the entire IoT ecosystem. Internet is concerned about IP addresses only & not if you are a human or a toaster. With IPv4 we were running out of IP addresses, but with IPv6 (launched in 2012) we now have 3.4*10^38 IP addresses!

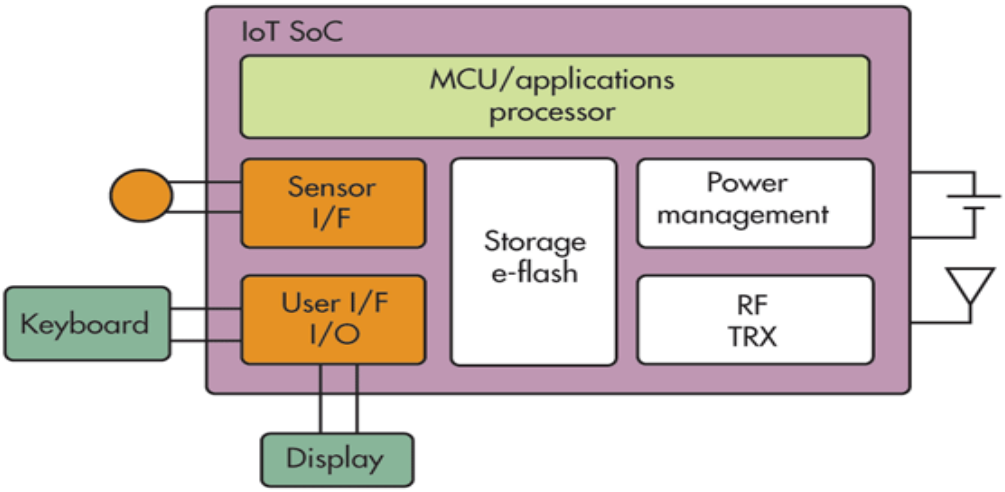


Fig: 2.3 IoT SOC

A temperature sensor network installed in the room will be integrated with the gateway. Gateway helps to connect the temperature sensor network (things) to the Internet through Cloud infrastructure.

Cloud/server possesses the detailed records about the each and every device connected to it – device id, current status of the device, who has accessed the device last time, how many times the device has been accessed and more.

Connection with the cloud is implemented using web services such as RESTful.

End-users like you and me interact with Cloud (and in turn devices installed in our homes) through the mobile app. Request will be sent to the cloud with the authentication and device information. Authentication is configured to ensure cyber security.

Cloud will identify the device with the help of the device id and will send the corresponding request to the appropriate sensor network using gateways.

Then, the temperature sensor will read the current temperature in the room and will send the response back to the cloud.

Cloud will identify the particular user who has requested the data and push the requested data to the app. So user will get the current information directly on his screen.

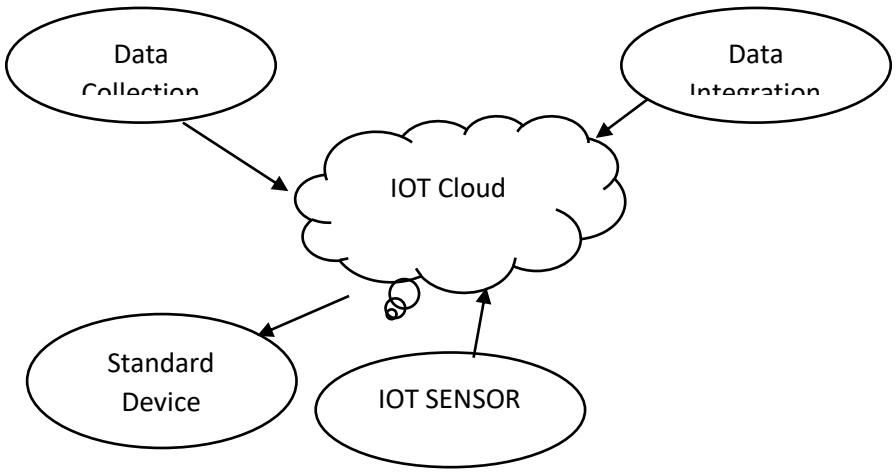


Fig : 2.4 : IoT Cloud Service

DATA COLLECTION

This software manages sensing, measurements, light data filtering, light data security, and aggregation of data. It uses certain protocols to aid sensors in connecting with real-time, machine-to-machine networks. Then it collects data from multiple devices and distributes it in accordance with settings. It also works in reverse by distributing data over devices. The system eventually transmits all collected data to a central server.

DEVICE INTEGRATION

Software supporting integration binds (dependent relationships) all system devices to create the body of the IoT system. It ensures the necessary cooperation and stable networking between devices. These applications are the defining software technology of the IoT network because without them, it is not an IoT system. They manage the various applications, protocols, and limitations of each device to allow communication

IOT SENSOR

The most important hardware in IoT might be its sensors. These devices consist of energy modules, power management modules, RF modules, and sensing modules. RF modules manage communications through their signal processing, WiFi, ZigBee, Bluetooth, radio transceiver, duplexer, and BAW.

STANDARD DEVICES

The desktop, tablet, and cellphone remain integral parts of IoT as the command center and remotes. The desktop provides the user with the highest level of control over the system and its settings. The tablet provides access to the key features of the system in a way resembling the desktop, and also acts as a remote.The cellphone allows some essential settings modification and also provides remote functionality.

REAL-TIME ANALYTICS

These applications take data or input from various devices and convert it into viable actions or clear patterns for human analysis. They analyze information based on various settings and designs in order to perform automation-related tasks or provide the data required by industry.

APPLICATION AND PROCESS EXTENSION

These applications extend the reach of existing systems and software to allow a wider, more effective system. They integrate predefined devices for specific purposes such as allowing certain mobile devices or engineering instruments access. It supports improved productivity and more accurate data collection.

IOT − KEY FEATURES

The most important features of IoT include artificial intelligence, connectivity, sensors, active engagement, and small device use. A brief review of these features is given below −

AI − IoT essentially makes virtually anything “smart”, meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favorite cereal run low, and to then place an order with your preferred grocer.

Connectivity − New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.

Sensors − IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.

Active Engagement − Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.

Small Devices − Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

IoT − Advantages

The advantages of IoT span across every area of lifestyle and business. Here is a list of some of the advantages that IoT has to offer −

Improved Customer Engagement − Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.

Technology Optimization − The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.

Reduced Waste − IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.

Enhanced Data Collection − Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyze our world. It allows an accurate picture of everything.

2.2 CONNECTED OF WIFI PORT WITH MICROCONTROLLER

GENERAL LAYOUT

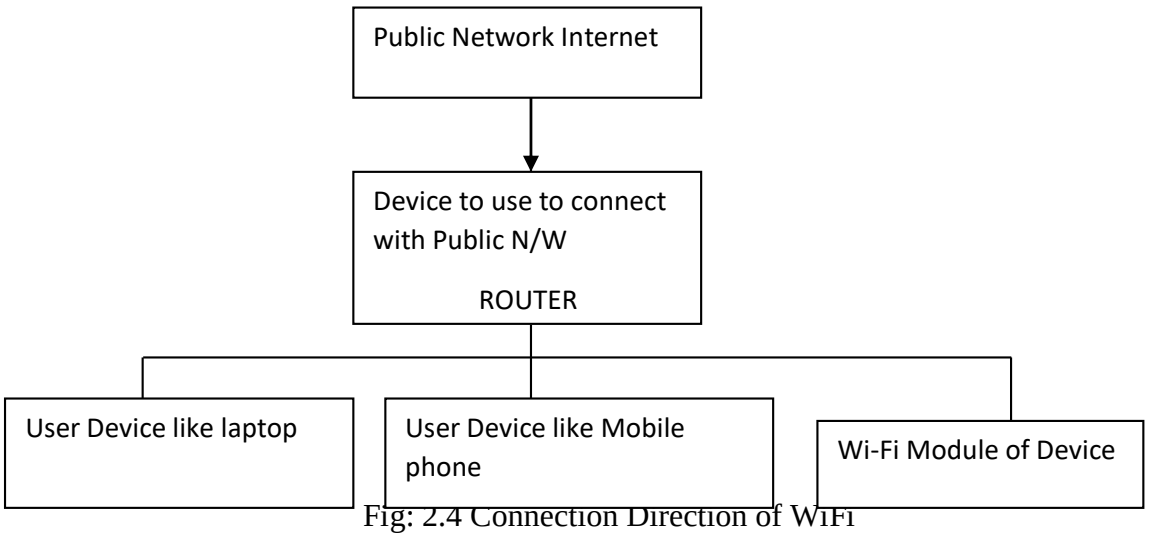


Fig: 2.4 Connection Direction of WiFi

2.3 IP ADDRESS ALLOCATION

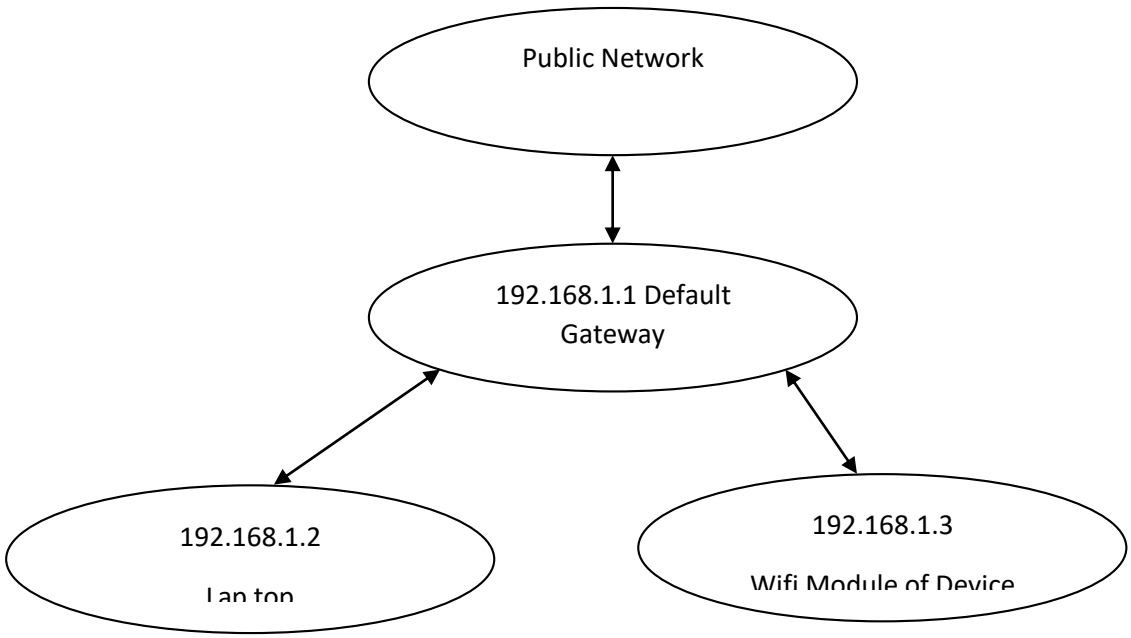


Fig: 2.5 IP Allocation

Wifi module used here is ESP8266 is a low-cost Wi-Fi chip with full TCP/IP stack and MCU (Micro Controller Unit). It has own modem which able to communicate with microcontroller by using AT command.

ESP-XX module then it needs to connect to the 3.3V TTL serial port during development. There are many USB to serial converter modules available which present a virtual serial connection to your host PC or laptop and connect to the chip's serial interface.

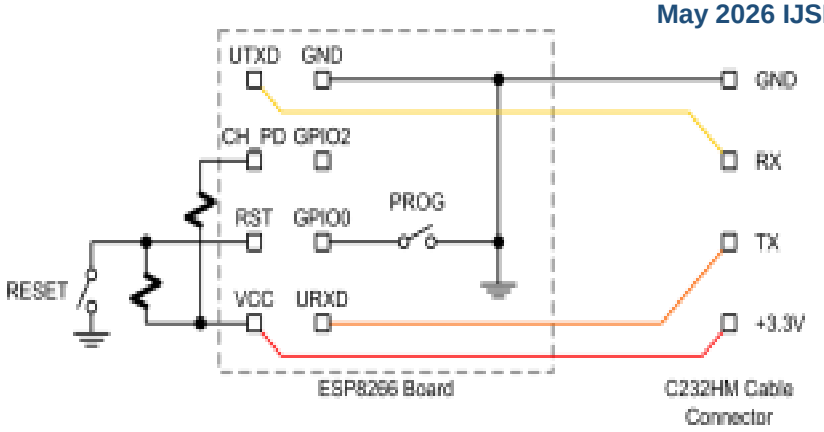


Fig :2.6 ESP8266 Module

ESP8266 WiFi module is used to connect microcontroller through RX and TX in TTL logic. Directly Tx and Rx line will connect to microcontroller without any level shifter. Configure baud rate between microcontroller and WiFi module as 9600bps serial type communication. Using AT Command configures IP address to WiFi module and get its own IP address for connection with browser.

ESP8266EX has been designed for mobile, wearable electronics and Internet of Things applications with the aim of achieving the lowest power consumption with a combination of several proprietary techniques. The power saving architecture operates mainly in 3 modes: active mode, sleep mode and deep sleep mode. By using advance power management techniques and logic to power-down functions not required and to control switching between sleep and active modes, ESP8266EX consumes about than 60uA in deep sleep mode (with RTC clock still running) and less than 1.0mA (DTIM=3) or less than 0.5mA (DTIM=10) to stay connected to the access point.

2.4 COMMANDS

AT+RST - Restart module.

AT+GMR - View version info.

AT+GSLP - Enter deep-sleep mode.

ATE - Enable / Disable echo.

AT+CWMODE - WIFI mode station, AP, station + AP）

AT+CWJAP - Connect to AP.

AT+CWLAP - Lists available APs.

AT Command is used to configure the Wifi Module with microcontroller through proper baud rate and serial link communication.

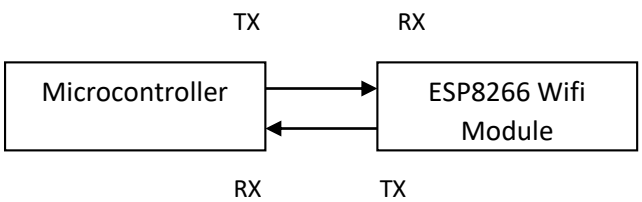


Fig :2.7 : Connection Between Wifi and Microcontroller

Data from microcontroller is send in serial format which acceptable by WiFi module

Atmega- 328

ATmega-328 is basically an Advanced Virtual RISC (AVR) micro-controller. It supports the data up to eight (8) bits. ATmega-328 has 32KB internal builtin memory. This micro-controller has a lot of other characteristics.

ATmega 328 has 1KB Electrically Erasable Programmable Read Only Memory (EEPROM). This property shows if the electric supply supplied to the micro-controller is removed, even then it can store the data and can provide results after providing it with the electric supply. Moreover, ATmega-328 has 2KB Static Random Access Memory (SRAM).

Other characteristics will be explained later. ATmega 328 has several different features which make it the most popular device in today's market. These features consist of advanced RISC architecture, good performance, low power consumption, real timer counter having separate oscillator, 6 PWM pins, programmable serial USART, programming lock for software security, throughput up to 20 MIPS etc. ATmega-328 is mostly used in Arduino.

ATmega328 is an eight (8) bit micro-controller. It can handle the data sized of up to eight (8) bits. It is an AVR based micro-controller. Its builtin internal memory is around 32KB. It operates ranging from 3.3V to 5V. It has an ability to store the data even when the electrical supply is removed from its biasing terminals. Its excellent features include the cost efficiency, low power dissipation, programming lock for security purposes, real timer counter with separate oscillator.

Atmega-328 is an AVR micro-controller having twenty eight (28) pins in total.

All of the pins in chronological order, are listed in the table shown in the figure given below.

ATmega328 Pins			
Pin Number	Pin Name	Pin Number	Pin Name
1	PC6	15	PB1
2	PD0	16	PB2
3	PD1	17	PB3
4	PD2	18	PB4
5	PD3	19	PB5
6	PD4	20	AVCC
7	Vcc	21	AREF
8	GND	22	GND
9	PB6	23	PC0
10	PB7	24	PC1
11	PD5	25	PC2
12	PD6	26	PC3
13	PD7	27	PC4
14	PB0	28	PC5

VCC is a digital voltage supply.

AVCC is a supply voltage pin for analog to digital converter.

GND denotes Ground and it has a 0V.

Port A consists of the pins from PA0 to PA7. These pins serve as analog input to analog to digital converters. If analog to digital converter is not used, port A acts as an eight (8) bit bidirectional input/output port.

Port B consists of the pins from PB0 to PB7. This port is an 8 bit bidirectional port having an internal pull-up resistor.

Port C consists of the pins from PC0 to PC7. The output buffers of port C has symmetrical drive characteristics with source capability as well high sink.

Port D consists of the pins from PD0 to PD7. It is also an 8 bit input/output port having an internal pull-up resistor.

ATmega 328 has three types of memories e.g. EEPROM, SRAM etc.

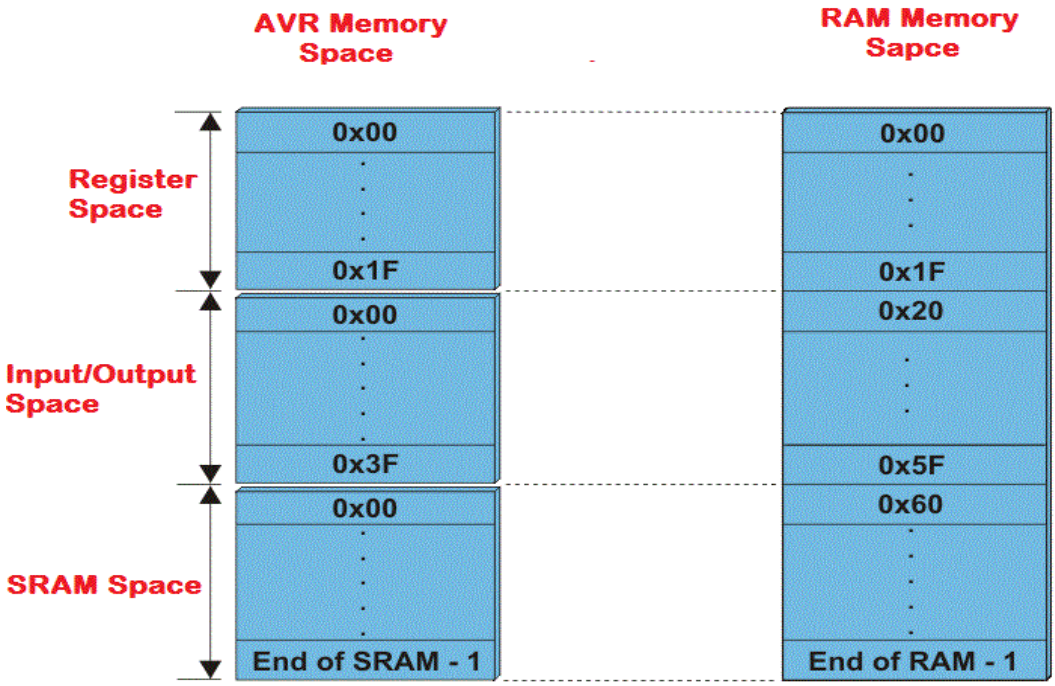
The capacity of each memory is eplained in detail below.

Flash Memory has 32KB capacity. It has an address of 15 bits. It is a Programmable Read Only Memory (ROM). It is non volatile memory.

SRAM stands for Static Random Access Memory. It is a volatile memory i.e. data will be removed after removing the power supply.

EEPROM stands for Electrically Erasable Programmable Read Only Memory. It has a long term data.

AVR Memory Spaces



ATmega-328 has thirty two (32) General Purpose (GP) registers.

These all of the registers are the part of Static Random Access Memory (SRAM).

All the registers are given in the figure shown below.

AVR General Purpose Registers

7 0	Addr.
R0	0x00
R1	0x01
R2	0x02
...	
R13	0x0D
R14	0x0E
R15	0x0F
R16	0x10
R17	0x11
...	
R26	0x1A
R27	0x1B
R28	0x1C
R29	0x1D
R30	0x1E
R31	0x1F

The different versions of the same device are denoted by the different packages of that device. Each package has different dimensions, in order to differentiate easily. ATmega 328 packages are given in the table shown in the figure given below. A complete package including ATmega 328 and Arduino can be used in several different real life applications.

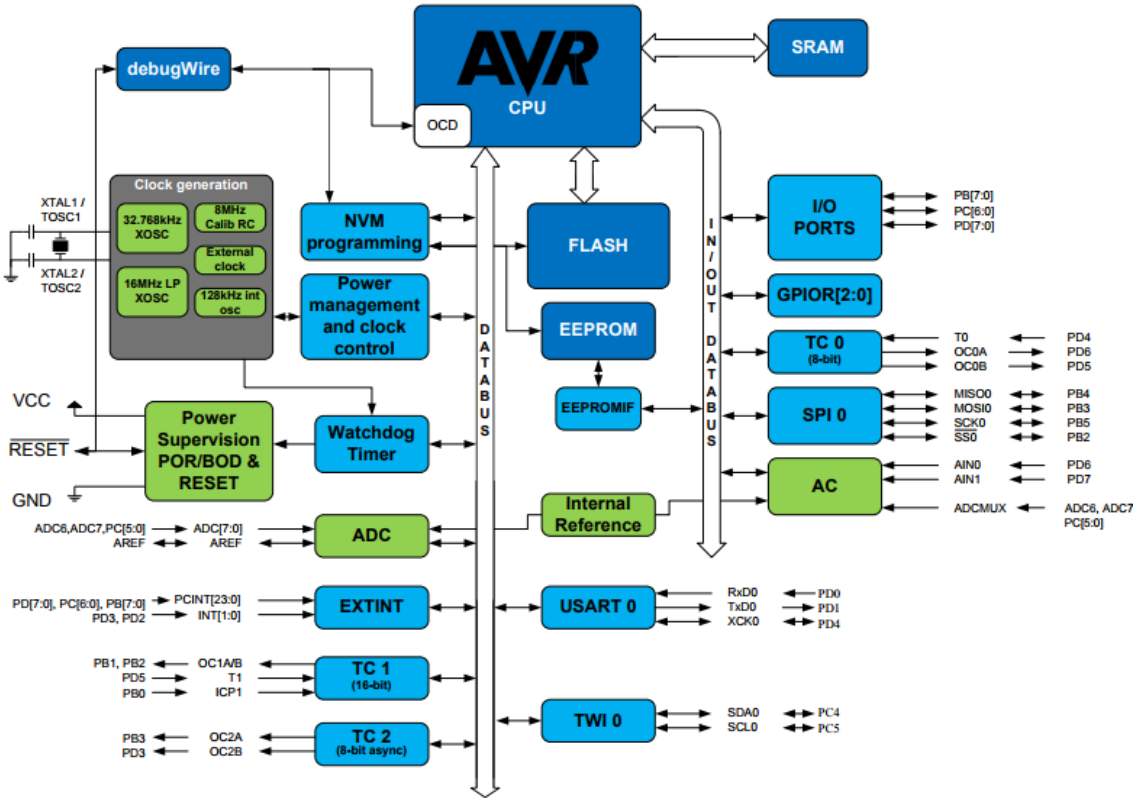
It can be used in embedded systems projects.

It can also be used in robotics.

Quad-copter and even small aeroplanes can also be designed through it.

Power monitoring and management systems can also be prepared using this device.

ATmega328 Block Diagram



Analog comparator: On-chip analog comparator is available. An interrupt is assigned for different comparison result obtained from the inputs.

External Interrupt: 3External interrupt is accepted. Interrupt sense is configurable.

Memory: It has 32Kbytes of In-System Self-programmable Flash program memory, 1024 Bytes EEPROM, 2Kbytes Internal SRAM. Write/Erase Cycles: 10,000 Flash / 100,000 EEPROM.

Clock: It can run at a frequency from 1 to 16 MHz. Frequency can be obtained from external Quartz Crystal, Ceramic crystal or an R-C network. Internal calibrated RC oscillator can also be used.

More Features: Up to 16 MIPS throughput at 16MHz. Most of the instruction executes in a single cycle. Two cycle on-chip multiplication. 32 × 8 General Purpose Working Registers

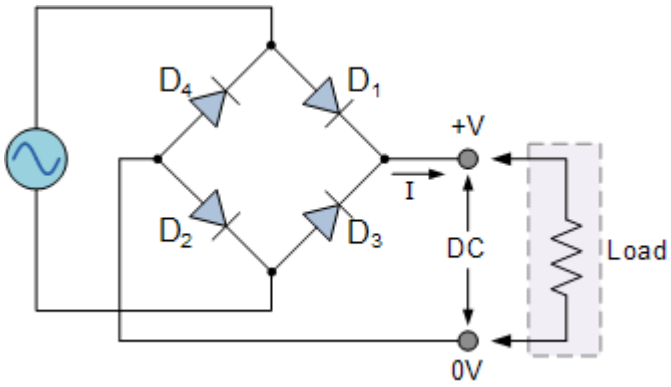
Debug: JTAG boundary scan facilitates on chip debug.

Programming: Atmega32 can be programmed either by In-System Programming via Serial peripheral interface or by Parallel programming. Programming via JTAG interface is also possible. Programmer must ensure that SPI programming and JTAG are not be disabled using fuse bits; if the programming is supposed to be done using SPI or JTAG.

DIODE BRIDGE RECTIFIER:

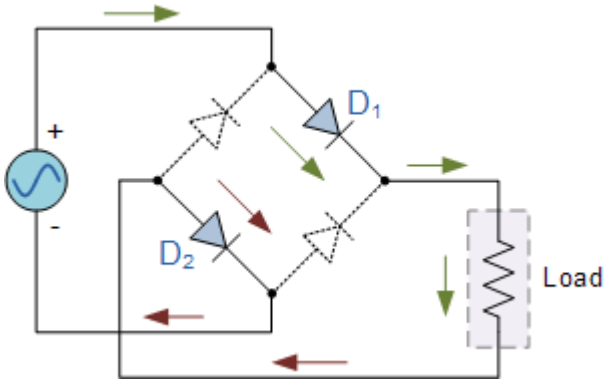
Full Wave Bridge Rectifier

The single phase rectifier uses four individual rectifying diodes connected in a closed loop "bridge" configuration to produce the desired output. The main advantage of this bridge circuit is that it does not require a special centre tapped transformer, thereby reducing its size and cost. The single secondary winding is connected to one side of the diode bridge network and the load to the other side as shown below.



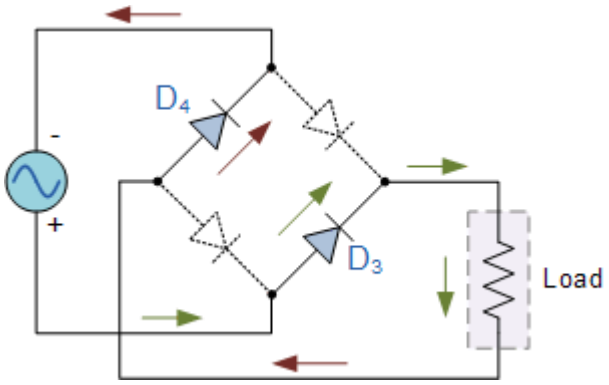
The four diodes labelled D1 to D4 are arranged in "series pairs" with only two diodes conducting current during each half cycle. During the positive half cycle of the supply, diodes D1 and D2 conduct in series while diodes D3 and D4 are reverse biased and the current flows through the load as shown below.

THE POSITIVE HALF-CYCLE



During the negative half cycle of the supply, diodes D3 and D4 conduct in series, but diodes D1 and D2 switch "OFF" as they are now reverse biased. The current flowing through the load is the same direction as before.

THE NEGATIVE HALF-CYCLE



As the current flowing through the load is unidirectional, so the voltage developed across the load is also unidirectional the same as for the previous two diode full-wave rectifier, therefore the average DC voltage across the load is 0.637Vmax.

However in reality, during each half cycle the current flows through two diodes instead of just one so the amplitude of the output voltage is two voltage drops (2 x 0.7 = 1.4V) less than the input VMAX amplitude. The ripple frequency is now twice the supply frequency (e.g. 100Hz for a 50Hz supply or 120Hz for a 60Hz supply.)

Although we can use four individual power diodes to make a full wave bridge rectifier, pre-made bridge rectifier components are available “off-the-shelf” in a range of different voltage and current sizes that can be soldered directly into a PCB circuit board or be connected by spade connectors.

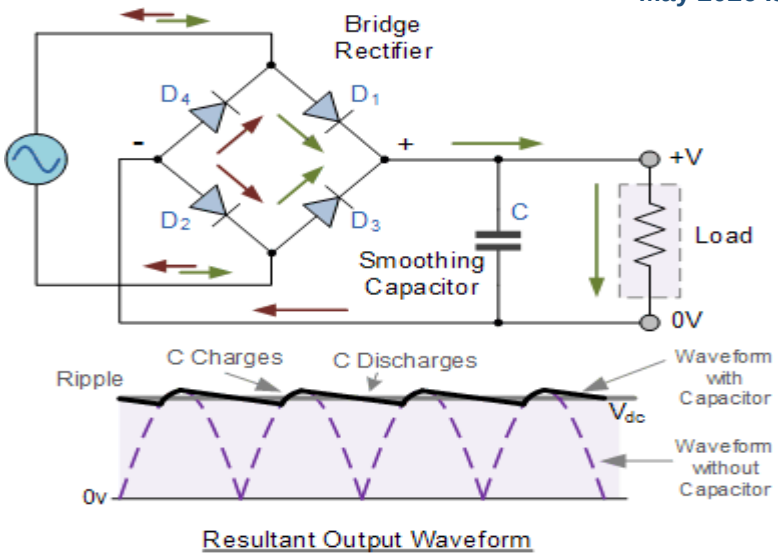
The image to the right shows a typical single phase bridge rectifier with one corner cut off. This cut-off corner indicates that the terminal nearest to the corner is the positive or +ve output terminal or lead with the opposite (diagonal) lead being the negative or -ve output lead. The other two connecting leads are for the input alternating voltage from a transformer secondary winding.

THE SMOOTHING CAPACITOR:

The smoothing capacitor converts the full-wave rippled output of the rectifier into a smooth DC output voltage. Generally for DC power supply circuits the smoothing capacitor is an Aluminum Electrolytic type that has a capacitance value of 100uF or more with repeated DC voltage pulses from the rectifier charging up the capacitor to peak voltage.

However, there are two important parameters to consider when choosing a suitable smoothing capacitor and these are its Working Voltage, which must be higher than the no-load output value of the rectifier and its Capacitance Value, which determines the amount of ripple that will appear superimposed on top of the DC voltage.

Too low a capacitance value and the capacitor has little effect on the output waveform. But if the smoothing capacitor is sufficiently large enough (parallel capacitors can be used) and the load current is not too large, the output voltage will be almost as smooth as pure DC.



Resultant Output Waveform

LINEAR REGULATOR:

The function of a linear voltage regulator is to convert a varying DC voltage to a constant, often specific, lower DC voltage. In addition, they often provide a current limiting function to protect the power supply and load from over current (excessive, potentially destructive current).

A constant output voltage is required in many power supply applications, but the voltage provided by many energy sources will vary with changes in load impedance.

Furthermore, when an unregulated DC power supply is the energy source, its output voltage will also vary with changing input voltage. To circumvent this, some power supplies use a linear voltage regulator to maintain the output voltage at a steady value, independent of fluctuations in input voltage and load impedance. Linear regulators can also reduce the magnitude of ripple and noise present appearing on the output voltage.

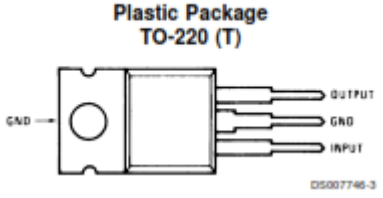
Common solid-state series voltage regulators are the LM78xx (for positive voltages) and LM79xx (for negative voltages), and common fixed voltages are 5 V (for transistor-transistor logic circuits) and 12 V (for communications circuits and peripheral devices such as disk drives).

In fixed voltage regulators the reference pin is tied to ground, whereas in variable regulators the reference pin is connected to the centre point of a fixed or variable voltage divider fed by the regulator's output.

FIXED REGULATORS:

"Fixed" three-terminal linear regulators are commonly available to generate fixed voltages of plus 3 v, and plus or minus 5 v, 6v, 9 v, 12 v, or 15 v, when the load is less than 1.5 amperes.

The "78xx" series (7805, 7812, etc.) regulate positive voltages while the "79xx" series (7905, 7912, etc.) regulate negative voltages. Often, the last two digits of the device number are the output voltage; e.g., a 7805 is a +5 v regulator, while a 7915 is a −15 v regulator. There are variants on the 78xx series ICs, such as 78l and 78s, some of which can supply up to 1.5 amps.



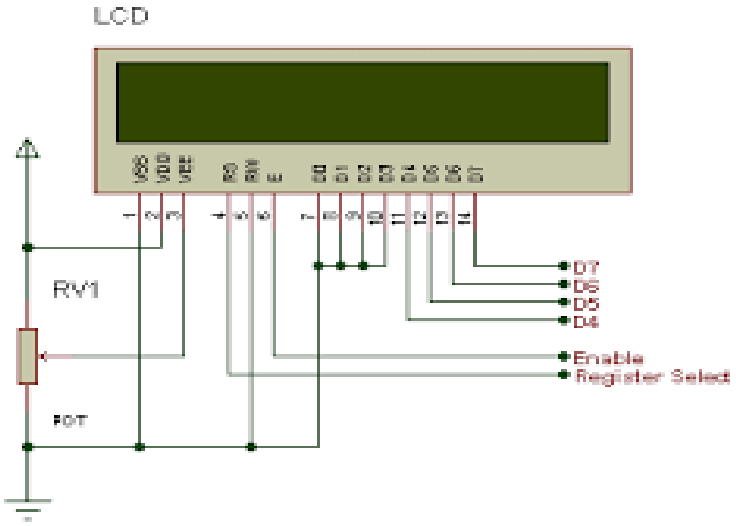
LCD DISPLAY:

The most commonly used Character based LCDs are based on Hitachi's HD44780 controller or other which are compatible with HD44580. In this project document, we will discuss about character based LCDs, their interfacing with various microcontrollers, various interfaces (8-bit/4-bit), programming, special stuff and tricks you can do with these simple looking LCDs which can give a new look to your application. LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits. These modules are preferred over seven segments and other multi segment LEDs. The reasons being: LCDs are economical; easily programmable; have no limitation of displaying special & even custom characters (unlike in seven segments), animations and so on.

A 16x2 LCD means it can display 16 characters per line and there are 2 such lines. In this LCD each character is displayed in 5x7 pixel matrix. This LCD has two registers, namely, Command and Data.

The command register stores the command instructions given to the LCD. A command is an instruction given to LCD to do a predefined task like initializing it, clearing its screen, setting the cursor position, controlling display etc. The data register stores the data to be displayed on the LCD. The data is the ASCII value of the character to be displayed on the LCD.

LCD Interface Circuit:



Pin Details:

PIN NUMBER	SYMBOL	FUNCTION
1	Vss	GND
2	Vdd	+ 3V or + 5V
3	Vo	Contrast Adjustment
4	RS	H/L Register Select Signal
5	R/$\overline{W}$	H/L Read/Write Signal
6	E	H →L Enable Signal
7	DB0	H/L Data Bus Line
8	DB1	H/L Data Bus Line
9	DB2	H/L Data Bus Line
10	DB3	H/L Data Bus Line
11	DB4	H/L Data Bus Line
12	DB5	H/L Data Bus Line
13	DB6	H/L Data Bus Line
14	DB7	H/L Data Bus Line
15	A/Vee	+ 4.2V for LED/Negative Voltage Output
16	K	Power Supply for B/L (OV)

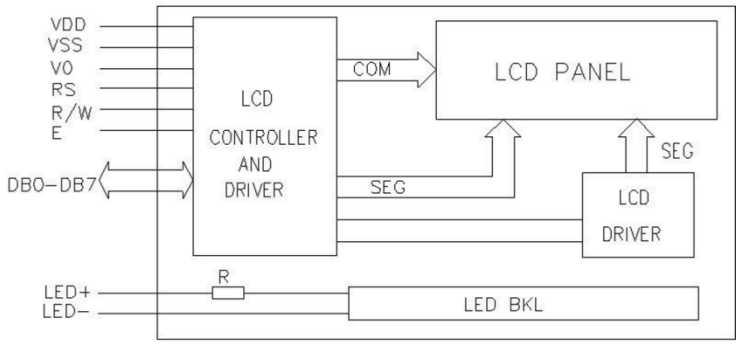
The LCD standard requires 3 control lines and 8 I/O lines for the data bus. Liquid Crystal Display is very important device in embedded system. It offers higher flexibility as the user can display any data on it. Copy and paste technique may not work when an embedded system engineer wants to apply LCD interfacing in real world projects.First thing to begin with is to know what LCD driver/controller is used LCD. LCD driver provides a link between microcontroller and LCD. In LCD initialization user has to send command bytes to LCD. Here the user sets the interface mode, display mode, address counter increment direction, set contrast of LCD, horizontal or vertical addressing mode, color format. The command register stores the command instructions given to the LCD.

A command is an instruction given to LCD to do a predefined task like initializing it, clearing its screen, setting the cursor position, controlling display etc.

The registers stores the data to be displayed on the LCD.

16 characters *2 lines display

4-bit or 8-bit MPU interfaces Display mode and back light variations



LCD Pin Description

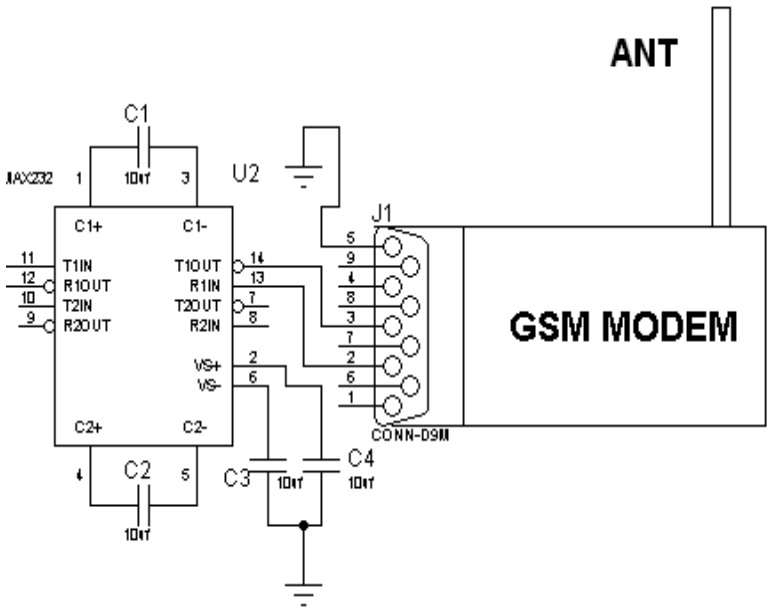
GSM MODEM

Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz.

Today the GSM cell or mobile phone system is the most popular in the world. GSM handsets are widely available at good prices and the networks are robust and reliable. The GSM system is also feature-rich with applications such as SMS text messaging, international roaming, SIM cards and the like. It is also being enhanced with technologies including GPRS and EDGE. To achieve this level of success has taken many years and is the result of both technical development and international cooperation.

A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves. The working of GSM modem is based on commands, the commands always start with AT (which means ATtention) and finish with a <CR> character. For example, the dialing command is ATD<number>; ATD3314629080; here the dialing command ends with semicolon.

The AT commands are given to the GSM modem with the help of PC or controller. The GSM modem is serially interfaced with the controller with the help of MAX 232. Here max 232 acts as driver which converts TTL levels to the RS 232 levels. For serial interface GSM modem requires the signal based on RS 232 levels. The T1_OUT and R1_IN pin of MAX 232 is connected to the TX and RX pin of GSM modem



Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz.

Today the GSM cell or mobile phone system is the most popular in the world. GSM handsets are widely available at good prices and the networks are robust and reliable. The GSM system is also feature-rich with applications such as SMS text messaging, international roaming, SIM cards and the like. It is also being enhanced with technologies including GPRS and EDGE. To achieve this level of success has taken many years

and is the result of both technical development and international cooperation. The GSM history can be seen to be a story of cooperation across Europe, and one that nobody thought would lead to the success that GSM is today.

The first cell phone systems that were developed were analogue systems. Typically they used frequency-modulated carriers for the voice channels and data was carried on a separate shared control channel. When compared to the systems employed today these systems were comparatively straightforward and as a result a vast number of systems appeared. Two of the major systems that were in existence were the AMPS (Advanced Mobile Phone System) that was used in the USA and many other countries and TACS (Total Access Communications System) that was used in the UK as well as many other countries around the world.

Another system that was employed, and was in fact the first system to be commercially deployed was the Nordic Mobile Telephone system (NMT). This was developed by a consortium of companies in Scandinavia and proved that international cooperation was possible.

The success of these systems proved to be their downfall. The use of all the systems installed around the globe increased dramatically and the effects of the limited frequency allocations were soon noticed. To overcome these a number of actions were taken. A system known as E-TACS or Extended-TACS was introduced giving the TACS system further channels. In the USA another system known as Narrowband AMPS (NAMPS) was developed.

Neither of these approaches proved to be the long-term solution as cellular technology needed to be more efficient. With the experience gained from the NMT system, showing that it was possible to develop a system across national boundaries, and with the political situation in Europe lending itself to international cooperation it was decided to develop a new Pan-European System. Furthermore it was realized that economies of scale would bring significant benefits. This was the beginnings of the GSM system.

To achieve the basic definition of a new system a meeting was held in 1982 under the auspices of the Conference of European Posts and Telegraphs (CEPT). They formed a study group called the Groupe Special Mobile (GSM) to study and develop a pan-European public land mobile system. Several basic criteria that the new cellular technology would have to meet were set down for the new GSM system to meet.

These included good subjective speech quality, low terminal and service cost, support for international roaming, ability to support handheld terminals, support for range of new services and facilities, spectral efficiency, and finally ISDN compatibility.

With the levels of under-capacity being projected for the analogue systems, this gave a real sense of urgency to the GSM development. Although decisions about the exact nature of the cellular technology were not taken at an early stage, all parties involved had been working toward a digital system. This decision was finally made in February 1987. This gave a variety of advantages. Greater levels of spectral efficiency could be gained, and in addition to this the use of digital circuitry would allow for higher levels of integration in the circuitry. This in turn would result in cheaper handsets with more features. Nevertheless significant hurdles still needed to be overcome. For example, many of the methods for encoding the speech within a sufficiently narrow bandwidth needed to be developed, and this posed a significant risk to the project. Nevertheless the GSM system had been started. A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves. The working of GSM modem is based on commands, the commands always start with AT (which means ATtention) and finish with a <CR> character. For example, the dialing command is ATD<number>; ATD3314629080; here the dialing command ends with semicolon.

The AT commands are given to the GSM modem with the help of PC or controller. The GSM modem is serially interfaced with the controller with the help of MAX 232. Here max 232 acts as driver which

converts TTL levels to the RS 232 levels. For serial interface GSM modem requires the signal based on RS 232 levels. The T1_OUT and R1_IN pin of MAX 232 is connected to the TX and RX pin of GSM modem.

GSM/GPRS RS232 Modem is built with SIMCOM Make SIM900 Quad-band GSM/GPRS engine, works on frequencies 850 MHz, 900 MHz, 1800 MHz and 1900 MHz. It is very compact in size and easy to use as plug in GSM Modem.

The Modem is designed with RS232 Level converter circuitry, which allows you to directly interface PC Serial port .The baud rate can be configurable from 9600-115200 through AT command. Initially Modem is in Auto baud mode. This GSM/GPRS RS232 Modem is having internal TCP/IP stack to enable you to connect with internet via GPRS. It is suitable for SMS as well as DATA transfer application in M2M interface.

The modem needed only 3 wires (Tx,Rx,GND) except Power supply to interface with microcontroller/Host PC. The built in Low Dropout Linear voltage regulator allows you to connect wide range of unregulated power supply (4.2V -13V). Yes, 5 V is in between !! .Using this modem, you will be able to send & Read SMS, connect to internet via GPRS through simple AT commands.

GSM Transceiver GSM (or Global System for Mobile Communications) was developed in 1990. The first GSM operator has subscribers in 1991, the beginning of 1994 the network based on the standard, already had 1.3 million subscribers, and the end of 1995 their number had increased to 10 million!

There were first generation mobile phones in the 70's, there are 2nd generation mobile phones in the 80's and 90's, and now there are 3rd gen phones which are about to enter the Indian market. GSM is called a 2ndgeneration, or 2G communications technology. In this project it acts as a SMS Receiver and SMS sender. The GSM technical specifications define the different entities that form the GSM network by defining their functions and interface requirements.

Global system for mobile communication (gsm) is a set of etsi standards specifying the infrastructure for a digital cellular service. The standard is used in approx. 85 countries in the world including such locations as europe, japan and Australia.

The GSM technical specifications define the different elements within the GSM network architecture. It defines the different elements and the ways in which they interact to enable the overall system operation to be maintained. The GSM network architecture is now well established and with the other later cellular systems now established and other new ones being deployed.

The basic GSM network architecture has been updated to interface to the network elements required by these systems. Despite the developments of the newer systems, the basic GSM system architecture has been maintained, and the network elements described below perform the same functions as they did when the original GSM system was launched in the early 1990s.GSM network architecture elements

CHAPTER 5

5. SOFTWARE MODULE

5.1 SOFTWARE TOOL

Arduino is an open source, computer hardware and software company, project, and user community that designs and manufactures microcontroller kits for building digital devices and interactive objects that can sense and control objects in the physical world. The project's products are distributed as open-source hardware and software, which are licensed under the GNU Lesser General Public License (LGPL) or the GNU General Public License (GPL),[1] permitting the manufacture of Arduino boards and software distribution by anyone. Arduino boards are available commercially in preassembled form, or as do-it-yourself kits.

Arduino board designs use a variety of microprocessors and controllers. The boards are equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (*shields*) and other circuits. The boards feature serial communications interfaces, including Universal Serial Bus (USB) on some models, which are also used for loading programs from personal computers. The microcontrollers are typically programmed using a dialect of features from the programming languages C and C++. In addition to using traditional compiler toolchains, the Arduino project provides an integrated development environment (IDE) based on the Processing language project.

The Arduino project started in 2003 as a program for students at the Interaction Design Institute Ivrea in Ivrea, Italy,[2] aiming to provide a low-cost and easy way for novices and professionals to create devices that interact with their environment using sensors and actuators. Common examples of such devices intended for beginner hobbyists include simple robots, thermostats, and motion detectors.

Over the years Arduino has been the brain of thousands of projects, from everyday objects to complex scientific instruments. A worldwide community of makers - students, hobbyists, artists, programmers, and professionals - has gathered around this open-source platform, their contributions have added up to an incredible amount of accessible knowledge that can be of great help to novices and experts alike.

Arduino was born at the Ivrea Interaction Design Institute as an easy tool for fast prototyping, aimed at students without a background in electronics and programming. As soon as it reached a wider community, the Arduino board started changing to adapt to new needs and challenges, differentiating its offer from simple 8-bit boards to products for IoT applications, wearable, 3D printing, and embedded environments. All Arduino boards are completely open-source, empowering users to build them independently and eventually adapt them to their particular needs. The software, too, is open-source, and it is growing through the contributions of users worldwide.

There are many other microcontrollers and microcontroller platforms available for physical computing. Parallax Basic Stamp, Netmedia's BX-24, Phidgets, MIT's Handyboard, and many others offer similar functionality. All of these tools take the messy details of microcontroller programming and wrap it up in an easy-to-use package. Arduino also simplifies the process of working with microcontrollers, but it offers some advantage for teachers, students, and interested amateurs over other systems:

- **Inexpensive** - Arduino boards are relatively inexpensive compared to other microcontroller platforms. The least expensive version of the Arduino module can be assembled by hand, and even the pre-assembled Arduino modules cost less than $50
- **Cross-platform** - The Arduino Software (IDE) runs on Windows, Macintosh OSX, and Linux operating systems. Most microcontroller systems are limited to Windows.

- **Simple, clear programming environment** - The Arduino Software (IDE) is easy-to-use for beginners, yet flexible enough for advanced users to take advantage of as well. For teachers, it's conveniently based on the Processing programming environment, so students learning to program in that environment will be familiar with how the Arduino IDE works.
- **Open source and extensible software** - The Arduino software is published as open source tools, available for extension by experienced programmers. The language can be expanded through C++ libraries, and people wanting to understand the technical details can make the leap from Arduino to the AVR C programming language on which it's based. Similarly, you can add AVR-C code directly into your Arduino programs if you want to.
- **Open source and extensible hardware** - The plans of the Arduino boards are published under a Creative Commons license, so experienced circuit designers can make their own version of the module, extending it and improving it. Even relatively inexperienced users can build the breadboard version of the module in order to understand how it works and save money.

Variables

A *variable* is a place for storing a piece of data. It has a name, a type, and a value. For example, the line from the Blink sketch above declares a variable with the name ledPin, the type int, and an initial value of 13. It's being used to indicate which Arduino pin the LED is connected to. Every time the name ledPin appears in the code, its value will be retrieved. In this case, the person writing the program could have chosen not to bother creating the ledPin variable and instead have simply written 13 everywhere they needed to specify a pin number. The advantage of using a variable is that it's easier to move the LED to a different pin: you only need to edit the one line that assigns the initial value to the variable.

Functions

A *function* (otherwise known as a *procedure* or *sub-routine*) is a named piece of code that can be used from elsewhere in a sketch. For example, here's the definition of the setup() function from the Blink example:

```
void setup()
{
        pinMode(ledPin, OUTPUT);
}
```

The first line provides information about the function, like its name, "setup". The text before and after the name specify its return type and parameters: these will be explained later. The code between the { and } is called the *body* of the function: what the function does.

pinMode(), digitalWrite(), and delay()

The pinMode() function configures a pin as either an input or an output. To use it, you pass it the number of the pin to configure and the constant INPUT or OUTPUT. When configured as an input, a pin can detect the state of a sensor like a pushbutton; As an output, it can drive an actuator like an LED.

The digitalWrite() functions outputs a value on a pin.

For example, the line:

digitalWrite(ledPin, HIGH);

The delay() causes the Arduino to wait for the specified number of milliseconds before continuing on to the next line. There are 1000 milliseconds in a second, so the line:

delay(1000);

setup() and loop()

There are two special functions that are a part of every Arduino sketch: setup() and loop(). The setup() is called once, when the sketch starts. It's a good place to do setup tasks like setting pin modes or initializing libraries. The loop() function is called over and over and is heart of most sketches. You need to include both functions in your sketch, even if you don't need them for anything.

Everything between the /* and */ is ignored by the Arduino when it runs the sketch (the * at the start of each line is only there to make the comment look pretty, and isn't required). It's there for people reading the code: to explain what the program does, how it works, or why it's written the way it is. It's a good practice to comment your sketches, and to keep the comments up-to-date when you modify the code. This helps other people to learn from or modify your code.

5.1 ATMEL STUDIO 7:

ATMEL Studio is an Integrated Development Environment (IDE) for writing and debugging applications for AVR/ARM platforms. Currently as a code writing environment, it supports the included AVR Assembler and any external AVRGCC/ARMGCC compiler in a complete IDE environment.

Using ATMEL Studio as an IDE gives you several advantages:

1. Editing and debugging in the same application window allows for a faster error tracking.
2. Breakpoints are saved and restored between sessions, even if the code was edited in the meantime.
3. Project item management is made convenient and portable.

4.2 PROGRAMMING FOR ATMEGA IC:

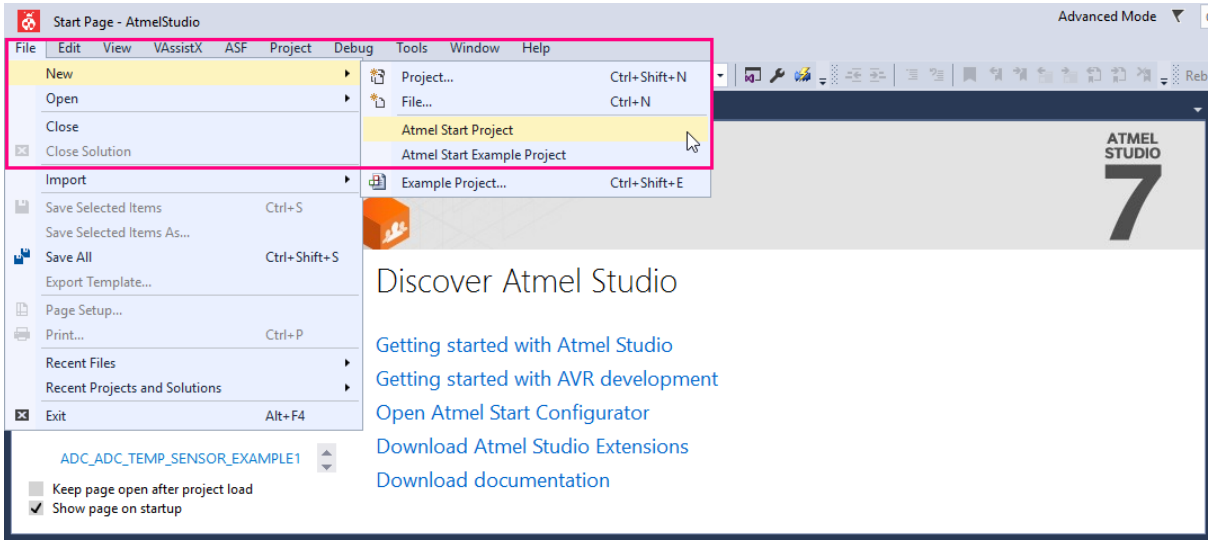
1. Go to the ATMEL website and download ATMEL studio 7. The download link is below and it can be download and install either the web installer or the offline installer.
2. The second step to program ARDUINO using ATMEL Studio 7 is to add AVR dude as an external tool. To do this, open ATMEL studio and go to Tool > External Tools. There you will see a form for specifying external tool. Here we have to setup the AVRdude.exe that ARDUINO uses as our external tool so that ATMEL studio can use it.
3. The final step to program ARDUINO using ATMEL Studio 7 is to write, compile and upload the program into the Microcontroller via USB. As we said we will use C program to write the code. Start a new GCC C Executable Project, provide some name and finally select the ATMEGA328P as your device. This also works if you want to use C++ programming language.
4. The External Tool ARDUINO UNO Programmer that we created in the earlier step. But before that you have to connect the ARDUINO to your PC.
5. To do this, go to Tools menu in the toolbar and select/click ARDUINO UNO Programmer. The hex code will be burned into the microcontroller and you should see a message “avrdude.exe done. Thank you.” in the output window.

To use ARDUINO Uno (with ATMEGA328P device) outside of the ARDUINO software environment. We will use ATMEL Studio 7 for programming the ARDUINO Uno in C. The use of ATMEL Studio gives you complete flexibility and control over microcontroller and will help you to create interesting ARDUINO Uno Projects. The board used in this tutorial is ARDUINO Uno R3.

Creating a New Solution

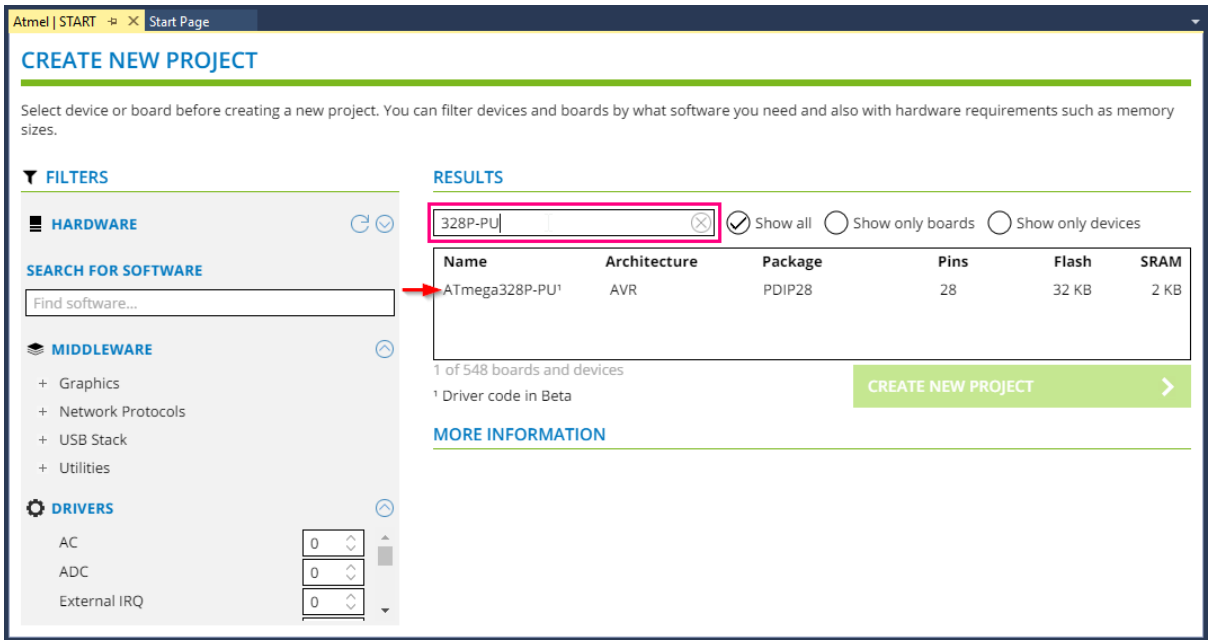
Launch ATMEL Studio 7

Click File > New > ATMEL Start Project



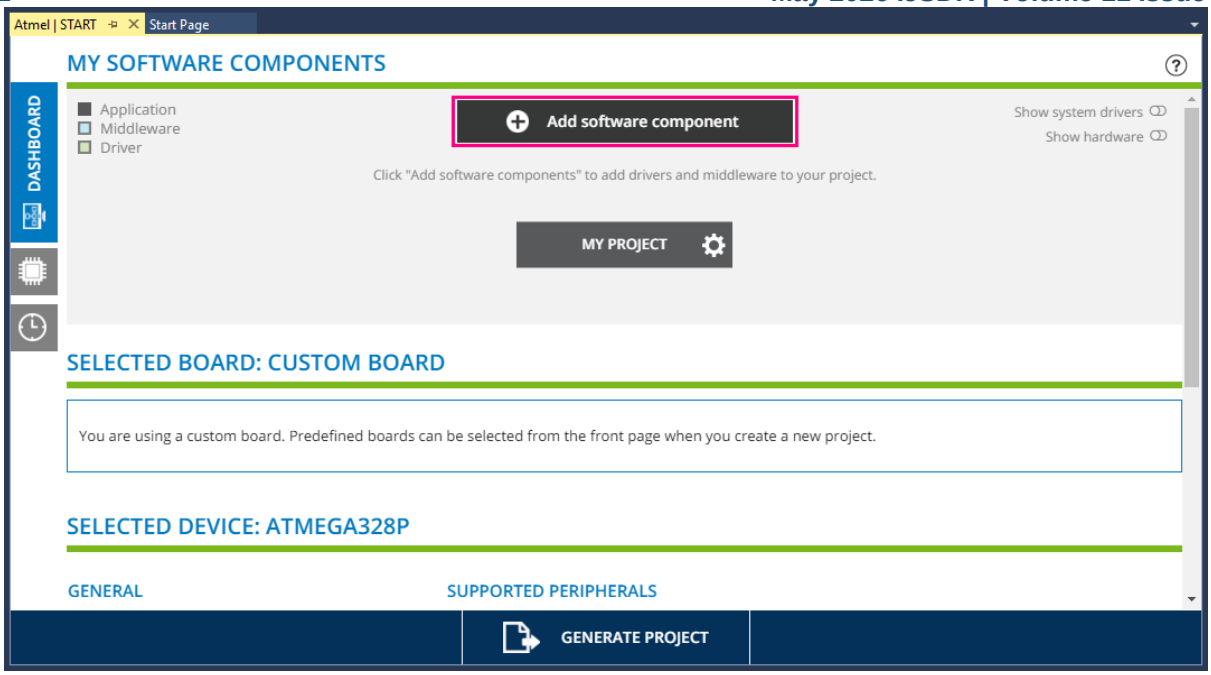
This will open the ATMEL Start Wizard, you will see Create New Project page.

Type 328P-PU in the device filter box and select ATMEGA328P-PU from the list and click on CREATE NEW PROJECT button

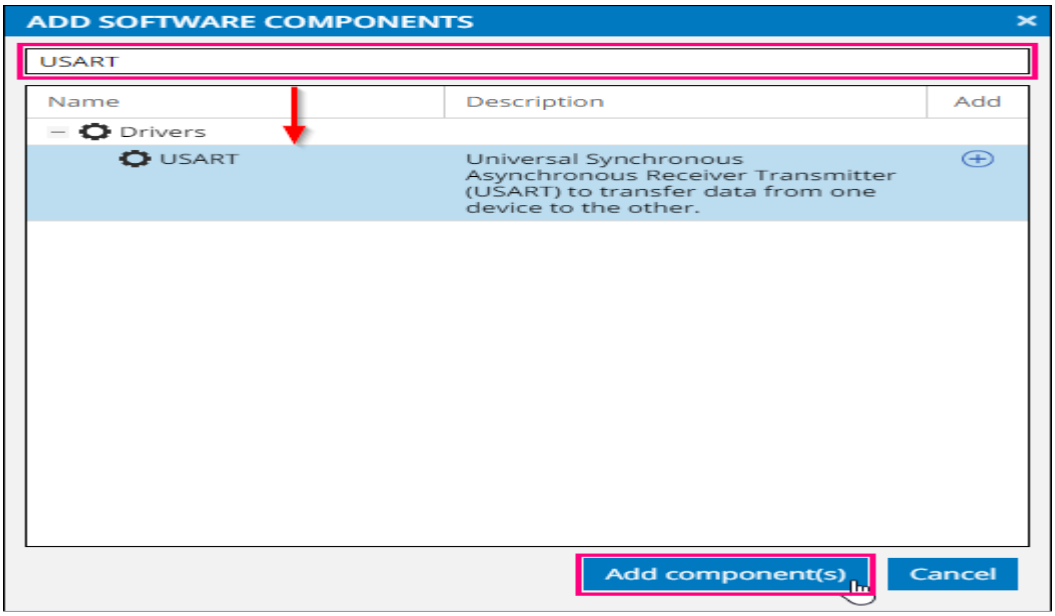


Now you will see the DASHBOARD On this page we will have to add software libraries which we are planning to use for our project. These software libraries are referred to as Software Components in ATMEL Studio Environment.

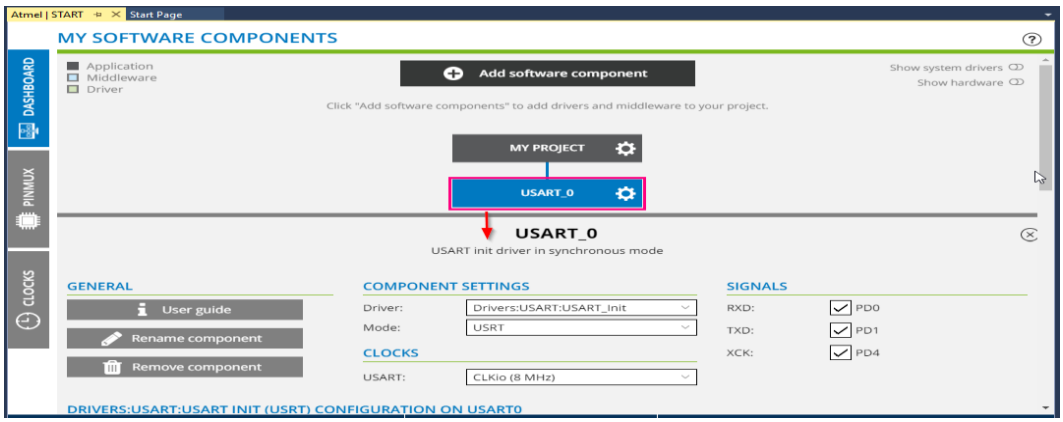
Under MY SOFTWARE COMPONENTS section, click on Add Software Component button.



You will see the list of available Middleware and Driver components for the device that you have selected. Type USART in the Filter text box, select USART driver from the list of displayed drivers and click Add component(s) You can repeat this process multiple times to add more software components



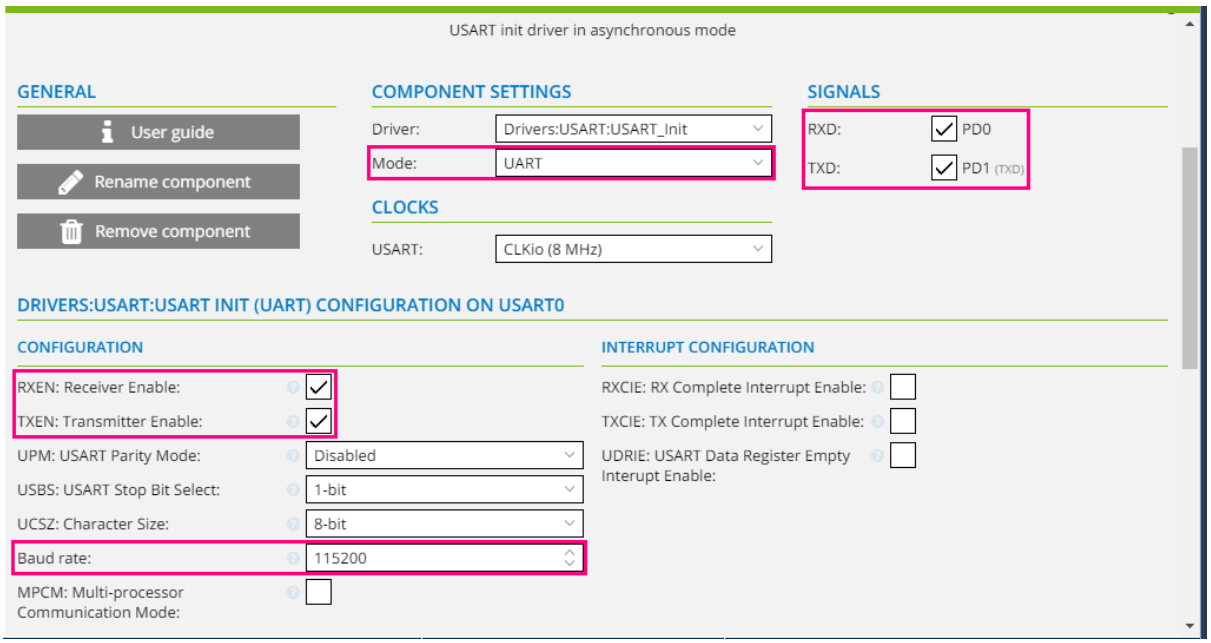
You will see a software component USART_0 has got added in the project.
Click on the USART_0 This opens the USART configuration pane.



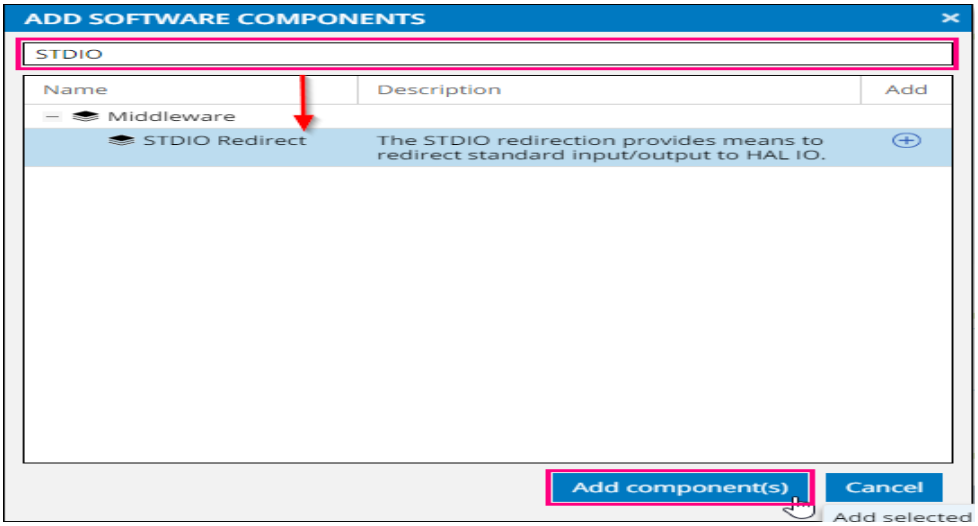
In the USART_0 configuration pane, select the following settings :
Component Settings
Mode: UART
We need asynchronous operation without flow control to keep things simple. This is how most of the people will use UART on any microcontroller.

SIGNALS:
Ensure both RXD and TXD have been selected. The RXD signal is on PD0, and TXD signal is on PD1 pin of the microcontroller

CONFIGURATION:
RXEN: Receiver Enable should be selected
TXEN: Transmitter Enable should be selected
Baud rate should be set to 115200

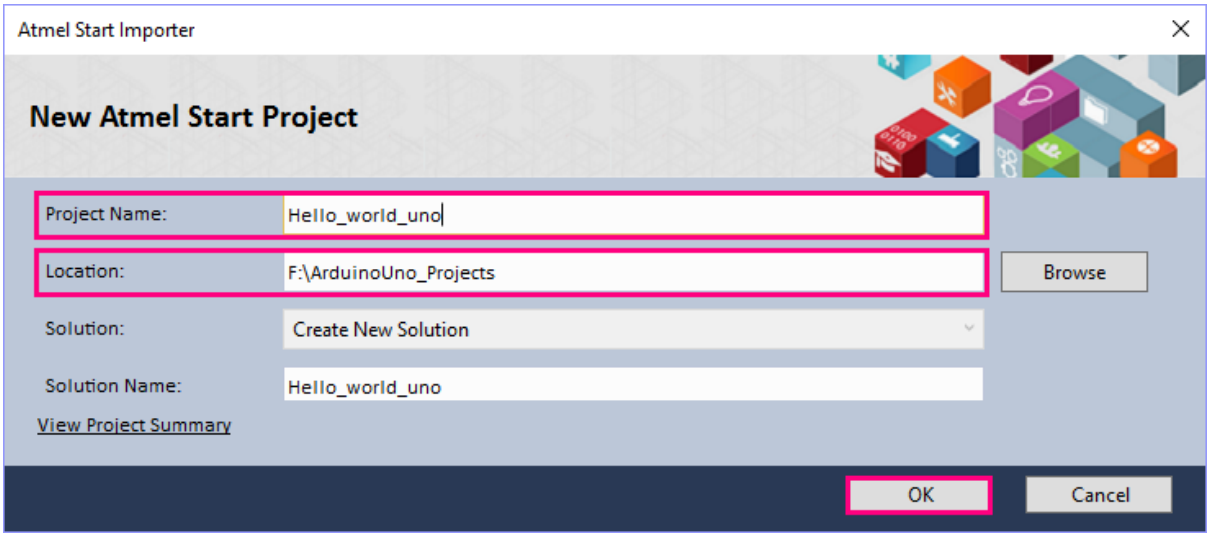


Similarly, click on click on Add Software Component button to add STDIO Redirect middleware component. This component is required to configure standard input / output streams such that the printf() and scanf() functions can use the serial port of the microcontroller.



As Uno board has a 16 MHz crystal we need to change the clock frequency from 8 MHz to 16 MHz. This number will be used to calculate correct register values required to produce given Serial port baud rate.

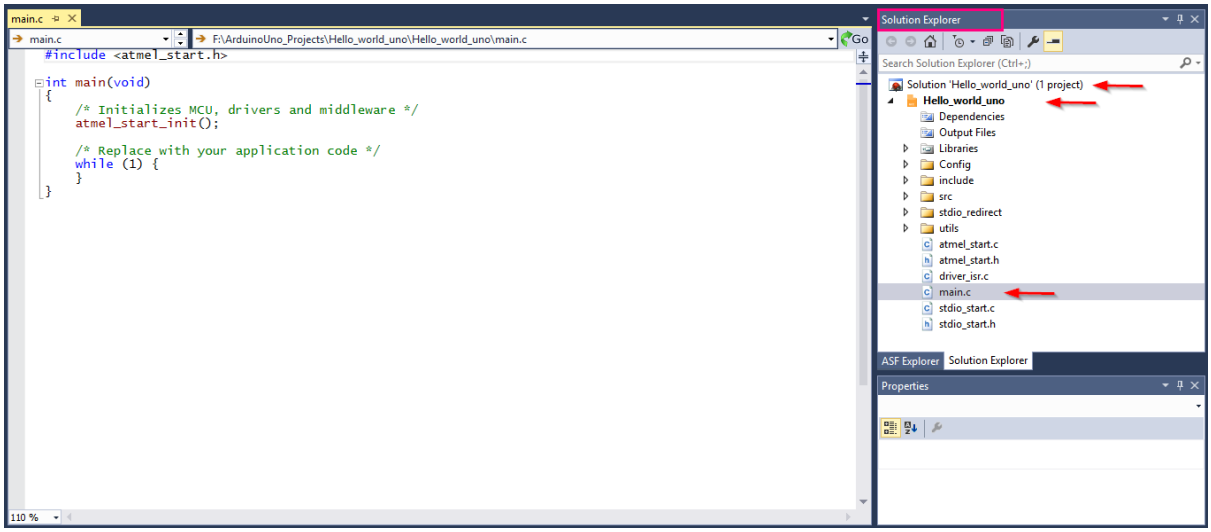
Click on GENERATE PROJECT to generate the project. You will need active internet connection for this. Provide the Project Name and location, and click OK.



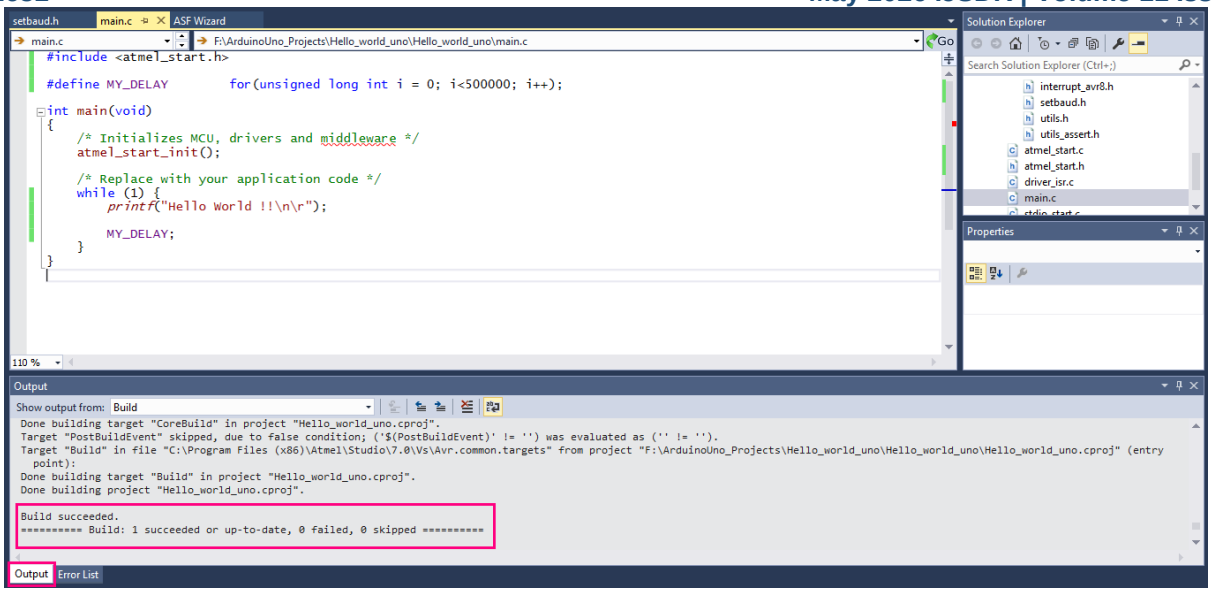
Note that, the ATMEL studio project becomes a part of the **Solution.** One solution can have multiple projects. It is always better to create a new solution for the new project.

If you receive a warning about the component versions, just click **YES.** Wait for few seconds to let ATMEL Studio create your project.

Writing Program From the Solution Explorer, expand the Solution, ARDUINO project and open c file **Note**: If Solution Explorer is not visible to you, then click Window > Reset Window Layout to see this pane.



Click Build > Build Solution to build the project. After few seconds, output window should show the success message.



Chapter 6

Conclusion

The proposed electricity theft detection system based on **Change-and-Transmit Advanced Metering Infrastructure (AMI)** provides an effective and intelligent solution to address the growing challenges of electricity theft in modern power distribution networks. By continuously monitoring electrical parameters such as voltage, current, and power factor at both the input main source and the distribution point, the system is capable of accurately identifying discrepancies that indicate unauthorized electricity usage or tampering activities. This real-time monitoring capability significantly improves the reliability and efficiency of the electricity distribution system.

The integration of advanced technologies such as microcontrollers, sensors, GSM communication, GPS location tracking, and machine learning enhances the system's ability to detect theft quickly and respond promptly. The Change-and-Transmit mechanism reduces unnecessary data transmission by sending information only when abnormal conditions occur, thereby improving communication efficiency and reducing operational costs. Additionally, the automatic alert system and relay control mechanism help protect electrical equipment and minimize energy losses by enabling immediate corrective action.

Overall, the proposed system contributes to improved billing accuracy, enhanced grid security, and reduced non-technical losses in the power distribution network. It provides a scalable and cost-effective solution suitable for residential, commercial, and industrial applications within modern smart grid infrastructure. With further development and integration of advanced data analytics and secure communication technologies, the system can play a vital role in achieving reliable, efficient, and sustainable electricity management in the future.

REFERENCE

[1] M. Ahmed, A. Khan, M. Ahmed, M. Tahir, G. Jeon, G. Fortino, and F. Piccialli, "Energy theft detection in smart grids: Taxonomy, comparative analysis, challenges, and future research directions," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 4, pp. 578–600, Apr. 2022.

[2] H. Iftikhar, M. S. Khan, and A. Ahmad, "Electricity theft detection in smart grid using machine learning," *Frontiers in Energy Research*, vol. 12, pp. 1–15, 2024.

[3] B. Kabir, U. Qasim, N. Javaid, and A. Khan, "Detecting electricity theft in smart grids using optimized machine learning ensemble techniques," *Energy Reports*, vol. 11, pp. 1025–1035, 2025.

[4] P. M. Kgaphola and S. M. Marebane, "Electricity theft detection and prevention using technology-based models: A systematic literature review," *Electricity*, vol. 5, no. 2, pp. 334–350, 2024.

[5] M. Z. Gunduz and R. Das, "Smart grid security: An effective hybrid CNN-based approach for detecting energy theft using consumption patterns," *Sensors*, vol. 24, no. 4, pp. 1148–1162, 2024.

[6] N. M. Elshennawy,"An efficient electricity theft detection based on deep learning," *Scientific Reports*, vol. 15, pp. 1–12, 2025.

[7] M. S. Iqbal, A. Rehman, and Z. Khan, "A critical review of technical case studies for electricity theft detection in smart grids," *Energy Strategy Reviews*, vol. 49, pp. 101–110, 2025.

[8] A. Alshehri, M. Khan, and S. Alsharif, "Deep anomaly detection framework utilizing federated learning for electricity theft detection," *Sensors*, vol. 24, no. 10, pp. 3236–3248, 2024.

[9] A. T. El-Toukhy, M. M. Badr, and M. M. Mahmoud, "Electricity theft detection using deep reinforcement learning in smart power grids," *IEEE Access*, vol. 11, pp. 59558–59574, 2023.

[10] A. N. Alkuwari, S. Al-Kuwari, and M. Qaraqe, "Efficient and privacy-preserving ConvLSTM-based detection of electricity theft cyber-attacks in smart grids," *IEEE Access*, vol. 12, pp. 153089–153104, 2024.

[11] J. Shan, C. Zeng, and Y. Wang, "Advanced deep learning-based electricity theft detection using multi-dimensional analysis," *Engineering Applications of Artificial Intelligence*, vol. 132, pp. 106–115, 2025.

[12] M. Badr, M. Ibrahem, and H. Kholidy, "Review of data-driven methods for electricity fraud detection in smart metering systems," *Energies*, vol. 16, no. 6, pp. 2852–2865, 2023.

[13] C. L. Zulu and O. Dzobo, "Real-time power theft monitoring and detection system in distribution networks," *Electrical Engineering*, vol. 105, pp. 203–215, 2023.

[14] A. H. Massarani and M. Badr, "Efficient and accurate zero-day electricity theft detection using smart meter sensor data," *Sensors*, vol. 25, no. 13, pp. 4111–4122, 2025.

[15] H. Yang, Z. Huang, J. Lin, and Y. Chen, "Detecting electricity theft using AMI data and machine learning, "*IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2831–2841, 2019.

[16] R. Jiang, Q. Chen, and Y. Wang, "Robust data-driven detection of electricity theft adversarial evasion attacks in smart grids, "*IEEE Transactions on Smart Grid*, vol. 14, no. 1, pp. 663–676, 2023.

[17] A. Jokar, N. Arianpoo, and V. C. Leung, "Electricity theft detection in AMI using customers' consumption patterns, "*IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 216–226, 2015.

[18] Y. Peng, C. Kang, and Q. Xia, "Electricity theft detection in advanced metering infrastructure based on clustering and local outlier factor, "*IEEE Access*, vol. 9, pp. 107250–107259, 2021.

[19] S. Singh, R. Bose, and A. Joshi, "PCA-based electricity theft detection in advanced metering infrastructure," *Proc. IEEE International Conference on Power Systems*, pp. 441–445, 2017.

[20] T. H. T. Nguyen, K. S. Yap, and S. K. Tiong, "Electricity theft detection in power grid with a hybrid machine learning model," *ACM International Conference on Smart Grid Systems*, pp. 1–6, 2021.