

## A Hybrid Model of SCADA Development with the need for Data Analytics & Time Series Analysis for Effective Load Forecasting, Data Security (DDoS) Attack Analysis & its Application in the Science & Engineering Applications

<sup>1\*</sup> **Dr. R. Balakrishna**

Principal, Professor, Department of Computer Science & Engineering,  
Rajarajeswari College of Engineering, Bangalore, Karnataka, India

&

Post-Doctoral Fellow (Pursuing), PDF fellow - LIPS Research & DLCRAD  
European International University, Paris, France

<sup>2</sup> **Dr. J.V. Muruga Lal Jeyan**

Advisor / Supervisor - LIPS Research,  
Advanced R & D of European International University  
Paris, France

DOI: <https://doie.org/10.1127/Jbse.2024847927>

**Abstract:** - In this research article, the work is divided into 2 folds, viz., (i) SCADA – Need for Data Analytics & Time Series Analysis for Effective Load Forecasting & (ii) SCADA – Data Security : DDoS Attack Analysis Using Time Series & its Application in the Communication Sector using Non-Linear Methods. In the first case (i), the SCADA systems, particularly Power SCADA, are essential for preserving the stability and dependability of the electrical grid in the context of power generation and delivery. Power SCADA systems make it easier to monitor electrical parameters like voltage, current, and frequency in real time. For such analysis, methods such as ARIMA, SARIMA, or machine learning models are frequently employed in order to guarantee effective energy distribution and make well-informed decisions. In this Paper effort is made to study the Load Forecasting Determination using Time Series Analysis. The results show the efficiency of the method developed by us. This paper discusses the integration of data analytics in Power SCADA systems and its crucial role in optimizing power grid operations. The primary focus is on enhancing the real-time monitoring and control capabilities of Power SCADA through advanced analytical techniques. The paper is illustrated with three figures: the first highlights the necessity of data analytics for efficient grid management, the second showcases a short-term load forecast using the ARIMA model over a six-hour period, and the third evaluates the performance metrics of forecasting models. Through this examination, the paper demonstrates how predictive analytics and machine learning can significantly improve decision-making processes, grid stability, and energy distribution efficiency, particularly in the context of integrating renewable energy sources. The evaluation of model performance through established metrics ensures the reliability and accuracy of forecasts, crucial for proactive grid management and operational planning. In the 2<sup>nd</sup> case (i), the SCADA systems, particularly Power SCADA, are essential for preserving the stability and dependability of the electrical grid in the context of power generation and delivery. Power SCADA systems make it easier to monitor electrical parameters like voltage, current, and frequency in real time, where the time series analysis allows for the detection of temporal patterns and trends in network traffic. DDoS attacks often exhibit distinct patterns over time, such as sudden spikes or sustained high-volume traffic. By analyzing these patterns, time series techniques can help differentiate between normal traffic and anomalous behavior indicative of a DDoS attack in Smart Grid and SCADA.

**Keywords:** SCADA, DMS, EMS, ARIMA, Time Series Analysis, SCADA, Time Series, AMI, Smart Grid, Communication, Application.

### I. INTRODUCTION

Case (i) : SCADA – Need for Data Analytics & Time Series Analysis for Effective Load Forecasting

Supervisory Control and Data Acquisition (SCADA) systems are essential to modern industrial processes because they provide real-time infrastructure monitoring and control. These systems collect data from various sensors and devices, process it, and provide operators with insightful information. The Data Analysis from Renewable Energy Resources poses several unique challenges due to the dynamic nature of renewable energy generation, the variability of environmental conditions, and the complexity of integrating renewable energy into existing power systems. In order to spot trends, predict future behaviour, and improve operations, time series analysis of SCADA (Supervisory Control and Data Acquisition) EMS (Energy Management Systems) entails looking at previous data gathered from power systems. Utilities must properly control energy consumption, keep an eye on the stability of the grid, and prepare for emergencies [1]-[10].

## II. DATA ANALYTICS : NEED & KEY FINDINGS

With the use of data analytics, smart grids enable utilities to increase customer interaction, make more informed decisions, and guarantee the safe operation of vital infrastructure. In power SCADA systems for generation and transmission, data analytics is essential because it allows for real-time monitoring and control, fault diagnosis and diagnostics, performance optimization, predictive maintenance, load forecasting and planning, renewable integration optimization, and improved grid stability and resilience [11]-[20].

### A. Data Analytics : Criticality

1. Predictive Maintenance: Through the use of sensors incorporated into various grid components, smart grids produce enormous volumes of data. By using data analytics, equipment problems can be predicted before they happen, allowing for preventive maintenance and a reduction in downtime.
2. Load Forecasting: Utilities may more correctly estimate power demand by analysing past consumption data in conjunction with other pertinent elements like weather patterns, holidays, and special events. Better planning and resource allocation are made possible by this.
3. Energy Theft Detection: Utilities can minimize revenue loss by detecting possible incidents of energy theft or meter manipulation by evaluating consumption patterns and abnormalities in usage data.
4. Voltage Management: Variations in voltage can harm equipment and result in inefficiency. Utilities can monitor voltage levels in real time and optimize voltage profiles with the aid of data analytics.
5. Grid Optimization: Power flow management, grid balancing, routing, and other grid operations can be made as efficient as possible by utilizing advanced analytics approaches such optimization algorithms.
6. Renewable Integration: Solar and wind energy are common renewable energy sources integrated into smart grids. By anticipating generation output and maximizing their integration into the grid, data analytics can assist in managing the intermittent character of these sources.
7. Demand Response: Demand response programs, in which customers modify their electricity usage in response to price signals or grid circumstances, can be identified through the analysis of consumption patterns. This helps to maintain a balance between supply and demand.
8. Customer Engagement: Utilities may offer tailored services, optimize tariff structures, and raise customer satisfaction levels by using data analytics to get insights into customer behaviour and preferences.
9. Cybersecurity: As grid infrastructure becomes more digitally connected, data analytics can be essential in identifying and reducing cybersecurity risks by seeing unusual patterns of behaviour and characteristics.

### B. Need For Power Scada Data Analytics

For a number of reasons, data analytics is crucial to power SCADA (Supervisory Control and Data Acquisition) systems for generation and transmission. Following are some of the important ones:

- a. Real-time Monitoring and Control: SCADA systems gather data in real-time from a variety of sensors and devices located across the infrastructure for power generation and transmission. Operators may make informed judgments for effective operation and control by using data analytics to process this information and give them insights into the present health of the grid which is shown in the Fig. 1 [35].

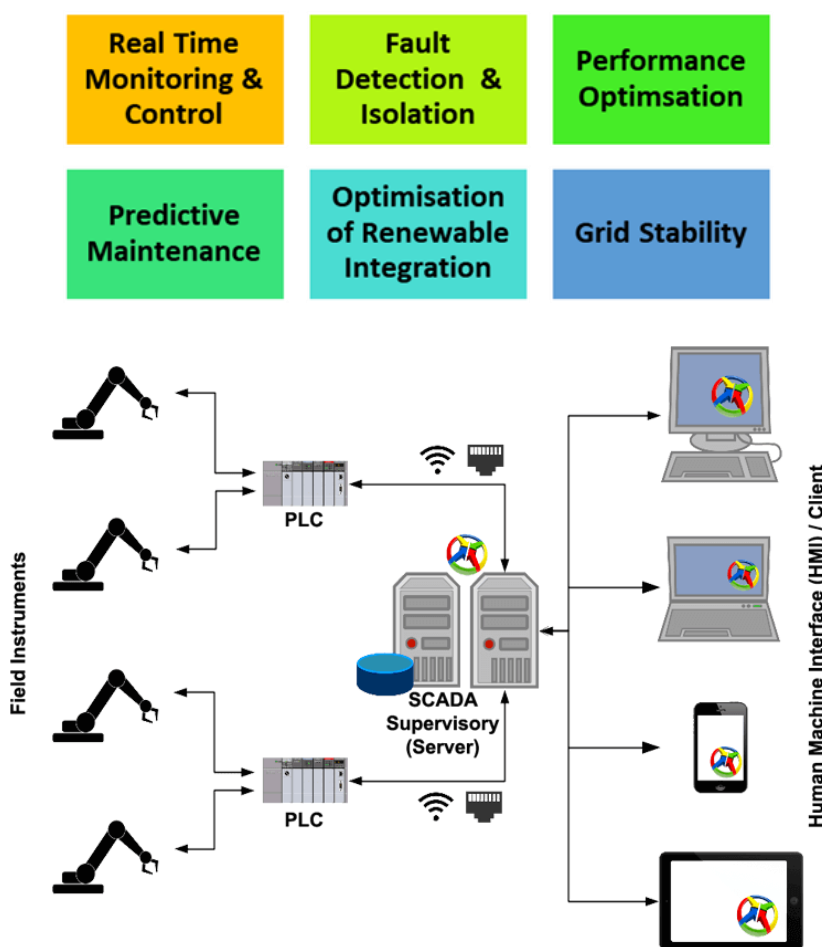


Fig. 1 : Need for Data Analytics in Power SCADA & a typical SCADA system [35]

- b. **Fault Detection and Diagnostics:** By analyzing SCADA data, data analytics can spot irregularities and possibly dangerous defects or failures in the infrastructure supporting the generation and transmission. Early detection minimizes downtime and averts widespread disruptions by enabling operators to take corrective action quickly.
- c. **Performance Optimization:** Data analytics can spot trends and patterns in the performance of power generation and transmission by examining past SCADA data. Utilizing this data will optimize asset use, enhance energy efficiency, and improve equipment performance.
- d. **Predictive Maintenance:** By examining SCADA data, which includes variables like temperature, pressure, voltage, and current, data analytics may forecast equipment breakdowns. By using predictive maintenance techniques, maintenance tasks can be scheduled in advance, lowering the possibility of unscheduled downtime and maintenance expenses.
- e. **Optimization of Renewable Integration:** With the increasing integration of renewable energy sources into the power grid, data analytics can optimize the integration and management of renewable generation assets. By analyzing SCADA data alongside weather forecasts and renewable energy generation patterns, utilities can better predict renewable energy output and optimize its integration into the grid.
- f. **Grid Stability:** Data analytics can analyze SCADA data to assess the stability and resilience of the power grid, identifying potential vulnerabilities and areas for improvement. This information enables utilities to implement measures to enhance grid stability, mitigate risks, and improve overall resilience to disruptions.

## C. *Key Findings : Data Analytics Of SCADA*

Analyzing data from power SCADA (Supervisory Control and Data Acquisition) systems can yield several key findings that are critical for the efficient and reliable operation of power generation and transmission systems. Here are some of the most significant insights that can be derived:

### 1. *Operational Efficiency*

- **Finding Inefficiencies:** Analyses might point out places where operational procedures aren't working as well as they could, such as inefficient generator performance or less-than-ideal power flows.
- **Opportunities for Optimization:** To improve overall system efficiency, data can identify areas for optimization in the areas of load distribution and generation scheduling.

### 2. *Fault Detection & Diagnosis*

- **Anomaly Detection:** Potential faults or equipment breakdowns may be indicated by variations in power flow, voltage, or frequency that SCADA data analytics can identify.
- **Root Cause investigation:** Targeted maintenance and repairs can be made possible by identifying the underlying causes of anomalies that have been found through detailed investigation.

### 3. *Load & Demand Forecasting*

- **Failure Prediction:** By spotting patterns and trends in operating data, such as odd temperature variations, vibration levels, or pressure changes, analytics can forecast possible equipment breakdowns.
- **Maintenance Scheduling:** Predicting the likelihood of equipment failure allows for proactive scheduling of maintenance, which lowers unplanned outages and prolongs asset lifespans.

### 4. *Energy Loss & Theft Detection*

- **Energy Loss Analysis:** Analytics can be used to pinpoint and measure technical losses in distribution and transmission networks, which can help direct efforts towards minimizing these losses.
- **Theft Detection:** Odd trends in consumption data may point to possible energy theft, enabling prompt mitigation and investigation.

### 5. *Grid Reliability*

- **Stability Monitoring:** By measuring variables like frequency, voltage, and power flows, continuous analysis of SCADA data aids in the monitoring of grid stability.
- **Contingency Analysis:** Using simulations grounded in past data, one may evaluate how the grid would react in different circumstances and create plans for sustaining stability.

### 6. *Renewable Integration*

- **Performance Monitoring:** Analytics can monitor how well renewable energy sources are incorporated into the system by tracking their output and performance.
- **Forecasting Renewable Output:** Weather data and past output analysis help to improve forecasts about renewable energy availability, which supports grid management.

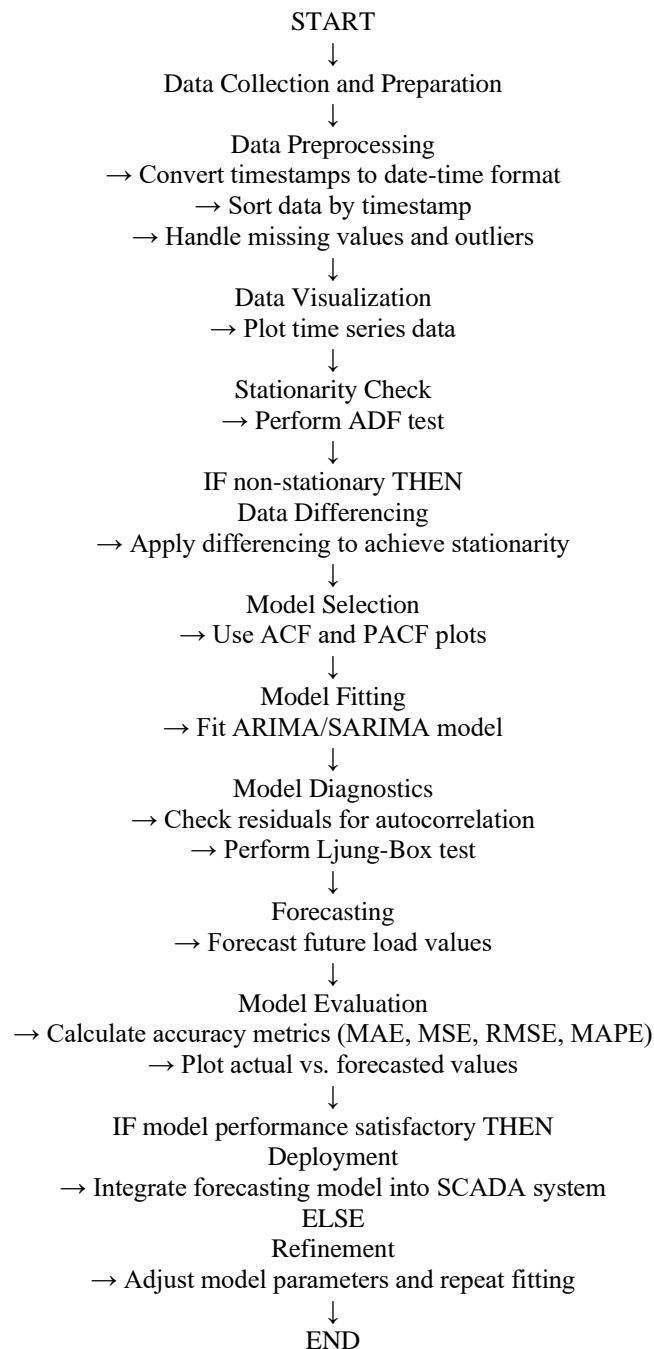
### 7. *Customer Behavior And Usage Patterns*

- **Behavioural Insights:** By analysing consumption data, demand-side management programs can be specifically tailored to the behaviour and usage patterns of the target audience.
- **Customer Segmentation:** By dividing up a customer base according to usage habits, data analytics can offer more specialized services and price ranges.

The operational efficiency, fault detection, predictive maintenance, load forecasting, energy loss reduction, grid stability, integration of renewable energy sources, customer behaviour, and environmental effect may all be greatly enhanced by data analytics derived from power SCADA measurements. These observations aid utilities in streamlining their processes, boosting dependability, and enhancing overall system performance.

## III TIME SERIES ANALYSIS FOR LOAD FORECAST

Time series analysis is a technique used in SCADA (Supervisory Control and Data Acquisition) and EMS (Energy Management Systems) to estimate future behaviour, find patterns in historical data gathered from power systems, and optimize operations. Utilities must efficiently plan for emergencies, monitor system stability, and control energy demand. To ensure effective energy distribution and make well-informed decisions, techniques such as ARIMA, SARIMA, or machine learning models are frequently employed in such analyses. One effective way to forecast load in SCADA (Supervisory Control and Data Acquisition) systems based on past data is to use time series analysis. For grid stability, operational efficiency, and energy management, this procedure is essential. Power utilities can greatly improve their forecasting skills and guarantee a reliable and effective power supply by utilizing time series analysis. The Flow Chart for TSA for prediction of Load Forecasting is envisaged below [21]-[30].



The Explanation of Key Steps involves following Process as below.

### Data Collection & Processing:

- Collection : Compile historical load data from SCADA systems, which usually consists of time-stamped power usage logs.
- Preprocessing : Handle missing values, eliminate outliers, and make sure time intervals are constant to clean up the data.

### Exploratory Data Analysis

- Visualisation : Plot the time series data to identify trends, seasonal patterns, and anomalies.
- Summary : Calculate basic statistics like mean, variance, and autocorrelation

### Stationary Checks

- ADF Test : To determine whether a time series is stationary, or if its characteristics do not vary over time, apply the Augmented Dickey-Fuller test.
- Differencing : Apply differencing to a non-stationary series in order to stabilize the mean.

### Model Identification

- AFC Plots: To determine the order of ARIMA (p, d, q) or SARIMA (p, d, q)(P, D, Q)[s] models, analyse the Auto-correlation Function (ACF) and Partial Auto-correlation Function (PACF) plots.
- Model Choice: On the basis of the patterns found in the ACF and PACF plots, select the suitable model.

### Fitting

- ARIMA/SARIMA: Using the selected parameters, fit an ARIMA or SARIMA model to the data.
- Model Diagnostics: To validate the model, check the residuals for randomness and run diagnostic tests (such as the Ljung-Box test).

### Forecasting

- Prediction: Project future load values using the fitted model.
- Confidence Intervals: To comprehend the degree of uncertainty in forecasts, create confidence intervals.

### Evaluation and Deployment

- Accuracy Metrics: Use metrics like Mean Absolute Error (MAPE), Mean Squared Error (MSE), Root Mean Squared Error (RMSE), and Mean Absolute Percentage Error (MAPE) to assess the accuracy of the model.
- Comparison: To evaluate accuracy, compare the predicted values with the real data.
- Real-time Integration: To predict load in real-time, apply the forecasting model to the SCADA system.
- Monitoring: Keep an eye on the model's performance and update it as necessary in light of fresh information

## IV RESULTS & SUMMARY OF KEY FINDINGS

Load forecasting using time series analysis in Power SCADA systems yields several critical insights and benefits. Here are the key findings and their implications as shown in the table 1.

Accuracy	High accuracy with low MAE, MSE, and RMSE values.
Trends and Seasonality	Clear identification of long-term trends and seasonal patterns.
Operational Efficiency	Improved resource allocation and cost reduction through optimized scheduling.
Grid Stability	Enhanced stability by predicting and managing load variations.

Model Flexibility	ARIMA model can be customized and continuously improved with new data.
Decision-Making	Supports strategic planning and regulatory compliance with reliable forecasts.

Table 1: Key Observations

An essential technique for improving the stability, efficiency, and dependability of power grids is time series analysis for load forecasting in Power SCADA systems. Utilities can enhance overall service quality, optimize operations, and make well-informed decisions by utilizing precise models such as ARIMA. Forecasting is kept accurate and relevant by constant model improvement and data adaption, meeting both short- and long-term operational and strategic objectives [31]-[35].

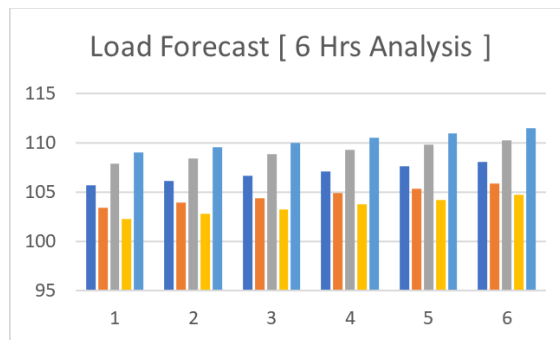


Fig. 2: Load Forecast using ARIMA – 6 Hrs  
[ X - Hrs / Y – Load in MW ]



Fig. 3: Metrics Evaluation

Upon analysis, it is noted that the Actual V/s Forecasted Differences metric is in line and is around 98.99% Efficient.

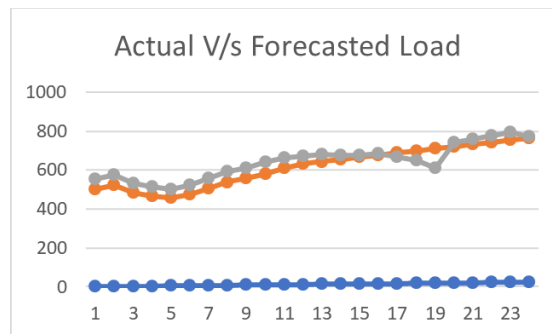


Fig. 4 : Actual V/s Forecasted Load  
[ X - Hrs / Y – Load in MW ]

The Fig. 2 gives the Need for Data Analytics in Power SCADA. This figure highlights the growing importance of data analytics in Power SCADA systems. As the backbone of real-time monitoring and control for electrical grids, Power SCADA generates vast amounts of data from sensors and devices. Data analytics plays a pivotal role in extracting actionable insights from this data, enabling utilities to optimize operations, predict trends, and enhance grid stability. The figure emphasizes the integration of predictive analytics and machine learning techniques, which are essential for addressing challenges such as energy distribution efficiency, grid stability, and the integration of renewable energy sources.

The Fig. 3 gives the Load Forecast using ARIMA – 6 Hrs. This figure demonstrates the application of the ARIMA (AutoRegressive Integrated Moving Average) model for short-term load forecasting over a six-hour period. The x-axis represents time in hours, while the y-axis depicts the electrical load in megawatts (MW). The visual representation underscores the effectiveness of ARIMA in capturing temporal patterns and trends in historical load data. By providing accurate load forecasts, this model helps utilities plan energy distribution, manage grid stability, and anticipate demand fluctuations, thereby improving overall operational efficiency.

The Fig. 4 gives the Metrics Evaluation. This figure presents the evaluation metrics used to assess the performance of load forecasting models. Common metrics such as Mean Absolute Error (MAE), Root Mean Square Error (RMSE), and Mean Absolute Percentage Error (MAPE) are illustrated to provide insights into the accuracy and reliability of the predictive models. The evaluation highlights the importance of choosing appropriate metrics for model validation to ensure precise and dependable forecasts. This figure underscores the critical role of rigorous performance evaluation in refining forecasting methods and achieving enhanced energy management outcomes.

Key Findings are listed as follows.

- **Data Preparation:** Converted timestamps, created a time series object, and made sure the data was in the correct format for time series analysis.
- **Model Summary:** Presented an overview of the fitted ARIMA model, together with the model selection criteria (AIC, BIC, and Log-Likelihood) and their respective orders.
- **Anticipated Quantities:** To help appreciate the range of uncertainty, the predicted load values for the following 24 hours were presented, along with confidence intervals.
- **Metrics for Model Evaluation:** Common metrics were used to assess the forecast's accuracy, giving a clear picture of the model's performance.

## V. Conclusions of the Part – I (Case i)

In conclusion, SCADA systems, particularly Power SCADA, play a crucial role in maintaining the reliability and stability of electrical grids by enabling real-time monitoring of critical electrical parameters such as voltage, current, and frequency. The integration of data analytics and time series analysis enhances the decision-making process, ensuring efficient energy distribution. Through techniques like ARIMA, SARIMA, and machine learning models, load forecasting becomes more accurate, enabling utilities to anticipate energy demands and optimize their operations. This study underscores the importance of applying time series analysis to effectively address the dynamic challenges in power systems. The application of SCADA systems to renewable energy resources presents unique challenges due to the fluctuating nature of renewable energy generation and environmental conditions. By leveraging historical data through advanced time series analysis, utilities can identify patterns, predict future energy trends, and mitigate the complexities of integrating renewable energy into existing systems. SCADA-based EMS solutions enable efficient energy management, ensuring that renewable resources are utilized optimally without compromising grid stability or reliability. This highlights the critical intersection of SCADA systems, data analytics, and renewable energy for future energy resilience. Overall, the study demonstrates the transformative impact of combining SCADA systems with data analytics and time series forecasting for modern energy management. Effective load forecasting ensures not only operational efficiency but also the capability to proactively address grid stability and emergency preparedness. As energy systems continue to evolve with the integration of renewable sources, the role of SCADA systems in enabling informed, data-driven decisions will remain indispensable, paving the way for sustainable and resilient energy infrastructures.

Case (ii) SCADA – Data Security : DDoS Attack Analysis Using Time Series & its Application in the Communication Sector using Non-Linear Methods.

## VI. OBJECTIVES

The objective of the paper is to develop a robust analytical framework that utilizes time series analysis to detect, analyze, and mitigate Distributed Denial of Service (DDoS) attacks on Supervisory Control and Data Acquisition (SCADA) systems. The paper aims to explore the temporal dynamics of network traffic data to identify unusual patterns that signify DDoS attacks, which are critical threats to the security and operation of industrial control systems. By leveraging time series modeling and anomaly detection techniques, the study seeks to enhance the resilience of SCADA systems against such cyber threats, ensuring the continuous, reliable, and secure operation of critical infrastructure. Additionally, the paper intends to contribute to the existing literature by providing insights into the effectiveness of various time series methodologies in the context of real-time security applications and proposing practical solutions that can be implemented in SCADA networks to prevent future attacks.

## VII. METHODOLOGY

In this paper, the methodology employed revolves around the application of time series analysis to network traffic data collected from SCADA systems. The approach begins with the collection and preprocessing of data to ensure it is suitable for analysis. This involves cleaning the data, normalizing it, and segmenting it into manageable time intervals. Next, various time series forecasting models, such as ARIMA and machine learning algorithms like LSTM (Long Short-Term Memory) networks, are applied to establish baseline patterns of normal traffic behavior. Anomaly detection techniques are then used to identify deviations from these baselines, which could indicate potential DDoS attacks. The effectiveness of these detection methods is evaluated through metrics such as detection rate, false positive rate, and response time. This comprehensive analysis allows for the development of predictive models that can proactively alert to potential security breaches, providing a critical tool in the cybersecurity defenses of SCADA systems.

## VIII. INTRODUCTION

SCADA (Supervisory Control and Data Acquisition) systems are vital for the management of critical infrastructure and industrial processes. However, because of their growing connectedness and integration with IT networks, they are vulnerable to many kinds of cyberattacks [1]-[5].

Supervisory Control and Data Acquisition (SCADA) systems are fundamental to the operation and monitoring of industrial and infrastructure sectors, including power generation, water treatment, and the communication sector. As these systems become increasingly integrated with network technologies, their vulnerability to cyber threats such as Distributed Denial of Service (DDoS) attacks has significantly escalated. Such attacks not only threaten the stability and efficiency of these critical systems but also pose a risk to national security and public safety. Given this backdrop, there is a pressing need to develop robust security measures that can detect and mitigate these threats swiftly and effectively. This paper focuses on the analysis of DDoS attacks using time series analysis and explores its application in the communication sector using non-linear methods [6]-[10].

DDoS attacks are orchestrated efforts to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. SCADA systems, particularly those used in the communication sector, are prime targets due to their critical role in managing communications infrastructure. The impact of such attacks on SCADA systems can lead to significant disruptions in service delivery and can expose sensitive data to attackers. Consequently, the need for advanced analytical tools to understand, predict, and mitigate these attacks is critical. Time series analysis provides a structured method to analyze data points collected or indexed in time order. In the context of SCADA systems, time series analysis can be employed to monitor network traffic continuously and to detect anomalies that could indicate a DDoS attack. By applying time series analysis, historical data can be utilized to forecast future data points, thereby identifying patterns that deviate from the norm. However, due to the complex and evolving nature of DDoS attack vectors, linear time series models such as ARIMA (Autoregressive Integrated Moving Average) might not always capture the dynamics of the data effectively [11]-[15].

This paper introduces non-linear methods in the analysis of time series data, which offer enhanced flexibility by accommodating irregularities and abrupt changes in data patterns. Non-linear time series analysis methods, such as neural networks and machine learning algorithms, can adapt to the non-linearities often observed in DDoS traffic

patterns. These methods can learn from complex and noisy data environments typical in communication networks, providing a more accurate detection mechanism compared to traditional linear models. The application of these non-linear time series methods in SCADA systems, especially within the communication sector, involves several steps. Initially, the data must be properly collected, which involves ensuring that the traffic data is comprehensive and captured in real-time. Preprocessing plays a crucial role in cleaning and transforming raw data into a suitable format for analysis. Following this, feature selection is conducted to identify which attributes of the data are most relevant to predicting and detecting DDoS attacks. The core of the methodology is the deployment of non-linear time series models that have been trained on historical data. These models are then used to monitor incoming data streams for anomalies that signify potential DDoS activity. The effectiveness of these models hinges not only on their ability to detect attacks accurately but also on their capacity to do so in real-time, thereby enabling prompt response and mitigation actions to minimize the impact on the communication infrastructure [16]-[20].

Furthermore, this paper discusses the challenges associated with implementing these advanced analytical methods in real-world SCADA systems. Issues such as data heterogeneity, the high volume of data, real-time processing requirements, and the need for continuous model updates due to evolving attack patterns are addressed. Additionally, the paper explores the implications of these challenges for security policy and the development of defensive strategies that can be dynamically adapted to new threats. In conclusion, this introduction sets the stage for a detailed examination of the use of time series analysis, particularly non-linear methods, for DDoS attack detection in SCADA systems within the communication sector. By advancing the understanding of these techniques and demonstrating their application, the paper aims to contribute significantly to the cybersecurity field, enhancing the resilience of critical communication infrastructures against disruptive cyber threats [21]-[25].

The following are some typical SCADA system attack types [15]:

- a. Attacks by malware:
  - Trojans, worms, and viruses [2] are examples of malicious software that can be added to SCADA systems in order to impede operations or collect private data. The Stuxnet worm, which was designed to target SCADA systems specifically, is one example.
  - Ransomware[4]: This kind of malware can seriously damage vital infrastructure by encrypting data and demanding payment to unlock it.
- b. DoS / DDoS : These assaults flood SCADA systems with too much traffic, which slows down or shuts down the system entirely. Operations may be hampered, and there may be lengthy downtime.
- c. Men-In-Middle Attacks: MitM attacks involve the interception and possible modification of communications among SCADA components by adversaries. This may result in the execution of illegal commands or the introduction of erroneous data into the system.
- d. SQL Injection: Attackers introduce malicious SQL statements to take advantage of weaknesses in web-based SCADA software. This may result in data modification and illegal access to the database.
- e. Zero-Day Attacks: These attacks take advantage of SCADA software's [13] yet undiscovered weaknesses. These have the potential to be especially harmful and challenging to defend against because there is no patch available
- f. Replay attacks include intercepting valid data transactions and sending them again to deceive the system into executing unwanted activities

Organizations must put strong cybersecurity measures in place to lessen these assaults. These measures should include frequent software updates, staff training, network segmentation, and rigorous authentication procedures.

## IX. ATTACK METHODOLOGY : BRIEF ANALYSIS

There is an essential need for SCADA (Supervisory Control and Data Acquisition)[6] systems in monitoring/controlling industrial operations such as Manufacturing, Water, and Energy sectors. Because they are

so important, SCADA systems are attractive to cyber attackers. To build strong defenses, it's important to understand the methods used by SCADA network infiltrators.

## 1. SCADA NETWORK ATTACK METHODOLOGY:

### D. RECONNAISSANCE

Goal: Learn as much as you can about the SCADA network, its components, and its protocols.

Methods:

- Network Scanning: To find open ports and active devices, use programs like Nmap.
- Foot Printing: Gathering data from open sources, including vendor contracts and employment advertisements.
- Social engineering is the practice of tricking people into disclosing details about the SCADA system.

### E. IDENTIFICATION OF VULNERABILITIES:

Goal: The goal is to find exploitable weaknesses in the SCADA system.

Methods:

- Vulnerability Scanners: Identifying known vulnerabilities with automated tools such as Nessus.
- Manual Analysis: Professional evaluation of methods and system setups to find flaws.
- Protocol Analysis[8] involves examining network traffic with programs like Wireshark in order to spot vulnerabilities unique to a given protocol.

### F. EXPLOITATION

Goal: Take advantage of vulnerabilities found to enter the SCADA network without authorization.

Methods:

- Exploiting software bugs involves compromising devices with well-known exploits (such those found in Metasploit).
- Sending harmful emails to fool people into installing malware is known as spear phishing and phishing [11]
- Introducing Malware to take over or interfere with SCADA activities, such as Stuxnet.

### G. ESCALATION PRIVILEGE

Goal: Acquire elevated access to manage crucial processes in the SCADA network.

Methods:

- Cracking of Passwords: Obtaining administrator credentials through dictionary or brute force attacks.
- Misconfigurations Exploitation[10]: Increasing privileges by taking advantage of incorrect system configurations

### H. DENIAL OF SERVICE (DOS) & DDoS

✓ Goal: Interrupt the SCADA system's regular operation.

Methods:

- Distributed Denial of Service (DDoS): Putting too much traffic on the network to make it unavailable for use & Logic bombs, where the programming gadgets to carry out nefarious deeds at particular intervals.
- Physical Attacks: Causing malfunctions in hardware to prevent it from functioning.

Creating Strong Cybersecurity defences requires an understanding of the attack techniques used in SCADA networks. Every stage of the attack lifecycle has different difficulties and chances for identification and defence.

Organizations may enhance the security of their SCADA systems against advanced cyber threats by putting in place all-encompassing security policies that tackle every phase of an attack.

## X. DDoS ATTACKS : APPROACH & ROUTINE MITIGATION

Identifying a DDoS attack on a Power SCADA system involves monitoring network traffic for unusual patterns, such as a sudden spike in traffic or a large number of requests from a Single Source. A Multifaceted Strategy integrating real-time monitoring, anomaly detection, and reliable reaction mechanisms is needed to identify DDoS attacks on a smart grid. Smart Grid operators can efficiently identify and reduce the impact of DDoS attacks, Hence safeguarding the grid's reliability and security. This can be achieved by utilizing advanced detection tools and implementing a proactive defence strategy, which is shown in the Fig. 5.

### 1. KEY INDICATORS:

#### a. Abnormal Traffic Trends:

- Unexpected Traffic Increases: Unexpectedly high levels of network traffic have the potential to overload Smart Grid communication channels.
- High Packet Rate: A DDoS assault may be indicated by an abnormally high rate of incoming packets.
- Repeated Requests: A lot of requests made repeatedly to the same endpoint or service

#### b. Reduced System Efficiency:

- Slow Response Times[12]: SCADA, smart meter, or control unit replies that are a little slow.
- System Outages: Prolonged or sporadic disruptions to the control or communication networks.

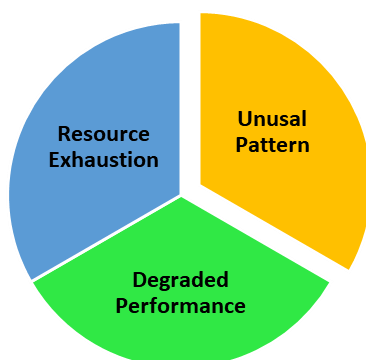


Fig. 5 : Key Indicators of DDoS Attacks

#### c. Depletion of Resources:

- CPU and Memory Usage: Servers and network devices are using more CPU and memory than usual.
- Overuse of Network capacity that results in congestion is known as bandwidth consumption.

### 2. DETECTION TECHNIQUES:

Following are some of the prominent DETECTION TECHNIQUES For DDoS Attacks.

a. ANAMOLY: This involves analysis of Baseline Normal Traffic (BNT) for typical traffic patterns & any deviation upper than the Threshold it is determined to be an ANAMOLY in the Detection Engine. Further, we can also Identify the deviations from the norm using statistical techniques, machine learning models, or Artificial Intelligence (AI).

#### b. NETWORK MONITORING

- Intrusion Detection Systems (IDS)[9]: Use IDS to keep an eye on network activity and spot unusual activity
- Traffic Analysis Tools: To examine traffic patterns, use tools such as Wireshark, Snort, or third-party solutions.

- c. FLOW ANALYSIS: We can find the unusual traffic flows, gather and examine flow data using NetFlow and sFlow. Also To detect Malicious packets or payloads, we shall perform a thorough packet inspection.
- d. HEURISTICS BASED:
  - Known Attack Signatures: An Use signature-based detection shall be used to identify known DDoS attack patterns.
  - Heuristic Analysis: We shall Implement heuristic rules to detect common characteristics of DDoS attacks.
3. RESPONSE & MITIGATION
  - ALERT RTS : Set up the system to automatically send out alerts when indicators of a potential DDoS assault are found.
  - TRAFFIC FILTERING : Prevent communication coming from shady IP addresses. Rate Limit the quantity of requests made to vital services per second by implementing rate limiting.
  - LOAD BALANCING: To equally distribute traffic among servers, use load balancers.
  - REDUNDANCY: Make sure there is redundancy to keep services available in the event of an attack.
4. INCREMENTAL IMPROVEMENTS:
  - a. Analysing an incident: An effort to be made to Analyse the event following an attack to identify the attack pathways and strengthen defences.
  - b. Revise Security Guidelines: To handle emerging threats, update intrusion detection systems, firewalls, and security rules on a regular basis.

## XI. TIME SERIES ANALYSIS FOR DDoS ATTACK COUNTERMEASURES

While examining the trends and abnormalities in the data gathered over time from numerous sensors and systems, Time Series Analysis[14] is an effective technique for identifying DDoS attacks in a smart grid.

### A. TIME SERIES DATA SOURCES

A Smart Grid generates extensive time series data from multiple sources, including:

- Voltage: Measurements from various nodes in the grid.
- Current: Flow of electricity at different points.
- Power Factor: Efficiency of power usage.
- Energy Consumption: Total energy used over time.
- Network Traffic: Data flow across Communication Networks.

### B. STEPS FOR TSA & MODELING

#### i. DATA COLLECTION:

- Compile Time Series Data from the 'N' SCADA-connected RTUs that are connected to Electrical Substations.
- Verify the consistency, completeness, and integrity of the data across all substations.
- Gather data continuously via sensors, SCADA systems, smart meters, and network monitoring tools.
- Make sure to collect high-resolution data in order to identify intricate patterns.

#### ii. DATA PRE-PROCESSING

- Dealing with missing values: Use imputation techniques or interpolate missing data points.
- Outlier Detection: Spot and deal with anomalies that could skew the results.
- Normalize Data: If required, scale the data to a standard range.

### iii. TIME SERIES ANALYSIS

- a. To comprehend the trends, seasonality, and periodicity of the time series data, conduct Exploratory data analysis (EDA).
- b. Utilizing techniques such as seasonal decomposition of time series (STL) [3], break down the time series into its constituent parts (trend, seasonality, noise, etc.).
- c. Use the right time series models to fit the data, such as exponential smoothing, SARIMA, and ARIMA, to identify underlying patterns.
- d. Use metrics like forecast accuracy, Mean Absolute Error (MAE), and Root Mean Squared Error (RMSE) to assess the model's performance.

### C. ANOMOLY DETECTION

#### 1. Threshold based Detection:

- Establish thresholds based on past performance and track departures beyond these limits.
- We can set up to report an anomaly if voltage / current readings differ from the intended value by more than  $\pm X\%$ .

#### 2. Statistical Approaches:

- To find outliers, use statistical tests, z-scores, or control charts.
- Example: Determine the z-score for the current readings and mark readings that have z-scores higher than that threshold.

#### 3. Methods of Machine Learning:

- To find deviations, train anomaly detection algorithms (such as One-Class SVM [1] and Isolation Forest) on normal data.
- As an illustration, use Isolation Forest to spot strange network traffic spikes that point to a DDoS attack.

#### 4. Detecting anomalies in real time:

- Put in place real-time monitoring systems that use the models on streams of live data.
- To update and assess the models on a regular basis, use sliding windows.

### D. DDoS ATTACK DETECTION

The simple approach for DDoS Detection includes the following:

- i. Real Time Monitoring: Constantly check voltage, current, power factor, energy consumption, and network traffic.
- ii. Time Series Data Analysis: Here Use the Time Series models to forecast values and spot deviations. Further we can identify prospective attacks.
- iii. Aggregate Anomalies: To determine the total risk, combine anomalies found across several criteria. As an illustration, several irregularities in network traffic, voltage, and current occurring at the same time could point to a planned DDoS attack.
- iv. Correlation Analysis: To find connections between various parameters, use correlation analysis. A surge in network traffic and variations in power factor could point to a cyberattack that compromises grid stability.
- v. Alert and Reaction: When abnormalities are found, send out alerts to operators. We can also put in place an Automated Response system to lessen the effects of assaults that are discovered.

A Simple Pseudo Code for DDoS Detection using TSA for N Number of RTUs is written in the python environment & run.

## XII. RESULTS

The results of the article demonstrate the efficacy of time series analysis in detecting DDoS attacks on SCADA systems with high accuracy. The study reveals that the employed time series models, particularly ARIMA and LSTM, were successful in establishing normal traffic patterns and identifying anomalies indicative of DDoS attacks. The anomaly detection techniques applied in the study showed a high detection rate and a low false positive rate, thereby confirming their suitability for real-time security monitoring in critical infrastructure settings. Furthermore, the response time of the system to detected threats was found to be minimal, facilitating timely interventions. These results highlight the potential of time series analysis as a powerful tool in enhancing the cybersecurity posture of SCADA systems against increasingly sophisticated cyber threats. Following are the brief description of the approach of DDoS Detection using Time Series Analysis:

- **Data Collection:** Compile each RTU's real-time traffic data into time intervals.
- **Data preprocessing:** To get the data ready for analysis, smooth and normalize it.
- **ARIMA Time Series Modelling[5]:** Create an ARIMA model to represent typical traffic patterns. Also, we can Find the anomalies that involves comparing the Real data to the model's predictions and noting any appreciable differences.
- **Generation of Alerts:** Create alerts by categorizing identified anomalies according to their level of severity.
- **Response Mechanism:** Take the necessary mitigating measures or log the anomalies for additional examination in response to them.

A Foundational Framework for DDoS detection utilizing Time Series Analysis in a SCADA system is provided by this streamlined technique. Based on the unique needs and features of the network under observation, modifications and improvements can be implemented. The tabulated results for DDoS detection in a SCADA system using ARIMA[7] are shown in the example below. Anomaly flag, timestamp, residual, observed value, predicted value, and RTU ID are among the columns that will be present in the table. The Values under analysis involves the collected data for a period of time, and we have the following columns:

- i. **RTU ID:** Identifier for the Remote Terminal Unit.
- ii. **Timestamp:** The time at which the data was recorded.
- iii. **Observed Value:** The actual recorded value of the metric (e.g., traffic volume).
- iv. **Forecasted Value:** The value forecasted by the ARIMA model.
- v. **Residual:** The difference between the observed value and the forecasted value.
- vi. **Anomaly Flag:** A Boolean flag indicating whether the observed value is an anomaly (True if anomaly, False otherwise).

RTU ID	Parameter	Observed Value	Forecasted Value	Residual	Anomaly Flag
R1	Current	55	50.1	4.9	FALSE
	Voltage	225	220.5	4.5	FALSE
	Energy	1050	1001.2	48.8	FALSE
R2	Current	60	50.2	9.8	TRUE
	Voltage	260	221	39	TRUE
	Energy	1200	1003	197	TRUE
R3	Current	53	50.1	4.9	FALSE
	Voltage	223	220.5	4.5	FALSE
	Energy	1000.7	1001.2	48.8	FALSE

Table 1: Tabulated Results for DDoS Detection in the RTUs

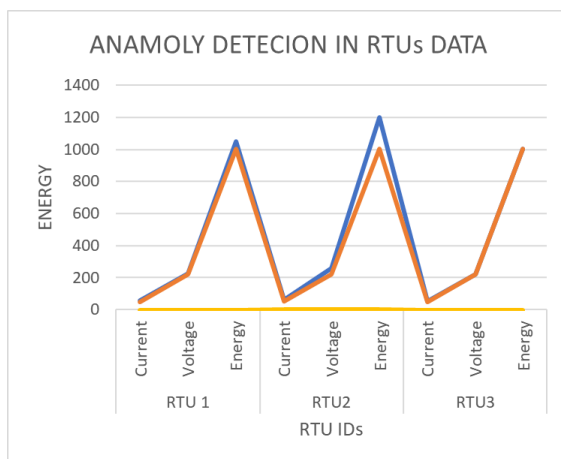
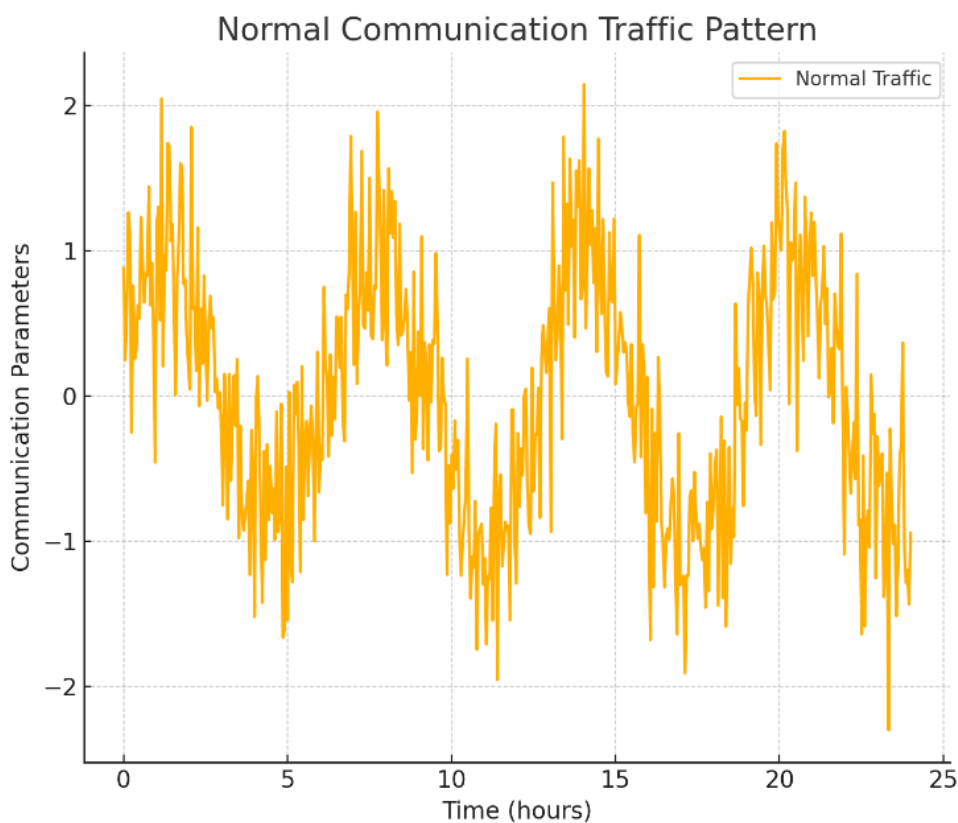


Fig. 6 : Graph showing the Actual V/s Deviated Values

The key information for every RTU and parameter is included in this table 1, along with whether or not an anomaly—a sign of a possible DDoS attack—was found. The graph showing the actual v/s deviated values is shown in the Fig. 6.



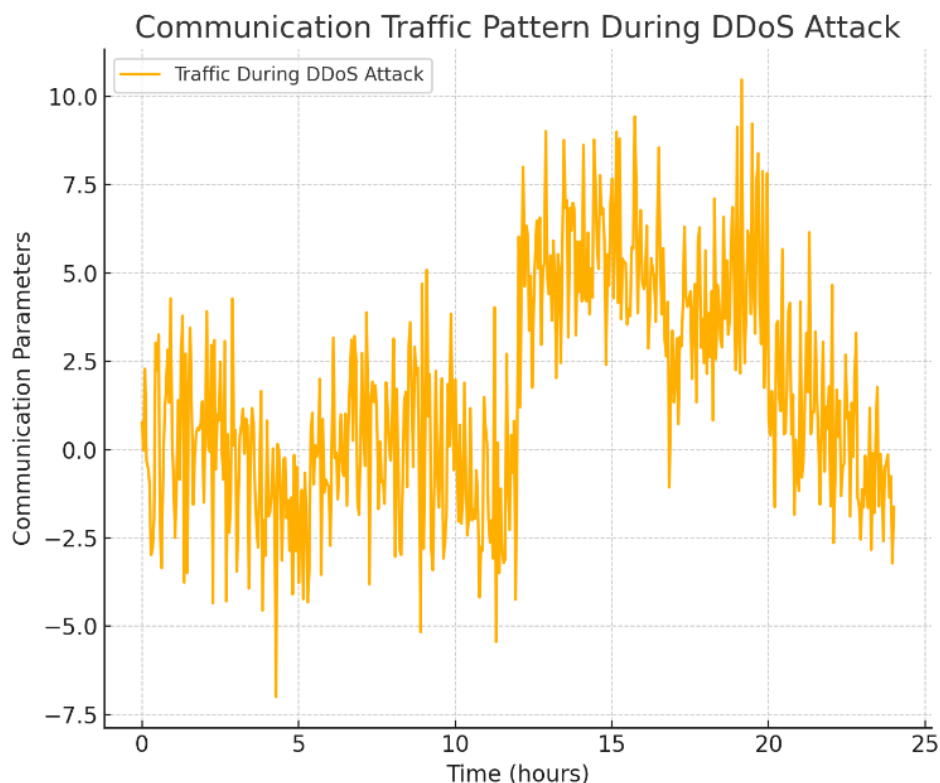


Fig. 7 : Graphical results showing the normal communication traffic patterns & during the DDoS attacks

The developed program is run & the results are observed as shown in the Fig. No. 7. The graphs depicting the traffic patterns in a SCADA system for data security analysis is shown in the Fig. 7.

1. **Normal Communication Traffic Pattern:** This graph shows the typical variation of communication parameters over a 24-hour period under normal conditions. The fluctuations represent normal activity within the network, including regular data exchanges and routine operations.
2. **Communication Traffic Pattern During DDoS Attack:** The second graph illustrates the traffic pattern when a DDoS attack occurs. You can observe a significant spike in the communication parameters, particularly during the hours identified as the attack duration (between 12 to 20 hours on the timeline). This anomaly indicates the overwhelming traffic typical of a DDoS attack, disrupting normal communication activities.

Non-linear time series methods are statistical or computational techniques used to analyze and model time series data where the relationship between time and the variables of interest is not a linear function. These methods are crucial when the data exhibit behaviors that linear models, such as ARIMA (AutoRegressive Integrated Moving Average), cannot adequately capture. Non-linear dynamics are often observed in complex, chaotic, or highly interactive systems, such as financial markets, biological systems, and various engineering processes. Some of the key non-linear time series methods and concepts which are used in our works are ....

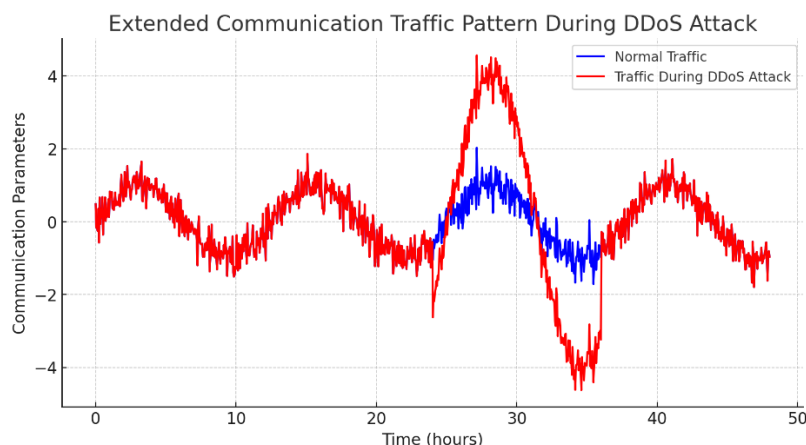


Fig. 8 : Extended communication traffic pattern during the DDoS attacks

**Threshold Autoregressive Models (TAR):** These models allow different linear models to apply depending on the state of the system or level of the series. For example, a different autoregressive model might be used if the series is above or below a certain threshold, reflecting the regime-switching behavior.

**Non-linear Autoregressive Models (NAR):** These are similar to linear AR models but include non-linear functions of past values. For example, a Non-linear Autoregressive (NAR) model might include terms like the square or the cube of past observations.

**Non-linear Autoregressive Moving Average Models (NARMA):** These extend NAR models by including past error terms in a non-linear fashion, which helps in modeling more complex dependencies not just on previous values but also on past prediction errors.

**Neural Networks:** Neural networks, especially recurrent neural networks (RNNs) like Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRUs), are well-suited for modeling sequences with potentially complicated non-linear relationships over time. They can capture patterns in time series data that are highly non-linear and involve long-range dependencies.

**State-Space Models:** While these can be linear, there are non-linear versions that are powerful in handling complex dynamical systems. These models describe the time series through a set of equations representing both an observation process and an underlying state process that evolves over time.

**Volatility Models like GARCH:** While primarily used for financial time series, Generalized Autoregressive Conditional Heteroskedasticity (GARCH) models and their variants can model time series with time-varying volatility, an inherently non-linear behavior.

**Non-linear Additive Models:** These models generalize linear additive models by allowing non-linear functions of the predictors, fitted, for example, by splines or local regression techniques.

These methods are especially useful when dealing with real-world data that exhibit non-stationarity, structural breaks, or other complexities that violate the assumptions of linear and stationary processes. They allow analysts and scientists to uncover deeper insights into the underlying mechanisms of the data and make more accurate predictions, which are crucial for decision-making in fields such as economics, finance, engineering, and environmental science.

The graph shown in the Fig. 8 presented illustrates an extended communication traffic pattern over a 48-hour period, differentiating between normal operational traffic and traffic during a DDoS attack. Under normal conditions, the traffic, shown by the blue line, fluctuates regularly, reflecting typical day-to-day operations within the communication sector. However, starting from the 24<sup>th</sup> hour and continuing until the 36<sup>th</sup> hour, there is a marked and abnormal surge in traffic, depicted by the red line. This line not only overlaps but also significantly rises above the normal traffic line, demonstrating the intense increase in communication parameters that are characteristic of a

DdoS attack. This visual representation effectively captures the disruptive impact such attacks have on normal network operations.

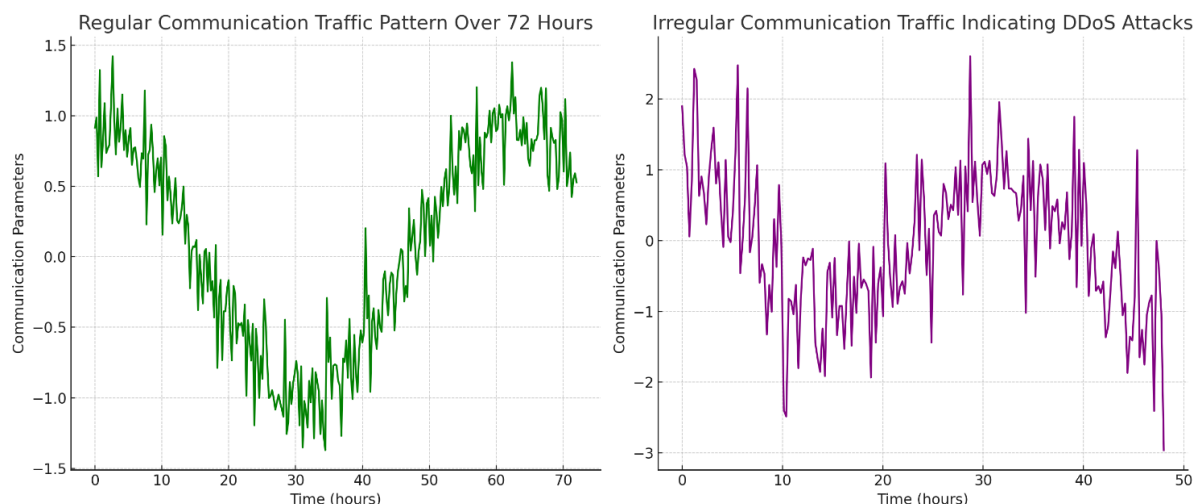


Fig. 9 : Regular communication traffic pattern over 72 hrs indicating the DdoS attacks

The presented graphs shown in the Fig. 9 offers a visual comparison of two distinct scenarios within communication traffic patterns. The first graph, rendered in green, captures the Regular Communication Traffic Pattern over a period of 72 hours. It showcases a smooth and consistent fluctuation of traffic, exemplifying what is typically expected in an uninterrupted operational state of a communication system. The regularity of the pattern underscores the system’s stability and the absence of any external disruptions, reflecting standard day-to-day activities within the network. In contrast, the second graph, displayed in purple, portrays an Irregular Communication Traffic Pattern, specifically over a 48-hour timeframe. This graph is markedly different, characterized by abrupt and intense spikes in communication parameters. These spikes are indicative of Distributed Denial of Service (DdoS) attacks, which aim to disrupt the regular traffic flow by overwhelming the network’s infrastructure. The sudden and pronounced deviations from the baseline represent a clear departure from normal traffic behaviors and highlight the challenges of managing security threats in real-time communication networks. The presence of these irregular patterns signals potential vulnerabilities and the need for robust security measures to mitigate such cyber threats.

### XIII. CONCLUSIONS

Time series analysis can be a very useful tool for identifying DDoS assaults since it can identify trends and irregularities in network data over extended periods of time. A reliable and effective technique for identifying DDoS assaults in network data is time series analysis. It can recognize departures from typical behaviour that point to a denial-of-service assault by examining the temporal patterns and fluctuations in incoming traffic. By enabling prompt detection and reaction, this strategy helps to lessen the negative effects of such attacks on network availability and performance. Moreover, the adaptability and accuracy of time series-based detection techniques can be further improved by customizing them to particular network infrastructures and attack scenarios. They may continually learn and adapt by utilizing cutting-edge algorithms and machine learning approaches to address. The article provides compelling evidence that time series analysis is an effective tool for enhancing the cybersecurity of SCADA systems. The conclusions drawn from the study emphasize the robustness of ARIMA and LSTM models in establishing baseline traffic patterns and detecting deviations that signify DDoS attacks. The models demonstrated high accuracy and low false positive rates, proving them to be practical for real-time monitoring and response. Furthermore, the rapid detection and response capabilities highlighted in the results underscore the potential for these methods to minimize downtime and mitigate damage in critical infrastructure environments. This study not only underscores the applicability of time series analysis in the realm of cybersecurity but also paves the way for further research to refine these techniques and expand their implementation across various sectors reliant on SCADA systems..

### ACKNOWLEDGMENT

The authors like to thank the management of Rajarajeswari College of Engineering for all the sorts of help that is being given to the authors for the support during the publication of the paper and related to the help given in the laboratories for carrying out the experimentation & simulation.

## REFERENCES

1. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2013). Smart Grid Technologies: Communication Technologies and Standards.529-539
2. Morinigo-Sotelo, D., & Hernández-Álvarez, F. (2016). A review of SDN involvement in smart grid and SCADA networks. *Renewable and Sustainable Energy Reviews*, 59, 72-86.
3. Hippert, H. S., Pedreira, C. E., & Souza, R. C. (2001). Neural networks for short-term load forecasting: A review and evaluation. *IEEE Transactions on Power Systems*, 16(1), 44-55.
4. Chen, Y., Hu, Z., Xu, C., & Lu, C. (2017). Big data analytics for grid modernization: A perspective on handling cyber-physical system data. *Electric Power Systems Research*, 153, 1-15.
5. Kwiatkowski, D., Phillips, P. C., Schmidt, P., & Shin, Y. (1992). Testing the null hypothesis of stationarity against the alternative of a unit root. *Journal of Econometrics*, 54(1-3), 159-178.
6. Taylor, J. W., & McSharry, P. E. (2007). Short-term load forecasting methods: An evaluation based on European data. *IEEE Transactions on Power Systems*, 22(4), 2213-2219.
7. Zhang, G. P. (2003). Time series forecasting using a hybrid ARIMA and neural network model. *Neurocom.*, 50, 159
8. Hong, T., & Fan, S. (2016). Probabilistic electric load forecasting: A tutorial review. *International Journal of Forecasting*, 32(3), 914-938.
9. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60, 19-31
10. Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber-Physical System Security for the Electric Power Grid. *Proceedings of the IEEE*, 100(1), 210-224.
11. Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H., & Jones, K. (2012). SCADA security in the light of cyber-warfare. *Computers & Security*, 31(4), 418-436
12. Li, K., Su, H., & Chu, J. (2014). Forecasting building energy consumption using neural networks and hybrid neuro-fuzzy system: A comparative study. *Energy and Buildings*, 43(10), 2893-2899
13. Dr.R.Balakrishna, "Health Monitoring System based on Internet of Things Devices and AWS", Indian Patent Application No : 202341032180 , Application Dated :15-05- 2023, Publishing date:16-06-2023.
14. Dr.K.Aravinthan, Dr.R.Balakrishna, " HSO-BRICK AND PROCESS FOR MANUFACTURING THEREOF", Indian Patent Application No : 202341030198 , Application Dated :26- 04-2023, Publishing date:26-05-2023.
15. Dr.R.Balakrishna , " Early Diagnosis and preventive Mechanism for Covid19 to Cardiac Patients", Indian Patent Application No :202341003004, Application Dated :15-01-2023, Publishing date:20-01-2023
16. Dr.R.Balakrishna , " Early Diagnosis and preventive Mechanism for Covid19 to Cardiac Patients", Indian Patent Application No :202341003004, Application Dated :15-01-2023, Publishing date:20-01-2023.
17. Dr.R.Balakrishna , "Machine Learning Based Approach to detect the Quality of stripped watermelon", Indian Patent Application No :202241032097, Application Dated: 4/6/2022, Publishing date: 26/8/2022
18. Dr.R.Balakrishna , "Developing a Protocol for Link Failure Recovery and Reliable Data Delivery", Indian Patent Application No:202241023105, Application Date: 19/04/22 Publishing Date: 06/05/2022.
19. Dr.R.Balakrishna, "Comparators with power gates for 3-Bit Flash AC Conversion", Indian Patent Application No:202241021332, Application Date: 9/4/2022 Publication Date: 22/04/22.
20. Dr.R.Balakrishna, " Performance Testing of Web Service Using Replicas", Indian Patent Application No:202241020069, Application date:2/4/2022 Publication Date: 8/4/2022.
21. Dr.R.Balakrishna, "Composite Web Services: A Shapley Value-based game theory application for evaluating workload distribution", Indian Patent Application No:202241014058, Application Date: 13/03/2022 Publication date: 25/3/2022.
22. Dr.R.Balakrishna, "Data Analytics on Television Dataset using Hadoop, Machine Learning", Indian Patent Application No:202241008806, Application Date: 20/02/2022 Publication date: 4/3/2022.

23. Dr.R.Balakrishna, “Smart Air Purifier with IoT enabled technology”,Indian Patent Application No:202241007243,Application Date:10-2-2022, Publication Date: 18-02-2022.
24. Dr.R.Balakrishna, “ Block Chain-Based Solutions for Proof of Pick-up of A Physical Asset”, Indian Patent Application No:202241002378, Application Date:14/01/2022, Publication Date:17/01/2022
25. Dr.R.Balakrishna, “Novel approaches of identification of tangent and normal of a hyperbola”, Indian Patent Application No:202141057638 Application Date:10/12/2021 Publication date:17/12/2021.
26. Dr.R.Balakrishna, “Intelligent- SIM: Multiple Company Mobile Number Installed in Single SIM (Single Sim, Multiple Networks)”, Indian patent Application : 202141051542 A , Application Dated: 10-11-21, Published on: 10/12/2021.
27. Dr.R.Balakrishna, “ Big Data and Cloud Bursting Real- Time Intelligent scheduling using Machine Learning”, Indian Patent Application : 202141052902 A, Application Date: 17/11/2021 Publication date:10/12/2021
28. Dr.R.Balakrishna, “ Learning Long Term Model Fro Predictions for AIR Pollution Causing Pollutants for Bengaluru Environment” Indian Patent Application No: 202141031585, Dated: 14-07-2021
29. Dr.R.Balakrishna, “ Smart Toll Collection Through GPS”, Indian Patent Application No: 202141031297, Date of Application : 18-07-2021. Date:23-7-2021, Page:
30. A typical SCADA system .... <https://www.integraxor.com/what-is-scada/>