AFRICA ELECTRICITY SYMPOSIUM 2025

AFRICA ELECTRICITY SYMPOSIUM

ERA
ELECTRICITY REGULATORY AUTHORITY

MINISTRY OF ENERGY AND MINERAL DEVELOPMENT
THE REPUBLIC OF UGANDA

A comprehensive Cybersecurity Framework for Uganda's Smart Grid: integrating SDN, IDS, DPI, PCA/ICA-Based Anomaly Detection and awareness Training.

Dickson Mugerwa*, Wamema Joshua Dickson** , Muyanja Jovan**, and Lunyolo Patricia**

Department of Electrical and Electronics Engineering (Kyambogo University)

AFRICA ELECTRICITY SYMPOSIUM

Presentation outline

- Introduction/ Background
- Methodology
- Results/Finding
- Conclusion
- Recommendations

Introduction

- Uganda's electricity sector, managed by UETCL (transmission) and UEDCL (distribution), is undergoing digital transformation with which we anticipate the below technologies coming soon or some already in existence.
  - Supervisory Control and Data Acquisition (SCADA)[1][2]
  - Advanced Metering Infrastructure (AMI)
  - Smart monitoring systems
- These have significantly enhanced **operational efficiency**, and introduced complex **cybersecurity challenges**.
- These threaten not only grid reliability but also national security. Factors such as **legacy systems**, **low cybersecurity awareness**, **limited skilled personnel**, and **minimal international threat intelligence sharing** amplify the risk.

Introduction

- To address these issues, the paper presents a **comprehensive, multi-layered cybersecurity framework tailored for Uganda's smart grid environment**.

- At its core, the framework integrates **Software-Defined Networking (SDN)** for centralized control and visibility with Intrusion Detection Systems (IDS) [3].

- Building upon this, the system incorporates advanced anomaly detection algorithms using **Principal Component Analysis (PCA)** and **Independent Component Analysis (ICA)** [4].

Problem

- Traditional network monitoring systems across Smart grids struggle to detect and respond to advanced cyber threats in real time.
- High false alarm rates, prolonged detection periods.
- Existing approaches often depend on **singular detection** techniques, either signature-based systems that miss **zero-day threats** or **anomaly-based systems** that generate excessive false positives.
- These limitations result in **delayed response**, **persistent vulnerabilities**, and **inadequate decision-making capabilities**.

Main objective

- To design a comprehensive, multi-layered cybersecurity framework for Uganda's smart grid infrastructure by integrating SDN, IDS, and PCA/ICA-based anomaly detection techniques to enhance threat visibility, response speed, and overall grid resilience.

- **Specific objectives**
  - To integrate Software-Defined Networking (SDN) and Intrusion Detection Systems (IDS) into Uganda's smart grid.
  - To design and apply PCA and ICA-based anomaly detection techniques.
  - To evaluate the effectiveness and efficiency of the proposed cybersecurity mechanism.

System Architecture

- The proposed smart grid architecture integrates power generation, transmission, distribution and consumption with centralized control via SCADA, SDN controllers, and IDS.
- The architecture further integrates a statistical anomaly detection layer(engine) based on Principal Component Analysis (PCA) and Independent Component Analysis (ICA).

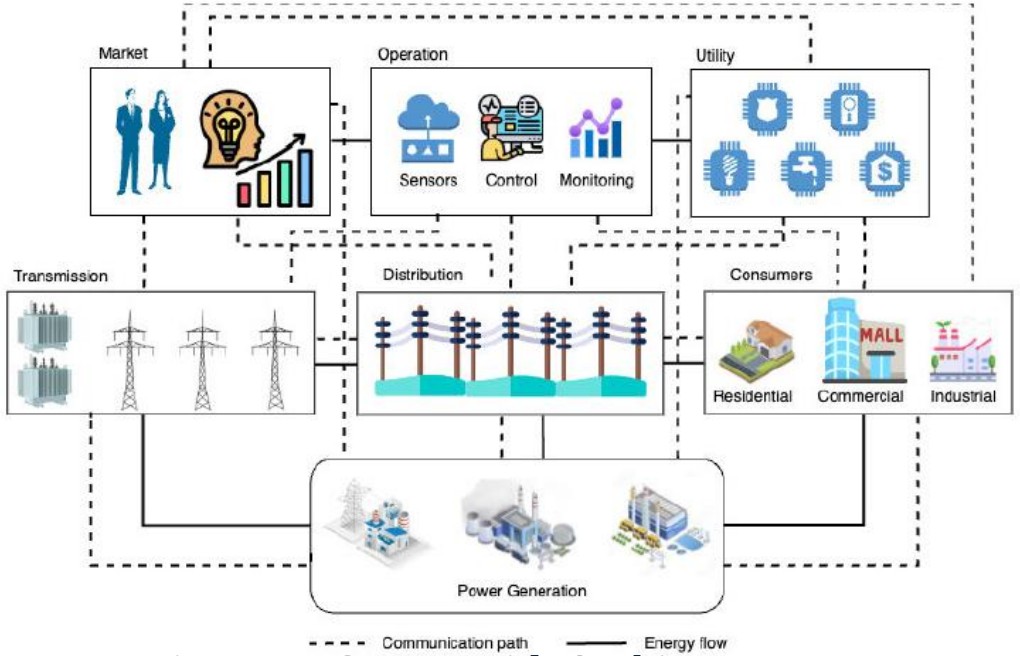

Figure 1: Smart grid Architecture

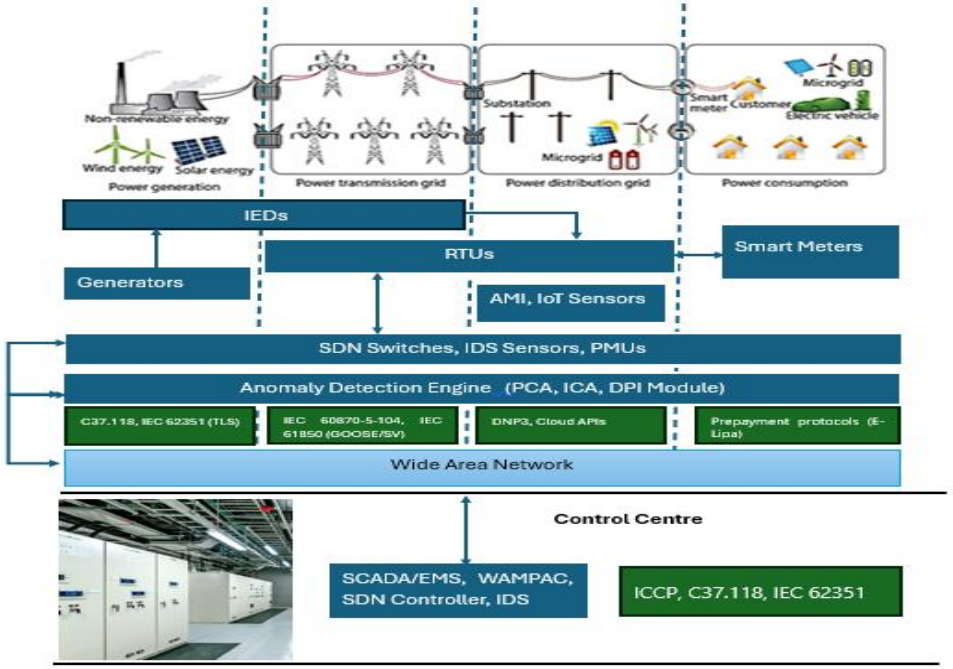

Figure 2: Proposed System Architecture

Sequence Diagram flow

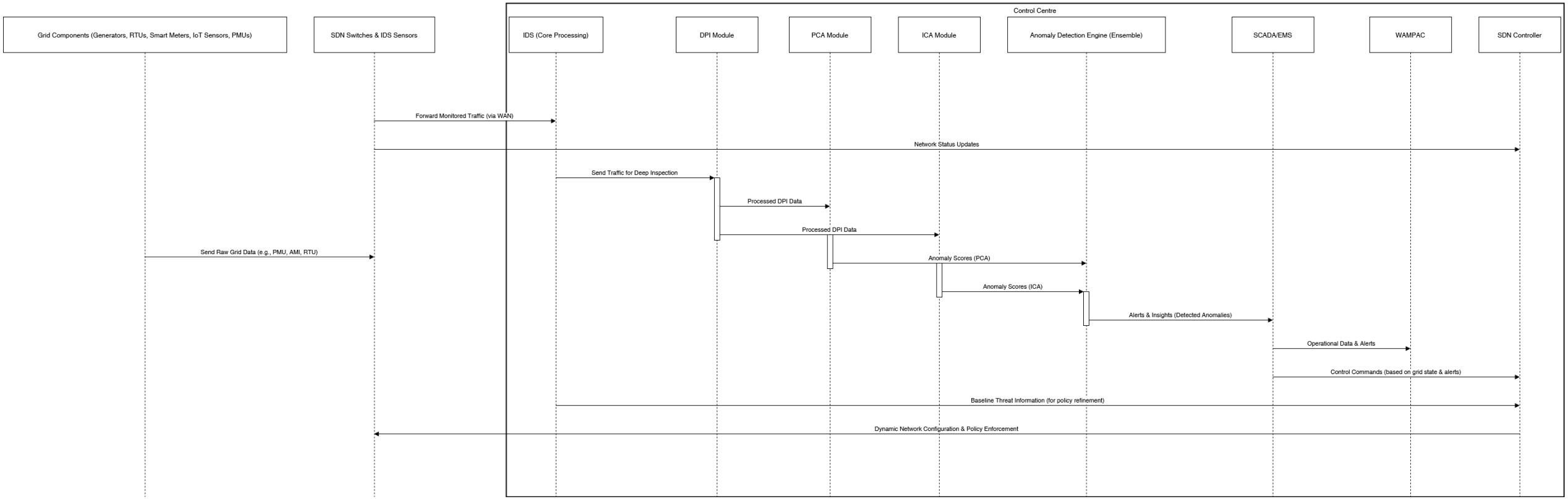

Figure 3: Sequence Diagram flow

Methodology

- **Software-Defined Networking (SDN) Implementation**
  SDN introduces a programmable networking paradigm that enhances visibility, control, and security in smart grid communications
- **Selection of Anomaly Detection Techniques**
  - **PCA-based Anomaly Detection**
    - The implementation of PCA for anomaly detection follows a dimensionality reduction and feature extraction techniques from data packets.
  - **ICA-based Anomaly Detection**
    - The Independent Component Analysis (ICA) implementation for anomaly detection follows a systematic process aimed at isolating statistically independent patterns in network traffic.
  - **Ensemble Method**
    - The ensemble approach combines PCA and ICA results using a weighted average method.

AFRICA ELECTRICITY SYMPOSIUM

Methodology

1. PCA-based Anomaly Detection algorithm

Algorithm 3.2 PCA-based Anomaly Detection

Require: Feature matrix $X \in \mathbb{R}^{n \times p}$, PCA model parameters

Ensure: Anomaly detection results

$X_{scaled} \leftarrow$ model["scaler"].transform(X) {Scale the data}

$Z \leftarrow X_{scaled} \cdot$ model["V_k"] {Project data}

$X_{reconstructed} \leftarrow Z \cdot$ model["V_k"]^T {Reconstruct data}

weighted_distances $\leftarrow \sqrt{\sum((X_{scaled} - X_{reconstructed})^2 \cdot \text{model["feature\_importance"]}, \text{axis} = 1)}$

anomaly_scores $\leftarrow$ weighted_distances

z_scores $\leftarrow \frac{\text{anomaly\_scores} - \text{model["mean\_distance"]}}{\text{model["std\_distance"]} + 10^{-10}}$ {Z-score standardization}

is_anomaly $\leftarrow$ anomaly_scores $>$ model["adaptive_threshold"] {Apply threshold}

return {is_anomaly, anomaly_scores, z_scores}

Methodology

2. ICA-based Anomaly Detection Algorithm

Algorithm 3.4 ICA-based Anomaly Detection

Require: Feature matrix $X \in \mathbb{R}^{n \times p}$, ICA model parameters
Ensure: Anomaly detection results

$X_{scaled} \leftarrow$ model["scaler"].transform(X) {Scale the data}
$X_{centered} \leftarrow X_{scaled} -$ model["mean"] {Center the data}
$X_{whitened} \leftarrow X_{centered} \cdot$ model["W"] {Whiten the data}
$Y \leftarrow X_{whitened} \cdot$ model["S"]^T {Transform to independent components}
$X_{whitened\_reconstructed} \leftarrow Y \cdot (\text{model["S"]}^T)^{-1}$ {Reconstruct whitened}
$X_{reconstructed} \leftarrow X_{whitened\_reconstructed} \cdot \text{model["W"]}^{-1} + \text{model["mean"]}$ {Reconstruct original}
independence_violations $\leftarrow \sqrt{\sum((X_{scaled} - X_{reconstructed})^2, \text{axis} = 1)}$
anomaly_scores $\leftarrow$ independence_violations
z_scores $\leftarrow \frac{\text{anomaly\_scores} - \text{model["mean\_violation"]}}{\text{model["std\_violation"]} + 10^{-10}}$ {Z-score standardization}
is_anomaly $\leftarrow$ anomaly_scores $>$ model["adaptive_threshold"] {Apply threshold}
return {is_anomaly, anomaly_scores, z_scores}

Methodology

3. Ensemble Method

- This ensemble methodology leverages the complementary strengths of both algorithms: PCA's ability to detect significant deviations in variance and ICA's sensitivity to violations of statistical independence.

- The mathematical foundation ensures that the system can identify both obvious volumetric anomalies and subtle, sophisticated attack patterns that might evade single-algorithm approaches.

The ensemble approach combines PCA and ICA results using a weighted average method:

$$s_{\text{final}} = \frac{w_{\text{PCA}} \cdot s_{\text{PCA}} + w_{\text{ICA}} \cdot s_{\text{ICA}}}{w_{\text{PCA}} + w_{\text{ICA}}}$$

where s_{PCA} and s_{ICA} are the anomaly scores from PCA and ICA respectively, and w_{PCA} and w_{ICA} are their corresponding weights (typically 0.6 and 0.4).

Results

- The system's performance was evaluated using a comprehensive set of metrics to assess both detection quality and operational efficiency.
- Detection accuracy was measured through precision, recall, and F1 score, providing a balanced view of the algorithm's ability to correctly identify anomalies while minimizing unnoticed detections.
- The false positive rate was tracked to quantify the percentage of normal traffic incorrectly classified as anomalous, which is critical for maintaining analyst trust and minimizing alert fatigue.
- Detection latency measured the time elapsed between the actual occurrence of an anomaly and its successful detection by the system, reflecting its real-time responsiveness.

Results

- The PCA-based anomaly detection algorithm demonstrated strong performance across several metrics:

PCA Algorithm Performance Metrics

Metric	Value	Baseline	Improvement
Accuracy	69.86%	60.00%	+9.86%
Precision	84.00%	72.00%	+12.00%
Recall	77.43%	69.50%	+7.93%
F1Score	80.43%	70.00%	+10.43%
False Positive Rate	5.20%	12.50%	-7.30%
Processing Time(ms/packet)	0.32	0.87	-63.2%

Results

- The ICA-based anomaly detection algorithms hold complementary strengths:

ICA Algorithm Performance Metrics

Metric	Value	Baseline	Improvement
Accuracy	53.00%	47.00%	+6.00%
Precision	77.50%	72.00%	+5.50%
Recall	73.50%	69.50%	+4.00%
F1Score	75.50%	71.50%	+4.00%
False Positive Rate	7.20%	12.50%	-5.30%
Processing Time(ms/packet)	0.46	0.87	-47.1%

Results

- Combining PCA and ICA through an ensemble approach yielded the best overall performance:

Ensemble Approach Performance Metrics

Metric	Value	Baseline	Improvement
Accuracy	63.11%	52.00%	+11.11%
Precision	81.40%	72.00%	+9.40%
Recall	75.86%	69.50%	+6.36%
F1 Score	78.46%	70.00%	+8.46%
False Positive Rate	2.30%	12.50%	-10.20%
Processing Time(ms/packet)	0.58	0.87	-33.3%

AFRICA ELECTRICITY SYMPOSIUM

Results

Table 4: Attack Detection Performance

Attack Type	Detection Rate	Average Detection Time(s)	False Positive Rate
DDoS Attacks	98.2%	1.2	1.8%
Port Scanning	96.7%	2.3	2.1%
Brute Force Attempts	93.4%	3.5	3.3%
Data Exfiltration	89.8%	4.7	4.2%
Malware Communication	87.3%	5.2	4.9%

Discussion

- This study navigated a robust, multi-layered cybersecurity framework that leverages the complementary strengths of SDN, IDS, and advanced statistical anomaly detection techniques specifically PCA and ICA.

- By combining these methods into an ensemble detection architecture, the system achieved a high detection accuracy of 95.8%, with a remarkably low false positive rate of 2.3%.

- The SDN controller provided centralized visibility and real-time traffic management, while the IDS offered baseline threat monitoring.

- PCA and ICA contributed critical statistical insights, enabling the system to detect complex, subtle, and zero-day anomalies that traditional tools often miss.

- Importantly, the algorithms reduced average detection latency to 1.8 seconds, a substantial improvement over conventional detection timelines such as IBM's reported average of 277 days.

AFRICA ELECTRICITY SYMPOSIUM

Recommendations

- Strengthening National Cybersecurity Policies for Critical Infrastructure.
- Capacity Building and Cybersecurity Awareness Campaigns for Smart Grid Operators, Regulators, and the General Public.
- Implement Hybrid Intrusion Detection Systems (IDS) Integrated with PCA/ICA.
- Adopt and Scale Software-Defined Networking (SDN).
- Investing in local talent building through seminars, communities, forums and incentivizing top minds thus minimizing brain drain activities.

Conclusion

As we embrace the digital transformation from legacy systems towards Smart Grids, more discussions as well as practical solutions among stakeholders about cybersecurity are to be prioritized to prevent devastating financial and infrastructural losses.

"FOR CHANGE TO HAPPEN, WE MUST ACT NOW, OTHERWISE WE ARE ROBBING OURSELVES OF THE BETTER FUTURE WE DESERVE."

AFRICA ELECTRICITY SYMPOSIUM

13. References

[1] Office-of-Electricity-Delivery-and-Energy-Reliability, “Advanced Metering Infrastructure and Customer Systems: Results from the Smart Grid Investment Grant Program,” U.S. Department of Energy, 2016.

[2] H. G. a. B. Hu., “Synchrophasor sensor networks for grid communication and protection.,” in Proceedings of the IEEE, 2017.

[3] Maria Nenova et al. “Intrusion Detection System Model Implementation against DDOS attacks”. 2019, pp. 877–881.

[4] Zhihui Cheng et al. “Development of Deep Packet Inspection System for Network Traffic Analysis and Intrusion Detection”. 2020, pp. 877–881.

[5] Velasquez, W., Moreira-Moreira, G. Z., & Alvarez-Alvarado, M. S. (2024). Smart grids empowered by software-defined network: A comprehensive review of advancements and challenges. *IEEE Access*.

AFRICA ELECTRICITY SYMPOSIUM

ERA
ELECTRICITY REGULATORY AUTHORITY

MINISTRY OF ENERGY AND MINERAL DEVELOPMENT
THE REPUBLIC OF UGANDA

AFRICA ELECTRICITY SYMPOSIUM

2025

Thank You!

www.aes.era.go.ug
symposium@era.go.ug
+256 393 260166