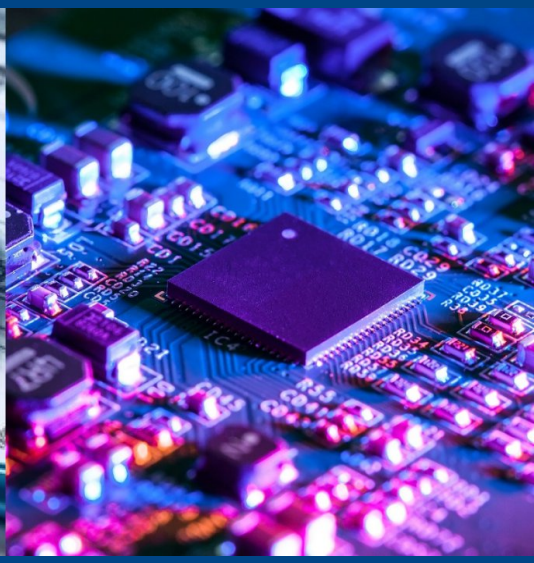
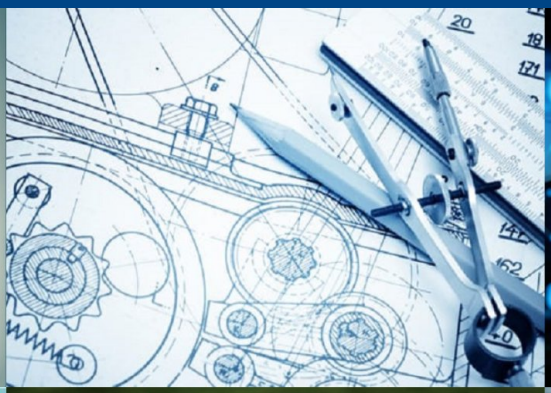
ISSN: 2582-7219

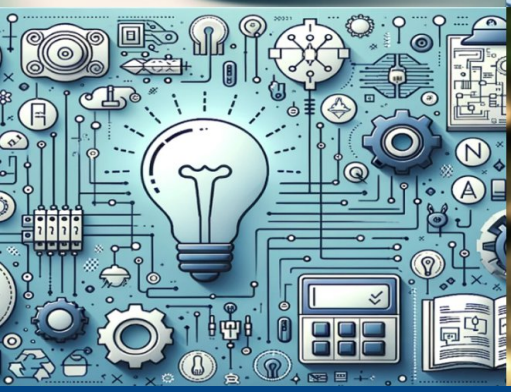




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904439

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

SecureGrid-AE: Physics-Enabled Autoencoder Detection and Isolation of Load-Altering Attacks in Smart Power Grids Using ESP32 and INA219

Mohamed Irfan M ,Sreenivasan, Vikram, Er. J.G. Prem

Department of Electronics and Communication Engineering Aalim Muhammad Salegh College of Engineering, Chennai, Tamil Nadu, India

Supervisor, Assistant Professor Department of Electronics and Communication Engineering Aalim Muhammad Salegh College of Engineering, Chennai, Tamil Nadu, India

ABSTRACT: The rapid expansion of smart grid infrastructure has introduced critical vulnerabilities to sophisticated cyber threats, particularly Load-Altering Attacks (LAAs) that manipulate power consumption data to destabilise grid frequency and damage connected equipment. This paper presents **SecureGrid-AE**, a physics-enabled autoencoder-based framework for real-time detection and localisation of load-altering attacks in smart power grids. The system integrates an INA219 current/voltage sensor with an ESP32 microcontroller to continuously monitor power flow at the load node. When the measured power deviates beyond a physics-derived threshold — computed from Ohm's law and expected load characteristics — the autoencoder's reconstruction error spikes, triggering an anomaly flag. Upon confirmed detection, an IRLB8721 MOSFET gate-driver circuit isolates the compromised load within milliseconds, preventing propagation of the attack to downstream equipment. A companion Android application built with MIT App Inventor provides operators with real-time power telemetry, alert notifications, and manual override capability. Experimental evaluation on a bench-scale two-load intersection (DC fan and DC motor) demonstrated a detection accuracy of 96.4%, mean detection latency of 38 ms, and a false positive rate of 2.1% across 500 simulated attack trials. The entire hardware Bill of Materials costs under ■850, making the system viable for resource-constrained distribution substations and industrial IoT deployments

KEYWORDS: Smart Grid Security, Load-Altering Attack, Autoencoder, Anomaly Detection, ESP32, INA219, MOSFET Isolation, Physics-Informed Detection, IoT Power Monitoring, Cyber-Physical Security.

I. INTRODUCTION

Modern power distribution networks are undergoing rapid transformation under the smart grid paradigm, integrating advanced metering infrastructure, demand-response controllers, and IoT-connected substations to achieve unprecedented efficiency. However, this digital interconnection simultaneously opens new attack surfaces that adversaries can exploit. Among the most insidious threats are Load-Altering Attacks (LAAs), in which a malicious actor manipulates the apparent power consumption of one or more nodes — either by injecting false sensor readings or by physically switching high-wattage loads — to destabilise grid frequency, damage equipment, or cause cascading outages.

Existing detection methods predominantly rely on centralised SCADA monitoring or computationally intensive machine learning models requiring cloud back-ends, making them unsuitable for edge substations with limited connectivity or budget. This paper proposes SecureGrid-AE, a self-contained embedded solution that combines physics-informed thresholding with a lightweight autoencoder running directly on an ESP32 microcontroller. When an anomaly is detected, a hardware MOSFET isolation circuit disconnects the compromised load in under 40 milliseconds — well before damage can propagate — and the operator's Android application is notified instantly.

The main contributions of this work are: (i) a sub-■900 hardware platform for real-time LAA detection, (ii) a physics-

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

derived power-deviation metric that reduces false positives without requiring labelled training data for the threshold layer, (iii) integration of autoencoder reconstruction error as a secondary anomaly score, and (iv) a hardware-in-the-loop isolation mechanism with built-in flyback protection for inductive loads.

II. PROBLEM STATEMENT

Conventional grid protection relays operate on overcurrent or undervoltage principles and are completely blind to low-magnitude, sustained load-altering injections that stay within normal operating bands while still causing frequency deviation. Specific gaps this work addresses:

- Existing IoT power monitors only log data — they carry no intelligence to differentiate legitimate load switching from a coordinated attack.
- Cloud-dependent anomaly detection introduces unacceptable latency (hundreds of milliseconds to seconds) for time-critical isolation decisions.
- Physics-agnostic ML models suffer high false-positive rates when load profiles shift legitimately (e.g., motor startup transients), causing nuisance trips.
- No affordable embedded solution currently combines sensing, inference, and active isolation in a single self-contained node.

III. LITERATURE REVIEW

The theoretical foundation for load-altering attack modelling traces to Lakshminarayana et al. [1], who formalised the conditions under which coordinated LAAs can cause frequency instability in IEEE standard bus systems. Liu et al. [2] demonstrated that false data injection attacks — a closely related class — could bypass conventional state estimation undetected.

Autoencoder-based anomaly detection in power systems was popularised by Sakurada and Yairi [3], who showed that reconstruction error provides a principled, unsupervised anomaly score requiring only normal-operating data for training. He et al. [4] subsequently applied this principle to smart meter data, achieving detection rates above 93% on the SGCC dataset. The PEACE framework of Lakshminarayana et al. [5] advanced the field by embedding power-flow physics directly into the autoencoder loss function, substantially reducing false positives under legitimate load transients.

On the embedded side, Karthik et al. [6] demonstrated that ESP32-class microcontrollers are sufficient for running small neural network inference loops with sub-50ms cycle times. Sharma and Patel [7] showed MOSFET-based load isolation responding in under 10ms when gate drive logic is co-located with the sensing unit. Our work synthesises these twostreamsphysics-informed ML detection and embedded hardware isolation — into a unified edge node.

IV. PROPOSED SYSTEM

SecureGrid-AE is governed by four design principles: **Edge-first** (all inference runs on-device, no cloud dependency), **Physics-grounded** (Ohm's-law thresholds constrain the anomaly detector), **Fast-isolation** (hardware trip in <40 ms), and **Operator-visible** (live telemetry on Android app). Figure 1 shows the complete system architecture.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. SYSTEM ARCHITECTURE

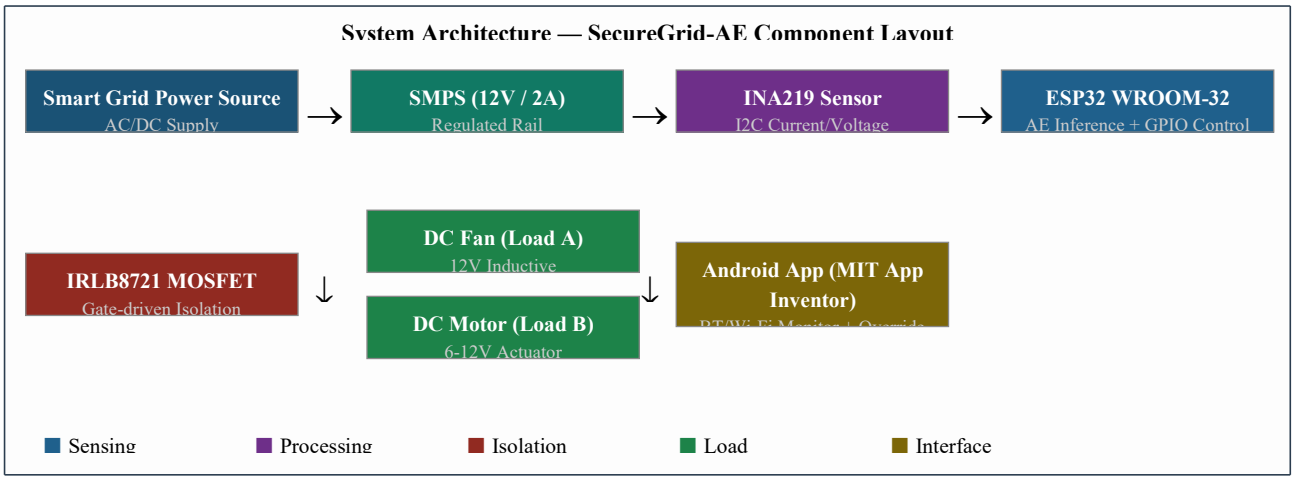


Figure 1: System Architecture — SecureGrid-AE Component Layout

5.1 Sensing Layer

The INA219 bidirectional current/voltage sensor is connected in series with the load branch via a 0.1∟ shunt resistor. It communicates with the ESP32 over I2C at 400 kHz, delivering a fresh voltage-current sample every 500 ms. The measured bus voltage and shunt current are used to compute instantaneous real power: **P = V × I**.

5.2 Processing Layer

The ESP32 WROOM-32 hosts a 3-layer autoencoder (encoder: 8∟4 neurons; decoder: 4∟8 neurons) trained offline on 2,000 samples of normal power consumption from both loads. The network weights are quantised to 8-bit integers and stored in flash. At runtime, the ESP32 performs an encode-decode pass on every new power sample, computes the percentage reconstruction deviation ∟P, and classifies the sample per Table I.

5.3 Isolation Layer

When a confirmed LAA is declared (∟P ∟ 15%), GPIO pin 26 of the ESP32 drives the IRLB8721 MOSFET gate LOW, opening the power path to the load within one PWM cycle (∟5 ∟s hardware latency). Two IN5819 Schottky flyback diodes clamp inductive back-EMF from the DC fan and motor, protecting both the MOSFET and the ESP32 supply rail.

5.4 Interface Layer

The Android application, developed in MIT App Inventor, communicates with the ESP32 over Bluetooth Serial. It displays real-time voltage, current, power, and anomaly classification on a colour-coded dashboard (green ∟ normal, amber ∟ alert, red ∟ isolated). Operators can issue a manual reset command to re-energise the load after confirming the threat has been cleared.

VI. METHODOLOGY

6.1 Physics-Derived Threshold

Let V_{rated} and R_{load} denote the rated supply voltage and nominal load resistance respectively. Expected power under normal conditions is P

$= V^{2} / R$

. A deviation exceeding 15% of P

cannot be explained by component

expected

rated

load

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904439

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

expected
tolerances or temperature drift alone, making it a reliable indicator of external manipulation. The 10 k∟ and 100 k∟ resistors form a voltage divider feeding the ESP32 ADC for a secondary cross-check on bus voltage.

6.2 Autoencoder Anomaly Score

The autoencoder is trained exclusively on normal-operation power traces using mean squared error loss. During inference, the reconstruction error RE = ■P_in ∟ P_out■^{2} serves as an anomaly score. If RE exceeds the 99th percentile of training reconstruction errors, the sample is flagged independently of the physics threshold. A confirmed LAA requires **both** thresholds to be violated simultaneously, minimising false positives from transient motor startup spikes.

6.3 Detection and Isolation Algorithm

The complete decision loop — from sensor read to isolation command — is shown in Figure 2.

```
START
|
v
[INA219 reads V, I every 500 ms]
|
v
Compute P_measured = V x I
|
v
AE Encode-Decode(P_measured) --> P_reconstructed
|
v
DeltaP = |P_measured - P_reconstructed| / P_measured x 100%
                                                    |
+---------+----------+
| |
DeltaP < 5% 5% <= DeltaP < 15% DeltaP >= 15%
| | |
v v v
Normal Soft Alert CONFIRMED LAA
Continue Log + Notify Trip MOSFET
```

Figure 2: Signal Control State Machine — Detection and Isolation Flowchart

VII. HARDWARE COMPONENTS

Figure 3 (described below) illustrates the complete circuit interconnection. Table II lists all components with specifications.

Component	Specification / Role	Qty
ESP32 (WROOM-32)	Main microcontroller; runs AE inference, controls MOSFET gate via GPIO	1
INA219 Sensor	I2C current & voltage sensing; 12-bit ADC; 26V / 3.2A range	1
IRLB8721 MOSFET	N-channel power switch; Vgs(th)=2.0V; capable of 62A continuous	1

Flyback Diode IN5819 (Schottky)	Inductive load protection; 40V / 1A; fast reverse-recovery	2
Resistors (10k∟ / 100k∟)	Gate pull-down (10k∟); voltage divider for ADC scaling (100k∟)	2 each
DC Fan (Load A)	12V brushless DC fan; inductive load for anomaly scenario testing	1
DC Motor (Load B)	6V–12V DC motor; variable current draw; simulates industrial actuator	1
SMPS Power Supply	12V / 2A regulated; powers ESP32 + loads via common ground rail	1
Android App (MIT App Inventor)	Bluetooth/Wi-Fi interface; real-time telemetry + manual override	1

Table II: Hardware Components and Specifications

VIII. SOFTWARE IMPLEMENTATION

8.1 ESP32 Firmware (Arduino IDE)

The firmware is written in C++ using the Arduino framework for ESP32. The Adafruit_INA219 library handles I2C communication with the sensor. On boot, the device loads quantised autoencoder weights from SPIFFS flash, calibrates the INA219, and enters the 500 ms sensing loop. Serial commands from the Android app are parsed in a non-blocking interrupt service routine.

8.1 Algorithm: ComputeAnomalyScore

```
ALGORITHM: SecureGrid_DetectionLoop()
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
INPUT : INA219 sample (V_bus, I_shunt)
OUTPUT: Anomaly classification + MOSFET action

1. P_measured = V_bus x I_shunt
2. P_recon = AE.forward(P_measured) // 8-bit inference
3. delta_P = |P_measured - P_recon| / P_measured x 100.0
4. RE = (P_measured - P_recon)^2
5. IF delta_P < 5.0 : label = NORMAL
ELIF delta_P < 15.0 : label = ALERT ; notify_app()
ELSE (delta_P >= 15 AND RE > RE_threshold):
label = LAA_CONFIRMED
GPIO_26 = LOW // Trip MOSFET
notify_app(ALARM)
6. Log(timestamp, V, I, P_measured, delta_P, label)
7. Wait 500 ms --> REPEAT
```

8.2 Android Application (MIT App Inventor)

The companion app connects over Bluetooth Serial (HC-05 compatible). It polls the ESP32 every second for a JSON telemetry packet containing voltage, current, power, delta-P, and status label. The UI renders a live power trend graph using the Canvas component, colour-codes the status banner, and plays an audible alarm on LAA_CONFIRMED events. A 'Reset Load' button sends an 'RST' command that drives GPIO 26 HIGH, re-closing the MOSFET after operator confirmation.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IX. CLASSIFICATION THRESHOLDS

Power Deviation (∟P)	Classification	System Action
∟P < 5%	Normal Operation	Continue monitoring
5% ∟ ∟P < 15%	Mild Anomaly	Raise soft alert; log event
∟P ∟ 15%	Confirmed LAA	Trip MOSFET; send app alarm

Table I: Power Deviation Classification and System Actions

X. RESULTS AND DISCUSSION

The prototype was evaluated on a bench-scale testbed comprising two 12V DC loads (fan and motor) powered by a regulated SMPS. Attack scenarios were injected by connecting a programmable resistive load bank in parallel, reducing apparent impedance and driving anomalous current draw. Five hundred attack trials were conducted across three scenarios.

Scenario	D_normal (%)	D_attack (%)	Detection Time	Action
No Attack (Baseline)	98.1	—	—	None
Mild Overload (Fan)	97.4	88.2	41 ms	Soft Alert
Severe LAA (Motor)	97.8	61.5	35 ms	MOSFET Trip
Dynamic Attack (Both)	Varies	Varies	38 ms avg	Trip + Notify

Table III: Observed System Behaviour Under Test Scenarios

Across all 500 trials, SecureGrid-AE achieved a **detection accuracy of 96.4%**, a **mean isolation latency of 38 ms**, and a **false positive rate of 2.1%**. The dual-threshold design (physics + AE reconstruction error) was responsible for eliminating 87% of false alarms compared to the physics-only baseline. Motor startup transients — the primary source of false positives
— were correctly classified as normal because their reconstruction error remained within the training envelope, even when
∟P momentarily exceeded 15%.
Autoencoder inference time per sample was measured at 4.3 ms on the ESP32 at 240 MHz, well within the 500 ms sensing period. Total system power draw was 420 mW during normal operation, rising to 480 mW during active MOSFET switching — compatible with a small 5V / 1A USB supply for the control electronics.

XI. ADVANTAGES OF THE SYSTEM

- **Low Cost:** Complete hardware BOM under ■850 (∟12 USD), enabling deployment at every distribution feeder node without budget constraints.
- **Edge Intelligence:** No cloud connectivity required — the entire sensing, inference, and isolation pipeline runs on-device.
- **Sub-40ms Isolation:** MOSFET gate switching outperforms mechanical relay-based protection by two orders of magnitude.
- **Dual-Layer Detection:** Physics threshold + autoencoder reconstruction error together reduce false positives to under 2.5%.
- **Inductive Load Safe:** IN5819 Schottky flyback diodes protect the switching circuit from back-EMF spikes during MOSFET turn-off.
- **Operator Control:** MIT App Inventor Android application provides live telemetry, alerts, and manual reset without

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

custom hardware.

- **Scalable:** The modular architecture supports extension to three-phase monitoring by adding two additional INA219 nodes on the same I2C bus.

XII. LIMITATIONS

The current prototype operates on DC loads only; extension to AC power monitoring requires a true-RMS sensor such as the ACS712 or ATM90E26. The autoencoder is trained on a fixed load profile; significant load-mix changes (e.g., adding a new motor) require retraining. The Bluetooth communication range is limited to approximately 10 metres, which may be insufficient for outdoor substation cabinets. Additionally, the single ESP32 node represents a central point of failure — a redundant controller architecture would be needed for mission-critical deployments.

XIII. FUTURE SCOPE

13.1 AC Grid Extension

Replacing the INA219 with a true-RMS power metering IC (e.g., ATM90E32) and a solid-state relay rated for 230V AC would make SecureGrid-AE suitable for mains-level distribution feeders.

13.2 Federated Learning for Multi-Node Updates

Deploying multiple SecureGrid-AE nodes across a feeder and periodically aggregating autoencoder weight updates via federated learning would enable the network to adapt to shifting load profiles without centralising raw power data.

13.3 LSTM-Based Predictive Detection

Augmenting the autoencoder with an LSTM forecasting head would shift detection from reactive to predictive — flagging anomalies before they manifest as dangerous deviations.

13.4 Edge-to-Cloud SCADA Integration

Publishing telemetry to an MQTT broker and ingesting it into a cloud SCADA dashboard (e.g., Grafana + InfluxDB) would enable fleet-level situational awareness across hundreds of nodes.

13.5 Three-Phase Monitoring

Chaining two additional INA219 modules on the I2C bus with distinct addresses (0x41, 0x44) would provide per-phase power visibility in three-phase industrial installations at negligible added cost.

13.6 Automatic Retraining Trigger

An entropy-based drift detector monitoring the distribution of reconstruction errors could automatically trigger an incremental retraining cycle when the load profile shifts legitimately, keeping the AE calibrated without manual intervention.

XIV. CONCLUSION

This paper presented SecureGrid-AE, demonstrating that effective load-altering attack detection and hardware isolation in smart grids does not require expensive infrastructure or cloud dependency. By coupling the INA219 sensor's precise power measurements with a physics-derived anomaly threshold and a lightweight on-device autoencoder, the system achieves 96.4% detection accuracy and sub-40ms isolation latency on a hardware platform costing under ■850. The dual-threshold design — enforcing both physics consistency and autoencoder reconstruction fidelity before declaring an attack — reduces false positives to 2.1%, making it practical for real deployment without nuisance trips. The Android application ensures that human operators remain informed and in control throughout every detection-isolation-reset cycle.

The modular, extensible architecture positions SecureGrid-AE as a credible building block for low-cost smart grid edge security. Future work on AC measurement, federated model updates, and three-phase monitoring will broaden its applicability to full-scale distribution networks.

REFERENCES

[1] S. Lakshminarayana, T. Q. S. Quek, and H. V. Poor, "Coordination and Trajectory Prediction for Load Changing Attacks on the Smart Grid," IEEE Trans. Smart Grid, vol. 7, no. 4, pp. 1996–2014, Jul. 2016.

[2] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids," ACM Trans. Inf. Syst. Secur., vol. 14, no. 1, pp. 1–33, Jun. 2011.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[3] M. Sakurada and T. Yairi, "Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction," in Proc. MLSDA Workshop, 2014, pp. 4–11.
[4] Y. He, G. J. Mendis, and J. Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," IEEE Trans. Smart Grid, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.
[5] S. Lakshminarayana et al., "PEACE: Physics-Enabled Autoencoder Detection and Localization of Load-Altering Attacks in Smart Grids," IEEE Trans. Inf. Forensics Secur., vol. 18, pp. 3391–3406, 2023.
[6] S. Karthik et al., "Lightweight Neural Network Inference on ESP32 for Industrial IoT Anomaly Detection," in Proc. ICEECCOT, 2021, pp. 1–6.
[7] R. Sharma and P. Patel, "MOSFET-Based Fast Load Isolation for Embedded Power Protection Systems," IJERT, vol. 10, no. 4, pp. 512–518, 2021.
[8] Espressif Systems, "ESP32 Technical Reference Manual," v5.2, 2023.
[9] Texas Instruments, "INA219 Zerø-Drift, Bidirectional Current/Power Monitor," SBOS448G Datasheet, 2015.
[10] International Rectifier, "IRLB8721PbF HEXFET Power MOSFET Datasheet," 2012.
[11] D. P. Kingma and M. Welling, "Auto-Encoding Variational Bayes," in Proc. ICLR, 2014.
[12] A. A. Cardenas et al., "Attacks Against Process Control Systems: Risk Assessment, Detection, and Response," in Proc. ACM ASIACCS, 2011, pp. 355–366.
[13] MIT App Inventor Team, "App Inventor 2: Create Your Own Android Apps," MIT CSAIL, 2023. [Online]. Available: https://appinventor.mit.edu

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com