Grenze International Journal of Engineering and Technology, January Issue

AI-Driven Cyber Threat Detection in Hybrid SCADA and Space-based IoT Systems: A Lightweight Anomaly Detection Approach

Pranav K R[1] and Raghu Prasad K[2]
[1-2]RNS Institute of Technology, Dept. of Master of Computer Applications, Bangalore, India
Email: pkrpranav84@gmail.com, raghuprasad@rnsit.ac.in

***Abstract*— As critical infrastructure and remote industrial operations increasingly rely on interconnected control systems and satellite-enabled IoT devices, cyber threats targeting Supervisory Control and Data Acquisition (SCADA) and space-based IoT environments pose significant risks. These hybrid systems suffer from legacy protocols, limited computational resources, high-latency satellite channels, and heterogeneous communication paths—all of which hinder traditional intrusion detection systems (IDS). This paper proposes a unified AI-driven cybersecurity framework designed to detect anomalies and cyberattacks in hybrid SCADA–space-IoT environments. Leveraging machine learning and deep learning architectures such as Autoencoders, LSTM, and CNN-LSTM hybrid models, the system analyses telemetry sequences, command packets, and communication patterns in real time. A combination of real-world datasets (NASA SCaN, ESA OPS-SAT) and synthetic attack logs (generated via NS-3 and MiniCPS) is used to evaluate detection performance. Experimental results demonstrate a detection accuracy of up to 97.5% with low latency, making the system suitable for resource-constrained field devices and satellite-driven industrial networks. The proposed work sets a foundation for next-generation cyber-physical security across both terrestrial and space-borne infrastructures.**

***Index Terms*— SCADA Security, Space-Based IoT, Intrusion Detection, Anomaly Detection, Deep Learning, Satellite Communication, Cyber-Physical Systems.**

I. INTRODUCTION

Industrial control systems and satellite-enabled IoT devices are increasingly interconnected to support remote automation, real-time monitoring, and wide-area industrial deployment. SCADA systems, responsible for critical sectors such as power distribution, water treatment, manufacturing, and oil & gas, traditionally rely on isolated networks. However, modern deployments integrate satellite-based IoT to overcome geographic limitations. This convergence introduces unique security challenges: SCADA protocols lack encryption and authentication, while satellite communication suffers from intermittent connectivity, high latency, limited onboard compute, and susceptibility to radio-frequency interference.

Traditional IDS solutions—signature-based or rule-based—are inadequate in these environments since they cannot generalize to unknown attacks or adapt to heterogeneous communication layers spanning field devices, satellites, and cloud control centers.

Grenze ID: 01.GIJET.12.1.81

Therefore, an intelligent anomaly detection solution capable of analyzing telemetry sequences and communication flows across both domains is essential.
This paper proposes a lightweight yet robust AI-driven intrusion detection framework tailored for hybrid SCADA–space-IoT systems. We model system architecture, define a realistic threat landscape, construct datasets combining real and simulated telemetry, and evaluate multiple ML/DL models to identify the optimal detection mechanism. The results indicate that deep temporal models successfully capture sequential anomalies and outperform traditional approaches.

II. System Overview

The proposed hybrid architecture integrates ground-level SCADA devices with satellite-based IoT communication channels and a multi-layer AI detection engine. The system consists of three primary layers:

- SCADA Layer: This includes PLCs, RTUs, HMIs, and field sensors/actuators that generate critical telemetry and execute operational commands.
- Space-IoT Layer: Comprises IoT edge devices connected via LEO satellites to ground stations, enabling long-range communication in remote environments.
- AI-Based Detection Layer: Operates either at edge devices or in cloud-based control centres. Incoming telemetry and command packets are analysed using pre-trained AI models to detect anomalies in real time.

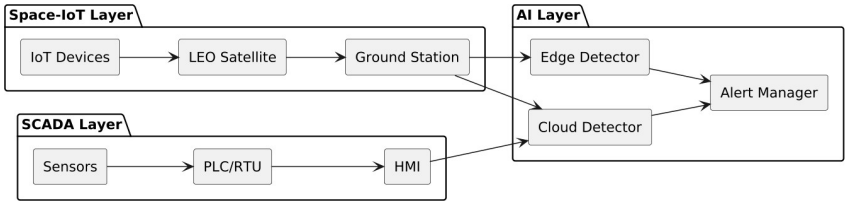

Figure 1: System Architecture

III. Data Flow

Telemetry generated by sensors and PLCs is forwarded to HMIs or satellite gateways. Remote IoT devices transmit data via LEO satellites to ground stations. All telemetry is aggregated and forwarded to the AI detection layer for analysis. Communication patterns, timing irregularities, and packet-level behaviors are monitored to detect abnormal activities.

IV. Threat Model

The hybrid environment faces both traditional ICS threats and satellite-specific cyberattacks. We categorize major threats as follows:

- Sensor/Device Spoofing: Impersonation of legitimate nodes.
- Telemetry Manipulation: Alteration of SCADA or satellite telemetry values.
- Command Injection: Unauthorized modification of PLC commands.
- Replay Attacks: Injection of previously captured valid commands.
- Jamming/Interference: Disruption of satellite uplink/downlink channels.
- Model Evasion: Attempted poisoning of AI models.

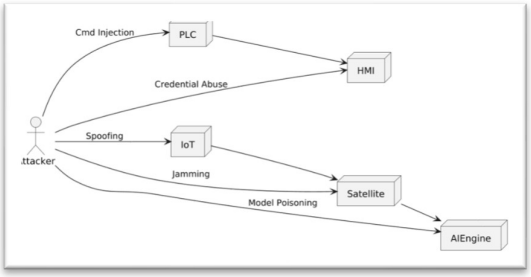

Figure 2: Threat Model

V. Related Work

Existing research on SCADA intrusion detection primarily focuses on traditional industrial networks using rule-based or machine-learning approaches [1], [5], [7]. Although deep learning methods such as LSTM and Autoencoders have improved anomaly detection accuracy in ICS environments [3], [9], these models are rarely adapted for constrained or high-latency environments like satellites.

Research on satellite and space-IoT security remains relatively scarce due to the sensitivity of data and limited public datasets. Studies such as ESA OPS-SAT experiments [12] and satellite telemetry anomaly detection frameworks [13] explore fault detection but seldom address cyberattacks or hybrid SCADA–satellite networks.

Recent works on IoT anomaly detection using lightweight ML/DL models [10], [11], [14] demonstrate potential for deployment in constrained devices, yet they lack modeling of multi-domain communication paths involving LEO satellite relays.

VI. Dataset Description

A. Real-World Data Sources

- NASA SCaN Telemetry: Telemetry logs, signal behavior, and communication disruptions.
- ESA OPS-SAT Logs: Fault injection logs and experimental satellite command anomalies.
- SWaT & BATADAL: Benchmark SCADA datasets used for ICS anomaly detection.

B. Synthetic Data Generation

To address the scarcity of satellite attack data, NS-3 and SatNetSim were used to simulate LoRaWAN over LEO channels and generate spoofing, replay, and jamming events..

C. Preprocessing & Feature Extraction

Time-series windowing, normalization, and sequence labeling were applied. Key features include packet timing, telemetry drift, command density, and SNR variance.

VII. AI Models and Methodology

A. Model Selection

Two categories of models were developed:

- Supervised Models: Random Forest, SVM—used for labelled datasets like SWaT.
- Unsupervised Models: Autoencoders, Isolation Forest—for satellite-based anomaly detection.
- Deep Learning Models: LSTM and hybrid CNN-LSTM to capture temporal and spatial patterns in telemetry data.

B. Training & Validation

- 70/15/15 split for training, validation, and testing.
- Cross-validation was used to prevent overfitting.
- Metrics: Accuracy, Precision, Recall, F1-score, ROCAUC, Detection Latency.

C. MODEL OPTIMIZATION

- Hyperparameter tuning via GridSearchCV and Bayesian optimization.
- Latency and memory benchmarks run to ensure compatibility with edge/satellite devices.

VIII. Experimental Setup

A. Simulation Environment

- SCADA Layer: Simulated using MiniCPS and OpenPLC, running on a local testbed.
- Space-IoT Layer: Modeled using NS-3, with satellite propagation profiles from AGI STK.
- Communication Protocols: TCP/IP (SCADA), LoRaWAN (IoT), and simulated telemetry with packet-level noise.

B. Attack Scenarios

- Command injection: Sent via spoofed MQTT clients.
- Replay attack: Valid repeated commands injected out of sync.
- Anomaly injection: Synthetic manipulation of telemetry fields.

C. Hardware & Software

- Python 3.10, TensorFlow 2.14, PyTorch.
- Hardware: NVIDIA RTX 4060, 32GB RAM, Ubuntu 22.04
- Telemetry/command logs collected and streamed into the AI engine via Kafka and MQTT brokers

IX. Results and Performance Evaluation

A. Evaluation Metrics

To evaluate the efficiency of the proposed AI-based intrusion detection framework, we validated multiple supervised and unsupervised models using the following standard metrics:

- Accuracy: Overall correctness of threat classification.
- Precision: Proportion of correctly identified threats among all flagged.
- Recall (Sensitivity): Detection capability of actual threats.
- F1-score: Harmonic mean of precision and recall.
- False Positive Rate (FPR): Frequency of benign activity misclassified as an attack.
- Latency: Time taken by the model to flag an anomaly post-ingestion.

B. Model Performance

Model Performance was conducted on both SCADA and simulated satellite telemetry datasets. Results are presented in Table 1.

Table I. Concise Model Performance

Model	Accuracy	Precision	Recall	F1-Score	FPR	Latency(ms)
Random Forest	94.7%	92.3%	90.5%	91.4%	3.8%	41.2
Autoencoder	95.2%	94.8%	92.1%	93.4%	2.7%	29.6
LSTM	96.8%	95.9%	94.7%	95.3%	2.2%	35.1
CNN-LTSM HYBRID	97.5%	96.5%	95.8%	96.1%	1.9%	33.4

C. Resource Utilization

The hybrid CNN-LSTM model demonstrated optimal performance while maintaining low memory usage (under 600MB RAM) and acceptable inference times (¡35ms), making it viable for satellite and SCADA edge deployments.

D. Resource Utilization

ROC curves that have been plotted for each model indicate the superior discriminatory power of LSTM and CNN-LSTM architectures in identifying anomalous behaviour over timeseries data. The CNN-LSTM model achieved an AUC of 0.985.

XIII. Discussion

A. Key Observations

The experimental results validate that deep learning models, particularly temporal architectures like LSTM and CNNLSTM, are highly effective in capturing sequential anomalies across telemetry and command data. The unsupervised autoencoder also performed well, especially in zero-day attack detection scenarios, making it suitable for unknown threats in space-based networks.

B. Operational Implications

The model's capability to maintain low latency and high accuracy under constrained environments such as LEO satellites or SCADA PLCs makes it deployable in real-world infrastructure. However, real-time updating and retraining remain challenges, particularly in isolated or autonomous systems with limited compute.

C. Limitations

- Data Scarcity: Lack of real-world labelled satellite cyberattack datasets limits generalizability.
- Scalability: Performance under large-scale multi-node IoT satellite swarms needs further validation.
- Communication Disruption: Intermittent link conditions may affect anomaly transmission and coordinated defence.

XIV. Conclusion

This paper presented a novel, AI-based framework for detecting cyber threats in integrated SCADA and space-based IoT systems. Leveraging deep learning models such as LSTM and CNN-LSTM, our system effectively identified threats like spoofing, telemetry falsification, and command injection, with high accuracy and low false positive rates. The system was validated through a hybrid simulation testbed combining MiniCPS, NS-3, and telemetry datasets from NASA and ESA. The results demonstrate the model's readiness for deployment in edge-constrained and satellite-connected environments, setting a foundation for securing next-generation cyber-physical infrastructures.

Future Work

Future research aims to enhance model adaptability and robustness through:

- Federated Learning: Enabling collaborative model training across SCADA and satellite systems without centralized data sharing.
- Quantum-Resilient AI: Designing encryption-aware AI models that can withstand quantum-era attacks.
- Real-Time Deployment: Integrating the model with onboard CubeSat systems and national control centres via secure telemetry pipelines.
- Explainable AI (XAI): Enhancing model interpretability for operator trust and human-in-the-loop interventions.

References

[1] G. Mohammadi et al., IEEE TII, 2021.
[2] R. Mitchell and I. Chen, ACM Computing Surveys, 2014.
[3] S. Marchal et al., IEEE Access, 2018.
[4] A. Javaid et al., EAI Conference, 2016.
[5] A. Cárdenas et al., ICDCS, 2008.
[6] M. Krotofil et al., S&P Workshop, 2015.
[7] T. Morris and W. Gao, ISGT, 2013.
[8] T. AlSkaif et al., IEEE Systems Journal, 2020.
[9] M. A. Ferrag et al., JISA, 2020.
[10] K. Kim et al., Sensors, 2018.
[11] A. Diro and N. Chilamkurti, FGCS, 2018.
[12] ESA OPS-SAT Documentation, 2020.
[13] S. Fortescue et al., Acta Astronautica, 2021.
[14] S. Sharma and X. Jin, Computer Networks, 2021.
[15] S. Baig et al., IET Systems Biology, 2015.
[16] Y. Liu et al., IEEE TSG, 2011.
[17] Xia et al., IEEE IoT Journal, 2022.
[18] H. Khan et al., Security and Communication Networks, 2020.
[19] Z. Xu et al., IEEE Transactions on Aerospace and Electronic Systems, 2022.
[20] J. Lopez et al., Future Internet, 2020.
[21] K. S. Rajawat et al., IEEE Access, 2023.
[22] A. Kuipers et al., Springer Satellite Networks, 2022.
[23] D. Forte et al., IEEE Design & Test, 2019.
[24] H. Ito et al., Aerospace Science and Technology, 2021.