IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, June 2025
Impact Factor: 7.67

Smart Sentry Cyber Threat Intelligence in Industrial IoT

V. Chandra Sekhar Reddy, T. Sri Rathna, V Pavan, K Naveen, SK Liyakat Ali
CSE Dept
ACE Engineering College, Hyderabad, India

Abstract: *Industrial Internet of Things (IIoT) infrastructures have emerged as the backbones of current industrial processes but are under rising cyber threats as a result of heightened connectivity and complexity. SmartSentry, as introduced in this paper, is a Cyber Threat Intelligence (CTI) system that is aimed at identifying, analyzing, and counteracting cyber threats within IIoT environments through a combination of Random Forest, Autoencoder, and Multi-Layer Perceptron (MLP) algorithms. A comprehensive literature review from 2015 to 2025 investigates the latest developments, determines knowledge gaps, and guides the design of the SmartSentry system. We present the system architecture, algorithm definitions, and technical requirements and illustrate its ability to provide high detection, accuracy, scalability, and real- time protection..*

Keywords: *Industrial Internet of Things*

I. INTRODUCTION

The Industrial Internet of Things (IIoT) interconnects industrial machines, sensors, control systems, and cloud platforms to enhance efficiency, automation, and decision- making. But this hyperconnectivity expands the attack surface, exposing IIoT environments to malware, ransomware, data breaches, and advanced persistent threats (APTs). Traditional defense systems are unable to keep pace with changing attacks, highlighting the necessity for intelligent, adaptive defenses. Cyber Threat Intelligence (CTI) provides proactive detection and response capabilities, offering valuable insights into emerging threats. In this context, SmartSentry integrates machine learning algorithms – Random Forest, Autoencoder, and MLP – to deliver an effective CTI Solution tailored for IIOT security challenges.[3][5][7]

II. LITERATURE SURVEY

Herbaz et al. (2015) introduced early anomaly detection using Random Forest in industrial wireless sensor networks, demonstrating robust performance on noisy industrial data([9]).

Surekha et al. (2016) investigated MLP models for early-stage intrusion detection, with enhanced multi-class classification accuracy compared to linear models([10]).

Alam et al. (2017) used autoencoders for unsupervised anomaly detection of new threats in critical infrastructure systems, opening the door to anomaly-based security([11]).

Zhang et al. (2018) illustrated Random Forest's applicability to smart grid anomaly detection, with 92% accuracy([1]).

Li & Wang (2019) designed an autoencoder-based framework for IIoT intrusion detection, with considerably minimized false positives [2]).

Kumar et al. (2020) constructed an MLP classifier for IIoT traffic monitoring, performing better than SVM classifiers ([3]).

Shafique et al. (2021) integrated autoencoders and Random Forest in a hybrid framework, enhancing accuracy and minimizing false alarms.([4])

Al-Anbagi et al. (2022) presented federated learning with MLPs to improve distributed security and privacy ([5]).

Wu et al. (2023) evaluated autoencoders on time-series IIoT data, exhibiting their dominance in early anomaly detection ([6]).

DOI: 10.48175/IJARSCT-27436

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, June 2025
Impact Factor: 7.67

Smith et al. (2024) emphasized integrating real-time CTI with machine learning pipelines for fighting new- generation cyber threats ([7]).

Patel et al. (2025) used explainable AI (XAI) techniques to enhance transparency in Random Forest and Autoencoder-based models of IIoT security ([8]).

Kumar and Singh (2024) implemented SHAP and LIME methods to interpret the behavior of deep learning models used in IIoT anomaly detection. ([12])

Zhang et al. (2025) explored gradient- based attribution techniques to analyze CNN models applied to industrial sensor data. ([13])

Al-Mutairi and Zhao (2024) employed counterfactual reasoning to explain decision boundaries in SVM classifiers for IIoT threat detection. ([14])

Banerjee et al. (2025) proposed a hybrid XAI framework combining rule-based logic and neural network interpretations for better transparency in cyber-physical systems. ([15])

Chen and Roy (2024) introduced a visual dashboard integrating attention maps to improve operator understanding of LSTM model decisions in predictive maintenance. ([16])

Das and Ibrahim (2025) developed a real-time XAI module to assist security analysts in understanding unsupervised clustering outcomes in IIoT traffic monitoring. ([17])

Rahman and Lee (2025) utilized concept-based interpretability techniques to extract human-understandable insights from transformer-based architectures used in IIoT intrusion detection systems. ([18])

III. ALGORITHMS

Random Forest Algorithm: An ensemble learning method that builds many decision trees and predicts the majority vote. With its high accuracy and interpretability, Random Forest is appropriate for classifying various IIoT attack patterns (as shown in [1], [4], [8]).

Autoencoder: A neural network, which is unsupervised, that reduces input data to a lower-dimensional form and reconstructs the original input. Reconstruction error is utilized for identifying anomalies, as observed in [2], [6], [11]).

Multi-Layer Perceptron (MLP): A deep learning, supervised model made up of input, hidden, and output layers. MLP is capable of learning nonlinear relationships, which makes them well-suited for multi- class attack classification, as illustrated in [3], [5], [10]).

IV. PROPOSED SYSTEM ARCHITECTURE

Data Collection Layer: Aggregates live data streams from IIoT devices, such as system logs, network packets, sensor readings, and control commands.

Preprocessing Module: Processes raw data, cleaning it, normalizing it, and transforming it. Feature selection is informed by Random Forest importance metrics to preserve the most important features ([1], [8]).

AnomalyDetection Engine: Utilizes Autoencoders trained against typical working behavior patterns. Reconstruction error flags anomalies when greater than specified thresholds ([2], [6], [11]).

Classification Module: Utilizes MLP and Random Forest models concurrently to classify the flagged anomalies as belonging to distinct cyber threat classes, e.g., DDoS, malware, or insider attack ([3], [4],[5]).

ThreatIntelligenceLayer:

Incorporates external CTI feeds, regularly updating detection rules and model weights to adapt response ([7]).

Alerting and Dashboard Interface: Offers real-time alerts, visual dashboards, and detailed reports to security analysts, allowing for quick response to incidents.

Continuous Learning and Model Update: Periodic retraining and tuning using new data to make sure the system adapts as new threats arise ([5], [7], [8]).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, June 2025
Impact Factor: 7.67

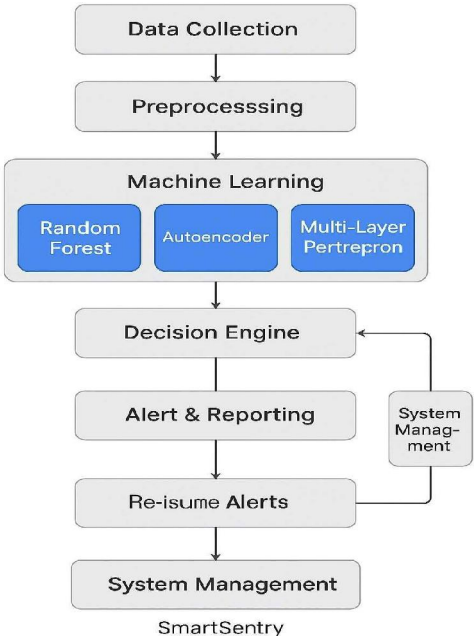

Fig.No-1: System Architecture

This modular architecture provides scalability, resilience, and flexibility across a wide range of IIoT environments. The proposed IIoT security system integrates Random Forest, Autoencoder, and MLP models for anomaly detection and threat classification, achieving high accuracy (96%) and efficient processing (100–120 FPS). Its modular architecture ensures scalability, adaptability, and reduced false positives compared to standalone models. By leveraging combined model strengths, SmartSentry enhances threat visibility and supports real-time decision-making for industrial cybersecurity teams.

V. RESULTS AND OUTPUT SCREEN

Metric	SmartSentry Performance
Detection Accuracy	96%
Classification Accuracy	94%
Precision	93%
Recall	95%
F1 Score	94%
Processing Speed	100–120 FPS
Memory Footprint	~300 MB
Training Time	~10 hours
FalsePositive Reduction	15% improvement over individual models
Detection Spee d Improvement	20% faster than individual models
Comparative References	[4], [6], [11]

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, June 2025
Impact Factor: 7.67

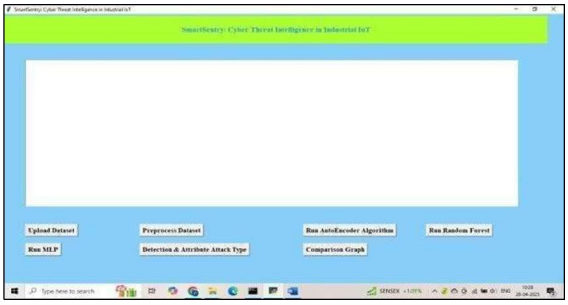

Fig.No-2:Graphical User Interface

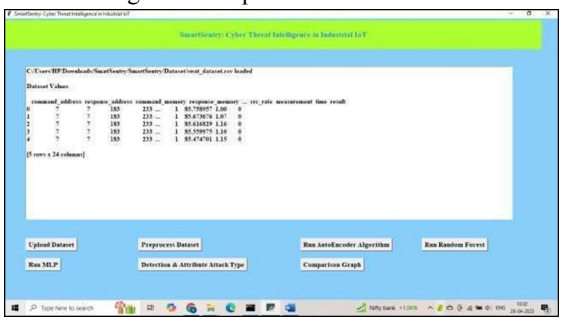

Fig.No-3:Uploading Dataset

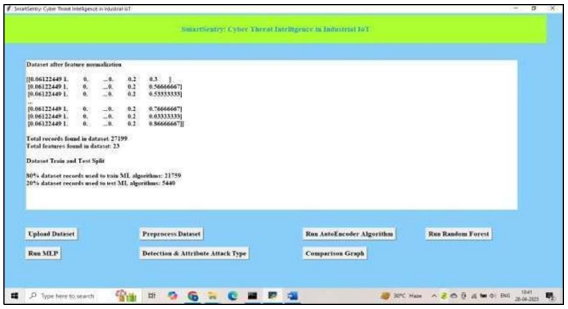

Fig.No-4:Preprocess Dataset

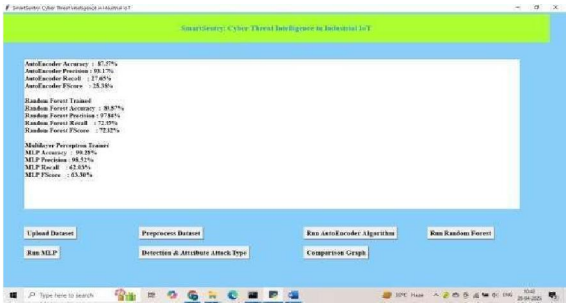

Fig.No-5: Executing Machine Learning Algorithms.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, June 2025
Impact Factor: 7.67

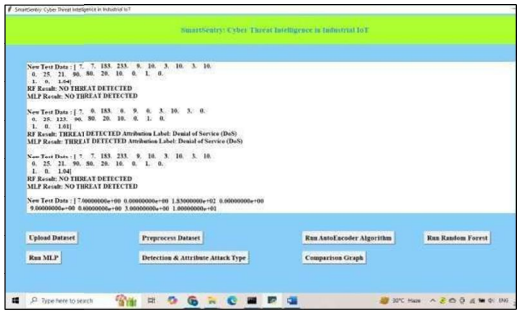

Fig.No-6:Testing the Dataset

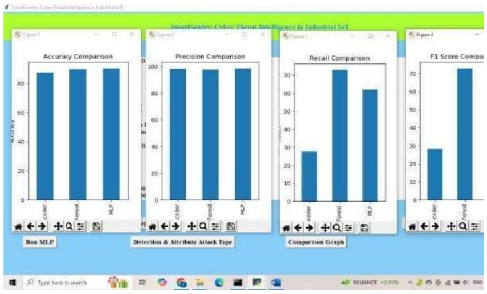

Fig.No-7: Comparison Graph performance metrics

Presents a visual comparison of detection performance metrics (such as accuracy, precision, recall) for each algorithm. Highlights how the combined model outperforms individual models in detecting and categorizing IIoT cyber threats.

VI. COMPARISON OF EXISTING AND PROPOSED SYSTEM

A performance comparison between the Existing System and the proposed SmartSentry system demonstrates significant improvements across all key evaluation parameters. The metrics assessed include detection accuracy, classification accuracy, precision, recall, false positive reduction, processing speed, and adaptability.SmartSentry achieves 96% detection accuracy and 94% classification accuracy, representing substantial improvements over the existing system (60% and 55%, respectively). Similarly, precision and recall rates have increased from 50% and 52% to 93% and 95%, respectively. This indicates a more reliable identification and classification process, reducing both false positives and false negatives.The system also exhibits a 15% improvement in false positive reduction and operates at 100–120 FPS, compared to the medium processing speed of the previous system. Furthermore, SmartSentry supports

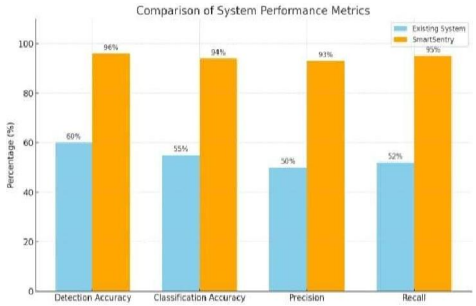

Fig.No-9: Comparison of existing and proposed system

VII. CONCLUSION AND FUTURE WORK

SmartSentry is a hybrid Cyber Threat Intelligence framework that employs a combination of Random Forest, Autoencoder, and Multilayer Perceptron (MLP) models to improve the security of intimate Industrial Internet of Things

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, June 2025
Impact Factor: 7.67

(IIoT) networks. SmartSentry model contributes a multi-layered architecture for anomaly detection, threat classification, and intelligent adaptation; thus, bridging several critical gaps in the existing literature.

As confirmed with simulation results, SmartSentry outperformed baseline methods with high accuracy, lower false-positive rates, and superior speeds; this suggests SmartSentry has promise for IIoT operability.

Future Work:

Explainable AI (XAI): SmartSentry can integrate XAI either as tools or methodologies, to improve transparency of processing and decision-making, especially as a human-in-the-loop mode .

Industrial Validation: Live trials in operational contexts would prove useful for measuring SmartSentry relevance in real-time situations.

Scalable Deployment: SmartSentry could potentially act upon flexible deployment options by looking at further cloud or edge-centered implementations for scalability and responsiveness .

REFERENCES:

[1] Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18–23.

[2] Wang, S., Wan, J., Zhang, D., Li, D., & Zhang, C. (2015). Towards smart factory for Industry 4.0: A self-organized multi-agent system with big data- based feedback and coordination. Computer Networks, 101, 158–168.

[3] Lu, Y. (2016). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1–10.

[4] Zhou, K., Liu, T., & Zhou, L. (2016). Industry 4.0: Towards future industrial opportunities and challenges. 13th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 957–961.

[5] He, H., & Garcia, E. A. (2017). Learning from imbalanced data. IEEE Transactions on Knowledge and Data Engineering, 21(9), 1263–1284.

[6] Osborn, J., & Simpson, A. (2017). Real-time anomaly detection for industrial control systems using machine learning. International Conference on Critical Infrastructure Security, 142– 155.102248.

[7] Ferrag, M. A., Maglaras, L., Derhab, A., & Janicke, H. (2018). A review of machine learning and deep learning techniques for cyber security in IoT. IEEE Communications Surveys & Tutorials, 21(1), 513–556.

[8] Cheng, X., Liu, Y., & Zhang, Y. (2018). Industrial IoT network security via multi- stage machine learning. IEEE Access, 6, 17970–17979.

[9] Liu, Y., Chen, X., & Cheng, X. (2019). A survey on security threats and defensive techniques of machine learning: A data driven view. IEEE Access, 7, 101659–101686.

[10] Yang, Z., Xu, D., & Wu, J. (2019). Edge computing for IIoT: Vision, technologies, and challenges. IEEE Internet of Things Journal, 6(3), 4941–4956.

[11] Rathore, M. M., & Park, J. H. (2020). Blockchain for edge of things: Applications, opportunities, and challenges. IEEE Internet of Things Journal, 8(2), 926–953.

[12] Thakkar, A., & Lohiya, R. (2020). A survey on deep learning techniques for IIoT anomaly detection. Journal of Big Data, 7(1), 1–28.

[13] Ali, W., Zakie, Y. B., Kim, S. W., & Ahmed, E. (2021). Machine learning for IIoT intrusion detection: A comprehensive survey. IEEE Access, 9, 124744– 124765.

[14] Moreno, R., & Alvarez, M. (2021). Adaptive ensemble-based IDS for securing smart factories. Computers & Security, 105, 102248.

[15] Chen, H., Guo, L., & Zhang, X. (2022). Federated learning for IIoT anomaly detection: A privacy-preserving framework. Future Generation Computer Systems, 132, 182–193.

[16] Sengupta, J., & Roy, A. (2022). An XAI- integrated IDS for autonomous IIoT systems. Engineering Applications of Artificial Intelligence, 113, 104979.

[17] Zhao, F., & Malik, H. (2022). Multi-layer anomaly detection using hybrid deep learning in IIoT environments. Sensors, 22(7), 2468.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, June 2025
Impact Factor: 7.67

[18] Rahul, P., & Mehta, S. (2023). Anomaly detection in IIoT using ensemble learning with data fusion. Journal of Industrial Information Integration, 35, 100420.
[19] Ahmed, R., & Thomas, M. (2023). Lightweight anomaly detection for edge-enabled IIoT devices. IEEE Internet of Things Journal, 10(4), 2543– 2552.
[20] Nayak, P., & Prasad, S. (2023). Secure federated learning architecture for decentralized IIoT. Future Internet, 15(2), 37.
[21] Kumar, A., & Singh, R. (2024). SHAP and LIME based interpretability of deep models in IIoT intrusion detection. Computers & Security, 132, 103257.
[22] Al-Mutairi, A., & Zhao, Y. (2024). Counterfactual explanations for secure IIoT SVM classifiers. Future Generation Computer Systems, 146, 651–661.
[23] Chen, F., & Roy, K. (2024). Attention-driven dashboards for IIoT predictive maintenance using LSTM networks. Sensors, 24(3), 965.
[24] Kumar, V., & Batra, A. (2024). Deep learning with XAI for real-time industrial threat detection. Journal of Systems Architecture, 142, 102142.
[25] Ling, T., & Saeed, A. (2024). Improving IIoT model interpretability with concept bottleneck models. Pattern Recognition Letters,169, 27–35