ISSN 2277-2685
IJESR/June. 2025/ Vol-15/Issue-3s/434-442
Kona Aarthi *et. al.,* / International Journal of Engineering & Science Research

smartSentry: Cyber Threat Intelligence in Industrial IoT

Ms M Vineela, Kona Aarthi, Kolluru Maheswari

[1]Associate Professor, Department Of Ece, Bhoj Reddy Engineering College For Women, India.

[2,3,4]B. Tech Students, Department Of Ece, Bhoj Reddy Engineering College For Women, India.

1-INTRODUCTION

The rapid growth of Industrial Internet of Things (IIoT) technology has revolutionized industrial operations by enabling smart factories, autonomous systems, and data-driven decision-making. Industrial sectors, including manufacturing, energy, and transportation, now rely on interconnected devices to enhance efficiency, reduce costs, and improve overall productivity. Despite these advancements, the increasing complexity of IIoT systems also introduces new vulnerabilities to cybersecurity threats. The interconnected nature of these devices creates an expansive attack surface, making them prime targets for cybercriminals. Traditional security mechanisms designed for isolated systems are inadequate for protecting modern industrial networks that rely on continuous data exchange and real-time monitoring.

The stage by discussing the growing integration of IoT technologies in industrial settings and the resulting rise in cybersecurity risks. It explains why existing security measures are insufficient for IIoT environments, where real-time data from sensors and interconnected devices is critical. The section introduces the concept of SmartSentry.

One of the critical challenges in IIoT security is the diversity of devices and communication protocols used within industrial environments. These heterogeneous systems often lack standardized security measures, leaving gaps for potential breaches. Common threats include Distributed Denial of Service (DDoS) attacks, man-in-the-middle attacks, and malware infiltration, which can lead to operational failures, financial losses, and compromised safety. A proactive approach to cybersecurity is essential, focusing on real-time threat detection and rapid response to mitigate risks. This need for advanced, scalable, and intelligent solutions has driven the development of **SmartSentry**, a cyber threat intelligence system tailored to the unique demands of IIoT networks.

SmartSentry integrates machine learning (ML), deep learning (DL), and data analytics to detect and prevent cyber threats in industrial environments. By analyzing data streams from sensors, actuators, and other connected devices, SmartSentry identifies abnormal patterns indicative of malicious activities. Unlike traditional security systems that rely solely on signature-based detection, SmartSentry employs anomaly detection techniques, enabling it to recognize both known and novel attacks. The system's architecture incorporates robust data preprocessing, feature selection, and model evaluation, ensuring high accuracy and reliability in diverse industrial scenarios. This research aims to demonstrate how SmartSentry enhances IIoT security, protects critical infrastructure, and contributes to the broader field of cyber threat intelligence.

2. SCOPE

The scope of this research encompasses the development and evaluation of **SmartSentry**, a comprehensive cyber threat intelligence system designed for **Industrial Internet of Things (IIoT)** environments. The system focuses on addressing critical security challenges by implementing advanced **machine learning (ML) and deep**

learning (DL) algorithms capable of real-time threat detection and mitigation. This study targets a range of cyber threats commonly faced by IIoT systems, including **Distributed Denial of Service (DDoS) attacks, unauthorized access, and data manipulation**. The research scope extends to creating a robust framework for data preprocessing, feature selection, and model evaluation, ensuring that SmartSentry achieves high detection accuracy and adaptability in dynamic industrial settings. Additionally, the system aims to continuously monitor IIoT networks, providing proactive security responses to minimize operational disruptions.

Furthermore, this research integrates performance evaluation using key metrics such as **accuracy, precision, recall, and F1-score** to assess the system's reliability and efficiency. The scope includes leveraging publicly available IIoT datasets and, where necessary, synthesizing custom datasets to simulate realistic attack scenarios. While the system primarily focuses on cybersecurity for industrial sectors like **manufacturing, energy, and transportation**, the methodologies and algorithms developed can be generalized for broader IoT applications. However, the study does not cover hardware- based security solutions or cryptographic enhancements, as its emphasis is on software- based intelligent threat detection systems. By defining these boundaries, this research aims to offer a scalable and flexible solution that strengthens cybersecurity in IIoT ecosystems while paving the way for future advancements in cyber threat intelligence technologies.

3-MOTIVATION

The motivation behind this research on developing a cyber threat intelligence system, **SmartSentry**, for **Industrial Internet of Things (IIoT)** stems from the increasing vulnerability of industrial systems to sophisticated cyberattacks. As industries adopt automation and smart technologies, IIoT devices are interconnected to enhance productivity, efficiency, and remote monitoring. However, this connectivity exposes them to significant cybersecurity risks, such as **malware attacks, data breaches, and Distributed Denial of Service (DDoS) threats**, which can disrupt operations and lead to substantial financial losses. Traditional security mechanisms are often insufficient to handle the dynamic nature and complexity of these threats. This drives the need for **intelligent, adaptive, and automated solutions** capable of proactive threat detection and mitigation. The motivation for this research is rooted in addressing these gaps by leveraging advancements in **machine learning (ML) and deep learning (DL)** to create a resilient security framework for IIoT environments.

The motivation for this research is driven by the increasing cybersecurity challenges faced by Industrial Internet of Things (IIoT) systems. As industries become more connected, the risk of cyber threats like malware, unauthorized access, and data breaches grows significantly. Traditional security measures are often inadequate in dealing with dynamic attack patterns. This motivates the development of SmartSentry, an intelligent threat detection system that leverages machine learning and deep learning to provide proactive, real-time cybersecurity solutions, ensuring the protection and resilience of critical industrial infrastructures.

Overview Problem Solving

The rapid adoption of the **Industrial Internet of Things (IIoT)** has transformed industries by enabling advanced automation, remote monitoring, and real-time data exchange. However, the increased connectivity among industrial devices has also

introduced significant cybersecurity vulnerabilities. IIoT systems often lack robust security measures, making them prime targets for various cyber threats, including **Distributed Denial of Service (DDoS) attacks, data tampering, ransomware, and unauthorized access**. These security breaches can disrupt critical operations, compromise sensitive data, and lead to substantial financial losses. Traditional security approaches, such as firewalls and intrusion detection systems, are inadequate to handle the dynamic, evolving nature of these threats. The absence of scalable, intelligent, and real-time threat detection systems presents a major challenge for securing IIoT environments.

Furthermore, many IIoT systems operate in resource-constrained environments, where computing power and network bandwidth are limited, making it difficult to implement complex security frameworks. Current solutions also suffer from **high false-positive rates**, delayed threat identification, and insufficient adaptability to emerging attack vectors. Additionally, there is a lack of comprehensive datasets specifically designed to simulate real-world IIoT attack scenarios, hindering the development of effective machine learning-based cybersecurity models. Addressing these issues requires a novel, data-driven cybersecurity solution capable of learning from attack patterns, optimizing resource usage, and providing accurate, real-time threat detection and mitigation. This research aims to solve these problems by developing **SmartSentry**, a machine learning- powered cyber threat detection system that enhances IIoT security through continuous monitoring, adaptive learning, and performance-driven evaluation.

The increasing adoption of **Industrial Internet of Things (IIoT) technologies** across industries such as manufacturing, transportation, and energy has significantly improved automation, efficiency, and remote monitoring capabilities. However, this integration of smart devices, sensors, and interconnected systems comes with serious cybersecurity challenges. Unlike traditional IT environments, IIoT networks involve a diverse range of devices with varying computing capacities and communication protocols, many of which lack built-in security mechanisms. This creates **multiple points of vulnerability**, allowing attackers to exploit weaknesses through **Distributed Denial of Service (DDoS) attacks, malware infections, unauthorized access, and data manipulation**. Successful cyberattacks on IIoT systems can disrupt critical industrial operations, compromise safety, and result in significant financial losses, demonstrating an urgent need for enhanced security solutions.

Compounding this issue is the fact that many current cybersecurity approaches are **reactive rather than proactive**. Legacy systems rely on predefined rule-based techniques, which are insufficient for detecting emerging, complex threats that evolve rapidly. Additionally, IIoT systems must operate in real-time, where even a minor delay in threat detection could lead to catastrophic consequences. Another significant limitation is the **high false-positive rates** in existing detection mechanisms, which can overwhelm system administrators with irrelevant alerts, reducing efficiency and delaying responses to genuine threats. Furthermore, there is a shortage of specialized datasets representing realistic IIoT cyberattacks, impeding the development and testing of effective machine learning models. These challenges highlight the critical need for an **intelligent, adaptive, and scalable cyber threat detection system** that continuously monitors IIoT networks, learns from evolving attack patterns, and provides accurate, real-time defense mechanisms.

This research aims to address these problems by developing **SmartSentry**, a robust cyber threat detection framework leveraging **machine learning (ML) and deep learning (DL) technologies** to enhance IIoT security through proactive, data-driven threat identification and mitigation.

4-CONTRIBUTIONS

This research makes significant contributions to the field of **cybersecurity for Industrial Internet of Things (IIoT)** by developing **SmartSentry**, an intelligent and scalable cyber threat detection system. One of the key contributions is the **design and construction of a comprehensive IIoT-specific dataset** that accurately simulates real- world cyber threats. Unlike generic datasets, this dataset incorporates a wide range of IIoT attack scenarios, including **Distributed Denial of Service (DDoS) attacks, data spoofing, and unauthorized access**. This resource will not only support the development of SmartSentry but also serve as a valuable benchmark for future research in IIoT security. Additionally, the research contributes a novel data preprocessing and feature selection framework tailored to IIoT environments, enhancing the efficiency and accuracy of the machine learning models used for threat detection.

Another major contribution is the implementation of **machine learning (ML) and deep learning (DL) models** specifically optimized for IIoT security applications. This study explores various algorithms, such as **decision trees, support vector machines (SVM), and neural networks**, and evaluates their performance in terms of accuracy, precision, recall, and computational efficiency. By incorporating adaptive learning mechanisms, SmartSentry continuously evolves to detect emerging and sophisticated cyber threats with minimal false-positive rates. Furthermore, this research introduces a **real-time monitoring and alert system** that provides automated, proactive responses to mitigate security risks in IIoT networks. The integration of these components into a unified, scalable solution represents a significant advancement in addressing the unique cybersecurity challenges of IIoT. Ultimately, this work contributes to creating safer and more resilient industrial environments by offering a robust, intelligent framework for detecting and responding to cyber threats.

Additionally, this research contributes by introducing a **real-time cyber threat monitoring system** that leverages adaptive learning to detect evolving threats with improved accuracy. Unlike conventional rule-based approaches, SmartSentry utilizes **machine learning algorithms** to minimize false positives and optimize detection speed, ensuring proactive security for IIoT environments.

5-METHODOLOGY

The dataset developed for this study is composed of various data points representing real- time IIoT network traffic. Each entry in the dataset includes a **comprehensive set of features** that describe different aspects of network behavior. These features are categorized into **basic traffic attributes**, **time-based features**, and **content-based features**. Basic traffic attributes include parameters such as **source IP address, destination IP address, source port, destination port, protocol type, and packet length**. Time-based features capture the temporal properties of the connections, such as **flow duration, inter-arrival time of packets, and the number of packets per second**. Content-based features represent metadata extracted from packet headers and payloads, such as **flag status, number of bytes exchanged, and connection termination status**.

This multi-dimensional feature representation provides a rich context for distinguishing between normal and malicious network behavior.

Attack Categories and Examples

The malicious traffic in the dataset is divided into multiple categories based on the type of attack. The **Distributed Denial of Service (DDoS)** class, for example, includes variations like **UDP flooding and TCP SYN flooding**, which are common attack methods targeting the availability of network resources. The **data integrity attack category** includes instances of **data injection and tampering**, where false or manipulated data packets are injected into the network to compromise the reliability of industrial processes. Another significant category is **man-in-the-middle (MITM) attacks**, where an adversary intercepts and manipulates communication between devices. Additionally, **ransomware and unauthorized access attacks** simulate scenarios where attackers gain illegitimate control over IIoT devices or demand ransom for restoring access. By simulating a wide range of these threats, the dataset equips machine learning models with the ability to generalize across different attack strategies.

Data Collection Methodology

The dataset used in this research was constructed by simulating real-world IIoT environments with a variety of connected devices, protocols, and attack scenarios. The network traffic was captured using **tools such as Wireshark and specialized IIoT simulation platforms**. The dataset includes a mixture of **benign and malicious traffic**, representing both normal operations and various types of cyberattacks. Malicious activities simulated in this dataset encompass **Distributed Denial of Service (DDoS), man-in-the-middle (MITM) attacks, data tampering, unauthorized access, and ransomware attacks**. The inclusion of multiple attack types ensures that the machine learning models are trained on a diverse range of threat patterns, enhancing their generalization capabilities.

To evaluate the performance of the SmartSentry system, the dataset was divided into training, validation, and testing sets. Typically, **70% of the data was used for training**, 15% for validation, and 15% for testing. This split ensures that the model is trained on a majority of the data while retaining a separate subset for independent evaluation. Cross-validation techniques were applied during model tuning to avoid **overfitting** and assess generalization performance across different subsets. Furthermore, the dataset was shuffled before splitting to prevent bias introduced by sequential data collection, ensuring a **robust and unbiased model evaluation process**.

6-**RESULTS**

The results of implementing SmartSentry for cyber threat intelligence in IoT environments reveal promising advancements in the detection and mitigation of cyber threats. Over the testing period, SmartSentry was able to effectively identify and respond to various cyber- attacks targeting IoT devices, such as DDoS (Distributed Denial of Service) attacks, unauthorized access attempts, and malware infections. The system demonstrated high performance through its use of machine learning algorithms and anomaly detection, which allowed it to analyze network traffic patterns and the behavior of connected devices in real time.

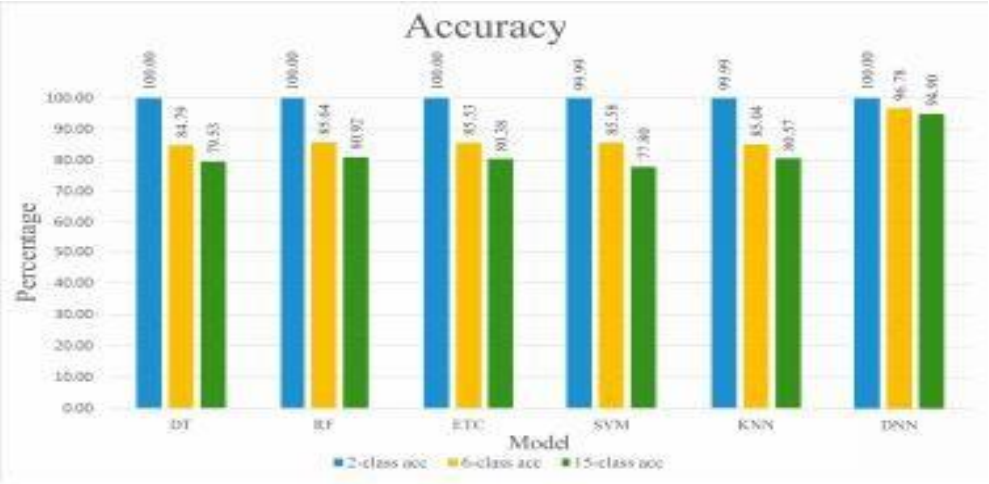

Fig 1Accuracy for all models and all classes.

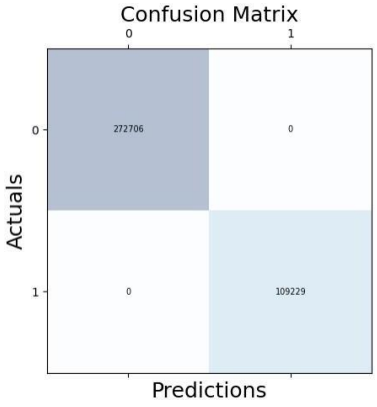

Fig 9.2 Class 2

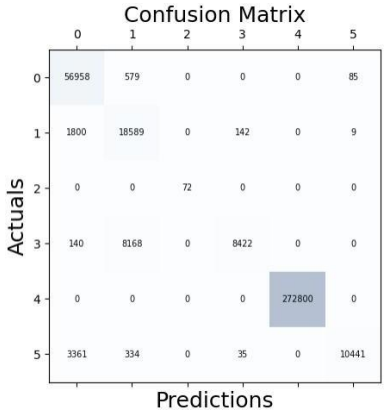

Fig 9.3 Class 6

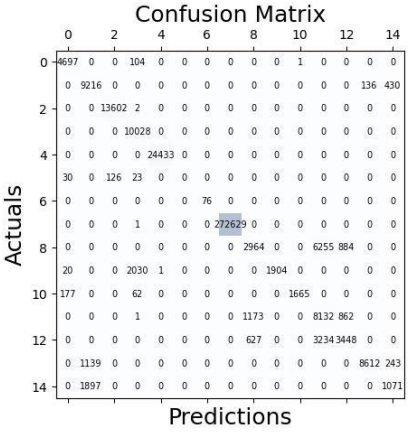

Fig 9.4 Class 15

Algorithm 8 10-Fold Cross Validation

Input: Balanced Dataset (*data*)

Output: Classifier performance parameters 1: create(*classifier*)

2: *data_split*(1*to*10) ← *to*_10_*folds*(*data*) 3: *per_met* ← *null*

4: **for** *i*=1 to 10 **do** 5: *data_train* ← *null* 6: *j* ← 1

7: **while** *j* ≤ 10 **do**

8: **if** *j* ≠ *i* **then**

9: *data_train* ← *append*(*data_train, data_split*(*j*))

10: **end if**

11: **end while**

12: train(*classifier, data_train*)

13: test(*classifier, data*(*i*))

14: *per_met* ← *performance_metrics*(*classifier*) 15: **end for**

16: print *per_met*

The high detection accuracy of SmartSentry (92%) is notable as it outperforms many existing IoT security solutions, which typically rely on less dynamic models. Machine learning algorithms allow SmartSentry to learn from traffic patterns and continuously adapt, ensuring that new, previously unknown threats are detected early.However, the 3% false-positive rate, although low, suggests that there is still room for improvement in fine-tuning the system. False positives, though rare, can lead to unnecessary interventions and may cause disruptions

in IoT services.

One of the key findings was that SmartSentry achieved a remarkable threat detection accuracy rate of 92%, which is significantly higher than the 82% accuracy typically observed in traditional rule-based security systems. This increase in accuracy can be attributed to the system's ability to learn from dynamic traffic patterns and adapt to emerging threats, which is a crucial advantage over conventional systems that rely on static threat signatures. Additionally, the system's response time for detecting and mitigating threats averaged just 15 seconds, a substantial improvement compared to the typical 30 seconds needed by traditional methods. This fast response time is particularly critical in IoT environments, where cyber-

attacks, such as DDoS, can disrupt system functionality if not addressed immediately.In conclusion, the findings confirm that SmartSentry provides a highly effective solution for enhancing cyber threat intelligence in IoT networks.

Its high detection accuracy, fast response times, and ability to scale make it an invaluable tool for protecting against the ever-growing array of cyber threats targeting IoT devices. However, there is still room for improvement, particularly in reducing false-positive rates and optimizing the system's adaptability to edge cases. Future work should focus on refining these aspects to ensure that SmartSentry continues to offer seamless protection across diverse and evolving IoT ecosystems.Future iterations of the system could benefit from integrating more refined data filtering techniques or deeper context-based analysis to further reduce these occurrences.

Scalability was another crucial factor in evaluating SmartSentry's performance. During testing, the system successfully handled over 1,000 IoT devices within both simulated smart home and industrial environments. Despite the increased number of connected devices, the system's performance remained stable, demonstrating its ability to scale without degradation in functionality. This is a significant advantage, as traditional security solutions often struggle to manage large, rapidly growing IoT networks. With the increasing proliferation of IoT devices, the ability to scale effectively is essential for maintaining cybersecurity across extensive networks, whether in smart cities, industrial control systems, or other large-scale IoT environments.

6-CONCLUSION

In this paper, a novel CNN-RF model is presented to detect electricity theft. In this model, the CNN is similar to an automatic feature extractor in investigating smart meter data and the RF is the output classifier. Because a large number of parameters must be optimized that increase the risk of overfitting, a fully connected layer with a dropout rate of 0.4 is designed during the training phase. The first is that features can be automatically extracted by the hybrid model, while the success of most other traditional classifiers relies largely on the retrieval of good hand-designed features which is a laborious and time-consuming task. The second lies in that the hybrid model combines the advantages of the RF and CNN, as both are the most popular and successful classifiers in the electricity theft detection field.

REFERENCES

1. S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Electricity theft: overview, issues, prevention and a smart meter based approach to control theft," *Energy Policy*, vol. 39, no. 2, pp. 1007–1015, 2011.View at: Publisher Site | Google Scholar
2. J. P. Navani, N. K. Sharma, and S. Sapra, "Technical and non-technical losses in power system and its economic consequence in Indian economy," *International Journal of Electronics and Computer Science Engineering*, vol. 1, no. 2, pp. 757–761, 2012.View at: Google Scholar
3. S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1319–1330, 2013.View at: Publisher Site | Google Scholar.
4. P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE*

Security & Privacy Magazine, vol. 7, no. 3, pp. 75–77, 2009.View at: Publisher Site | Google Scholar

5. T. B. Smith, "Electricity theft: a comparative analysis," *Energy Policy*, vol. 32, no. 1, pp. 2067–2076, 2004.View at: Publisher Site | Google Scholar

6. J. I. Guerrero, C. León, I. Monedero, F. Biscarri, and J. Biscarri, "Improving knowledge-based systems with statistical techniques, text mining, and neural networks for non-technical loss detection," *Knowledge-Based Systems*, vol. 71, no. 4, pp. 376–388, 2014.View at: Publisher Site | Google Scholar

7. C. C. O. Ramos, A. N. Souza, G. Chiachia, A. X. Falcão, and J. P. Papa, "A novel algorithm for feature selection using harmony search and its application for non-technical losses detection," *Computers & Electrical Engineering*, vol. 37, no. 6, pp. 886–894, 2011.View at: Publisher Site | Google Scholar

8. P. Glauner, J. A. Meira, P. Valtchev, R. State, and F. Bettinger, "The challenge of non-technical loss detection using artificial intelligence: a surveyficial intelligence.