Adaptive Open Cyber Intelligence for SOAR: Reduced False Positives in Low-Resource Environments

Shunmugam U*, Rajesh D
Department of Computer Science and Engineering,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India

***Abstract*—The increasing use of resource-constrained cyber-physical devices emphasizes the need for effective and flexible methods in the deployment of threat intelligence. The Open Cyber Intelligence Framework (OCIF), an architecture that applies Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) capabilities to resource-constrained environments, is presented in this study. The OCIF uses lightweight machine learning models in an adaptive way to process cyber threat intelligence (CTI) with greater precision and effectiveness. By using Wazuh to monitor the behavior of machines and OpenSearch for modeling the results of the analysis, the OCIF can reduce false positives by up to 6% in real-world implementations. The model ensures sufficient threat mitigation without taxing the system by striking a balance between anomaly detection, context, and decreased communication overhead. Because of its open-source propagation and modular form factor, OCIF promotes innovation and makes it possible for CTI to be built and used in restricted resources with optimal detection and operational efficiency.**

***Keywords*—Open Cyber Intelligence Framework; SOAR; SIEM; Cyber Threat Intelligence; false positive reduction; threat mitigation; anomaly detection**

I. Introduction

The proliferation of resource-constrained devices permeates every aspect of the connected world in the modern digital era, making the critical need for cybersecurity tailored to these devices' particular challenges indisputable. A paradigm shift in how we protect sensitive data and infrastructure is required due to the emergence of Internet of Things (IoT) sensors, embedded systems, and other limited devices [1]. Adaptive Deployment Strategies and Threat Intelligence Integration are two crucial aspects of the Open Cyber Intelligence Framework (OCIF) that are thoroughly examined in this research study.

Resource-constrained devices, characterized by limitations in processing power, memory, and bandwidth, inherently pose a formidable challenge to traditional cybersecurity frameworks. Recognizing this, the OCIF emerges as a beacon of innovation, seeking to not merely address these challenges, but to redefine the parameters of adaptive and effective cybersecurity tailored explicitly for devices with constrained resources [2].

Traditional cybersecurity frameworks are inherently challenged by resource-constrained devices, which are defined by limitations in processing power, memory, and bandwidth. Acknowledging this, the OCIF becomes a shining example of innovation, aiming to redefine the parameters of effective and adaptive cybersecurity specifically designed for devices with limited resources, rather than just addressing these issues [2]. For IoT and cyber-physical systems, the majority of current intrusion detection and CTI solutions are still too bulky, insufficiently flexible, and prone to a high rate of false positives in environments with limited resources. In actuality, the majority of CTI and SOAR/SIEM models make assumptions about high bandwidth and processing power, which leaves a crucial gap for severely constrained devices [3].

For IoT and cyber-physical systems, the majority of current intrusion detection and CTI solutions are still too bulky, insufficiently flexible, and prone to a high rate of false positives in environments with limited resources. In actuality, the majority of CTI and SOAR/SIEM models make assumptions about high bandwidth and processing power, which leaves a crucial gap for severely constrained devices [3]. The expansion of the Internet of Things (IoT) exposes lightweight computing devices to an increasing number of attacks, necessitating the urgent need for a low-overhead, adaptable framework that integrates automated deployment and CTI. This work uses the Open Cyber Intelligence Framework, or OCIF, to address this need.

The Threat Intelligence Integration component of OCIF takes on the task of efficiently absorbing and processing real-time threat data in order to support the adaptive deployment initiatives. Context-aware integration, scalable data processing methods, the creation of an ongoing feedback loop, and reliable experimental validation are all given special attention in this area of study. This dimension seeks to bridge theoretical underpinnings with empirical evidence and to offer useful insights into efficient Threat Intelligence Integration methodologies for resource-constrained devices by utilizing platforms like Wazuh [4] in conjunction with predefined machine learning algorithms available in OpenSearch.

A. Cyber Threat Intelligence (CTI) for IoT

Due to the growing amount of Digital Connectivity and the addition of Internet of Things (IoT) devices across every aspect of every person's life, the need for a Proactive and Adaptive Cybersecurity Paradigm is higher than it's ever been before. Cyber Threat Intelligence (CTI) has become a pivotal discipline for providing increased Cyber Resilience to IoT Ecosystems in an evolving Threat Landscape. The rapid

*Corresponding author.

Growth of this interconnected Ecosystem has created many Security Challenges for IoT devices, from Smart Home Devices to Industrial Sensors, requiring a Sophisticated and Context-Aware approach.

B. The IoT Landscape

The internet of things (IoT) consists of a large number of electronically connected devices, which together make up a matrix of vulnerabilities and attack vectors that can be exploited by hackers. The features and functions incorporated into IoT devices are designed to add convenience and efficiency for the user; however, due to the limited processing power and variety of communication protocols between these devices, they are susceptible to cyberattacks. Therefore, to successfully secure the IoT ecosystem, it is critical to fully comprehend the functionality of IoT devices and have continuous monitoring of the continually changing cyber threat landscape.

C. Dynamics of Cyber Threat Intelligence

In the context of IoT, cyber threat intelligence is a proactive and strategic method of identifying, reducing, and eliminating cyberthreats. It entails gathering, evaluating, and sharing useful information about possible risks to IoT networks and devices. By offering contextual insights into the strategies, tactics, and practices used by adversaries in the IoT space, CTI enables organizations to go beyond reactive defense mechanisms, in contrast to traditional cybersecurity measures.

D. Contextualizing Threats in the IoT landscape

To properly secure IoT devices and networks from cyber attacks, an IoT expert must understand the threats to the device/network at a high level. This is accomplished through the use of Cyber Threat Intelligence (CTI) applied to IoT. When CTI is applied to IoT, it doesn't just allow the IoT expert to identify malicious traffic; it also enables the expert to understand how to interpret the traffic associated with a particular IoT device, how to spot patterns in the traffic, and how to identify abnormal behaviour based on the patterns when viewed in the context of the overall IoT ecosystem.

E. Integrating Threat Intelligence into IoT Security Posture

To stay ahead of the competition, IoT security postures must incorporate Cyber Threat Intelligence. To find possible threats, it makes use of machine learning algorithms, advanced analytics, and real-time monitoring. Organizations can strengthen the resilience of IoT devices and networks by improving their capacity to identify and address new threats through the integration of threat intelligence feeds.

F. Contributions of this Research

- Integrated Framework for Adaptive Deployment and Threat Intelligence
- Adaptive deployment strategies specifically tailored for resource-constrained devices.
- Context-Aware Threat Intelligence Integration
- Application of Machine Learning Algorithms
- A significant contribution of the research is its explicit focus on reducing false positives, a common challenge in cybersecurity operations

G. Novelty of this Research

- The study suggests an integrative strategy that combines continuous threat intelligence integration with adaptive deployment strategies. This entire framework, which is integrated into the OCIF, offers a complete solution for protecting devices with limited resources.
- In order to ensure the best cybersecurity measures while taking into account the limitations of these devices, the research presents Adaptive Deployment Strategies designed especially for resource-constrained devices. This entails not only understanding and profiling the devices but also implementing lightweight communication protocols, modular deployment architectures, and adaptive resource allocation.
- The ongoing integration of threat intelligence is tailored to environments with limited resources. This includes context-aware integration, real-time data ingestion, and scalable data processing techniques made to function well in settings with constrained computational power.

The organization of this research study is clear and consists of five main sections. In Section II, we will conduct a complete literature survey that reviews the current literature related to Cybersecurity for Resource-Constrained Devices (RCRDs), Adaptive Deployment Strategies, and Continuous Threat Intelligence Integration, while identifying any gaps in the existing body of knowledge. In Section III, we will discuss the methods used, including the creation of an Open Cybersecurity Infrastructure Framework (OCIF), and present Adaptive Deployment Strategies that include Device Profiling, Lightweight Protocols, and Contextual Awareness. In addition, we will discuss Continuous Threat Intelligence Integration techniques, which consist of Real-Time Data Ingestion and Scalable Processing. Section IV contains a detailed description of the Experimental Setup used in this study, which includes Wazuh and OpenSearch as well as a discussion of the results and their effect on the number of false positives. Section V concludes this research by summarizing the major results and discussing the implications for the community.

II. Related Works

The limited resources of devices, such as processing power, memory, and energy, pose serious challenges to traditional approaches to cyberattack detection. Devices are vulnerable to a number of potential attacks, including data manipulation, resource depletion, and denial of service (DoS). AlWaisi et al. [1] have presented a novel framework to address these problems. This framework uses machine learning (ML) models optimized for low-resource devices to combine anomaly detection, feature extraction, and lightweight data collection. The main objective is to reduce computational load and memory usage by optimizing machine learning models while taking available resources into account. Effective attack detection is made possible by this methodology, which also saves operating time and monitors energy consumption.

Kornaros et al. [2] have explored hardware-assisted methods to overcome these resource constraints. Examples include engineered architectures with specialized memory units, dedicated accelerators for specific ML tasks, and secure enclaves for trusted execution. However, incorporating hardware accelerators requires careful evaluation of compromises related to expense, power usage, and complexity. Moreover, achieving a balance between latency, accuracy, and memory usage is crucial to optimizing machine learning models for devices with limited resources. Arshad et al. [3] introduced an intrusion detection framework tailored for energy-constrained IoT devices. This framework addresses obstacles such as processing capacity restrictions and energy consumption limitations. It highlights the importance of implementing a specialized intrusion detection system to efficiently mitigate security risks.

A methodology for protecting IoT nodes with limited resources is presented by Shalaginov et al. [4], highlighting the importance of intelligent microcontrollers in distributed smart application attack detection. This entails incorporating advanced strategies like intelligent microcontrollers, machine learning algorithms, or other approaches intended for effective operation on IoT nodes with constrained resources. Increased security, fewer false positives, and less demand on device resources are possible advantages. The increasing use of fog computing in critical infrastructure systems and the ensuing security issues are acknowledged by Khan et al. [5]. They stress the importance of proactive defense tactics against possible cyberthreats. A hybrid DL-driven framework for SDN-enabled cyber threat detection in the Internet of Things is presented by Javeed et al. [6]. The framework likely centres on some of the main components of SDN. The authors believe that SDN provides additional customisation of networks and that the use of SDN also boosts the ability of detection algorithms to identify new cyberthreats. The second aspect of cybersecurity is the work by Khan et al. [7], who present a model for using data analysis to enable the detection and mitigation of malicious/internal human threats. An assessment of the data analytics methods used, as well as measurable rates of accuracy and the ability of the system to adapt to differing characteristics within IoT environments, will be included in this model.

Jeffrey et al. [8] performed an exhaustive review of current research on anomaly detection methods in the CPS Security field and classify the methods into three categories: statistical, machine learning, and hybrid methods. The authors' assessment will include various aspects, including false-positive rates, scalability, the rate of accuracy in detecting anomalies, and adaptability to dynamic CPS environments. The paper by Bradbury et al. [9] provides an assessment of the basic principles for threat modelling used to establish the trust mechanisms in outsourced task deliveries for IoT devices that have limited resource capability. The authors discuss examples of where the methods proved successful in identifying, deterring secure delegated tasks, and maximising the efficient use of resources. The study by Aljuhani et al. [10] presents the integration of AI methods as an enhancement to the intelligence of IoMT sensors/devices having limited resource capacity.

This entails using AI algorithms, such as machine learning and deep learning, to identify unusual behavior and possible security risks. The assessment might offer a thorough description of particular AI models or algorithms that are employed, highlighting their advantages in adjusting to changing threat environments. They might also go over how the recommended SaaS-based IDS ensures interpretability and clarity, enabling system administrators and healthcare professionals to comprehend and trust the system's output. Celdrán et al. [11] emphasize the significance of creating creative and resource-efficient strategies to lessen ransomware attacks, especially on Internet of Things (IoT) devices and other computing devices with limited capabilities.

This investigation is intended to examine the major principles of how Behavioral Fingerprinting works, including how this method provides a basis for identifying and tracking the distinct behaviors of ransomware in resource-limited systems. In regards to the Passban IDS, Eskandari et al. [12] have done extensive work on how the Passban IDS was built, including a review of its conceptual framework and the methodologies used to create it, including the methods by which the system applies intelligent anomaly detection in IoT devices, which may be highlighted by the use of modern technologies, such as machine learning or artificial intelligence, which assist the system in establishing the difference between normal and anomalous behavior. Zhu et al. [13] focus their work on the conceptual framework and design of the GV-FL methodology in APT detection for IoT devices, and their work will address the theoretical basis for the Federated Learning concepts and what adaptations will be necessary to adapt this to the APT detection area. With particular modifications made to the field of APT detection, the study is anticipated to concentrate on the theoretical foundations of federated learning. Crucially, a global viewpoint can be taken into account, elucidating how an integrated and federated approach enhances the ability to learn and detect among a group of devices with limited capacity.

Liaqat et al. [14] provide contextual information in the IoMT domain by highlighting the growing integration of medical technologies and devices into networked systems to improve healthcare services. The talk describes the particular security challenges that IoMT faces, highlighting how vulnerable medical devices are to cyberattacks and promoting resilient and adaptable security measures.

In the IoMT domain, Liaqat et al. [14] offer contextual information by emphasizing the increasing incorporation of medical devices and technologies into interconnected systems to enhance healthcare provisions. The discourse outlines the unique security dilemmas encountered by IoMT, emphasizing the susceptibility of medical devices to cyber threats and advocating for security mechanisms that are both adaptive and resilient.

The analysis of low-rate DDoS attacks attacks using the MQTT protocol in Software-Defined IoT is addressed in Al-Fayoumi et al. [15]. Al-Fayoumi et al.'s work provides insights into the challenges of low-rate DDoS attacks and proposes a potential solution by using Software-Defined Network (SDN) for Internet of Things (IoT) [15]. The authors develop their

methodology by integrating SDN with a deep learning algorithm to detect intrusions into the IoT network. Doriguzzi-Corin et al. [16] detail in their work an SDN and deep learning-based Intrusion Detection System for IoT (IDSIoT-SDL). They highlight the complexity of IoT security and provide extensive analysis of the complexities of IoT security.

Doriguzzi-Corin et al.'s [16] IDSIoT-SDL methodology integrates deep learning algorithms with SDN to provide an intrusion detection system for IoT. Lauf et al. [17] describe a distributed intrusion detection system and hint that understanding of the system's architecture may be warranted to assess how the system distributes detection of intrusions over the network. From Lauf et al.'s analysis, it is evident that distributing the detection process will reduce the workload on each IoT device and allow the architecture to use the advantages of the collaborative approach to support the security of the entire network. In their analysis of the state of deep learning-based DDoS attack detection, Doriguzzi-Corin et al. [18] highlight the LUCID system as a novel and useful method. An overview of the growing threat environment posed by Distributed Denial of Service (DDoS) attacks is anticipated to open the discussion, highlighting the vital significance of putting in place efficient detection systems.

In an examination of an alternative aspect of cybersecurity, Khan et al. [19] investigate the distinctive obstacles and susceptibilities linked to IoMT devices. The severity of the potential repercussions of security breaches in medical environments is duly recognized. The discourse may encompass prevalent challenges and avenues of entry that specifically target healthcare networks and medical devices, with an emphasis on the criticality of implementing resilient and intelligent malware detection systems. In their comprehensive analysis, Aliabadi et al. [20] thoroughly investigate the unique characteristics of CPS constrained by resources, particularly focusing on limitations imposed by computing capacity, memory, and energy. The authors also direct their attention towards the consequences of these limitations on traditional intrusion detection approaches. They underscore the critical need for inventive and effective methods specifically designed to overcome the obstacles presented by environments with limited resources. Concerning the mitigation of DDoS attacks, Adat et al. [21] may provide further details regarding the operational principles and architectural design of a framework. Their discourse might emphasize how the suggested framework tackles the unique obstacles when attempting to alleviate DDoS attacks in Internet of Things environments. It is possible to highlight the significance of device heterogeneity, scalability, and real-time responsiveness in the framework's design.

Ayyat et al. [22] investigate the ramifications of implementing class-aware neural networks for peripheral device intrusion detection in a related context. The authors highlight the capacity of these networks to address the distinct obstacles arising in environments with limited resources. Nguyen et al. [23] provide an exhaustive examination of the present state of network intrusion detection systems (NIDS) concerning IoT gateways, adopting a broader viewpoint. Their investigation illuminates the shortcomings of conventional NIDS approaches and methodologies concerning IoT gateways. The analysis likely highlights the unique attributes of IoT networks, such as heterogeneity, limited resources, and the ever-changing nature of IoT traffic. These distinctive characteristics present obstacles for traditional intrusion detection systems.

From the literature, it is noted that in the realm of cybersecurity, several studies highlight distinct challenges and vulnerabilities associated with emerging technologies. One examination focuses on the security implications of IoT devices in medical contexts, recognizing the potential gravity of breaches in healthcare environments. A lot of study explores the limitations of CPS, particularly those constrained by resources like computing capacity, memory, and energy, emphasizing the necessity for innovative intrusion detection methods in such environments. Addressing the mitigation of Distributed Denial of Service (DDoS) attacks in IoT settings, a different set of frameworks are discussed, underlining considerations of device heterogeneity, scalability, and real-time responsiveness. In a broader context, the exploration of class-aware neural networks for peripheral device intrusion detection highlights their adaptability to challenges in resource-limited environments. Additionally, an extensive examination of network intrusion detection systems (NIDS) for IoT gateways sheds light on the inadequacies of conventional approaches in addressing the unique attributes of IoT networks, including heterogeneity, limited resources, and dynamic traffic patterns. Collectively, these studies underscore the diverse cybersecurity challenges associated with emerging technologies, emphasizing the imperative for specialized and adaptive security measures. Hence this research proposes a novel OCIF for automated deployment and advanced CTI.

III. Adoptive Deployment and Continuous Threat Intelligence Integration

In the proposed approach to make cybersecurity work well for devices with limited resources, we focus on two key parts: Adaptive Deployment and Continuous Threat Intelligence Integration. Adaptive Deployment deals with understanding these devices, making their communication efficient, and adjusting resources dynamically. On the other hand, Continuous Threat Intelligence Integration is about keeping an eye on the latest threats, adapting to the device's situation in real-time, and always learning from what's happening. These two methods, combined within the Open Cyber Intelligence Framework (OCIF), create a smart and effective cybersecurity plan. The goal is to make security fit the unique features of devices with fewer resources, making it adaptable and responsive to the ever-changing world of threats. Fig. 1 shows the architecture of the proposed OCIF.

A. Adaptive Deployment Strategies

The Adaptive Deployment Strategies component of the OCIF methodology focuses on tailoring the deployment process to the unique operational constraints and characteristics of resource-constrained devices. This involves a meticulous understanding of the diverse ecosystem encompassing Internet of Things (IoT) sensors, embedded systems, and other constrained devices. The adaptive nature of the OCIF ensures that the deployment process is optimized, minimizing the impact on device resources.

B. Device Profiling

In the context of OCIF's Adaptive Deployment Strategies, the process of device profiling involves more than a surface-level examination. It necessitates a comprehensive understanding of the hardware specifications, operating systems, and communication protocols that define the target device ecosystem. This depth of analysis is pivotal in forming robust device profiles, which subsequently inform tailored deployment strategies. The steps involved in real-time device profiling include:

- Conduct an in-depth analysis of the target device ecosystem to create comprehensive device profiles.
- Identify specific constraints such as limited processing power, memory, and bandwidth to inform adaptive deployment strategies.
- Categorize devices based on their functionalities and criticality to prioritize deployment efforts.

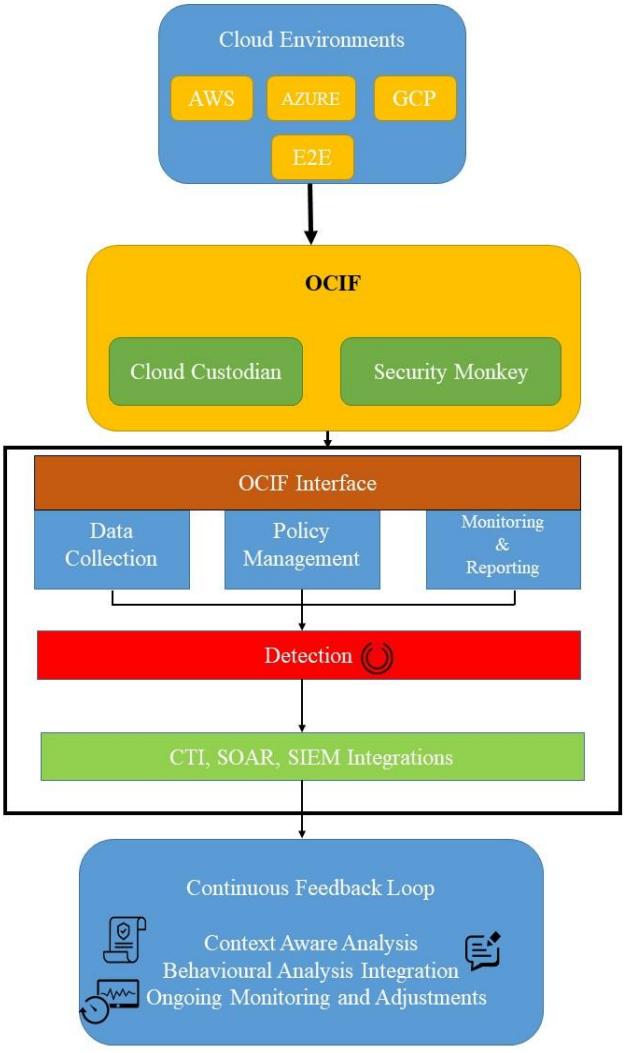


Fig. 1. Architecture of the proposed OCIF.

C. Lightweight Protocols

The design and implementation of lightweight communication protocols are central to the success of OCIF's Adaptive Deployment Strategies. As a researcher, the focus here lies in striking a delicate balance between efficiency and minimal overhead. Leveraging industry standards while customizing protocols ensures that the communication mechanisms are not only standardized but also adapted to the unique demands of resource-constrained environments.

D. Modular Deployment Architecture

The concept of a modular deployment architecture speaks to the flexibility required in adapting the OCIF to diverse devices incrementally. In this context, as a researcher, one must delve into the intricacies of modular design – ensuring that each module is not only adaptable but also able to seamlessly integrate with various devices. The goal is to create an architecture that is both scalable and responsive to the evolving demands of the device ecosystem. The design and deployment architecture includes:

- Design the OCIF with a modular architecture to allow for flexible and incremental deployment.
- Modules should be adaptable to different device types and functionalities, enabling a phased deployment approach.
- Ensure that each module aligns with the specific constraints of the targeted devices, enhancing scalability and ease of integration.

E. Threat Intelligence Integration

The Threat Intelligence Integration component of the OCIF methodology revolves around seamlessly incorporating threat intelligence feeds into the framework. This integration is designed to be agile, ensuring that devices can efficiently ingest and process threat intelligence data without compromising their limited computational resources.

F. Real-time Threat Data Ingestion

The process of real-time threat data ingestion is pivotal for OCIF's efficacy in responding promptly to emerging threats. In a research context, this involves exploring mechanisms that enable devices to receive threat intelligence updates with minimal latency. Investigating incremental updates and delta mechanisms becomes crucial to reduce the data transfer volume while ensuring the timely availability of the latest threat information. The steps involved in real-time threat data ingestion include:

- Develop mechanisms for real-time ingestion of threat intelligence data by resource-constrained devices.
- Implement protocols that enable devices to receive updates without significant latency, ensuring the timely availability of the latest threat information.
- Consider the use of incremental updates and delta mechanisms to minimize the data transfer volume.

G. Context-Aware Integration

The concept of context-aware integration speaks to the need for aligning threat intelligence feeds with the operational characteristics of each device. For a researcher, this necessitates an exploration of adaptive integration mechanisms that can dynamically adjust to device-specific threat indicators and indicators of compromise. The integration should not only consider the technical attributes but also incorporate the environmental context, refining threat detection algorithms for a more nuanced approach. The steps involved in real-time integration include:

- Tailor the integration process to be context-aware, aligning threat intelligence feeds with the operational characteristics of each device.
- Consider device-specific threat indicators and indicators of compromise to enhance the relevance and accuracy of threat intelligence data.
- Integrate contextual information about the device's environment to refine threat detection algorithms.

H. Scalable Data Processing

Scalable data processing within the OCIF framework is a research frontier that involves addressing the challenge of efficiently handling large volumes of threat intelligence data. This requires investigating parallel processing and distributed computing principles to design mechanisms that can accommodate the diverse scale of resource-constrained devices. Integrating machine learning algorithms into the processing pipeline becomes imperative to prioritize and categorize threat intelligence data based on severity and relevance. The steps involved in real-time data processing include:

- Implement scalable data processing mechanisms within the OCIF to handle large volumes of threat intelligence data efficiently.
- Utilize parallel processing and distributed computing principles to ensure that the framework can accommodate the diverse scale of resource-constrained devices.
- Integrate machine learning algorithms to prioritize and categorize threat intelligence data based on the severity and relevance to each device.

I. Continuous Feedback Loop

Establishing a continuous feedback loop is a research area critical for refining the Threat Intelligence Integration process within OCIF. This involves mechanisms where devices provide insights into the effectiveness of received threat intelligence data. As a researcher, exploring feedback mechanisms and algorithms that dynamically adjust and adapt threat intelligence feeds based on real-world observations is essential for the continuous optimization of the integration process. The steps involved in the feedback loop include:

- Establish a continuous feedback loop that enables devices to provide insights on the effectiveness of the threat intelligence data received.
- Implement mechanisms to adjust and adapt threat intelligence feeds based on the actual threat landscape observed by the devices.
- Leverage machine learning algorithms to dynamically refine the integration process, ensuring ongoing optimization based on real-world data.

By combining Adaptive Deployment Strategies with context-aware Threat Intelligence Integration, the OCIF ensures that the deployment process is finely tuned to the specific needs of resource-constrained devices. This comprehensive approach enhances the framework's effectiveness in safeguarding devices while minimizing the impact on their limited resources.

J. Experimental Setup

For a comprehensive assessment of our Adaptive Deployment and Continuous Threat Intelligence Integration methodologies within the Open Cyber Intelligence Framework (OCIF), to life, a carefully designed experimental setup becomes crucial. Here's a concise breakdown of our experimental environment.

1) Dataset curation in the in-house wazuh platform: For the comprehensive evaluation of our proposed Adaptive Deployment and Continuous Threat Intelligence Integration methodologies within the Open Cyber Intelligence Framework (OCIF), we have designed an experimental setup incorporating a specially curated dataset named CyberResilienceSim. This dataset encompasses diverse elements essential for simulating real-world scenarios and assessing the efficacy of the proposed methodologies. The CyberResilienceSim dataset comprises various categories to emulate the intricacies of cybersecurity challenges faced by resource-constrained devices. Firstly, we simulate data representative of such devices, capturing attributes like device types, communication protocols, and historical performance metrics. This foundational data establishes a virtual environment mirroring the limitations and characteristics of devices operating with constrained resources.

Next, the dataset includes a Threat Scenarios category, featuring a spectrum of cyber threats that resource-constrained devices might encounter. This dataset covers different types of threats, including malware attacks, Intrusion attempts, and data exfiltration incidents. Each threat scenario is enriched with details such as attack vectors, payloads, and timestamps, providing a comprehensive set of challenges for the methodologies. To enhance realism, we integrate Historical Threat Intelligence Feeds into the dataset, comprising indicators of compromise (IoCs), information about threat actors, and patterns associated with past cyber threats. This historical data injects a dynamic and evolving threat landscape into the dataset, reflecting the complexities of the real-world cybersecurity environment.

Contextual Device Information is another crucial aspect, providing details about the simulated devices. This includes device profiles, network configurations, and environmental factors. The Adaptive Deployment Strategies leverage this

contextual information to adapt and optimize cybersecurity measures based on the unique characteristics of each device. The dataset also incorporates Anomaly Indicators to evaluate the effectiveness of Continuous Threat Intelligence Integration. These indicators highlight deviations from baseline behavior, unexpected data flows, or unusual access patterns, allowing us to assess the system's capability to identify and respond to anomalous activities.

For practical application, a Real-world Scenarios Snapshot is included in the dataset, featuring recent cybersecurity incidents, threat intelligence reports, and data breaches. This provides a comparative analysis of our methodologies against real-world conditions. Finally, the dataset is structured to capture Performance Metrics Data Points, including false positive rates, response times, and adaptive adjustments made by the OCIF. These metrics are instrumental in quantifying the impact of our methodologies on cybersecurity effectiveness and the reduction of false positives.

2) Sample attack simulations and detection: In a simulated real-world scenario, we replicate an Advanced Persistent Threat (APT) intrusion targeting a network of resource-constrained devices within an industrial Internet of Things (IoT) environment. The APT actor conducts initial reconnaissance to gather information about the devices, followed by a phishing campaign aimed at compromising user credentials. Exploiting vulnerabilities within the devices, the attacker engages in lateral movement to escalate privileges and navigate through the ecosystem, ultimately seeking to exfiltrate sensitive operational data. Meanwhile, the proposed Continuous Threat Intelligence Integration methodology actively monitors real-time threat intelligence feeds, cross-referencing indicators of compromise (IoCs) to identify patterns associated with known APT campaigns. Simultaneously, Adaptive Deployment Strategies dynamically adjust security measures based on identified threat vectors and contextual information about compromised devices. For instance, if a device shows signs of compromise, the Open Cyber Intelligence Framework (OCIF) may temporarily restrict its network access or deploy additional security measures to contain the threat. This attack simulation, coupled with real-world use cases, serves to assess the adaptability and efficacy of the proposed methodologies in safeguarding resource-constrained devices against sophisticated cyber threats.

IV. Results and Discussion

Reducing false positives in Cyber Threat Intelligence (CTI) and Security Information and Event Management (SIEM) platforms is essential to enhance the efficiency and effectiveness of cybersecurity operations. A strategic approach involves a combination of fine-tuning existing processes, leveraging advanced technologies, and fostering a proactive organizational culture. Here's a comprehensive strategy that we followed:

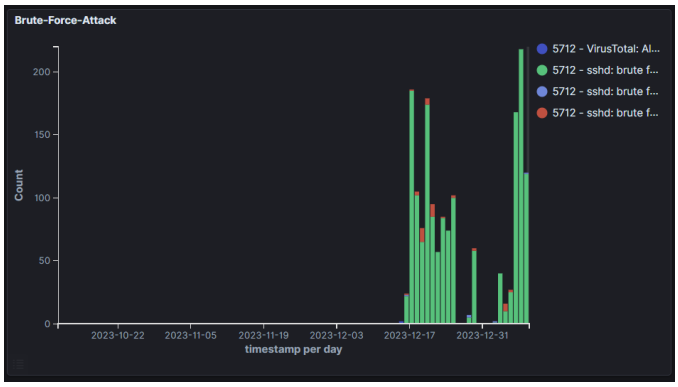
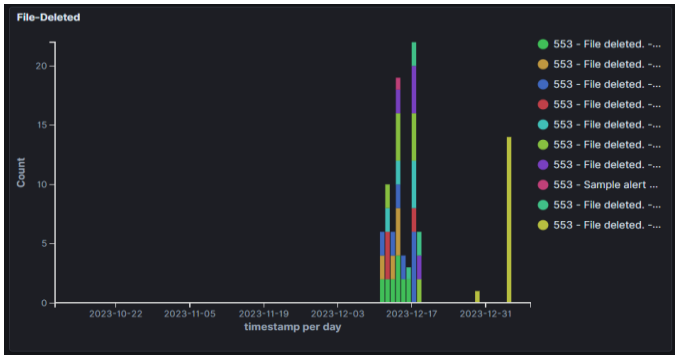


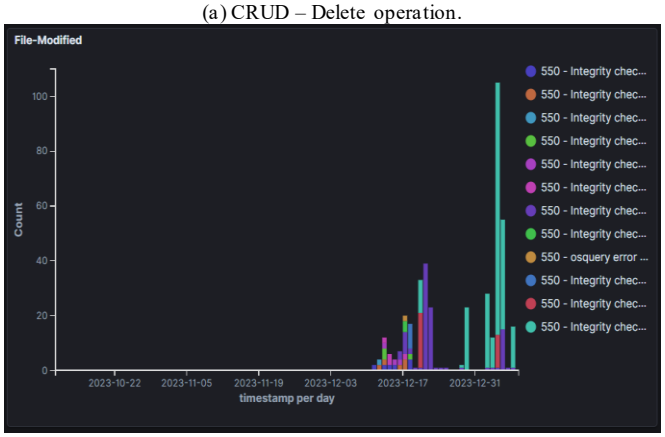
Fig. 2. Screenshot of brute force attack.

Precision in Alert Generation:

- Fig. 2 to Fig. 6 show the alerts of various events and use cases.
- Refinement of Detection Rules: Regularly review and refine detection rules in CTI and SIEM platforms to ensure they align with the organization's specific threat landscape. Incorporate threat intelligence feeds and customize rules based on the organization's context.
- Threshold Adjustments: Adjust threshold values for alerts, considering the organization's normal network behavior. Fine-tune thresholds to minimize false positives while maintaining sensitivity to potential threats. Fig. 2 shows the results of a brute force attack.



(a) CRUD – Delete operation.



(b) CRUD – Modification operation.

Fig. 3. Results of file auditing.

In Fig. 4, the plot likely represents a timeline with date stamps on the x-axis and associated alerts on the y-axis. Each point or bar on the plot corresponds to a specific alert triggered by an event related to the Mitre Attack Framework. The purpose of this visualization is to provide a chronological overview of detected events, allowing analysts to identify patterns, spikes, or clusters of alerts over time. This can be crucial for understanding the temporal aspects of the attack landscape and pinpointing periods of heightened threat activity.

Fig. 5 appears to illustrate the rule-level analysis categorized by tactics within the Mitre Attack Framework. The x-axis may represent different tactics employed by attackers based on the time stamps (e.g., Initial Access, Execution, Persistence), while the y-axis shows the rule levels associated with each tactic (Count). Each bar or data point on the plot likely corresponds to the number or severity of rules within a specific tactic. This visual representation aids in identifying which tactics have a higher concentration of rules, providing insights into the focus areas of the detection system and potential areas of vulnerability.

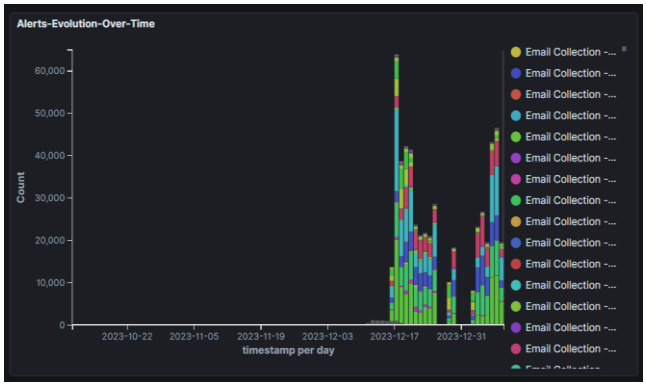


Fig. 4. Date stamps and their associated alerts.

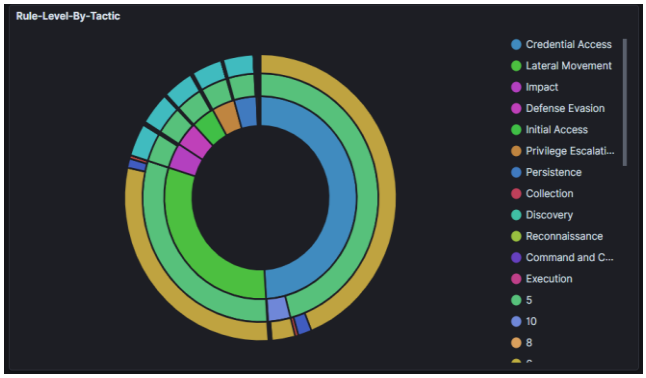


Fig. 5. Rule level by tactics.

Fig. 6 presents the detection results of the top tactics that were both simulated and recorded by the attacker. This plot likely showcases the effectiveness of the detection system in identifying and responding to specific attack tactics. Each bar or data point may represent the number of successfully detected tactics, providing an overview of the system's performance in mitigating simulated attacks. This information is valuable for assessing the detection capabilities and strengths of the implemented Mitre Attack Framework, offering insights into areas of improvement or optimization for better threat response.

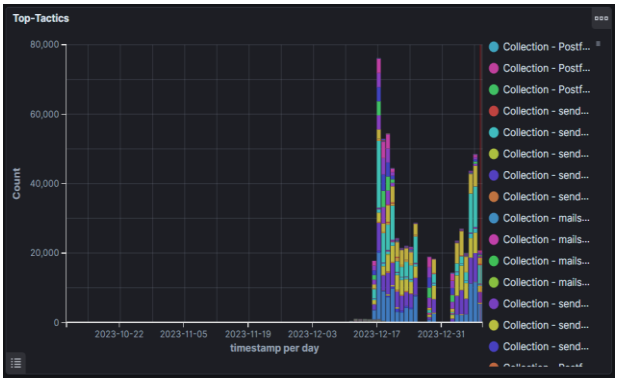


Fig. 6. Top tactics simulated and recorded.

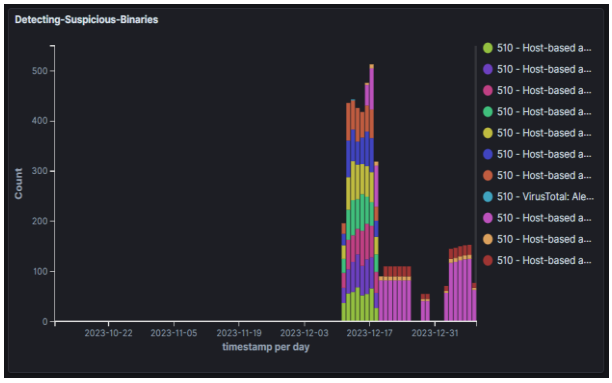


Fig. 7. Malicious file detection.

TABLE I. COMPARISON OF CYBERSECURITY DATASETS FOR RESOURCE-CONSTRAINED ENVIRONMENTS AND OCIF SUITABILITY

Dataset	Resource-Constrained Device Coverage	CTI/Attack Mapping (MITRE ATT&CK)	Suitability for Lightweight ML Models
NSL-KDD	Low	Basic mapping possible	High (small, clean dataset)
UNSW-NB15	Moderate	Good mapping to attack categories	Moderate
CICIDS2017	Low–Moderate	Strong mapping to MITRE techniques	Moderate
TON_IoT	High	Direct mapping available	High (sensor-level + network data)
Edge-IIoTset	High	Good mapping for APTs & DDoS	High
Wazuh + OpenSearch Logs (Used in Your Study)	Very High	Fully integrated (real-world MITRE ATT&CK mapping)	Very High (suitable for adaptive/lightweight models)

Among the existing datasets, TON_IoT and Edge-IIoTset provide the closest alignment to resource-constrained environments; however, neither of them comes with integrated SOAR/SIEM behavior is shown in Table I. The Wazuh + OpenSearch dataset developed in this work is uniquely positioned, with host-level telemetry, real-time CTI mapping, and compatibility for light-weight ML, thereby making it the ideal choice for testing OCIF's capabilities of Adaptive Deployment and False Positive Reduction.

A. Context-Aware Analysis

Enrichment with Threat Intelligence: Enhance alerts with contextual information from threat intelligence feeds. Enriching alerts with indicators of compromise (IoCs) and relevant threat context enables analysts to make more informed decisions. User and Entity Behavior Analytics (UEBA): Incorporate UEBA solutions to analyze user and entity behavior, allowing the detection of anomalies that might go unnoticed with rule-based approaches. This context-aware analysis contributes to reducing false positives. Fig. 3 shows the file auditing results.

B. Machine Learning and AI Integration in Malicious Operation Detection

Anomaly Detection: Implement machine learning algorithms to identify anomalous patterns in data. Train models with historical data to recognize normal behavior and flag deviations, contributing to more accurate threat detection and fewer false positives. Behavioral Analysis: Leverage AI-driven behavioral analysis to understand the typical behavior of users, devices, and applications. Identify deviations from established baselines to detect potential threats with greater accuracy. In Fig. 7, the plot visually captures the outcomes of malicious file detection, specifically focusing on the identification of suspicious binaries.

C. Continuous Monitoring and Feedback Loop

Continuous Evaluation: Establish a continuous monitoring process that includes regular evaluations of alerts and incident reports. This ongoing scrutiny ensures that the detection rules remain relevant and effective over time. Feedback Mechanism: Encourage security analysts to provide feedback on false positives. Establish a feedback loop between analysts and the security system to iteratively improve rules and reduce false positives.

D. Discussion

Through experimentation, promising results were achieved, demonstrating a notable reduction of up to 6% in false positive rates. The Adaptive Deployment and Continuous Threat Intelligence Integration methodologies proved their worth in real-world scenarios, contributing to a more adaptive and efficient cybersecurity defense. Fig. 4, Fig. 5, and Fig. 6 served as critical visual aids in the analysis of Mitre Attack Framework implementation. The chronological overview in Fig. 4 showcased date stamps associated with Mitre attacks, aiding in the identification of temporal attack patterns. Fig. 5 provided a rule-level breakdown by tactics, offering insights into the distribution and severity of rules within different attack categories. Meanwhile, Fig. 6 illustrated the detection results of top tactics, underlining the system's proficiency in responding to both simulated and recorded attacker tactics. The richness of these visualizations, coupled with the experimentation results, contributes to the overarching success of the proposed method. The OCIF, equipped with Adaptive Deployment, Continuous Threat Intelligence Integration, and Mitre Attack Framework analysis, emerges as a robust and adaptive solution for securing resource-constrained devices.

V. Conclusion

In conclusion, this research focused on the development and assessment of an innovative Open Cyber Intelligence Framework (OCIF) for safeguarding resource-constrained devices. The foundation of the investigation lay in proposing an Automated Security Operations and Analytics Response (SOAR) architecture, integrating multiple security tools and leveraging threat intelligence data. As the research unfolded, the attention shifted towards refining the architecture to address the specific challenges faced by devices with limited resources. The OCIF introduced novel strategies, such as Adaptive Deployment and Continuous Threat Intelligence Integration, tailored to resource-constrained environments. The first work showcased the potential of this framework in automating threat detection, response, and mitigation, emphasizing its capability to enhance an organization's cybersecurity posture and reduce the risk of successful attacks. The proposed framework was tested on a limited set of resource-constrained devices and predefined threat scenarios, which may not fully represent real-world environments. This therefore places future research on expanding OCIF into wider device ecosystems, advanced ML models that can dynamically adapt to evolving threats, and real-time performance validation at large-scale deployments. This research not only advances the theoretical understanding of cybersecurity in constrained environments but also provides tangible contributions to practical implementations.

References

[1] AlWaisi, Z. A. (2023). Optimized Monitoring and Detection of Internet of Things resources-constraints Cyber Attacks.

[2] Kornaros, G. (2022). Hardware-assisted machine learning in resource-constrained IoT environments for security: review and future prospective. IEEE Access, 10, 58603-58622.

[3] Arshad, J., Azad, M. A., Abdeltaif, M. M., & Salah, K. (2020). An intrusion detection framework for energy constrained IoT devices. Mechanical Systems and Signal Processing, 136, 106436.

[4] Shalaginov, A., & Azad, M. A. (2021). Securing resource-constrained iot nodes: Towards intelligent microcontroller-based attack detection in distributed smart applications. Future Internet, 13(11), 272.

[5] Khan, M. T., Akhunzada, A., & Zeadally, S. (2022). Proactive defense for fog-to-things critical infrastructure. IEEE Communications Magazine, 60(12), 44-49.

[6] Javeed, D., Gao, T., & Khan, M. T. (2021). SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT. Electronics, 10(8), 918.

[7] Khan, A. Y., Latif, R., Latif, S., Tahir, S., Batool, G., & Saba, T. (2019). Malicious insider attack detection in IoTs using data analytics. IEEE Access, 8, 11743-11753.

[8] Jeffrey, N., Tan, Q., & Villar, J. R. (2023). A review of anomaly detection strategies to detect threats to cyber-physical systems. Electronics, 12(15), 3283.

[9] Bradbury, M., Jhumka, A., Watson, T., Flores, D., Burton, J., & Butler, M. (2022). Threat-modeling-guided Trust-based Task Offloading for Resource-constrained internet of Things. ACM Transactions on Sensor Networks (TOSN), 18(2), 1-41.

[10] Aljuhani, A., Alamri, A., Kumar, P., & Jolfaei, A. (2023). An Intelligent and Explainable SaaS-Based Intrusion Detection System for Resource-Constrained IoMT. IEEE Internet of Things Journal.

[11] Celdrán, A. H., Sánchez, P. M. S., von der Assen, J., Shushack, D., Gómez, Á. L. P., Bovet, G., ... & Stiller, B. (2023). Behavioral fingerprinting to detect ransomware in resource-constrained devices. Computers & Security, 135, 103510.

[12] Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet of Things Journal, 7(8), 6882-6897.

[13] Zhu, H., Wang, H., Lam, C. T., Hu, L., Ng, B. K., & Fang, K. (2023, November). Rapid APT Detection in Resource-Constrained IoT Devices Using Global Vision Federated Learning (GV-FL). In International Conference on Neural Information Processing (pp. 568-581). Singapore: Springer Nature Singapore.

[14] Liaqat, S., Akhunzada, A., Shaikh, F. S., Giannetsos, A., & Jan, M. A. (2020). SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT). Computer Communications, 160, 697-705.

[15] Al-Fayoumi, M., & Al-Haija, Q. A. (2023). Capturing low-rate Ddos attack based on Mqtt protocol in software defined-Iot environment. Array, 19, 100316, Article (CrossRef Link).

[16] Wani, A., & Khaliq, R. (2021). SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL). CAAI Transactions on Intelligence Technology, 6(3), 281-290.

[17] Lauf, A. P., Peters, R. A., & Robinson, W. H. (2010). A distributed intrusion detection system for resource-constrained devices in ad-hoc networks. Ad Hoc Networks, 8(3), 253-266.

[18] Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martinez-del-Rincon, J., & Siracusa, D. (2020). LUCID: A practical, lightweight deep learning solution for DDoS attack detection. IEEE Transactions on Network and Service Management, 17(2), 876-889.

[19] Khan, S., & Akhunzada, A. (2021). A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT). Computer Communications, 170, 209-216.

[20] Aliabadi, M. R., Seltzer, M., Asl, M. V., & Ghavamizadeh, R. (2021). Artinali#: An efficient intrusion detection technique for resource-constrained cyber-physical systems. International Journal of Critical Infrastructure Protection, 33, 100430.

[21] Adat, V., & Gupta, B. B. (2017, April). A DDoS attack mitigation framework for internet of things. In 2017 international conference on communication and signal processing (ICCSP) (pp. 2036-2041). IEEE.

[22] Ayyat, M., Nadeem, T., & Krawczyk, B. (2023, September). Class-Aware Neural Networks for Efficient Intrusion Detection on Edge Devices. In 2023 20th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON) (pp. 204-212). IEEE.

[23] Nguyen, X. H., Nguyen, X. D., Huynh, H. H., & Le, K. H. (2022). Realguard: A lightweight network intrusion detection system for IoT gateways. Sensors, 22(2), 432.