Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 257 (2025) 575–582

Procedia Computer Science

www.elsevier.com/locate/procedia

The 16th International Conference on Ambient Systems, Networks and Technologies (ANT)
April 22-24, 2025, Patras, Greece

Experimental Implementation of a Low Cost Real-Time Threat Intelligence Solution for Smart Home Security

Samuel Kwaku Addison[a], Mohammad Tahir[a,*], Jouni Isoaho[a]

[a]*Department of Computing, University of Turku, Vesilinnantie 5, Turku 20014, Finland*

Abstract

The growing adoption of the Internet of Things (IoT) in smart home technology has revolutionized modern living, offering convenience and enhancing quality of life. However, integrating IoT devices into daily life has also introduced complex cybersecurity challenges. Existing approaches to smart home security often rely on static measures that struggle to keep pace with evolving threats. Although threat intelligence has a wide range of applications in organizational cybersecurity, its use in smart home environments is mostly under-explored. This study uses a Raspberry Pi to explore a proactive solution by integrating low-cost real-time threat intelligence using the Malware Information Sharing Platform (MISP) with intrusion detection and prevention systems (IDS/IPS) powered by Suricata. Simulating diverse cyber threats, including brute-force, denial-of-service (DoS) attacks, and malware infection the research evaluates how real-time updates from threat intelligence platforms enhance detection and mitigation. The findings reveal that incorporating dynamic threat intelligence drastically improves response accuracy, achieving a 99.9% detection and prevention rate. This approach outperformed traditional methods by enabling rapid adaptation to new attack patterns. The study takes a practical, adaptive method in the protection of smart homes and takes the aspect of IoT security a step ahead with real-time use of threat intelligence.

© 2025 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer review under the responsibility of the scientific committee of the Program Chairs

Keywords: Smart Home Security; IDS/IPS; Indicator of Compromise (IoC); Threat Intelligence; Firewall; IoT; Raspberry Pi; Cyber Threat Detection; MISP (Malware Information Sharing Platform)

1. Introduction

Smart home technology has become a part of our everyday life, making homes more connected and efficient, thereby improving the quality of life. Devices like smart lights, security cameras, and voice assistants have brought convenience and automation to millions of households. However, this connectivity comes with significant risks. Every connected device can be a potential target for cybercriminals. Events like the Mirai botnet attack, which exploited unsecured devices to cause massive disruptions, show how vulnerable smart homes can be [1].

* Corresponding author.
E-mail address: tahir.mohammad@utu.fi

1877-0509 © 2025 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer review under the responsibility of the scientific committee of the Program Chairs
10.1016/j.procs.2025.03.074

Many IoT security tools rely on outdated methods that were not designed to fend off the new types of cyber threats we face. Moreover, without real-time information on threats, it would even be more difficult to try to be proactive in mitigating risks. Traditional methods, like basic firewalls, are often not enough to deal with the complexity of modern cyber threats in the smart home environment. As a result, the need to secure these environments has never been greater.

This research, therefore, addresses these challenges by proposing an integration of real-time threat intelligence into smart home security systems. Threat intelligence uses real-time data about known and emerging threats to detect and prevent attacks. The proposed solution uses low-cost devices, such as a Raspberry Pi, to host tools like Suricata IDS/IPS, while integrating with platforms such as the Malware Information Sharing Platform (MISP) to enhance threat detection and response. These tools continuously monitor network traffic, detect new threats, stop malicious actions, and immediately alert the users. In this way, the solution reinforces smart home security without sacrificing the accessibility and affordability that ordinary users need from the solution.

Therefore, in order to address the growing threat of cyber attacks targeting smart homes, this research article aims to answer the following research questions:

- ***Research Question (RQ1)***: How to design and implement a low-cost threat intelligence solution for smart home security?
- ***Research Question (RQ2)***: How effective is the low-cost threat intelligence solution for smart home security?

The main research contributions of the article are as follows:

- A low-cost real-time threat intelligence solution for smart home systems using a Raspberry Pi.
- Test the effectiveness of the proposed threat intelligence solutions against common attacks on smart homes, such as brute force, denial-of-service, and malware infection.

The rest of the research article is organized as follows, Section 2 reviews existing research on smart home cybersecurity, exploring the gaps in traditional methods. Section 3 takes a look at threat intelligence and its application. Section 4 explains the experimental setup, focusing on integrating threat intelligence tools and simulated attack scenarios. Section 5 shares the results and its evaluation. Finally, Section 6 concludes the paper and suggests areas for future research.

2. Security Architecture for Smart Homes

Smart homes are becoming more complex, with each new device increasing the potential security risks. As more gadgets are added to the network, the challenge of keeping everything secure becomes even greater. Common threats like unauthorized access, data breaches, and denial-of-service (DoS) attacks highlight the urgent need for more robust security measures [2].

To secure IoT-based smart homes, various advanced security frameworks have been proposed to tackle emerging threats. One such framework, the loT-A ARM framework, emphasizes key components like context management, vulnerability and threat management, and a decentralized authorization system. Security is enhanced through mechanisms like Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs) that manage and regulate access control. In addition, a centralized vulnerability management system continuously monitors and addresses potential risks [3].

The proposed smart home security architecture by Mascarenhas et al.[4], based on a Central Hub, performs the monitoring of IoT devices using machine learning techniques such as XGBoost, detects anomalies, provides appropriate alerts, and isolates compromised devices to maintain the integrity of the network against intruders, who may acquire high-level credentials. This approach has highlighted the importance of proactive measures to oppose the continuous evolution of cyber threats and improve the resilience of smart homes. Rehman and Gruhn [5] propose a security architecture with a firewall between the central hub and the internet. This securely filters unauthorized traffic, blocks malicious access, and redirects all communications of smart homes securely, hence reducing the possibility of an attack to the minimum. In this structure, user data and privacy are closely protected, hence building more trust in smart home technology concerning the increasing demand for IoT-based security.

2.1. Security Landscape for Smart Homes

Many IoT devices are vulnerable due to weak passwords, poor encryption, and other security vulnerabilities. All of these make the lives of cyber criminals a lot easier when aiming at them. Furthermore, many smart devices lack the needed processing power to support traditional measures of security, hence leaving them exposed to evolving cyber threats [6]. More effective security solutions, hence, have to be implemented on an individual basis to protect these devices.

The STRIDE and OWASP IoT Top 10 frameworks have identified spoofing and tampering as some of the key vulnerabilities. Various studies indicate that better design practices, periodic updates, and enhanced encryption are required to secure IoT networks [7]. Real-world incidents, including breaches in Google Nest Hub and Amazon's video doorbells, emphasize the urgency for advanced measures. Techniques like "stochastic traffic padding" (STP), as proposed by Apthorpe et al. [8], provide innovative solutions by obfuscating traffic patterns to protect user privacy.

2.2. Smart Home Cybersecurity

IoT-based smart homes, provide convenience, but on the other hand, they have to deal with serious security challenges. The nature of such smart home deals with sensitive information and is in constant need of the internet, making it a hotbed for hackers. The use of regular security tools like firewalls and Intrusion Detection Systems can help maintain safety. However, evolving and complex threats, such as DDoS attacks, cannot be handled by these systems. This is mostly because they rely on fixed rules to find the threats. In dealing with such challenges, researchers are advising on incorporating threat intelligence into security frameworks. Such an approach could ensure the best reaction against newly arising threats. Researchers are working on new solutions that could help improve the security of smart homes. For example, [9] proposed the new Intrusion Prevention System, enhancing smart home security by merging robust encryption methods together with tools for unusual behaviour detection and detailed risk assessment. Preliminary results show that this system is effective in identifying various cyber threats.

Authors in [10] presented the HID-SMART hybrid IDS, which uses Random Forest and XGBoost machine learning techniques to detect abnormal network activities. This system reached a detection accuracy of over 90% when tested with the CSE-CIC-IDS2018 dataset [10]. The findings prove that machine learning plays an important role in significantly improving defences against cyber attacks. Researchers are now experimenting with deep learning models to detect various attack types. For instance, a ResNet-based system converts network traffic into images for pattern recognition. It achieved 99.99% accuracy in binary classifications [11]. Though effective, deep learning models have issues such as overfitting and require a high amount of quality-labeled data, limiting their adaptability to emerging threats.

3. Threat Intelligence

Threat intelligence (TI) refers to evidence-based knowledge about threats, providing actionable insights to mitigate risks. TI encompasses a comprehensive framework that includes context, mechanisms, indicators, implications, and actionable recommendations designed to address both existing and emerging threats. It involves gathering, analyzing, and sharing information about potential cyber threats from sources like security advisories, industry reports, and threat actor activities [12].

Incorporating TI enhances proactive cybersecurity measures for smart home environments. For instance, smart home users can utilize TI to detect and prevent malware, phishing, and unauthorized device access. Organizations such as MITRE classify threats using heuristics and signatures to provide actionable insights into adversary tactics and vulnerabilities [13]. Threat intelligence comes from various sources, including publicly available data (OSINT), curated threat feeds from commercial providers, and advisories from government agencies such as CISA and NIST [14]. Research communities and security vendors also publish reports and share actionable insights on emerging threats. Platforms like the Cyber Information Sharing and Collaboration Program and Multi-State Information Sharing and Analysis Center allow organizations, law enforcement, and researchers to collaborate in a manner that secures one entity, thus improving protection for all.

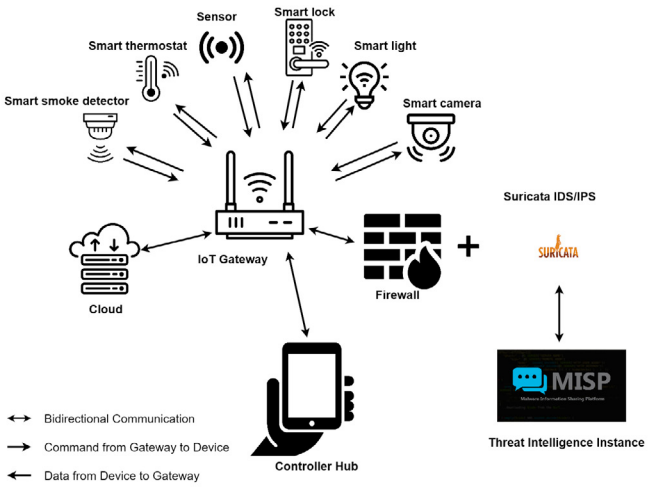

Fig. 1. Proposed security architecture for smart home;

Cyber Threat Intelligence (CTI) focuses on understanding the tactics, techniques, and procedures (TTPs) of cyber adversaries. It provides tactical, operational, and strategic insights, helping organizations concentrate their security efforts effectively [15]. CTI also informs risk management strategies, aiding in prioritizing defences and mitigating emerging threats. CTI enhances smart home security by enabling real-time detection of malicious activity. Platforms aggregate and analyze data from diverse sources, assigning threat scores to Indicators of Compromise (IoCs). Advanced platforms integrate machine learning to identify patterns in attack data, allowing for proactive measures [16]. The 2024 CrowdStrike Global Threat Report emphasizes the rising adoption of CTI, noting its role in incident response, threat hunting, and vulnerability management. Organizations increasingly leverage CTI to tailor their defences to adversarial tactics, enhancing overall resilience.

4. Implementation Framework and Methodology

The Raspberry Pi 4 Model B, equipped with 8GB memory was selected as the main device because of its cost-effectiveness, versatility, and processing capabilities. By emulating a Linux-based IoT device, it allowed for the development and testing of real-time cybersecurity solutions in a smart home setting. As shown in Fig. 1, the proposed architecture features various layers of security, including a firewall for traffic control, a Suricata IDS/IPS[1], and MISP[2] an open-source threat intelligence platform, for the real-time sharing of threat intelligence.

MISP serves as the core threat intelligence platform, which is integrated with the Raspberry Pi, collecting IoCs from various open-source feeds [17]. The workflow is orchestrated with the help of a custom Python script[3] that facilitates interaction between Suricata and MISP by retrieving IoCs periodically to update the Suricata ruleset dynamically for threat detection and prevention in real-time. Upon identifying a high-severity alert, Suricata forwards the alert to MISP for contribution to global threat intelligence sharing. In parallel, it sends the alert to Cohere's AI API for detailed information about the alert and potential mitigation steps. These details are then communicated to the user directly via email for quick awareness and actionable insight for response.

[1] https://suricata.io/
[2] https://www.misp-project.org/download/
[3] https://github.com/SamAddy/smart-home-cybersecurity/tree/main

In solving the resource issues of the Raspberry Pi, Suricata is installed on the Raspberry Pi, while MISP operates on a virtual machine connected to open-source threat feeds. This setup makes operations efficient even with hardware constraints. The Raspberry Pi acts as a representative IoT device in a smart home environment.

4.1. Simulated Attack Scenarios

To evaluate the system's performance, the following attack scenarios were simulated using a Kali Linux system configured as the attacker:

- Brute-Force Attacks: Automated password-guessing attempts targeting the Raspberry Pi's SSH login. This attack exploited weak credentials, assessing the system's ability to detect and block repeated unauthorized access attempts.
- Denial of Service (DoS) Attacks: Inundated the Raspberry Pi with an excessive number of requests, which overwhelmed its resources and made it unavailable for legitimate services. This scenario tested the framework's capability for detection and mitigation against high-volume attacks.
- Malware Infection: Introduces malicious software to compromise device integrity, mirroring techniques from Rodríguez et al. [18].

Each of these scenarios was crafted to mimic real-world threats that IoT devices face in smart homes. Suricata logs tracked network traffic, indicating allowed and blocked packets. Analysis of the logs will help determine how well the system was able to detect and respond to threats as they occurred. Key metrics include the accuracy of detection, time to response, and how effectively threats were mitigated to assess overall system performance.

5. Evaluation and Findings

In the experiments, various kinds of cyber attacks, such as brute-force attempts, DoS and malware infection, were simulated to understand how the integration of the MISP Threat Intelligence platform has enhanced the capabilities of IDS/IPS systems for detection and mitigation within a smart home environment.

5.0.1. Brute-Force Attack: Analysis and Outcomes

First, as demonstrated in Fig. 2 (a), the credentials of Raspberry Pi were successfully compromised through a simulated brute-force attack. However, the previous scenario has been counteracted using MISP threat intelligence data that updated IDS/IPS rules for the required IoCs. As depicted by Fig. 2 (b) and (c), all subsequent attempts have been blocked, thereby illustrating the criticality of real-time intelligence to inhibit unauthorized access and improve the security posture of systems.

5.0.2. DoS Attack: Impact and Mitigation

During the simulated DoS attack, the Raspberry Pi nginx server suffered from significant slowing down and eventually went offline as shown in Fig. 3 (a), until updating the IDS/IPS rules on IoCs from MISP made it block the attack and allowed the service to return to its normal state, as shown in Fig. 3 (b) and (c). Therefore, this shows how the system can adapt quickly to try to mitigate DoS attacks.

5.0.3. Malware Infection Detection and Mitigation

Real-time updates from MISP enabled the detection of malware activities by blocking communication attempts from known malicious IPs and command & control servers, as depicted by Fig. 4. This integration significantly improved the system's ability to block malware before it could spread across the network.

5.0.4. Performance and Efficiency

The system showed very good accuracy and speed, with a detection rate of 99.9% and a response time of only 2 milliseconds. The system updated its IoCs every 10 minutes to keep up with emerging threats. A detailed breakdown of the performance and efficiency of the system is provided in Table 1. Table 2 proves that the model proposed in

Fig. 2. (a) Brute-force attack on Raspberry Pi credentials; (b) Blocked brute-force attempt with IoC rules; (c) Suricata log of blocked brute-force attack.

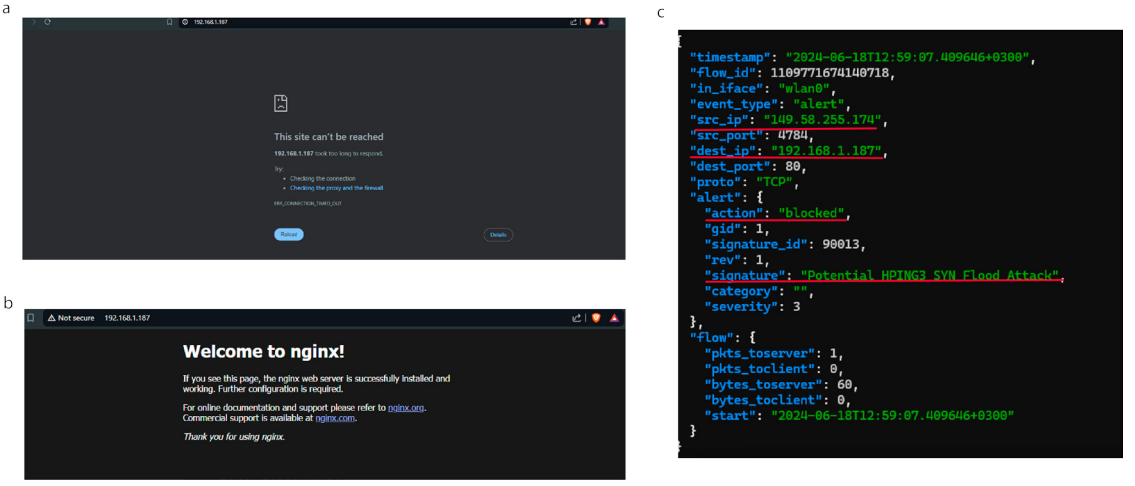

Fig. 3. (a) Nginx server under a DoS attack; (b) Blocked DoS attempt with IoC rules; (c) Suricata log of blocked DoS attack.

this work possesses beneficial traits when compared with current literature, particularly regarding cost-effectiveness and its real-time adaptability to new emerging threats. Cost criterion distinguishes between three categories: low, medium, and high, according to computational and financial capabilities for its use. Adaptability reflects a system's ability to respond effectively to new threats: low adaptability reflects a reliance on static models, moderate adaptability reflects infrequent retraining or predefined mechanisms, and high adaptability reflects real-time adaptations, such as integration with MISP in this work.

5.0.5. Limitations and Future Works

While the system showed efficiency in the detection and mitigation of cyber threats in controlled environments, a number of challenges arose during testing. For example, resource constraints of the Raspberry Pi are issues that severely limit scalability, especially in the case of high-volume DoS attacks. These reduce Suricata's logging and processing demands on CPU and memory. This can be further addressed in future work by using advanced hardware or

```
{
  "timestamp": "2024-09-11T21:59:12.573632+0300",
  "flow_id": 207462342857542 4,
  "in_iface": "wlan0",
  "event_type": "alert",
  "src_ip": "192.168.1.254",
  "src_port": 40114,
  "dest_ip": "192.168.1.187",
  "dest_port": 22,
  "proto": "TCP",
  "alert": {
    "action": "blocked",
    "gid": 1,
    "signature_id": 18971,
    "rev": 1,
    "signature": "IoC: Malicious IP Detected",
    "category": "",
    "severity": 3
  },
  "flow": {
    "pkts_toserver": 1,
    "pkts_toclient": 0,
    "bytes_toserver": 74,
    "bytes_toclient": 0,
    "start": "2024-09-11T21:59:12.573632+0300"
  }
}
```


Fig. 4. Suricata JSON log entry showing a blocked IP address associated with malware detection.

Table 1. Detection and Performance Metrics

Metric	Value	Description
Detection Rate	99.9%	Accuracy in identifying threats
False Positive Rate	0.1%	Incorrect threat identifications
Average Response Time	2 ms	Time to detect and mitigate threats
IoC Update Frequency	Every 10 minutes	Frequency of threat intelligence updates

Table 2. Comparison of Related Works and Proposed Solution

Work	Approach	Cost	Adaptability to New Threats	Detection Rate
[9]	IPS with encryption & behavior analysis	Medium	Moderate (fixed mechanisms)	Not reported
[10]	ML-based IDS (Random Forest, XGBoost)	High	Moderate (requires retraining)	90%
[11]	DL-based IDS (ResNet)	High	Low (overfitting risks)	99.99%
This Work	Real-time IoC with MISP and Suricata	Low	High (real-time IoC updates)	99.9%

cloud scaling for resource-intensive processes. Another limitation is that it is dependent on IoCs and hardly blocks any new threats in their absence. The system could be more resilient with the integration of machine learning techniques to detect anomalies and zero-day attacks independent of predefined IoCs. Also, without any mechanism for removing redundant IoCs from the ruleset, it caused unnecessary updates and resource usage. Developing an advanced filtering system to eliminate duplicates before updating rulesets would be much more efficient and reduce processing overhead.

6. Conclusion

This research has demonstrated how smart homes could be made safer with real-time threat intelligence. The proposed system, using a Raspberry Pi as a test device integrated with MISP, was able to detect and prevent 99.9% of the simulated attacks. It also proves that real-time updates of IoCs can significantly improve a system's detection and response against evolving threats, adding another layer of protection to existing security. The proposed approach is practical and economical to implement; hence, it would be easy to use in the usual smart home environments. It closes the gap from the available basic security tools to the current complex threat space by allowing the systems to act dynamically towards new attacks. This makes it valuable for smart homes where resource constraints and

more connected devices make security challenging. Despite its successes, the proposed solution also faced some limitations. The Raspberry Pi's hardware constraints affected scalability, suggesting that future implementations could benefit from cloud-based hosting or virtual machines. The network setup, while functional, highlighted areas for improvement, especially in routing efficiency. Adding machine learning techniques could further enhance the system's ability to detect new or previously unseen threats. The article, therefore, provides the basis on which further research will be built in smart home security.

References

[1] A. Husar. *IoT Security: 5 cyber-attacks caused by IoT security vulnerabilities*. Accessed: Jan. 17, 2024. Oct. 2022. URL: https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities.

[2] Iman Alhammadi et al. "Protecting Smart Home: Attack Scenarios, Risks & Threat Modeling". In: *2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. Yogyakarta, Indonesia, 2022, pp. 588–594.

[3] Shahrouz Sotoudeh, Sattar Hashemi, and Hossein Gharaee Garakani. "Security Framework of IoT-Based Smart Home". In: *2020 10th International Symposium onTelecommunications (IST)*. Tehran, Iran, 2020, pp. 251–256.

[4] Cynthia Mascarenhas et al. "Project Urban Patrol: Building an Attack Resilient Smart Home Architecture". In: *2021 4th Biennial International Conference on Nascent Technologies in Engineering (ICNTE)*. NaviMumbai, India, 2021, pp. 1–6.

[5] Shafiq ur Rehman and Volker Gruhn. "An approach to secure smart homes in cyber-physical systems/Internet-of-Things". In: *2018 Fifth International Conference on Software Defined Systems (SDS)*. Barcelona, Spain, 2018, pp. 126–129.

[6] *OWASP-IoT-Top-10-2018-final.pdf*. Accessed: Jun. 12, 2024. Feb. 2016. URL: https://wiki.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf.

[7] Sergei Sokolov et al. "IoT Security: Threats, Risks, Attacks". In: *Proceedings of the XIII International Scientific Conference on Architecture and Construction 2020*. Singapore: Springer Nature Singapore, 2021, pp. 47–56. ISBN: 978-981-33-6208-6.

[8] N. Apthorpe et al. "Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping Sleeping habits – Sense Sleep Monitor". In: *Proceedings on Privacy Enhancing Technologies* (2019).

[9] Fathima James. "IoT Cybersecurity based Smart Home Intrusion Prevention System". In: *2019 3rd Cyber Security in Networking Conference (CSNet)*. Quito, Ecuador, 2019, pp. 107–113.

[10] Faisal Alghayadh and Debatosh Debnath. "A Hybrid Intrusion Detection System for Smart Home Security". In: *2020 IEEE International Conference on Electro Information Technology (EIT)*. Chicago, IL, USA, 2020, pp. 319–323.

[11] Faisal Hussain et al. "IoT DoS and DDoS Attack Detection using ResNet". In: *2020 IEEE 23rd International Multitopic Conference (INMIC)*. Bahawalpur, Pakistan, 2020, pp. 1–6.

[12] W. Zhang, Y. Bai, and J. Feng. "TIIA: A blockchain-enabled Threat Intelligence Integrity Audit scheme for IIoT". In: *Future Generation Computer Systems* 132 (July 2022), pp. 254–265.

[13] Jon C. Haass. "Cyber Threat Intelligence and Machine Learning". In: *2022 Fourth International Conference on Transdisciplinary AI (TransAI)*. Laguna Hills, CA, USA, 2022, pp. 156–159.

[14] Rui Azevedo, Ibéria Medeiros, and Alysson Bessani. "PURE: Generating Quality Threat Intelligence by Clustering and Correlating OSINT". In: *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. Rotorua, New Zealand, 2019, pp. 483–490.

[15] Mohammed A Althamir, Jawhara Z Boodai, and M M Hafizur Rahman. "A Mini Literature Review on Challenges and Opportunity in Threat Intelligence". In: *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. Bali, Indonesia, 2023, pp. 558–563.

[16] Sagar Samtani et al. "Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective". In: *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Cham: Springer International Publishing, 2020, pp. 135–154. ISBN: 978-3-319-78440-3.

[17] Borce Stojkovski et al. "What's in a Cyber Threat Intelligence sharing platform? A mixed-methods user experience investigation of MISP". In: *Proceedings of the 37th Annual Computer Security Applications Conference*. ACSAC '21. Virtual Event, USA: Association for Computing Machinery, 2021, pp. 385–398. ISBN: 9781450385794.

[18] Elsa Rodríguez et al. "Difficult for Thee, But Not for Me: Measuring the Difficulty and User Experience of Remediating Persistent IoT Malware". In: *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*. Genoa, Italy, 2022, pp. 392–409.