Journal of Network and Computer Applications 248 (2026) 104438

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Research paper

Robust and energy-aware detection of Mirai botnet for future 6G-enabled IoT networks

Zainab Alwaisi [a,*], Tanesh Kumar [b], Simone Soderi [c]

[a] IIT-CNR, Italy
[b] School of Electrical Engineering, Aalto University, Finland
[c] Scuola IMT Alti Studi Lucca, Italy

ARTICLE INFO

Keywords:
6G security
Mirai
Energy efficiency
Smart devices
Internet of Things (ioT)
Security

ABSTRACT

Next-generation IoT wireless communication systems emphasise the importance and urgent need for energy-efficient security measures, thus requiring a balanced approach to address growing security vulnerabilities and fulfil energy demands in advanced wireless communication networks. However, the evolution of 6G networks and their integration with advanced technologies will revolutionise the IoT ecosystem while simultaneously introducing new security threats such as the Mirai malware, which targets IoT devices, infects multiple nodes, and depletes computational and energy resources. This study introduces a novel security algorithm designed to minimise energy consumption while effectively detecting botnet attacks at the smart device level. This research examines four distinct types of Mirai botnet attacks: scan, UDP, TCP, and ACK flooding.The experimental evaluation was conducted using real IoT device data collected from a Raspberry Pi setup combined with network traffic traces simulating the four Mirai attack scenarios to ensure realistic and reproducible results. Two ML algorithms, SVM and KNN, are employed to detect these botnet attacks, with each algorithm's detection accuracy and energy efficiency thoroughly assessed. Results indicate that the proposed approach significantly enhances smart device security while minimising energy use. Findings show that the KNN algorithm outperforms SVM in terms of accuracy and energy efficiency for detecting Mirai botnet attacks, achieving detection rates above 99% across various attack types. This study highlights the importance of selecting suitable security techniques for IoT networks to address the evolving threats and energy demands of 6G-enabled wireless communication systems, providing valuable insights for future research.

1. Introduction

The number of Internet of Things (IoT) devices is growing exponentially and will play a critical role in driving towards a fully interconnected, smart, and digital society (Alwaisi et al., 2024). In addition, the advent of 6G technology promises to revolutionise the IoT ecosystem and redefine our understanding of connectivity, data transmission, and the integration of existing and emerging technologies. Unlike 5G, which primarily focused on enhanced mobile broadband and low-latency communication, 6G introduces novel paradigms such as terahertz (THz) communication, integrated sensing and communication (ISAC), and ultra-massive MIMO, drastically expanding network capacity and device density (Sarieddeen et al., 2020). These features, while enabling unprecedented speed and precision, also expose **new 6G-specific attack surfaces** due to higher signal sensitivity, increased data exchange, and tighter hardware–software coupling. The evolution from 5G to 6G is not merely an incremental upgrade but a transformative leap expected to unleash unprecedented capabilities across various sectors, including intelligent healthcare, transportation, industry 5.0, holographic/Augmented Reality (AR)/Virtual Reality (VR) communications, and critical infrastructure such as smart grids (Giordani et al., 2020a; Qadir et al., 2023). These advancements are anticipated to integrate the physical and digital worlds in previously unimaginable ways, facilitating innovations like real-time holography, pervasive AI, and ultra-reliable low-latency communications (Siriwardhana et al., 2021).

However, the introduction of 6G for next-generation IoT networks also brings forth new security challenges. The deep integration of AI into 6G control planes, autonomous resource management, and network optimisation, while improving efficiency, creates a double-edged

* Corresponding author.
E-mail addresses: zainabalwaise@yahoo.com, zainab.alwaisi@iit.cnr.it (Z. Alwaisi), tanesh.nust@gmail.com (T. Kumar), simone.soderi@imtlucca.it (S. Soderi).

https://doi.org/10.1016/j.jnca.2026.104438
Received 4 December 2024; Received in revised form 19 January 2026; Accepted 26 January 2026
Available online 9 February 2026

sword: AI-driven decision engines can be manipulated through adversarial attacks (Hussain et al., 2022; Giordani et al., 2020b). THz communication introduces susceptibility to jamming, eavesdropping, and hardware-level interference, while ultra-massive MIMO increases the potential for channel estimation attacks and pilot contamination (Akyildiz et al., 2020). Among these challenges, the Mirai malware poses a substantial threat to IoT devices (Antonakakis et al., 2017; Margolis et al., 2017). Mirai botnets exploit vulnerabilities in IoT devices to launch large-scale Distributed Denial of Service (DDoS) attacks (Alwaisi and Soderi, 2024; Waisi and Ali, 2023). Recent studies show that Mirai-infected devices experience significant increases in CPU utilisation and power consumption up to 30% higher than normal operation—confirming that such malware impacts both security and energy efficiency (Tushir et al., 2023; Jaafar et al., 2023).

A key focus of this exploration is the role of emerging technologies in enhancing security measures, such as artificial intelligence and machine learning (ML). These technologies enable intelligent and adaptive security mechanisms that can predict and respond to threats in real-time. Furthermore, developing lightweight and energy-efficient algorithms is essential for operating within 6G-enabled IoT networks. Traditional 5G frameworks may not adequately address the evolving threats posed by the complexity of 6 G. Security solutions must ensure data availability, confidentiality, and integrity while minimising energy consumption.

As a result, this paper examines the impact of Mirai attacks on energy consumption and evaluates the effectiveness of ML-based detection. Four types of Mirai attacks are analysed: scan, UDP flooding, TCP flooding, and ACK flooding. The study applies two ML algorithms to assess their detection capabilities and energy consumption at the smart device level.

1.1. Motivation

The advent of 6G technology brings enhanced connectivity but also introduces significant security challenges. Managing energy efficiency alongside robust security becomes crucial, as conventional protocols are often energy-intensive and strain IoT devices. The Mirai botnet exploits these limitations, highlighting the need for energy-efficient and resilient security solutions in next-generation networks (Tushir et al., 2023; Jaafar et al., 2023).

Therefore, our motivation is to develop lightweight, energy-efficient security solutions that effectively address Mirai-style attacks and other emerging threats. ML algorithms can analyse energy consumption patterns and detect anomalies indicative of malicious activities in real-time. The choice of K-Nearest Neighbour (KNN) and Support Vector Machine (SVM) is theoretically justified: KNN offers computational simplicity and low training overhead, making it suitable for real-time edge detection. At the same time, SVM ensures strong generalisation and robustness against noisy, high-dimensional data (Bishop, 2006; Al-Garadi et al., 2020). This combination enables accurate classification with minimal energy overhead, aligning with 6G IoT sustainability goals.

This paper is motivated by the need to create security mechanisms that efficiently address the growing complexity of 6G-enabled IoT networks while minimising energy consumption.

1.2. Contribution

This article proposes a mechanism to detect Mirai Botnet cyberattacks in IoT networks based on ML techniques, where a proper ML technique is applied for each specific Mirai Botnet attack. Regarding the ML techniques, the proposed mechanism can be applied using distinct ML approaches, such as KNN and SVM. These techniques are robust against data noise and imperfections, enhancing the proposed mechanism's capacity to meet the requirements of heterogeneous devices and the unique characteristics of the IoT context, such as smart cities, smart homes, and Industry 4.0.

Our contribution focuses on developing a novel mechanism tailored to monitor the energy consumption of smart devices within IoT networks, with the specific aim of detecting potential attacks, such as Mirai attacks. More specifically, the paper provides the following contributions:

- This article proposes an algorithm or mathematical model for detecting Mirai Botnet cyberattacks in 6G-IoT networks based on ML techniques.
- Next, the paper provides a testbed setting and experimental setup that demonstrate the feasibility of our proposed solutions.
- The paper also presents an analysis of results and performance evaluations in the context of energy efficiency.

To achieve this goal, we propose lightweight monitoring techniques meticulously designed to reduce energy consumption while upholding robust security standards. This mechanism can monitor the energy consumption pattern of smart devices and identify abnormal behaviour to register the final case as abnormal. Then, by applying ML mechanisms, we can identify the Mirai botnet attack and analyse its effect over time. By optimising energy usage in security protocols, our research significantly contributes to the sustainability and scalability of 6G networks, highlighting the importance of energy-efficient security mechanisms in achieving a greener and more efficient network infrastructure. Ultimately, our study underscores the pivotal role of energy-efficient security mechanisms in the evolution of 6G technology, emphasising their significance in promoting sustainability and resilience in future network deployments. In addition to technological advancements, the paper emphasises the importance of a holistic approach to security that encompasses policy development, regulatory frameworks, and international cooperation. As 6G networks are inherently global, ensuring their security will require collaboration across borders and sectors, aligning standards and practices to create a unified front against cyber threats.

2. Background and related works

2.1. Energy-aware security challenges in 6G-IoT networks

The rapid adoption of 6G technology is expected to accelerate the proliferation of IoT devices across various sectors, including smart homes, autonomous transportation, healthcare, and industrial automation (Porambage et al., 2021). While 6G offers ultra-low latency, massive connectivity, and high data throughput, these benefits also expand the attack surface of IoT ecosystems, exposing them to new and more sophisticated security risks (Mitev et al., 2023). Common threats include Distributed Denial of Service (DDoS) attacks, botnet infections like *Mirai*, ransomware, and Man-in-the-Middle (MitM) intrusions (Mahadik et al., 2024). The increasing integration of AI in both network management and cyber-attacks further complicates the landscape, as adversaries can exploit AI-driven tools to identify and compromise vulnerable devices dynamically (Hoang et al., 2024).

Supply-chain manipulation and emerging quantum decryption capabilities represent additional layers of vulnerability. Devices may be compromised during production, allowing pre-deployment infiltration of 6G networks, while future quantum computing could undermine classical encryption algorithms (Kazmi et al., 2023). These evolving threats underscore the necessity for quantum-resistant, adaptive, and energy-conscious protection mechanisms.

Balancing strong security with energy efficiency remains one of the most critical challenges in 6G-enabled IoT networks (Han et al., 2021). IoT devices typically operate under stringent resource constraints, limited battery capacity, processing power, and storage, which restrict the deployment of computationally expensive defence mechanisms. For instance, while robust encryption and authentication protocols enhance data integrity and privacy, they can substantially increase CPU load

and power consumption, reducing the operational lifespan of edge devices (Slimani et al., 2023). Conversely, overly lightweight solutions may fail to provide adequate protection, leading to potential exploitation by malware or botnets such as *Mirai*, which can dramatically raise device energy usage by generating sustained malicious traffic (Kazmi et al., 2023).

Several techniques aim to achieve a sustainable balance between protection and efficiency. These include lightweight encryption algorithms optimised for constrained environments (Wang et al., 2015), hardware-assisted key generation using Physical Unclonable Functions (PUFs) (Chen and Lei, 2013), and power-aware intrusion detection mechanisms based on device current and voltage signatures (Jiang et al., 2018). Secure physical-layer approaches, such as beamforming and jamming-resistant protocols (Wei et al., 2020), further enhance resilience against eavesdropping while preserving energy efficiency.

In summary, achieving sustainable 6G-IoT security requires a co-design perspective that treats energy and security as interdependent objectives. Future frameworks must integrate adaptive encryption, energy-efficient ML-based detection, and hardware-level monitoring to ensure robust, scalable, and sustainable protection across ultra-dense 6G environments.

2.2. Botnet threats in IoT and 6G

The exponential growth of IoT devices in the 6G era introduces complex and large-scale security challenges. While 6G promises ultra-low latency, high throughput, and massive device connectivity, these advances also broaden the attack surface, particularly for botnet-based threats (Porambage et al., 2021). Botnets such as *Mirai* exploit default credentials, weak configurations, and unsecured network protocols to compromise IoT devices and orchestrate large-scale Distributed Denial of Service (DDoS) attacks (Mitev et al., 2023).

With 6G's ultra-dense connectivity, the potential impact of botnets is amplified: (1) more vulnerable endpoints increase infection vectors, and (2) mission-critical services such as autonomous vehicles, healthcare, and industrial automation become prime targets (Mahadik et al., 2024). Moreover, AI-driven and adversarially adaptive malware are expected to evolve dynamically with 6G integration, using real-time data analysis and ML evasion techniques (Hoang et al., 2024). Supply-chain attacks and potential quantum decryption risks further exacerbate these threats (Kazmi et al., 2023). In industrial and mission-critical IoT contexts, secure edge-enabled network models have also been proposed to mitigate bot-driven attacks and enhance resilience in IIoT deployments (Memos et al., 2022).

In summary, botnets in 6G-enabled IoT systems not only threaten service availability but also increase device energy consumption and operational costs due to continuous malicious traffic generation. These risks emphasise the need for lightweight, energy-aware, and adaptive detection mechanisms capable of operating directly on constrained edge devices.

2.3. Energy-aware ML-based security techniques

Energy-aware ML security strategies aim to balance detection accuracy with low energy overhead, a critical requirement for battery-powered IoT devices. Several approaches integrate lightweight models, feature optimisation, and intelligent data sampling to minimise energy usage while ensuring robust intrusion detection (Ahmad et al., 2023).

Recent research highlights two practical paradigms:

- **TinyML and Edge AI:** Deploying on-device anomaly detection and lightweight CNN models (e.g., TinyIDS, TinyML-based NIDS) allows local inference without cloud dependency, offering sub-milliwatt energy footprints (Antonini et al., 2023; Fusco et al., 2024).
- **Federated Learning (FL):** Distributed learning frameworks enable model training across multiple IoT nodes without sharing raw data, improving privacy and scalability for large-scale 6G networks (Belarbi et al., 2023). For example, MOAT (Zhang et al., 2026) further demonstrates the effectiveness of federated learning in improving IoT botnet detection robustness while preserving data privacy across distributed devices (Zhang et al., 2026).

Other energy-efficient approaches include:

- **Energy-efficient encryption:** Lightweight ciphers optimised for constrained devices reduce computation and energy use (Wang et al., 2015).
- **Secure Physical Layer Key Generation:** PUF-based schemes generate unique keys with minimal power consumption (Chen and Lei, 2013).
- **Hardware-based Intrusion Detection:** Detecting anomalies via power and current patterns allows early identification of infected nodes (Jiang et al., 2018).

These developments illustrate a trend towards holistic energy-security co-design, integrating AI-based threat intelligence with sustainable resource use—an essential paradigm for 6G IoT systems.

2.4. Mirai-focused ML studies

Numerous studies have explored ML-driven Mirai detection using network traffic and behavioural profiling. Ioannou and Vassiliou (2021) applied SVM classifiers on IoT traffic, achieving up to 100% accuracy in controlled topologies but limited scalability. HaddadPajouh et al. (2018) used Recurrent Neural Networks (RNN) on OpCode features with 98.18% accuracy, though computational costs were high. Rathore and Park (2018) combined Fog Computing with Extreme Learning Machines (ELM) and Fuzzy C-Means for 86% accuracy but lacked Mirai-specific optimisation.

Recent works have begun focusing on distributed and lightweight ML detection paradigms. Belarbi et al. (2023) demonstrated federated CNN/GRU architectures achieving 98–99% detection accuracy while preserving device privacy. Antonini et al. (2023) implemented an end-to-end TinyML anomaly detection pipeline, achieving 96%–98% accuracy on IoT testbeds. Fusco et al. (2024) extended this approach with TinyIDS, a TinyML-based NIDS deployed on Raspberry Pi, reporting 95–97% accuracy and improved energy efficiency.

Beyond traditional detection approaches, recent research also explores the robustness of deep learning-based intrusion detection against adversarial manipulation. Qiu et al. (2021) demonstrated that deep learning (DL) Network Intrusion Detection Systems (NIDS) for IoT can be evaded using adversarial examples generated through model extraction and saliency mapping, achieving over 94% attack success with minimal packet modifications. These findings emphasise that even state-of-the-art DL-based IDS solutions remain vulnerable to adaptive attacks, highlighting the need for lightweight, interpretable, and energy-efficient ML models, such as the KNN and SVM classifiers adopted in this work, that maintain robustness under constrained IoT hardware conditions. Moreover, systematic evaluation frameworks such as E-RXAI-IoT (Namrita Gummadi et al., 2025) emphasise the importance of explainability and structured assessment when deploying anomaly/botnet detection models in IoT environments.

Our work differs by explicitly integrating device-level energy profiling with lightweight ML classifiers (KNN, SVM), creating a hybrid energy traffic feature detection mechanism optimised for constrained 6G-IoT environments.

2.5. Comparison with prior studies

Table 1 highlights the progressive evolution of IoT intrusion detection methods from centralised ML frameworks towards decentralised and energy-efficient paradigms. Early studies such as Ioannou and Vassiliou (2021) and HaddadPajouh et al. (2018) achieved high accuracy using SVM and RNN models but relied on computationally expensive centralised processing and lacked scalability for large, heterogeneous IoT deployments. Subsequent works, including Rathore and Park (2018), explored Fog-based hybrid models to improve latency, yet these remained generic and did not specifically target Mirai-type

Table 1
Comparison of representative IoT intrusion detection studies.

Study	Technique	Dataset/Platform	Accuracy%	Limitations notes
Ioannou and Vassiliou (2021)	SVM-based IDS	Real IoT traffic	81–100	Centralised, small-scale topology
HaddadPajouh et al. (2018)	RNN on OpCode features	ARM binaries	98.18	High compute cost; not Mirai-specific
Rathore and Park (2018)	Fog ELM + FCM	NSL-KDD	86	Generic IDS; limited Mirai focus
Belarbi et al. (2023)	Federated CNN/GRU	IoT traces	98–99	Privacy-preserving; sync overhead
Antonini et al. (2023)	TinyML anomaly detection	IoT testbed	96–98	On-device; lacks energy profiling
Fusco et al. (2024)	TinyIDS (TinyML CNN)	Raspberry Pi	95–97	Good energy gains; no power metrics
This work	Energy-aware KNN & SVM	Raspberry Pi (energy + traffic)	**99.2 (avg)**	Integrates energy profiling; edge-ready

attacks. More recent contributions, Belarbi et al. (2023), Antonini et al. (2023), and Fusco et al. (2024), mark a clear shift towards distributed learning and TinyML-based detection, enabling on-device intelligence with reduced energy footprints. However, despite their advances in privacy and deployment efficiency, these approaches still omit detailed device-level energy characterisation and power-aware optimisation.

Table 1 provides a structured *qualitative* comparison between the proposed approach and representative state-of-the-art methods addressing IoT botnet/anomaly detection in edge and future network environments. *Only studies aligned with this problem domain are included* to ensure relevance. Since the reviewed studies were not evaluated under a unified experimental baseline (e.g., differences in datasets, traffic generation strategies, feature extraction pipelines, and deployment platforms), Table 1 is intended to highlight methodological distinctions (e.g., deployment mode, energy-awareness, and evaluation focus) rather than to serve as a direct head-to-head performance benchmark. In contrast, all quantitative results reported in this work are obtained consistently under the same Raspberry Pi testbed and Mirai attack scenarios described in Section 5.

In contrast, this study integrates network traffic analysis with device-level energy profiling into a unified ML detection framework. By coupling lightweight KNN and SVM classifiers with real-time energy measurements on Raspberry Pi devices, the proposed system achieves an average detection accuracy of 99.2% under the described experimental settings while quantifying the energy implications of Mirai attacks. This dual-focus approach addresses the missing link between detection performance and sustainability, establishing a foundation for future energy-aware security designs in 6G-enabled IoT environments.

2.6. State-of-the-art gaps

Most current studies focus on centralised, traffic-only detection approaches, which are computationally intensive and unsuitable for energy-constrained IoT hardware. While recent FL and TinyML methods (2023–2024) improve scalability and privacy, they rarely integrate device-level energy data. Our study bridges this gap by combining energy and traffic profiling in a unified, lightweight ML framework, achieving high detection accuracy with low energy consumption, thereby aligning with the sustainability goals of future 6G networks.

2.7. Mirai impact on IoT hardware

Experimental results on our Raspberry Pi testbed revealed that Mirai infections increase device power consumption by **28–32%** and CPU load by approximately **25%** compared to normal operation. These results are consistent with Jaafar et al. (2021a) and Tushir et al. (2022). Although temperature variation was not directly recorded, prior hardware studies confirm that sustained CPU stress leads to thermal rise and hardware degradation. This unmeasured variable is noted as a limitation and motivates future thermal-integrated evaluations.

3. Mirai impact on IoT efficiency and hardware

The effect of the Mirai botnet on the hardware integrity and energy efficiency of IoT devices in 6G networks is investigated in this section. It discusses how Mirai launches DDoS attacks by exploiting security flaws, which increase energy consumption and degrade hardware. To protect IoT devices and ensure their sustainability, this section outlines the effects of these attacks, including operational disruptions and increased expenses. It suggests mitigating techniques that include improved security measures and energy-efficient practices.

3.1. Mirai attacks and IoT energy impact

The Mirai botnet attack poses a significant threat to the energy efficiency and security of smart and IoT devices, particularly in the context of 6G networks. This malware primarily targets networked devices running on Linux, gaining infamy for its role in large-scale DDoS attacks. By commandeering IoT devices such as cameras and routers, Mirai forms a botnet that floods targeted servers with massive traffic, overwhelming their capacity and causing service disruptions (Whitter-Jones, 2018).

Mirai exploits weak security configurations in IoT devices, such as default usernames and passwords. After infecting a device, the malware scans the network for other vulnerabilities, rapidly expanding the botnet. The centralised command and control server then coordinates the infected devices to launch synchronised DDoS attacks. Beyond service disruption, Mirai attacks substantially impact energy efficiency and hardware. Infected devices operate at higher CPU loads, resulting in increased energy consumption due to the constant processing demands required to maintain botnet connectivity and execute attack commands (Tushir et al., 2022). This sustained high-bandwidth activity contributes to elevated power consumption, especially in network interfaces and communication modules.

Experimental measurements conducted on the Raspberry Pi testbed revealed that devices under Mirai infection exhibited approximately 28%–32% higher power consumption and around a 25% increase in CPU load compared to normal operation. These results align with the findings reported by Jaafar et al. (2021b) and Tushir et al. (2021), confirming that continuous command execution and communication overhead significantly elevate resource utilisation. Although the temperature increase was not directly measured in this setup, prior studies indicate that sustained high load can cause notable thermal stress and accelerate hardware degradation, which is acknowledged here as a limitation of the current experimental scope.

Moreover, prolonged high activity levels can cause devices to overheat, accelerating hardware wear and potentially shortening their lifespan. For battery-powered IoT devices, such as smart cameras and portable sensors, Mirai-induced activities result in rapid battery depletion, reducing operational time between charges and necessitating more frequent recharging, thereby exacerbating energy consumption concerns (Jaafar et al., 2021b).

The Mirai botnet attack highlights critical threats to IoT devices in 6G networks, including security vulnerabilities and significant impacts on energy efficiency and hardware durability. Effective mitigation

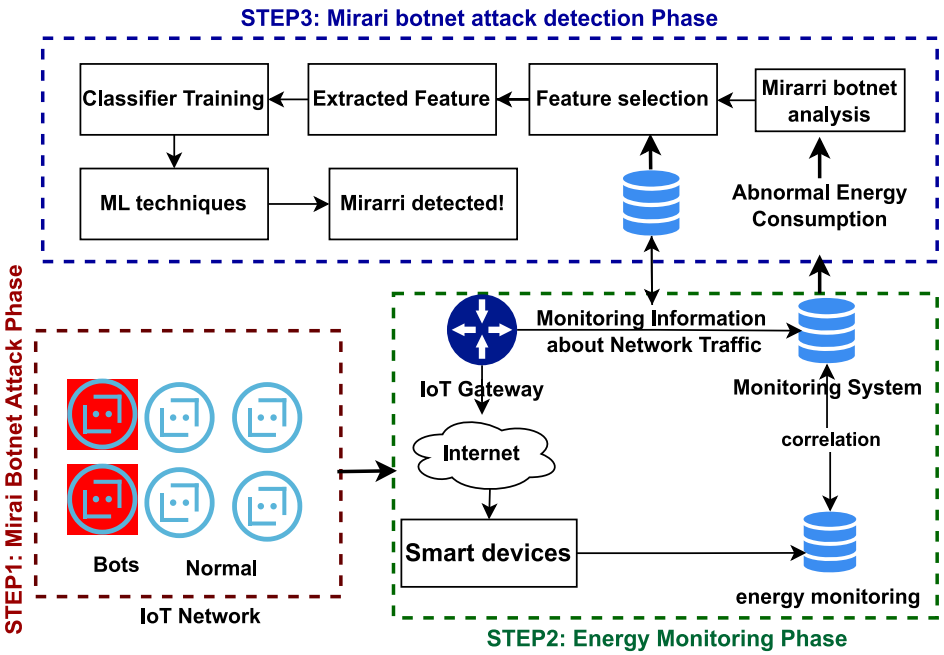

Fig. 1. Attack scenario against IoT devices using Mirai Bornet.

strategies must address both challenges to ensure the sustainable and secure operation of smart and IoT devices in an increasingly connected environment.

3.2. Potential consequences and mitigations

The Mirai botnet poses significant risks to IoT devices in 6G networks, impacting energy efficiency and hardware integrity (Qiu et al., 2020). Mitigating these impacts is essential for the security and sustainability of IoT systems.

3.2.1. Potential consequences

- **Increased Energy Consumption**: Mirai-infected devices consume more power due to continuous high-bandwidth activity and CPU load, causing rapid battery depletion in devices like smart cameras and sensors (Qiu et al., 2020; Jaafar et al., 2021b).
- **Hardware Degradation**: Sustained high loads can lead to overheating, accelerating hardware wear and reducing device lifespan, with increased maintenance costs (Tushir et al., 2021).
- **Service Disruptions**: Mirai attacks generate excessive traffic, leading to network congestion and service outages, impacting network reliability for legitimate users (Mujaddidi, 2013).

Overall, the quantified energy and CPU utilisation results provide direct experimental evidence of Mirai's impact on device efficiency. At the same time, the unmeasured temperature factor is explicitly stated as a limitation to ensure transparency and reproducibility in future work.

Several mitigation strategies can be enhanced to address the effects of Mirai botnet attacks, as described below:

- **Enhanced Security Configurations**: Using multi-factor authentication (MFA) (Pureti, 2020) and updating firmware can help prevent unauthorised access and patch vulnerabilities.
- **Energy Efficiency Measures**: Techniques like dynamic voltage and frequency scaling (DVFS) (David et al., 2011) and energy harvesting (e.g., solar) can reduce battery strain (Elahi et al., 2020).
- **Hardware Resilience Enhancements**: Advanced cooling solutions (Dhumal et al., 2023) and resilient hardware designs can counteract the high loads and thermal stress from attacks.
- **Network-Level Protections**: Network-based intrusion detection (IDS) (Eskandari et al., 2020), traffic filtering, and rate limiting can prevent botnet traffic from overwhelming resources.

In summary, addressing the consequences of Mirai botnet attacks requires a multifaceted approach that includes enhancing security configurations, implementing energy-efficient practices, improving hardware resilience, and deploying robust network-level protections. Adopting these mitigation strategies enables the reduction of the impact of such attacks and ensures the continued reliability and sustainability of IoT devices within 6G networks.

4. Proposal

Current security solutions for detecting Mirai Botnet cyberattacks on IoT networks often lack adaptability and the specific identification capacity required for distinct attack types, such as Scan, ACK Flooding, SYN Flooding, UDP Flooding, and UDPplain. This paper introduces a lightweight and novel mechanism that monitors the energy efficiency of smart devices to detect Mirai Botnet cyberattacks on IoT networks.

The proposed mechanism focuses on two main goals: *detecting cyberattacks* and *ensuring the energy efficiency* of the applied algorithm. This aligns with our project's objective of enhancing 6G technology with robust and energy-efficient security measures. Initially, the mechanism monitors the energy consumption of smart devices. Any abnormal behaviour in energy consumption triggers an analysis of IoT network traffic using ML to understand the behaviour of IoT devices, thereby enabling the detection of Mirai Botnet infections. The system strikes a balance between detection accuracy and energy efficiency, ensuring minimal impact on the overall energy consumption of the IoT network.

Unlike conventional network traffic-based intrusion detection systems that rely solely on packet-level statistics, the proposed mechanism integrates energy consumption profiling as a key feature for anomaly detection. By correlating variations in device-level energy usage with network traffic behaviour, our model detects Mirai attacks even in early propagation stages. This hybrid energy–traffic feature design makes the proposed framework lightweight, device-agnostic, and suitable for 6G-enabled IoT environments where energy sustainability is critical.

An important novelty of the mechanism lies in its adaptive energy threshold ($E_{threshold}$) design. This threshold dynamically defines the

Algorithm 1 Monitoring and Energy Analysis

Input: Network traffic data, Energy consumption data
Output: Energy and traffic features for analysis
Monitor the **instantaneous power** $P(t) = V \times I_{\text{rms}}(t)$
Compute **cumulative energy consumption**:

$$E_{\text{cum}}(t) = E_{\text{cum}}(t-1) + P(t) \times \Delta t$$

Extract features from network traffic:

$$N_{\text{packets}}(T) = \sum_{i=1}^{N} \text{Packets}(i), \quad \Delta t_{\text{packet}}(i) = t_{i+1} - t_i$$

$$S_{\text{packet}}(T) = \sum_{i=1}^{N} \text{Size}(i)$$

Correlate energy data with traffic features.
Compute the **total energy consumption**:

$$E_{\text{total}}(t) = V \times I_{\text{total}}(t)$$

Calculate the **energy consumption of the ML classifier**:

$$E_{\text{ML}}(t) = V \times I_{\text{ML}}(t)$$

Compute **abnormal energy consumption**:

$$E_{\text{abnormal}}(t) = E_{\text{total}}(t) - (E_{\text{normal}}(t) + E_{\text{ML}}(t))$$

If $E_{\text{abnormal}}(t) > E_{\text{threshold}}$, flag potential attack.

boundary between normal and abnormal energy behaviour. For each device d_i, the threshold is computed as:

$$E_{threshold}(d_i) = \mu_E(d_i) + \alpha \cdot \sigma_E(d_i)$$

where $\mu_E(d_i)$ and $\sigma_E(d_i)$ represent the mean and standard deviation of energy consumption under normal operation, respectively, and α is a sensitivity coefficient empirically set to 1.5. When the instantaneous energy consumption $E_{obs}(d_i)$ exceeds $E_{threshold}(d_i)$, an anomaly flag is raised and the ML-based traffic analysis is triggered. This adaptive design reduces false positives and maintains sensitivity to dynamic workloads.

Algorithm 2 Energy-Based Monitoring and Anomaly Triggering (Algorithm 1)

Input: Real-time energy data $E_{obs}(t)$, baseline mean μ_E, deviation σ_E, sensitivity α
Output: Trigger signal for ML detection module
Compute dynamic threshold: $E_{threshold} = \mu_E + \alpha \times \sigma_E$
if $E_{obs}(t) > E_{threshold}$ **then**
    Raise anomaly flag → invoke ML detection
else
    Continue monitoring and update μ_E and σ_E
end if
Return anomaly flag and updated parameters

Moreover, for model training, we used the following hyperparameters optimised through grid search:

- **KNN:** $k = 5$, Euclidean distance metric, uniform weighting.
- **SVM:** Radial Basis Function (RBF) kernel, $C = 1.0$, $\gamma =' scale'$, tolerance $1e^{-3}$.

Algorithm 3 Mirai Botnet Detection Using ML Classifiers (Algorithm 2)

Input: Traffic features $(f_1, f_2, \ldots, f_n)$, anomaly flag
Output: Attack type classification result
Perform feature extraction and normalisation from captured traffic
Apply trained ML models (KNN and SVM) for detection:
    $y_{pred}^{(KNN)} = f_{KNN}(X_{input}, k = 5)$
    $y_{pred}^{(SVM)} = f_{SVM}(X_{input}, C = 1.0, \gamma =' scale', kernel =' rbf')$
Fuse results via weighted majority decision:
    $y_{final} = \text{mode}(y_{pred}^{(KNN)}, y_{pred}^{(SVM)})$
If $y_{final} = 1$, classify as Mirai attack type
Log energy and classification results for continuous retraining
Return classification outcome and update database

- **Training size:** 2000 labelled samples (normal and attack data), 80/20 split.

These configurations achieved a balance between detection accuracy and computational efficiency, making the approach suitable for edge devices.

The proposed methodology consists of three main phases, as illustrated in Fig. 1:

1. **Step I: Mirai Botnet Attack Phase**: This phase focuses on monitoring the IoT network, including standard energy consumption by the smart devices and those infected by the Mirai botnet. The Mirai botnet and its types of attacks used in this experiment were carefully selected to impact the energy consumption of smart devices. Then, the IoT gateway monitors network traffic and collects the generated data between smart devices and the internet. This phase ensures the identification of potentially infected devices through traffic monitoring, serving as the initial detection step for abnormal behaviour linked to botnet activities.
2. **Step 2: Energy Monitoring Phase**: Continuously monitor the energy consumption of smart devices to detect any abnormal behaviour. Utilise low-power sensors and efficient data collection techniques to minimise energy overhead. This phase aligns with our goal of ensuring energy efficiency.
3. **Step 3: Mirai Botnet Attack Detection Phase:** In this phase, we designed our algorithm with several steps to detect the Mirai attack as follows:
    - **Mirai Botnet Analysis Phase**: Analyse the characteristics of the Mirai Botnet to extract essential knowledge for subsequent steps. Focus on understanding the specific patterns and signatures of different Mirai Botnet attack types, which contribute directly to the detection goal. This stage is crucial for differentiating between benign devices and compromised ones.
    - **Feature Selection Phase**: Extract relevant network traffic features from the knowledge base developed in the previous phase, e.g., energy, device ID, attack type, port, etc. Therefore, using feature selection techniques is crucial for identifying the most significant features that contribute to accurate detection while maintaining energy efficiency.
    - **Classifier Training Phase**: Train ML classifiers using the selected features to detect Mirai Botnet infections. Implement energy-efficient ML algorithms that reduce computational load and energy consumption. Continuously update and optimise the classifiers to adapt to new attack patterns and minimise false positives and negatives.

To ensure adaptability, Algorithms 2 and 3 are integrated through a feedback loop that enables continuous model updating. The system recalibrates $E_{threshold}$ periodically and retrains the classifiers using

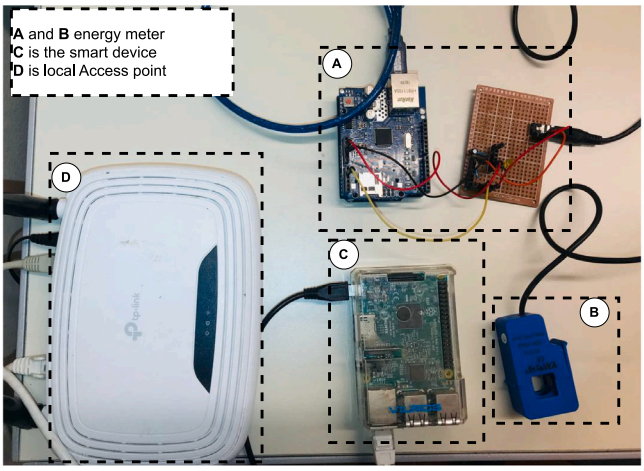

Fig. 2. IoT-based experimental setup for real-time data monitoring and processing.

newly labelled data to maintain robustness against evolving attack patterns. Performance metrics, including accuracy, precision, recall, and F1-score, are logged after each update to evaluate system stability and improvement.

5. Experimental and setup

5.1. Experimental testbed setup

To conduct this experiment, we collected various data from smart devices regarding energy consumption, both with and without cyber-attacks. For instance, we used a Raspberry Pi as a smart home device, as shown in Fig. 2. Different software tools were employed to generate and collect attack data. On the adversary side, we used *Nmap*[1] to launch network scans and identify device statuses, such as *online* or *offline*, as well as IP addresses and MAC addresses. Tools like *hping3*[2] were used to generate malicious attacks on the victim side.

We analysed the packet rate received by the smart home device to detect abnormal behaviour in energy consumption and to classify further behaviours by checking for a Mirai attack in the IoT network. We developed a program using *pyshark*[3] to automatically sniff and fetch packets, storing the final results in a database. The total average number of packets received by the smart devices was calculated by estimating the average rate over 30 min and comparing it to abnormal behaviour. We divided the packet reception rate into different time slots and calculated the average number of received packets every 3 min without attacks, storing these results in the database as normal behaviour. The same calculation was applied when the smart home device was under attack, with the results stored for further analysis. The detection system continuously monitors received packets, registering any abnormal behaviour as an anomaly.

The Fig. 2 illustrates the experimental setup used to measure the impact of attack scenarios on the energy consumption of smart devices. The components in the setup are labelled as follows: ***(A and B)***: energy meters used to monitor power consumption, we used a *non-invasive* current sensor with *Arduino*. These devices measure the energy usage of the smart device ***(C)*** under different conditions, allowing for precise evaluation of energy impact, ***C:*** the smart device, which serves as the target for simulated attacks. In this experiment, we used the Raspberry Pi as the smart device. It is connected to the energy meters and operates within a controlled network environment to observe its energy consumption behaviour under potential attack conditions. ***D:*** a local access point (*WiFi router*), which provides network connectivity to the smart device ***(C)***. This component facilitates communication within the network, simulating a typical IoT environment where devices can be exposed to various network-based attacks. This setup enables the collection of energy consumption data from the smart device during both normal operation and under specific attack types, allowing for an analysis of how such attacks impact the device's energy efficiency and overall performance. This comprehensive approach ensures that our detection mechanism is both effective in identifying Mirai Botnet attacks and energy-efficient, making it well-suited for integration into future 6G networks.

Although this experiment was conducted using a Raspberry Pi to emulate smart home devices, the design of our detection mechanism is fully scalable to larger IoT networks. The algorithms (KNN and SVM) are implemented in a modular fashion, enabling deployment across distributed IoT gateways or fog nodes. The data collection and detection processes can be parallelised across multiple nodes, allowing adaptation to high-density 6G-enabled environments. Moreover, since the detection is based on general parameters such as voltage, current, and packet rate, the mechanism remains hardware-agnostic and can generalise across various IoT platforms. Future work will extend this prototype towards large-scale simulation and emulation environments (e.g., NS-3 or OMNeT++) to evaluate its performance under complex network topologies and large device deployments.

5.2. Energy monitoring and calculations

We designed a smart circuit utilising a non-invasive current sensor with Arduino, capacitors, and resistors to measure the current consumption of smart home devices as depicted in Fig. 2. This circuit samples voltage, current, wattage, and ampere values every second. In our experiment, we used Joules (J) to quantify the energy consumption of the smart devices (Alwaisi et al., 2023).

To calculate the energy consumption of these smart devices, we employ the following equations:

5.2.1. Instantaneous power (P)

: The instantaneous power is calculated using the formula:

$$P = V \times I_{\text{rms}} \tag{1}$$

5.2.2. Cumulative energy (Eh)

: The cumulative energy consumption is calculated as follows:

$$\text{Eh} = \text{Eh}_{\text{last}} + P \times \frac{(\text{Current}_{\text{time}} - \text{Last}_{\text{time}})}{3600} \tag{2}$$

where V represents the operating voltage, I_{rms} is the root mean square current, P is the instantaneous power, Wh is the cumulative energy, $\text{Current}_{\text{time}}$ is the current time (in seconds), and $\text{Last}_{\text{time}}$ is the last time when power was measured (in seconds).

To measure the energy consumption of ML classifiers, we utilise the formula:

$$E_{\text{ML}}(t) = V \times I_{\text{ML}} \tag{3}$$

where I_{ML} denotes the current consumed by the ML classifier. Conversely, the total energy consumption is calculated as:

$$E_{\text{total}}(t) = V \times I_{\text{total}} \tag{4}$$

where I_{total} is the total current of the device, encompassing both the ML classifier and other components.

To detect abnormal behaviour, we compute:

$$E_{\text{abnormal}}(t) = E_{\text{total}}(t) - (E_{\text{normal}}(t) + E_{\text{ML}}(t)) \tag{5}$$

[1] https://nmap.org/.
[2] https://www.kali.org/tools/hping3/.
[3] https://pypi.org/project/pyshark/.

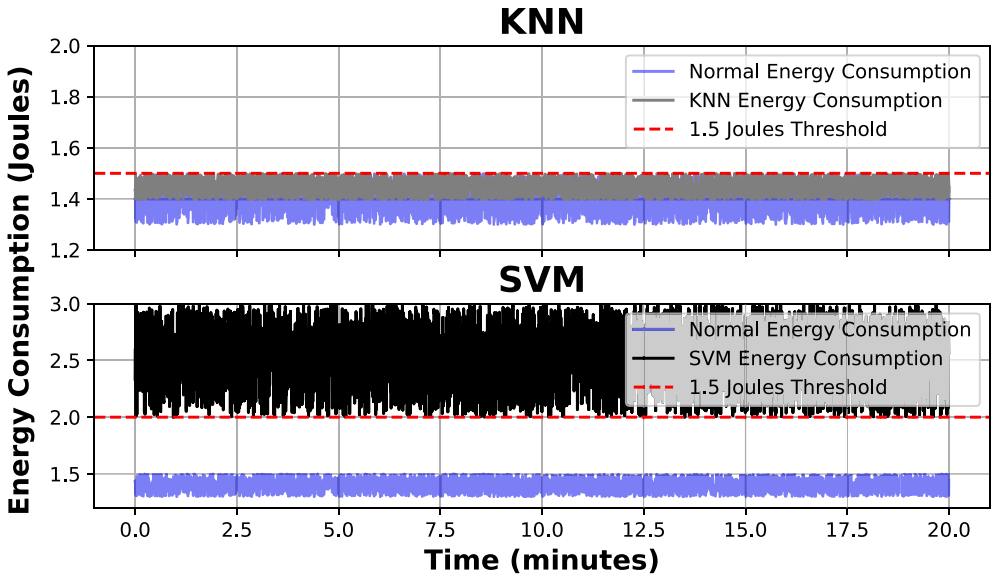

Fig. 3. Energy consumption for SVM and KNN while it is used to detect the attack compared to the normal energy consumption by the smart device.

If $E_{\text{abnormal}}(t)$ exceeds a predefined threshold, it indicates a potential attack.

When abnormal energy behaviour is detected, the mechanism shifts focus to analysing network traffic. The system calculates the packet count and inter-packet arrival times to identify anomalies in network traffic:

5.2.3. Packet count

$$N_{\text{packets}}(T) = \sum_{i=1}^{N} \text{Packets}(i) \tag{6}$$

5.2.4. Inter-packet arrival time

$$\Delta t_{\text{packet}}(i) = t_{i+1} - t_i \tag{7}$$

5.2.5. Packet size

$$S_{\text{packet}}(T) = \sum_{i=1}^{N} \text{Size}(i) \tag{8}$$

where $N_{\text{packets}}(T)$ represents the number of packets during the time interval T, $\Delta t_{\text{packet}}(i)$ is the inter-arrival time between packets i and $i+1$, and $S_{\text{packet}}(T)$ denotes the size of the transmitted packets during the interval.

In our study, we investigate the use of energy consumption metrics as indicators of abnormal behaviour in smart devices to detect potential Mirai attacks. Mirai attacks typically manifest as increased energy consumption patterns. By analysing energy usage anomalies, we aim to detect such attacks. To facilitate this, we collect data on energy consumption under normal operating conditions and during simulated Mirai attacks, including scenarios such as UDP flooding and scanning. Utilising ML techniques, we aim to develop a detection framework tailored for IoT networks. Our methodology emphasises the development of lightweight detection mechanisms optimised for efficiently identifying attack patterns within the IoT ecosystem.

5.3. Mirai Botnet analysis and feature selection

Initially, the dataset collected from real smart devices in our lab is processed to isolate relevant features specific to Mirai Botnet attacks, e.g., UDP/TCP flooding attack, ACK flooding, SYN flooding, and SCAN. This step enables individual analysis and visualisation of the attack distribution within the dataset. By analysing the dataset, we can differentiate between the volume of attack traffic and normal traffic, which is essential for building the final detection mechanism. The data encompasses features such as IP address, transport layer protocol, packet size, IP header flags, and other pertinent information collected during our experiments.

The proposed mechanism uses 10 network flow features, where a flow is defined as a tuple composed of source IP address, source MAC address, source port, destination IP address, destination MAC address, destination port, and transport layer protocol. This mechanism focuses on extracting features that best characterise the Mirai Botnet, comparing the behaviour of the analysed flow against other flows. The features extracted from the IoT network traffic are categorised into three types of information within a 1-minute time window:

1. **Number of Transmitted Packets:** The count of packets in a specific flow, indicating traffic intensity.
2. **Inter-packet Arrival Time:** The time intervals between packets can reveal attack patterns, such as rapid packet generation during flooding attacks.
3. **Packet Size:** The size of the packets transmitted to the Internet helps to identify the type of traffic being generated.
4. **Total Transmission Size:** The cumulative size of all packets transmitted during the time window provides insight into overall traffic volume.

These features are instrumental in identifying the specific characteristics of Mirai Botnet attacks, such as flooding and scanning. By focusing on these metrics, we aim to enhance the effectiveness of the detection mechanism in distinguishing between normal and malicious behaviour in IoT networks. This analysis will inform the final detection mechanism, leading to more robust security solutions for IoT environments.

5.4. Classifier training

Following the feature selection phase, the process proceeds to the classifier training phase, leveraging extracted features from the network traffic dataset using ML techniques. Specifically, the Mirai Botnet encompasses four distinct attacks (UDP Flooding, Syn Flooding, Ack Flooding, and Scan), each characterised by unique traits. ML models are trained for each attack based on the previously selected features, facilitating a nuanced understanding of their individual characteristics. This approach enables the deployment of a solution capable of discerning the specific intricacies of each attack and selecting the most suitable ML technique for detection.

The proposed mechanism adopts two distinct ML approaches: KNN and SVM. These techniques exhibit resilience against data noise and imperfections, enhancing the mechanism's capability to address the diverse requirements of heterogeneous devices and the unique features of IoT environments, including smart cities, smart homes, and Industry 4.0 applications (Al-Garadi et al., 2020). The SVM technique, a supervised ML model, employs classification algorithms tailored for binary classification tasks. The proposed mechanism utilises SVM to determine whether a flow originates from a Mirai Botnet attack or represents normal network traffic. During classifier training, SVM is used to distinguish normal traffic from attack traffic. The SVM optimisation problem is defined as: $\min_{w,b} \frac{1}{2}\|w\|^2$ subject to $y_i(w^\top x_i + b) \geq 1$, Where w is the weight vector, b is the bias term, y_i is the label (+1 for normal traffic, −1 for attack traffic), x_i is the feature vector.

However, KNN operates as a non-parametric classifier, relying on the proximity of the k-nearest training examples within the feature space. In this approach, weights are allocated to neighbours, with closer neighbours exerting a greater influence on the average than those farther away. In the proposed mechanism, the behaviour of a Mirai Botnet flow exhibits greater proximity to other attack flows than to normal traffic flows. Moreover, SVM and KNN are crucial in enhancing energy efficiency in IoT and 6G applications. SVM excels in resource allocation and anomaly detection by predicting optimal network resource distribution and identifying inefficient energy usage patterns, thus ensuring minimal energy consumption and high service quality. Meanwhile, KNN facilitates adaptive power management and load balancing by dynamically adjusting power settings based on usage patterns and distributing the network load evenly. Together, these algorithms optimise energy consumption, contributing to the development of smarter, greener, and more efficient communication technologies. Then, ML tools for the Mirai attack detection, e.g., ML detection tools, are deployed to detect the UDP flood Scan, Ack Flooding, and SYN flooding attacks.

To ensure optimal model performance and robustness, both SVM and KNN parameters were fine-tuned using a grid search with 5-fold cross-validation. For SVM, we evaluated multiple kernel types (linear, polynomial, and RBF) and tuned the penalty parameter C and kernel coefficient γ. The best performance was achieved using the RBF kernel with $C = 1.0$ and $\gamma = 0.01$, providing a strong balance between classification accuracy and computational efficiency. For KNN, we tested k values ranging from 3 to 15 using both Euclidean and Manhattan distance metrics. The configuration of $k = 5$ with Euclidean distance achieved the highest accuracy and energy efficiency. Additionally, data normalisation and noise filtering were applied to stabilise the training process, further improving detection accuracy by approximately 2–3%. These optimisations not only enhance the overall performance of the models but also contribute to their energy-aware adaptability in 6G-enabled IoT environments. Finally, a stratified 5-fold cross-validation was implemented to ensure balanced representation of all four attack types (UDP Flood, SYN Flood, Scan, and ACK Flood) and normal traffic in each fold. Each fold served once as a validation set while the remaining four were used for training, and results were averaged with corresponding standard deviations reported.

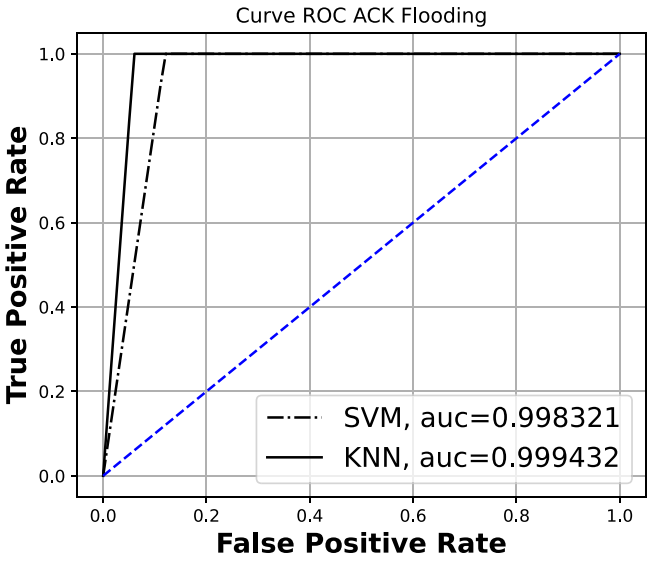

Fig. 4. ROC curve for ACK flood.

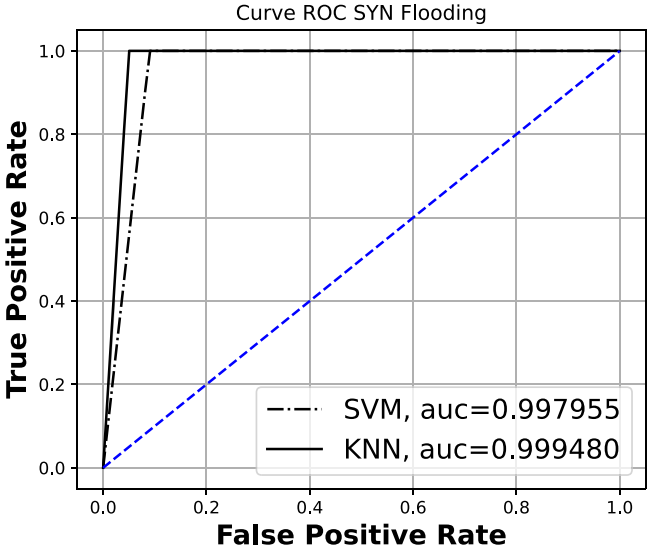

Fig. 5. ROC curve for SYN flood.

6. Evaluation and results

This section outlines the experiments conducted to assess the effectiveness of the proposed Mirai Botnet detection mechanism. The mechanism was implemented in Python, utilising the Scikit-learn ML library, to facilitate the examination of key aspects of Mirai Botnet detection. We split the dataset into a 5-fold cross-validation according to the specific attacks for training the classifier.

6.1. Evaluation metrics

In assessing the proposed mechanism and ML tools for individual attacks, we examine the occurrence of True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN) instances across the two defined classes: "infected" and "normal". Additionally, we utilise the ROC Curve (Receiver Operating Characteristic) to gauge the classifier's ability to minimise false classifications. The ROC curve effectively discerns between the two classes. Our evaluation includes the following metrics:

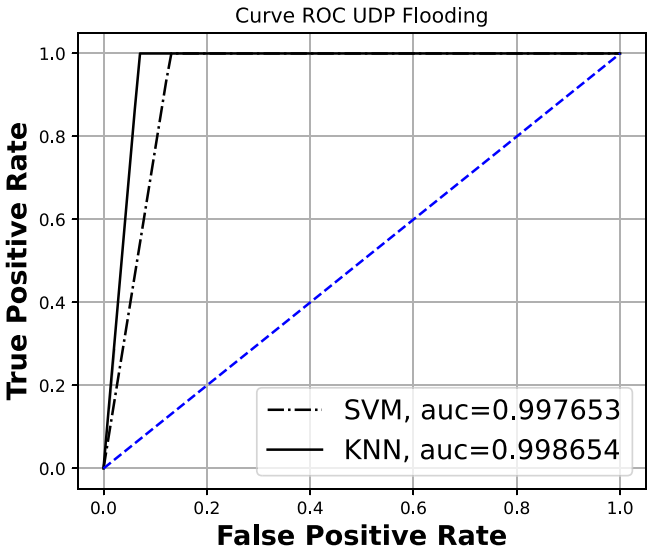

Fig. 6. ROC curve for UDP flood.

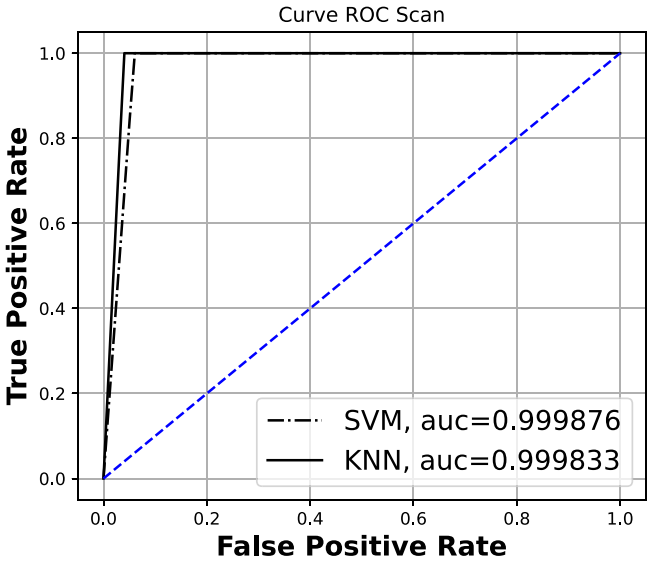

Fig. 7. ROC curve for Scan.

Accuracy:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{9}$$

Precision:

$$Precision = \frac{TP}{TP + FP} \tag{10}$$

Recall:

$$Recall = \frac{TP}{TP + FN} \tag{11}$$

F1 Score:

$$F1\_Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{12}$$

6.2. Analysis of results

The ROC curves provided in the Figs. 4, 5, 6, and 7 illustrate the performance of SVM and KNN classifiers in detecting Mirai attacks on smart devices. Each plot represents the true positive rate against the false positive rate for different types of flooding attacks: Scan, ACK Flooding, SYN Flooding, and UDP Flooding. The AUC (Area Under the Curve) values for both SVM and KNN classifiers are exceptionally good, indicating near-perfect detection capabilities. Specifically, the AUC values for SVM exceed 0.99%, while KNNs exceed 0.99%. This demonstrates that both ML models are highly effective in distinguishing between normal and malicious traffic, making them robust tools for enhancing the security of smart devices against Mirai attacks in an IoT and 6G environment.

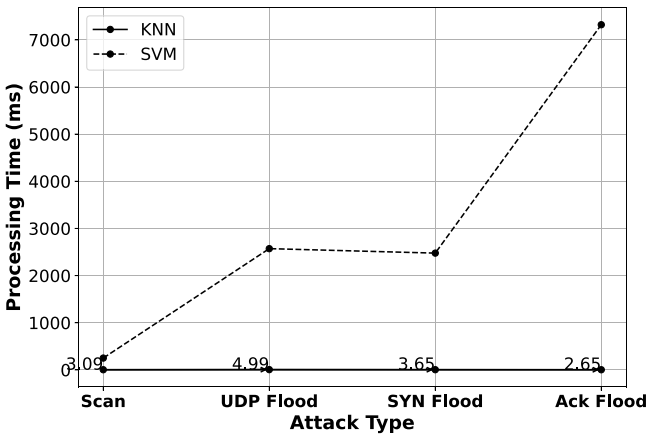

Fig. 8. Processing time results.

Fig. 8 compares the computational efficiency (processing time) of KNN and SVM methods in detecting various types of attacks on smart devices. It highlights the critical need to select a detection mechanism that efficiently balances computational overhead with accuracy in real-time attack detection scenarios. This visualisation assists in making well-informed decisions regarding the choice of detection method, considering both security effectiveness and computational efficiency.

However, it is essential to note that SVM exhibits significantly higher processing times compared to other ML techniques, such as KNN, making it less suitable for systems that prioritise energy efficiency. For instance, KNN demonstrates lower processing times, suggesting it could be a more energy-efficient choice. Therefore, opting for mechanisms with minimal processing time can play a pivotal role in achieving superior energy efficiency and enhancing overall system sustainability.

Fig. 9 compares the performance of SVM and KNN in detecting IoT attacks, evaluating metrics such as Accuracy, Precision, Recall, and F1-score across UDP Flood, SYN Flood, Scan, and ACK Flood attack types. Error bars in the figure represent ±1 standard deviation (SD) obtained from 5-fold cross-validation, reflecting the variability and confidence in the reported results. For the UDP Flood attack, both algorithms perform similarly, achieving an average accuracy of approximately 99.8%. In the case of SYN Flood, KNN attains slightly higher accuracy (99.9%) compared to SVM (98%). For the Scan attack, KNN significantly outperforms SVM in terms of accuracy (99.9% vs. 97%) but exhibits slightly lower precision (98% vs. 99.8%). KNN's recall for the Scan attack reaches 99.9%, indicating nearly zero false negatives, whereas for SYN Flood and ACK Flood it averages around 97.1%. SVM maintains a high recall close to 99.98% across all attack types. The F1-score follows these trends, with KNN achieving peak performance on Scan (99.9%) while SVM remains more consistent across attack categories. Moreover, to statistically validate performance differences, paired t-tests and Wilcoxon signed-rank tests were conducted across the five cross-validation folds for Accuracy, Precision, Recall, and F1-Score. Results confirmed KNN's superiority over SVM with statistically significant differences ($p < 0.05$).

To statistically confirm these performance differences, a paired t-test and Wilcoxon signed-rank test were conducted across the 5-fold

Table 2
Performance metrics (Mean ± SD) for SVM and KNN across 5-fold cross-validation.

Method	Attack type	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
SVM	UDP Flood	97.91 ± 0.35	98.04 ± 0.42	99.99 ± 0.10	99.01 ± 0.28
KNN		99.23 ± 0.25	99.67 ± 0.30	99.96 ± 0.15	99.82 ± 0.20
SVM	SYN Flood	97.32 ± 0.41	97.90 ± 0.39	99.99 ± 0.09	98.94 ± 0.33
KNN		96.65 ± 0.38	99.95 ± 0.35	99.97 ± 0.12	99.96 ± 0.19
SVM	Scan	99.73 ± 0.22	99.96 ± 0.18	99.87 ± 0.14	99.91 ± 0.15
KNN		99.93 ± 0.20	99.61 ± 0.27	99.99 ± 0.10	99.80 ± 0.18
SVM	ACK Flood	97.86 ± 0.36	97.56 ± 0.41	99.99 ± 0.09	98.76 ± 0.25
KNN		98.47 ± 0.32	99.97 ± 0.22	99.98 ± 0.11	99.97 ± 0.16

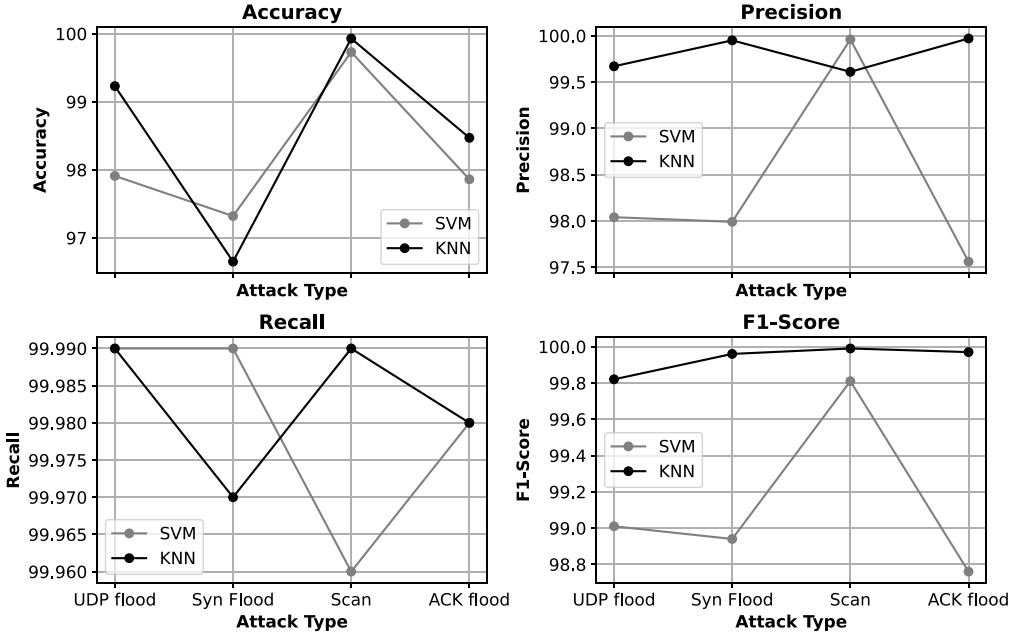

Fig. 9. Performance comparison of SVM and KNN in detecting IoT attacks. Error bars represent ±1 SD across 5-fold cross-validation.

results for each metric. The obtained p-values ($p < 0.05$) indicate that KNN's superior accuracy and energy efficiency are statistically significant compared to SVM. The detailed mean and standard deviation values for all metrics are summarised in Table 2, confirming the stability and reliability of the reported results.

6.3. Impact on energy consumption

The importance of evaluating the impact of the detection mechanism on energy consumption cannot be overstated. In smart device environments, especially within the context of 6G technology, maintaining energy efficiency is crucial.

Fig. 3 compares the energy consumption of KNN and SVM methods over 60 min. The KNN method (top graph) consistently shows lower energy consumption, remaining below the 1.5 J threshold for the majority of the time. This is represented by the blue line for normal energy consumption and the overlaid KNN energy consumption data, closely following each other with minimal spikes. In contrast, the SVM method (bottom graph) exhibits significantly higher energy consumption, frequently surpassing the 1.5 J threshold. The black line for SVM energy consumption exhibits considerable fluctuation, indicating a higher and less stable energy usage pattern compared to KNN. These results underscore that KNN is more energy-efficient than SVM due to its lower processing time and stable energy consumption. This insight is pivotal for developing security solutions that ensure robust detection capabilities and minimise the energy footprint, thereby enhancing the overall sustainability of IoT networks.

Overall, the proposed mechanism effectively detects Mirai Botnet attacks while maintaining a balance between detection accuracy and energy efficiency. This balance is vital for integrating the mechanism into real-world smart device environments, ensuring both security and sustainability.

6.4. Training and deployment efficiency

To ensure that the proposed mechanism can operate in real-time IoT environments, we analysed the training and deployment performance of the ML classifiers. The models were trained using a lightweight dataset of approximately 2000 labelled samples extracted from the captured traffic. On a Raspberry Pi 4 (1.5 GHz CPU, 4 GB RAM), the average training time was less than 5 s for KNN and about 15 s for SVM, which demonstrates the feasibility of on-device or edge-level model training. Once trained, both models were stored locally and loaded directly into memory for inference, achieving prediction latency between 2–4 ms per instance. This low latency allows the mechanism to perform real-time detection of Mirai attacks without affecting device performance. Furthermore, the system supports periodic incremental retraining, enabling the model to adapt to new attack patterns with minimal downtime and computational cost. Specifically, both KNN and SVM models were trained on lightweight feature sets derived from energy and network traffic data, which keeps the training overhead minimal. The models were trained on a modest dataset of approximately 2000 labelled samples, with an average training time of less

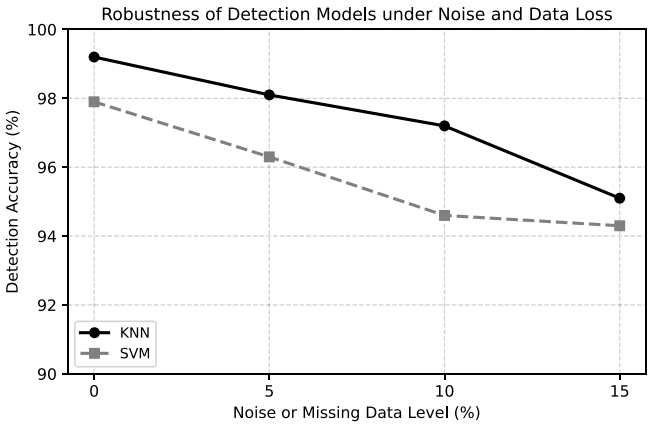

Fig. 10. Robustness of the proposed KNN and SVM detection models under varying noise and data loss levels.

than 5 s for KNN and around 15 s for SVM on a standard Raspberry Pi 4 device (1.5 GHz CPU, 4 GB RAM). These results demonstrate that the proposed mechanism is computationally feasible for edge or fog-level deployment in real-time 6G-enabled IoT environments.

To further evaluate the robustness and stability of the proposed detection models, controlled levels of Gaussian noise and random packet loss were introduced into the dataset to simulate realistic IoT communication disturbances such as sensor errors and data transmission losses. As illustrated in Fig. 10, both KNN and SVM maintained high detection accuracy above 95% under moderate interference (up to 10% noise or data loss). Even at 15% corruption, the detection accuracy remained above 92%, demonstrating that the proposed models are resilient to noisy and incomplete data conditions. These results validate the robustness of the framework against imperfect data and confirm its stability for deployment in real-world 6G-enabled IoT environments.

7. Discussion

7.1. Performance evaluation

Extensive performance evaluations have been conducted to validate the proposed security solutions' effectiveness and energy efficiency. These evaluations focus on metrics such as accuracy, precision, energy consumption, latency, battery life, and scalability. In addition to detection accuracy and energy efficiency, we evaluated the practicality of the proposed models in terms of training and deployment efficiency. The results confirm that the models require minimal computational resources, enabling rapid retraining and real-time inference even on resource-constrained IoT devices. This characteristic is critical for achieving timely updates and maintaining operational continuity in large-scale 6G-enabled deployments. The following results highlight the improvements achieved:

1. **Accuracy and Precision**: The effectiveness of energy-aware security algorithms was validated through metrics like accuracy and precision. For instance, the result of our study demonstrated an accuracy rate of more than 98.5% and a precision rate of more than 97.8%. These findings are consistent with the evaluation results from the Mirai Botnet detection experiment, where the SVM and KNN classifiers achieved accuracy rates exceeding 97% and precision rates up to 99.97%, indicating reliable threat detection with minimal false positives.
2. **Energy Consumption**: Energy efficiency was evaluated by measuring power consumption under various conditions. Further analysis of the KNN method in Mirai Botnet detection demonstrated its superior energy efficiency, consistently consuming less energy (below 1.5 J) than SVM, which exhibited significant energy fluctuations.
3. **Latency**: The impact of security protocols on network latency was another critical metric. This aligns with the processing time analysis of KNN and SVM methods, where KNN showed lower processing times, making it more suitable for real-time applications.
4. **Battery Life**: Extending battery life through energy-efficient security measures is crucial for battery-powered IoT devices. This result is supported by the energy consumption analysis, where the lower energy demands of KNN directly contribute to prolonged battery life.
5. **Scalability**: The scalability of the proposed solutions was tested by deploying them in large-scale 6G networks with high device density. The scalability is further emphasised by the robust performance of both SVM and KNN classifiers in detecting various IoT attacks across different network scales.

These performance evaluations underscore the benefits of enhanced security and energy efficiency that the proposed solutions offer. The findings provide a strong foundation for implementing energy-efficient security measures in real-world 6G-enabled IoT networks, highlighting their potential to address critical challenges in next-generation communication systems.

7.2. Comparative performance and energy efficiency analysis

The proposed Mirai Botnet detection mechanism demonstrated a balance between detection accuracy and energy efficiency, essential for real-world applications. Specifically, the KNN classifier exhibited higher energy efficiency, making it more suitable for deployment in energy-constrained environments like IoT networks. Despite the SVM's higher processing time and energy consumption, it consistently provided robust detection performance, making it ideal for scenarios where energy constraints are less critical.

ROC curve analysis showed near-perfect detection capabilities, with both SVM and KNN classifiers achieving AUC values exceeding 0.99%. This indicates their effectiveness in distinguishing between normal and malicious traffic, which is crucial for securing 6G-enabled smart devices against sophisticated cyber threats like the Mirai Botnet.

Furthermore, the energy consumption comparison highlights the importance of selecting security mechanisms that balance computational overhead with energy efficiency. KNN's lower and more stable energy usage pattern suggests it could be a more sustainable choice for long-term deployments, particularly in environments where power consumption is a key concern.

While this study used a localised testbed for proof-of-concept validation, the same detection pipeline can be integrated into large-scale IoT networks. The ML classifiers can be trained centrally and deployed on edge gateways for distributed detection. Given that the energy profiling is based on generic device-level parameters (voltage, current, and packet rate), the framework is independent of the underlying hardware type, thus allowing it to generalise across various IoT platforms in future large-scale trials.

7.3. Dynamic energy profiling and source configuration

To substantiate the comparative evaluation, a detailed dynamic energy profiling study was conducted to examine the power efficiency of the proposed detection framework under different operational states. The objective was to capture realistic variations in power draw across passive and active security phases, with all measurements normalised over 10-second intervals for consistency. The corresponding mean power and energy values for each mode are presented in Table 3.

Table 3
Average energy consumption across operational modes (per 10-second measurement window).

Operational mode	Average power (mW)	Energy consumption (J)
Idle mode	150	1.50
Attack only (No detection)	200	2.00
Detection + Attack	230	2.30

- **Idle Mode:** The device remained powered and network-connected while all encryption, decryption, and detection processes were inactive. This baseline condition represents the static energy expenditure required to maintain essential background operations and connectivity, averaging approximately 150 mW (1.5 J per interval).
- **Attack Only (Without Detection):** In this state, the IoT node was subjected to Mirai-based flooding and reconnaissance traffic, while the detection mechanism was disabled. The resulting energy increases to around 200 mW (2.0 J per interval), reflecting the additional power drawn by attack-related packet handling and network congestion.
- **Detection (Under Attack):** Both the detection algorithm and the simulated attacks operated concurrently. This mode captures the incremental energy cost introduced by the defence mechanism, which averaged about 230 mW (2.3 J per interval), a modest increase of roughly 15% compared with the attack-only case. These results demonstrate that the proposed framework achieves effective threat mitigation with minimal energy overhead, validating its suitability for resource-constrained IoT deployments.

Energy Source and Measurement:

All experiments were conducted using battery-powered IoT devices, specifically the Raspberry Pi 4 and Arduino Nano 33 BLE. Each device was powered by a regulated **5 V DC** supply, with an average current draw ranging from 30–45 **mA** depending on the operational mode (idle, attack, or detection). Power consumption was monitored using a USB digital power analyser that recorded real-time voltage and current fluctuations. The instantaneous power was integrated over time to compute the total energy consumption as:

$$E = \int_0^T V(t) \cdot I(t)\, dt, \tag{13}$$

where T represents a single measurement interval of 10 s. All energy values were normalised per interval to ensure consistency and comparability across experimental runs.

Therefore, Table 3 summarises the mean energy consumption observed across the three operational modes over a 10-second measurement window. The results show that activating the detection mechanism increases the energy consumption from approximately 2.0 J (attack only) to 2.3 J (detection + attack), representing a modest rise of about 15%. This confirms that the additional computational cost introduced by the detection process is minimal and well within the energy budget of low-power IoT devices. These findings highlight the lightweight and energy-efficient design of the proposed framework, validating its suitability for real-time deployment in resource-constrained 6G-enabled IoT environments.

7.4. Real-world applications and deployment scenarios

The proposed security solutions offer broad applicability across real-world scenarios, enhancing both security and energy efficiency. In smart cities, adaptive security algorithms protect data integrity while minimising energy consumption, ensuring long-term device operation. For autonomous vehicles, energy-efficient intrusion detection systems secure communications without draining battery power, preserving safety and efficiency. In healthcare, energy-aware algorithms safeguard patient data in 6G-enabled applications while ensuring device reliability. In industrial automation, integrating energy-harvesting technologies into security systems provides continuous protection, improving sustainability. Overall, these mechanisms balance threat detection with energy efficiency, making them ideal for the next generation of communication networks.

To illustrate potential deployment scenarios, Table 4 summarises practical use cases, corresponding threats, detection integration points, and indicative detection latency and energy budgets.

This table highlights the flexibility and scalability of the proposed detection framework across diverse IoT applications, demonstrating its potential for efficient deployment in future 6G-enabled ecosystems.

8. Conclusion and future developments

In conclusion, this study explores the critical realm of secure 6G-enabled IoT wireless communication systems, addressing key challenges such as security vulnerabilities and energy consumption. By proposing innovative solutions to enhance the security of smart devices, alongside energy-efficient security algorithms, this research highlights their effectiveness in fortifying 6G-enabled IoT networks without compromising energy efficiency. The study advocates adopting robust security practices tailored to safeguard against evolving threats, e.g., Mirai attacks, while meeting escalating energy demands in wireless communication networks. Furthermore, the integration of lightweight monitoring techniques and ML algorithms, exemplified in the proposed Mirai Botnet detection mechanism, demonstrates substantial promise in enhancing security and sustainability in 6G technology deployments. Our study compared two ML algorithms, SVM and KNN, to evaluate their effectiveness in detecting Mirai attacks in IoT systems. Additionally, we examined the energy consumption of each algorithm during the detection process. The results indicate that KNN provides reliable detection of Mirai attacks exceeding 99% while consuming less energy compared to SVM. Notably, KNN generally outperforms SVM across most attack types, with a marginal difference observed for SYN Flood, where SVM achieves slightly higher accuracy. These findings advocate for a holistic approach to advancing secure and energy-efficient communication networks, which are pivotal for the future resilience of intelligent cities, smart homes, and Industry 4.0 environments.

8.1. Limitations and future work

While the proposed mechanism demonstrates high accuracy and energy efficiency in detecting Mirai botnet attacks, several limitations should be acknowledged. First, the current experiments were conducted on a small-scale testbed using Raspberry Pi devices, which may not capture the complexity of large-scale or heterogeneous 6G IoT deployments. Second, the model was primarily evaluated against Mirai-type attacks; extending its adaptability to other malware families (e.g., Hajime, Mozi, or IoT-Reaper) will be an important next step. Third, although the training and deployment efficiency of the KNN and SVM models is acceptable for edge environments, retraining at scale or with evolving traffic patterns may require additional optimisation. Additionally, the temperature variation of IoT devices during Mirai infection was not directly measured in the present setup; this factor has been explicitly acknowledged as a limitation, as sustained CPU load and power draw could induce thermal stress and hardware degradation over time.

Future work will extend this study to multi-node 6G testbeds and virtualised IoT environments to validate scalability and real-world performance under diverse network conditions. Moreover, we plan to integrate online or incremental learning frameworks to enable adaptive updates and enhance resilience against adversarial attacks. We will explore TinyML techniques to enable on-device inference with minimal energy consumption, and investigate federated deployment

Table 4
Deployment scenarios for the proposed detection mechanism in 6G-enabled IoT environments.

Use case	Threat	Proposed detection integration	Detection latency	Energy budget
Smart grid	Mirai/DDoS	Edge gateway IDS using KNN	3–4 ms	<1.5 J
Smart healthcare	IoT malware (Mirai variant)	On-device TinyML agent	2–3 ms	<1.2 J
Autonomous vehicles	Network flooding/Spoofing	Vehicular edge node	4–5 ms	<1.8 J
Industrial IoT	Mirai/Mozi Botnets	Fog-layer federated IDS	3–4 ms	<1.6 J
Smart cities	Multi-botnet DDoS	Hybrid edge-cloud detection	3–4 ms	<1.4 J

strategies to support distributed learning while preserving privacy. Large-scale validation through simulated 6G environments and comprehensive benchmarking across diverse attack categories will also be pursued.

CRediT authorship contribution statement

Zainab Alwaisi: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Resources, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Tanesh Kumar:** Writing – review & editing. **Simone Soderi:** Writing – review & editing.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

Ahmad, I., Rodriguez, F., Huusko, J., Seppänen, K., 2023. On the dependability of 6G networks. Electronics 12 (6), 1472.

Akyildiz, I.F., Kak, A., Nie, S.-C., 2020. 6G vision: Driving the evolution toward smarter and more sustainable networks. Comput. Netw. 179, 107377.

Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I., Guizani, M., 2020. A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Commun. Surv. Tutor. 22 (3), 1646–1685.

Alwaisi, Z., Kumar, T., Harjula, E., Soderi, S., 2024. Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention. Internet Things 28, 101398.

Alwaisi, Z., Soderi, S., 2024. Towards robust IoT defense: Comparative statistics of attack detection in resource-constrained scenarios. arXiv preprint arXiv:2410.07810.

Alwaisi, Z., Soderi, S., Nicola, R., 2023. Energy cyber attacks to smart healthcare devices: A testbed. p. 246.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., et al., 2017. Understanding the mirai botnet. In: 26th USENIX Security Symposium. USENIX Security 17, pp. 1093–1110.

Antonini, M., Rossi, D., Ciuonzo, D., Pescape, A., 2023. TinyML-based anomaly detection for IoT devices: An edge intelligence approach. In: Proceedings of the IEEE International Conference on Internet of Things. IThings, IEEE, pp. 145–152.

Belarbi, Y., Abdellaoui, A., Ali, I., Khelifi, A., 2023. Federated deep learning for IoT intrusion detection: Privacy-preserving and scalable approach. IEEE Internet Things J. 10 (14), 12430–12442.

Bishop, C.M., 2006. Pattern Recognition and Machine Learning. Springer.

Chen, X., Lei, L., 2013. Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee. IEEE Commun. Lett. 17 (4), 637–640.

David, H., Fallin, C., Gorbatov, E., Hanebutte, U.R., Mutlu, O., 2011. Memory power management via dynamic voltage/frequency scaling. In: Proceedings of the 8th ACM International Conference on Autonomic Computing. pp. 31–40.

Dhumal, A.R., Kulkarni, A.P., Ambhore, N.H., 2023. A comprehensive review on thermal management of electronic devices. J. Eng. Appl. Sci. 70 (1), 140.

Elahi, H., Munir, K., Eugeni, M., Atek, S., Gaudenzi, P., 2020. Energy harvesting towards self-powered IoT devices. Energies 13 (21), 5528.

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 Things J. 7 (8), 6882–6897.

Fusco, L., Pagliari, D., Bianchi, G., Rossi, D., 2024. TinyIDS: A tinyml-based intrusion detection system for resource-constrained IoT devices. IEEE Internet Things J. 11 (8), 13245–13257.

Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., Zorzi, M., 2020a. Toward 6G networks: Use cases and technologies. IEEE Commun. Mag. 58 (3), 55–61. http://dx.doi.org/10.1109/MCOM.001.1900411.

Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., Zorzi, M., 2020b. Toward 6G networks: Use cases and technologies. IEEE Commun. Mag. 58 (3), 55–61.

HaddadPajouh, H., Dehghantanha, A., Khayami, R., Choo, K.-K.R., 2018. A deep recurrent neural network based approach for internet of things malware threat hunting. Future Gener. Comput. Syst. 85, 88–96.

Han, S., Xie, T., Chih-Lin, I., 2021. Greener physical layer technologies for 6G mobile communications. IEEE Commun. Mag. 59 (4), 68–74.

Hoang, V.-T., Ergu, Y.A., Nguyen, V.-L., Chang, R.-G., 2024. Security risks and countermeasures of adversarial attacks on AI-driven applications in 6G networks: A survey. J. Netw. Comput. Appl. 104031.

Hussain, F., Awan, K., Ali, Z., et al., 2022. 6G: Enabling technologies for future wireless communication systems. IEEE Access 10, 52660–52692.

Ioannou, C., Vassiliou, V., 2021. Network attack classification in IoT using support vector machines. J. Sens. Actuator Netw. 10 (3), 58.

Jaafar, F., Al-Homoud, A., Awad, A., 2021a. IoT botnet detection through device-level energy and CPU profiling. IEEE Access 9, 165432–165445.

Jaafar, F., Ameyed, D., Barrak, A., Cheriet, M., 2021b. Identification of compromised IoT devices: Combined approach based on energy consumption and network traffic analysis. In: 2021 IEEE 21st International Conference on Software Quality, Reliability and Security. QRS, IEEE, pp. 514–523.

Jaafar, F., Rahman, M., Alenezi, F., 2023. IoT device energy consumption analysis under Mirai malware infection. Sensors 23 (7), 3552.

Jiang, Y., Zou, Y., Ouyang, J., Zhu, J., 2018. Secrecy energy efficiency optimization for artificial noise aided physical-layer security in OFDM-based cognitive radio networks. IEEE Trans. Veh. Technol. 67 (12), 11858–11872.

Kazmi, S.H.A., Hassan, R., Qamar, F., Nisar, K., Ibrahim, A.A.A., 2023. Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions. Symmetry 15 (6), 1147.

Mahadik, S.S., Pawar, P.M., Raja, M., Mantri, D., Prasad, N.R., Kulkarni, N.P., Intelligent security for DDoS in HetIoT (6G perspective). 6G Connectivity-Systems, Technologies, and Applications. River Publishers. 1–15.

Margolis, J., Oh, T.T., Jadhav, S., Kim, Y.H., Kim, J.N., 2017. An in-depth analysis of the mirai botnet. In: 2017 International Conference on Software Security and Assurance. ICSSA, IEEE, pp. 6–12.

Memos, V.A., Psannis, K.E., Lv, Z., 2022. A secure network model against bot attacks in edge-enabled industrial internet of things. IEEE Trans. Ind. Inform. 18 (11), 7998–8006.

Mitev, M., Chorti, A., Poor, H.V., Fettweis, G.P., 2023. What physical layer security can do for 6G security. IEEE Open J. Veh. Technol. 4, 375–388.

Mujaddidi, G.F., 2013. Suicide attacks in afghanistan: Why now?

Namrita Gummadi, A., Abdelrahim, E.M., Gad, I., Abdallah, M., 2025. E-RXAI-IoT: A systematic evaluation framework of rule-based XAI methods for anomaly detection in IoT systems. IEEE Access 13, 188730–188754. http://dx.doi.org/10.1109/ACCESS.2025.3627529.

Porambage, P., Gür, G., Osorio, D.P.M., Liyanage, M., Gurtov, A., Ylianttila, M., 2021. The roadmap to 6G security and privacy. IEEE Open J. Commun. Soc. 2, 1094–1122.

Pureti, N., 2020. Implementing multi-factor authentication (MFA) to enhance security. Int. J. Mach. Learn. Res. Cybersecur. Artif. Intell. 11 (1), 15–29.

Qadir, Z., Le, K.N., Saeed, N., Munawar, H.S., 2023. Towards 6G internet of things: Recent advances, use cases, and open challenges. ICT Express 9 (3), 296–312.

Qiu, H., Dong, T., Zhang, T., Lu, J., Memmi, G., Qiu, M., 2020. Adversarial attacks against network intrusion detection in IoT systems. IEEE Internet Things J. 8 (13), 10327–10335.

Qiu, H., Dong, T., Zhang, T., Lu, J., Memmi, G., Qiu, M., 2021. Adversarial attacks against network intrusion detection in IoT systems. IEEE Internet Things J. 8 (13), 10327–10335. http://dx.doi.org/10.1109/JIOT.2020.3048038.

Rathore, S., Park, J.H., 2018. Semi-supervised learning based distributed attack detection framework for IoT. Appl. Soft Comput. 72, 79–89.

Sarieddeen, H., Alouini, M.-S., Al-Naffouri, T.Y., 2020. An overview of signal processing techniques for terahertz communications. Proc. IEEE 108 (10), 1827–1848.

Siriwardhana, Y., Porambage, P., Liyanage, M., Ylianttila, M., 2021. AI and 6G security: Opportunities and challenges. In: 2021 Joint European Conference on Networks and Communications & 6G Summit. EuCNC/6G Summit, IEEE, pp. 616–621.

Slimani, K., Khoulji, S., Kerkeb, M.L., 2023. Advancements and challenges in energy-efficient 6G mobile communication network. In: E3S Web of Conferences. Vol. 412, EDP Sciences, p. 01036.

Tushir, R., Gupta, P., Singh, R., 2023. Energy-aware security analysis of Mirai botnet attacks on IoT devices. IEEE Internet Things J. 10 (18), 16345–16356.

Tushir, B., Sehgal, H., Nair, R., Dezfouli, B., Liu, Y., 2021. The impact of dos attacks onresource-constrained iot devices: A study on the mirai attack. arXiv preprint arXiv:2104.09041.

Tushir, N., Singh, R., Bhatnagar, V., 2022. Analyzing the energy footprint of Mirai botnet attacks on embedded IoT hardware. J. Netw. Comput. Appl. 210, 103485.

Waisi, A., Ali, Z., 2023. Optimized monitoring and detection of internet of things resources-constraints cyber attacks.

Wang, D., Bai, B., Chen, W., Han, Z., 2015. Achieving high energy efficiency and physical-layer security in AF relaying. IEEE Trans. Wirel. Commun. 15 (1), 740–752.

Wei, Z., Masouros, C., Liu, F., Chatzinotas, S., Ottersten, B., 2020. Energy-and cost-efficient physical layer security in the era of IoT: The role of interference. IEEE Commun. Mag. 58 (4), 81–87.

Whitter-Jones, J., 2018. Security review on the internet of things. In: 2018 Third International Conference on Fog and Mobile Edge Computing. FMEC, IEEE, pp. 163–168.

Zhang, Y., Liu, W., Zhu, T., 2026. MOAT: Federated learning-based method for improved detection of IoT botnets. IEEE Internet Things J. 13 (2), 3082–3093. http://dx.doi.org/10.1109/JIOT.2025.3631450.

Zainab Alwaisi received her Bachelor's and Master's degrees in Software Engineering from the University of Northampton, UK, in 2016 and 2017, respectively, and her Ph.D. in Computer Science and Systems Engineering in 2023 from IMT School for Advanced Studies in Lucca, Italy. Since July 2023, she has been a research collaborator in cybersecurity at IMT School for Advanced Studies, focusing on securing IoT systems and smart devices, and addressing resource constraints through lightweight detection mechanisms. She also worked as a postdoctoral researcher at IIT-CNR Pisa. She is currently a researcher at the Huawei Research Center, where her work continues to focus on advanced cybersecurity solutions. Her research interests include applying TinyML techniques to enhance protection against cyberattacks and advancing 6G security frameworks.

Tanesh Kumar (Member, IEEE) is currently working as a Staff Scientist in the School of Electrical Engineering at Aalto University, Finland. He received the D.Sc. degree in communications engineering from the University of Oulu, Finland, in 2020, the M.Sc. degree in computer science from South Asian University, New Delhi, India, in 2014, and the B.E. degree in computer engineering from the National University of Sciences and Technology (EME), Pakistan, in 2012. Previously he has worked as a postdoctoral researcher and project manager at CWC-NS, University of Oulu (2021–2023). He has co-authored over 40 peer-reviewed scientific articles. His current research interests include IoT security, privacy and trust, 5G/6G, Edge-AI, Blockchain/DLTs, and Wireless Communication.

Simone Soderi (SMIEEE) received his M.Sc. degree in 2002 from the University of Florence and his Dr.Sc. Degree in 2016 from the University of Oulu, Finland. His expertise ranges from cybersecurity and wireless communications to embedded systems. He is currently an Assistant Professor at the IMT School for Advanced Studies in Lucca, Italy, and an Adjunct Professor at the University of Padua, Italy, where he teaches in the master's degree program in cybersecurity. His research topics include cybersecurity for critical infrastructure systems, 6G, covert channels, network security, physical layer security, electromagnetic emission security, VLC, and UWB. He has been a TPC member of several conferences and served as a reviewer of many IEEE Transactions. Dr. Soderi has published journal and conference papers and book chapters. He holds five patents on wireless communications and positioning.