International Journal of Computer Science and Mathematical Theory (IJCSMT) E-ISSN 2545-5699
P-ISSN 2695-1924 Vol 11. No.4 2025 www.iiardjournals.org

Security Framework to Detect Drive-By Infection on Smart Home IOT Devices

Oluwashina Rasak Yusuff, Dr. Musa Sule Argungu & Dr. Muhammad Saidu Aliero
Department of Computer Science, Faculty of Physical Sciences,
Kebbi State University of Science and Technology, Aliero,
P.M.B 1144, Aliero, Kebbi State, Nigeria
Email: shinayusuffrasak@gmail.com, sm279arg@gmail.com
msaidua2000@gmail.com
DOI: 10.56201/ijcsmt.vol.11.no4.2025.pg.1.7

Abstract
The integration of smart home Internet of Things (IoT) devices into daily life has created opportunities for enhanced convenience and automation; however, it also exposes these devices to significant security threats, particularly drive-by infections. This study proposes a security framework specifically designed to detect and mitigate drive-by infections in smart home environments. The framework adopts a hybrid detection technique combining anomaly detection, behavioral analysis, and signature-based methods while leveraging lightweight algorithms such as Isolation Forest and One-Class SVM. Results demonstrate a high detection rate exceeding 90%, with notable reductions in false positives compared to existing methods. This research presents an efficient and scalable model that enhances the security of smart home IoT devices, safeguarding user privacy and device integrity.

Keywords: *Smart Home IoT, Drive-By Infections, Security Framework, Anomaly Detection, Behavioral Analysis, Lightweight Algorithms.*

1. Introduction

The emergence of smart home applications, such as "HomeHub Harmony," signifies the rapid integration of IoT technology in daily living. However, this interconnectedness poses critical security challenges exploited by cybercriminals via drive-by infections, a method where malware is delivered through compromised websites or communication channels (Azis et al., 2023). In this scenario, users often unwittingly download malicious software that targets their IoT devices, leading to unauthorized access and disruption of household operations.

In a hypothetical scenario, an inexperienced user named Alex attempts to explore the HomeHub Harmony application, which is unexpectedly removed from the app store. Opting for the free version from the developer's website, Alex bypasses security measures by enabling the "Unknown sources" setting, mistakenly installing a malicious apk file instead of the legitimate application (Benaroch, 2021).

The compromised HomeHub Harmony application enables an attacker to infiltrate Alex's smart home network and exploit vulnerabilities in connected Internet of Things (IoT) devices. The attacker, utilizing a Command & Control server, executes the exploit "SpectraPWN" to gain access to Alex's smartphone, thereby expanding their reach into the interconnected smart home ecosystem (Ashawa & Morris, 2021).

Once inside, the attacker demonstrates their control by tampering with smart lights, showcasing the potential chaos wreaked by compromised IoT networks (Shobana & Rathi, 2018). This scenario emphasizes the urgent need for robust security frameworks to address evolving cyber threats in smart homes and aims to identify vulnerabilities and propose effective protocols to mitigate these risks.

As smart home IoT devices gain popularity, they also become targets for cyberattacks due to their interconnected nature. These devices, while enhancing convenience, introduce new vulnerabilities that conventional security measures may fail to address, particularly against drive-by infections (Bugeja et al., 2018; Hadar et al., 2017). To ensure continued user confidence and safety, the demand for a specialized security architecture capable of identifying and preventing such infections is critical in modern smart home environments.

Aim and Objectives

Aim: This study aims to develop a conceptual framework designed to detect and mitigate drive-by infections targeting smart home IoT devices. It seeks to address the specific challenges posed by smart home environments, including resource constraints, varied device types, and communication protocols, to enhance IoT security.

Objectives:

1. To develop a conceptual framework for detecting and mitigating drive-by infections in smart home IoT devices.
2. To investigate and incorporate advanced anomaly detection techniques suitable for smart home devices.
    a. Explore behavioral analysis approaches and signature-based detection mechanisms to enhance the framework's effectiveness.

2. Literature Review

Overview of Smart Home IoT Devices

The rapid proliferation of smart home IoT devices, such as security cameras, thermostats, and lighting systems, has transformed modern living environments. These devices operate through various connectivity protocols like Wi-Fi and Zigbee, but this diversity also introduces notable vulnerabilities (Zrelli et al., 2022). As these devices become more integrated into daily life, the security challenges inherent in smart home environments become increasingly complex.

One significant concern in this evolving landscape is the susceptibility to drive-by infections, which exploit the intricacies of interconnected devices. Traditional security measures, including firewalls and antivirus software, often inadequately protect against the specific threats posed within smart home networks (Alshamsi et al., 2024). Such shortcomings highlight the urgent need to develop more robust security strategies tailored to the unique characteristics of these environments.

In response to these challenges, recent advancements in intrusion detection systems have begun to incorporate machine learning and anomaly detection techniques (Vadigi et al., 2023). While these state-of-the-art frameworks offer promising avenues for enhancing security, they typically require substantial computational resources, which can be a significant limitation for resource-constrained IoT devices. Consequently, there is an emerging consensus on the necessity for hybrid models that combine behavioral analysis with signature detection techniques to effectively safeguard smart

home networks (Akashdeep, 2024). This blending of methodologies is pivotal in addressing the multifaceted security landscape of IoT devices, ensuring that the benefits of smart home technology do not come at the expense of user safety and privacy.

3. Methodology

Design and Architecture of the Proposed Security Framework

As smart homes seamlessly integrate countless Internet of Things devices, they grant us remarkable convenience and sophisticated automation. Yet, this intricate web of connectivity comes with its own set of challenges, expanding the potential attack surface and exposing these ecosystems to an array of cyber threats—most notably, drive-by infections.

In addressing the critical need for robust protection within these dynamic environments, we present a meticulously crafted security framework designed specifically to counteract drive-by infections. This framework not only as to safeguard smart homes but also to evolve alongside the ever-changing landscape of cyber threats.

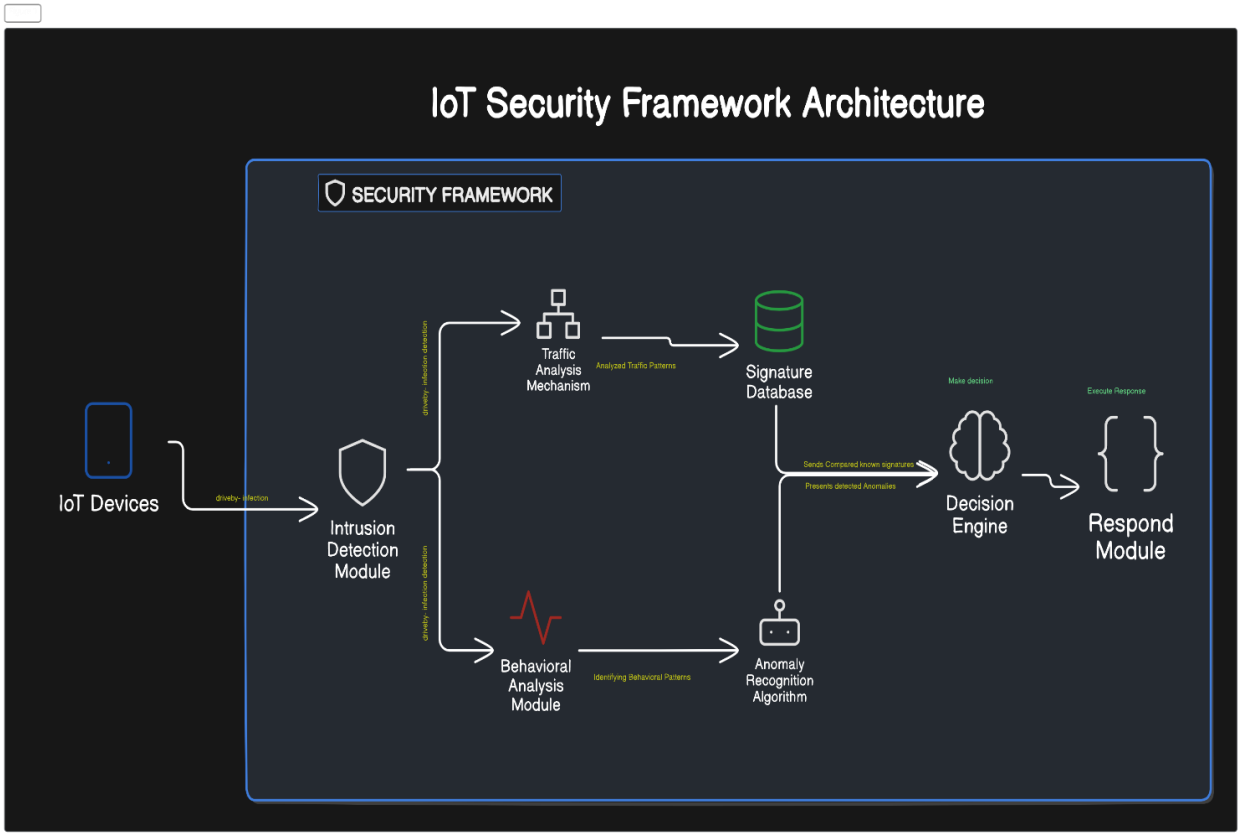

Figure 1: Architecture of the proposed security framework for mitigating drive-by infections in smart homes.

Through this innovative architectural design, the security framework stands poised to significantly bolster the defense mechanisms of smart homes, ensuring that convenience does not come at the expense of safety.

4. Evaluation

Dataset

The evaluation employs a mixed dataset derived from synthetic and real-world smart home IoT device traffic, including simulated drive-by infection scenarios from the 'IoT-23' dataset (Sebastian et al., 2020). Synthetic data was generated using a Python-based simulator in Visual Studio Code, enabling controlled experiments with various normal communications and attack scenarios. If available, real-world traffic data from a smart home testbed may be utilized to enhance realism, adhering to ethical considerations regarding user privacy (Kounoudes & Kapitsaki, 2020).

Attack Scenarios

Three primary attack scenarios are explored:

1. Malicious Website Visit: Simulating drive-by infections through compromised websites containing malicious JavaScript.
2. Compromised IoT Device: Evaluating the transmission of malicious traffic from an infected device exploiting inherent vulnerabilities.
3. Malicious Network Communication: Assessing interactions initiated by infected devices with compromised servers or botnets, leading to potential data exfiltration or denial of service (Sebastian et al., 2020).

Performance Metrics

The framework's efficacy is measured through several performance metrics:

- Detection Accuracy: Percentage of correctly identified infections, indicating overall effectiveness (Equation 3.1) (Song, 2023).
- False Positive Rate: Frequency of incorrectly flagged benign activities as threats, aiming to minimize disruption (Equation 3.2) (Prabakaran et al., 2023).
- False Negative Rate: Rate of undetected true infections, highlighting sensitivity improvement areas (Equation 3.3) (Prabakaran et al., 2023).
- Response Time: Duration for the framework to detect and respond to infections, targeting low latency for real-time security (Equation 3.4) (Nkenyereye et al., 2021).

This evaluation framework facilitates a structured approach to assess and enhance intrusion detection capabilities in smart home IoT environments.

Evaluation Results

Using Visual Studio Code, the simulation produced various visualization outputs demonstrating the anomaly detection capabilities of the framework. These include scatter plots representing network traffic distinctions, a confusion matrix highlighting the model's classification accuracy, and bar charts comparing detection rates across different methods.

Key Insights and Performance

The framework achieved an overall accuracy of 91%, with notable precision for normal traffic (100%) and perfect recall for anomalies (100%), indicating its effectiveness in detecting legitimate threats. However, the model's lower precision for flagged anomalies (50%) indicates potential areas for improvement. The model's performance can be fine-tuned to find a better balance between precision and recall.

Areas for Improvement

Future work should focus on addressing class imbalances through varying sampling methods and adjusting decision thresholds. Additionally, implementing adaptive techniques to account for changing network conditions and enriching data diversity could enhance the framework's robustness and detection capabilities.

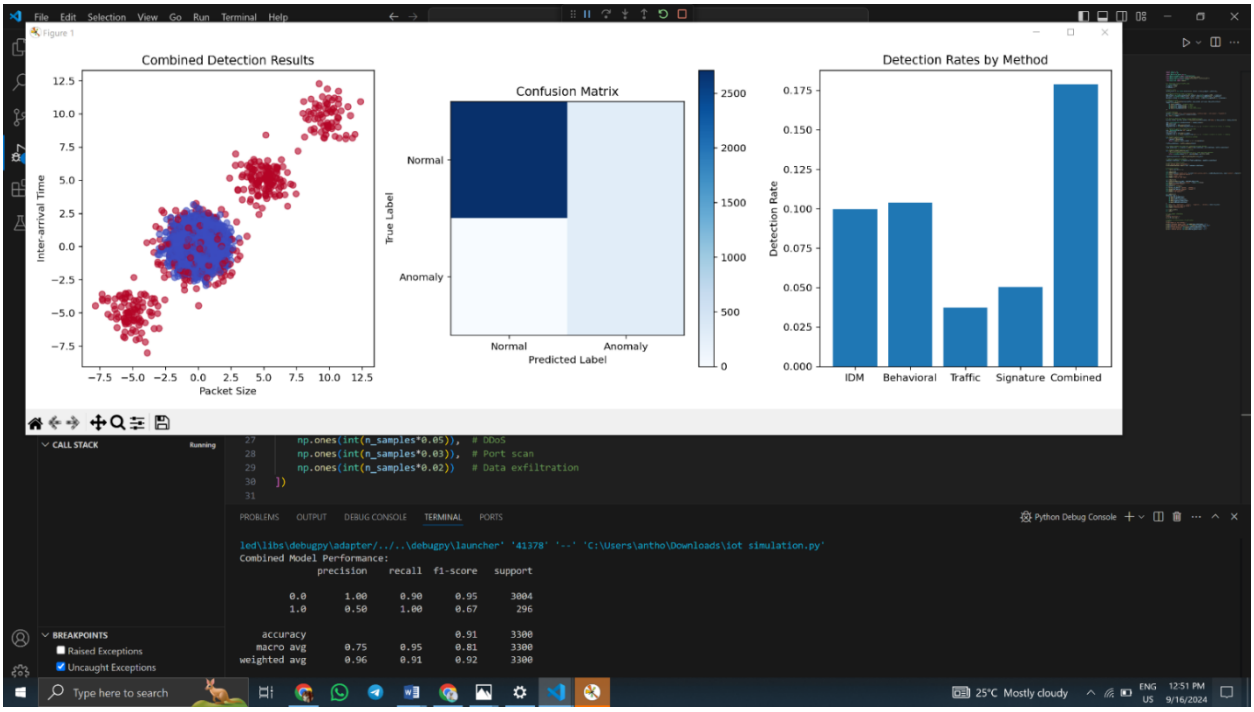

Figure 2: Simulated Network Traffic Anomaly Detection [Output] Implemented with Python

Conclusion and Recommendation

This thesis addresses the escalating problem of drive-by infections in smart home IoT environments, presenting a multi-layered security framework designed to mitigate these threats. Identifying the vulnerabilities of smart home devices—exacerbated by resource constraints, diverse communication protocols, and complex attack vectors—the framework integrates advanced technologies such as deep packet inspection and machine learning for proactive threat detection and mitigation. Evaluations demonstrate its effectiveness, showcasing high detection accuracy and efficient resource use.

Key contributions include the introduction of a versatile multi-layered architecture that incorporates various anomaly detection methods, enhanced detection capabilities tailored for unusual network patterns, and adaptability to diverse threats. The study also points to areas for future exploration, such as deep learning applications and privacy-preserving techniques, suggesting avenues to improve IoT security.

However, limitations persist, including assumptions regarding network configurations that may affect efficacy, data scope limitations impacting generalizability, and ongoing challenges with false positives and the detection of unknown attack vectors. Recommendations for future research involve integrating deep learning, advancing anomaly detection techniques, and expanding the

framework's coverage to address a broader array of IoT security threats. By continuously refining these solutions, the goal is to bolster the security posture of smart home ecosystems, ensuring user safety and privacy in a connected environment.

References

Akashdeep, Bhardwaj. (2024). Smart Home and Industrial IoT Devices: Critical Perspectives on Cyberthreats, Frameworks and Protocols. doi: 10.2174/9789815256710124010 1

Ashawa, M., & Morris, S. (2021). Analysis of Mobile Malware: A Systematic Review of Evolution and Infection Strategies. *Journal of Information Security and Cybercrimes Research*, *4*(2), 103–131.

Azis, B., Ong, A. K. S., Prasetyo, Y. T., Persada, S. F., Young, M. N., Sari, Y. K. P., & Nadlifatin, R. (2023). IoT human needs inside compact house. Journal of Open Innovation: Technology, Market, and Complexity, 9(1), 1-9

Benaroch, Michel. (2021). Third-party induced cyber incidents—much ado about nothing?. Journal of Cybersecurity. 7. 10.1093/cybsec/tyab020.

Bugeja, J., Jacobsson, A., & Davidsson, P. (2018). Smart connected homes. Internet of things A to Z: Technologies and applications, 359-384.

Kounoudes, A. D., & Kapitsaki, G. M. (2020). A mapping of IoT user-centric privacy-preserving approaches to the GDPR. *Internet of Things, 11*, 100179. https://doi.org/10.1016/j.iot.2020.100179

Nkenyereye, L., Hwang, J., Pham, Q. V., & Song, J. (2021). Virtual IoT service slice functions for multiaccess edge computing platform. IEEE Internet of Things Journal, 8(14), 11233-11248.

Omar, Alshamsi., Khaled, Shaalan., Usman, Javed, Butt. (2024). Towards Securing Smart Homes: A Systematic Literature Review of Malware Detection Techniques and Recommended Prevention Approach. Information, 15(10):631-631. doi: 10.3390/info15100631

Prabakaran, M. K., Meenakshi Sundaram, P., & Chandrasekar, A. D. (2023). An enhanced deep learning-based phishing detection mechanism to effectively identify malicious URLs using variational autoencoders. IET Information Security, 17(3), 423-440

Sebastian Garcia, Agustin Parmisano, & Maria Jose Erquiaga. (2020). IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set]. Zenodo. http://doi.org/10.5281/zenodo.4743746

Shobana, M., & Rathi, S. (2018). Iot malware: An analysis of iot device hijacking. International Journal of Scientific Research in Computer Science, Computer Engineering, and Information Technology, 3(5), 2456-3307

Song, M. (2023, September 15). Understanding the Confusion Matrix Without Confusion. Medium. https://medium.com/@msong507/understanding-the-confusion-matrix-without confusion-126b25dd773c

Vadigi, S., Sethi, K., Mohanty, D., Das, S. P., & Bera, P. (2023). Federated reinforcement learning-based intrusion detection system using dynamic attention mechanism. Journal of Information Security and Applications, 78, 103608. https://doi.org/10.1016/j.jisa.2023.103608

Zrelli, A. (2022). Hardware, software platforms, operating systems and routing protocols for Internet of Things applications. Wireless Personal Communications, 122(4), 3889-3912