International Journal of Cloud Applications and Computing
Volume 14 • Issue 1

Using Supervised Learning to Detect Command and Control Attacks in IoT

Muath AlShaikh, Saudi Electronic University, Saudi Arabia*
https://orcid.org/0000-0001-5550-7659

Waleed Alsemaih, Saudi Electronic University, Saudi Arabia

Sultan Alamri, Saudi Electronic University, Saudi Arabia

Qusai Ramadan, University of Koblenz, Germany
https://orcid.org/0000-0001-8159-918X

ABSTRACT

The rapid proliferation of internet of things (IoT) devices has ushered in a new era of technological development. However, this growth has also exposed these devices to various cybersecurity risks, including command and control (C&C) attacks. C&C attacks involve unauthorized entities taking control of IoT devices to carry out malicious activities. Traditional cybersecurity measures often fall short in addressing these evolving threats. To enhance IoT security and counter C&C threats, this study explores the potential of supervised learning, a subfield of machine learning. Supervised learning, a method that utilizes past data to train machine learning models capable of independently identifying patterns indicative of C&C threats in real time, offers additional protection to IoT networks. This article delves into the advantages and drawbacks of this approach, considering factors such as the need for well-defined labeled datasets, resource constraints of IoT devices, and ethical considerations surrounding data security.

KEYWORDS

Command and Control (C&C) Attacks, Cyber Threats, Cybersecurity, Internet of Things (IoT), IoT Ecosystems, IoT Security, Security Solutions, Supervised Learning, Threat Detection

INTRODUCTION

Internet of Things (IoT), which connects billions of devices ranging from smart household appliances to industrial sensors, has emerged as a paradigmatic technological shift that promises to revolutionize industries and everyday life (Kara, 2022). IoT device proliferation has contributed to unprecedented efficiency and convenience and ushered in a new age of cybersecurity problems. Command and Control (C&C) assaults are one of these dangers that are particularly serious and constantly changing. C&C attacks entail hostile actors taking control of IoT devices without authorization and using that access to carry out numerous destructive actions (Othman, 2023). These assaults may take many

DOI: 10.4018/IJCAC.334214 *Corresponding Author

forms, such as planning massive botnets for distributed denial-of-service (DDoS) attacks or collecting private information from infected devices. C&C attacks are a focus of IoT security research due to their variety and risk of damage.

Traditional cybersecurity defenses often fall short in the face of C&C criminals' highly developed attack strategies in the IoT environment. This has prompted the investigation of cutting-edge strategies, including machine learning, to improve IoT security. In this situation, supervised learning, machine learning, has shown promise in identifying and thwarting C&C assaults (Cuadra-Sánchez & Aracil, 2015). Leveraging historical data to train machine learning models is the foundation for incorporating supervised learning into IoT security methods. After that, these models can independently recognize patterns and abnormalities suggestive of C&C threats in real-time, adding another layer of security for IoT networks (Atzori et al., 2010). IoT devices' often restricted computational resources, such as little memory and processing power, are one of their distinguishing characteristics (Abuagoub, 2022). Implementing effective security measures is made more difficult by these resource constraints. In contexts with limited resources, it may be difficult for conventional intrusion detection systems to function well, which makes machine learning—with its capacity to utilize data effectively—an appealing option.

There are two stages to the supervised learning process. First, a model is trained using examples of known C&C attacks and typical device behavior from a labeled dataset. The model learns about the distinguishing traits of C&C assaults at this phase. The model is then deployed in a real IoT context to observe device behavior once trained continually. A predetermined warning or reaction is started when the model notices behavior that resembles a C&C attack to lessen the hazard.

Although the combination of supervised learning with IoT security offers an appealing path, it is important to understand both the benefits and constraints of this strategy. The benefits include better threat detection accuracy, reduced likelihood of false positives, and flexibility of machine learning models to change attack techniques. There are obstacles to overcome, such as the need for solid labeled datasets, resource limitations on IoT devices, and ethical issues related to data protection (Ahsan et al., 2022). To identify C&C threats in IoT, this survey study article attempts to review the state of the art in this field thoroughly. The study aims to contribute significantly to the expanding body of knowledge in IoT security by analyzing lessons learned from earlier research and weighing the advantages and disadvantages of current works. Researchers, practitioners, and policymakers working in safeguarding IoT ecosystems are among its target audience members. This will help to create safer and more robust IoT environments for all stakeholders (Cioffi et al., 2020).

This study's synthesis of prior research is one of its main contributions. This survey article compiles a plethora of knowledge and ideas that would otherwise be scattered throughout many academic publications and conference proceedings by methodically analyzing prior research endeavors (Wood & Slhoub, 2022). In addition to helping practitioners and policymakers obtain a comprehensive understanding of the possible solutions and their ramifications, this information consolidation is helpful to researchers looking to delve further into this specialized field. Additionally, the critical assessment of the advantages and disadvantages of previous efforts provides value by illuminating the applicability and efficiency of supervised learning techniques in C&C attack detection. This report provides decision-makers and security experts with invaluable advice on choosing and using security solutions in their IoT implementations. Making judgments about using resources and creating strategies might become more informed as a result (Vitorino et al., 2022).

The fundamental objective of this study is to evaluate the existing methods for detecting and mitigating command and control assaults on Internet of Things devices that are both effective and efficient and are based on supervised learning. To accomplish this objective, the research will concentrate on answering the following research questions:

1. How can supervised learning be used to identify C&C threats in IoT network data, and what are the most important traits to look for?