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?

With supervised learning algorithms, this study tries to determine the most important characteristics of IoT network traffic to identify C&C threats. IoT network parameters, such as traffic type, volume, and device-to-device communication patterns, will guide the feature selection procedure.

2. What is the best-supervised learning algorithms for identifying and protecting against C&C threats on IoT gadgets?

This study aims to evaluate and contrast several supervised learning methods for protecting IoT devices from C&C assaults. Metrics will be used to assess the algorithms' effectiveness, including accuracy, precision, recall, and F1 score.

This study aims to address these issues to shed light on using supervised learning to detect C&C attacks against IoT devices. The results of this study will aid in the ongoing endeavour to strengthen the security of the IoT ecosystem by guiding the creation of new solutions for protecting connected devices.

Several areas of cybersecurity and the IoT ecosystem might benefit from this study of IoT C&C threats and how they can be detected using supervised learning techniques. The study has the potential to significantly contribute to cybersecurity and the IoT ecosystem through supervised learning techniques for detecting or mitigating IoT C&C threats. This study can also pave the way for future studies on the usefulness of supervised learning approaches for IoT security (Laouid, 2018) . Overall, this study has the potential to greatly influence the evolution of IoT security solutions in the future, strengthening the safety and reliability of the IoT ecosystem (Al-Qerem, 2020).

In conclusion, the suggested study offers great promise in boosting the IoT ecosystem's security and resilience through supervised learning techniques for identifying or mitigating IoT C&C threats. In the issue description, we saw that C&C assaults on IoT devices are becoming more commonplace, and in the research questions and goals, we saw that we needed to come up with something new to combat this. The study hypothesis proposes that supervised learning approaches help identify C&C threats on IoT devices, and the research scope has covered many facets of IoT security. Key contributions of this study have been noted in the research contributions/significance section; these include better C&C threat detection and mitigation, increased IoT security, a unique application of supervised learning techniques, a real-world assessment, and generalizability (Fawdur et al., 2022). Overall, the suggested research can pave the way for additional study in this field, leading to a more secure and robust IoT environment by providing useful insights into the efficacy of supervised learning approaches for IoT security.

LITERATURE REVIEW

The survey study paper's part on using supervised learning to recognize or stop C&C attacks against the IoT provides a review of the relevant literature. This section presents a comprehensive examination of the relevant scholarly research and literature. This section's goal is to evaluate the current state of the art for using supervised learning to identify or thwart C&C attacks on IoT devices. This section aims to draw attention to areas that might need further study as well as the gaps and limitations in the data already available. A section termed a literature review, which evaluates past research to provide the groundwork for the inquiry, must be included in every study publication. By reading the available literature, experts may find knowledge gaps, close them, and progress in their field. The analysis of the literature may also reveal the benefits and drawbacks of the preceding research, which might then affect the design and course of the study.

Organization of Literature Review

There are six key components in this literature review. IoT and IoT security are briefly discussed in Part II, along with its architecture, security issues, and potential remedies. C&C assaults in the IoT

are the topic of Part III, which also covers their definition, variations, results, and current methods of detection and avoidance. The definition, methods, benefits, and drawbacks of supervised learning for IoT security are covered in Part IV. The study on applying supervised learning to detect or thwart IoT C&C risks is examined in Part V. This subject includes studies on IoT C&C threat detection and mitigation, method comparisons, a critical analysis of previous research, and research needs. The key results, knowledge gaps, and research implications are broken down in Section VI, along with a synopsis of the literature study.

Overview of IoT C&C Security

Recently, there has been a lot of interest in and acceptance of the IoT, a rapidly expanding network of connected computer devices. It refers to a system in which many components connect and organize their functions online. The application of the IoT in several sectors, including industry, transportation, agriculture, and healthcare, offers immense promise (Yagoub, 2019). However, as it expands, more stringent security precautions are required to avoid potential threats. The IoT architecture is divided into four levels: applications, middleware, networks, and perception. A variety of sensors and data-transmitting devices make up the perception layer. Controlled data transit occurs between the network layer and the application layer (Gupta et al., 2020). The middleware layer stores and handles the data, while the application layer controls the user interface. Effective security measures are thus required to guard against the many risks and vulnerabilities that come along with this increase.

IoT security is limited by both long-standing and new cybersecurity problems, such as device variety, resource limitations, and interoperability problems. One of the main challenges is the lack of proper safety measures. Because many IoT devices lack reliable security measures, they are vulnerable to attacks. The majority of vulnerabilities in traditional devices are caused by their outdated firmware, security protocols, and other precautions. Interoperability issues are also frequent. Devices connected to the IoT often use different communication protocols, which makes it challenging to integrate them into a single network (Tsukerman, 2020). Implementing security measures is more difficult when devices are incompatible with one another. Another barrier is the availability of resources being constrained. Deploying robust security measures may be challenging since many IoT devices have low computing, storage, and battery capabilities.

The enormous diversity of gadgets on the market is yet another serious issue. IoT devices come in a wide variety of form factors and capacities (Gueye et al., 2022). It isn't easy to implement a unified security approach because of the large range of potential devices. Privacy issues provide further challenges. Due to the vast amounts of data that IoT devices gather, users' privacy may be in danger. Because IoT devices collect and store personal data, certain privacy requirements and safeguards are required.

To address these problems there are a number of ways to enhance IoT security. The process of encrypting data to prevent unwanted access is called encryption (Kara a, 2023). The use of encryption in IoT devices may increase the security of data sent via networks. To authenticate anything is to verify that it is indeed genuine. Using strong authentication techniques like two-factor authentication, IoT security may be increased (Kara b,2023). The IoT networks and devices should only be accessible to authorized users. Two examples of access control systems that may be used to increase the security of the IoT are firewalls and access control lists. IoT device security must be strengthened, and vulnerabilities must be fixed with frequent firmware updates. Enabling automated firmware updates may increase the security of IoT devices. Utilizing security guidelines such as ISO 27001 and the NIST cybersecurity architecture may help to increase IoT security. By teaching supervised learning algorithms to examine network data and spot anomalies, C&C threats may be identified and countered. These systems might examine historical data to find abnormalities that would indicate a live cyberattack (Gangolli et al., 2022).

A C&C attack involves the attacker seizing control of an IoT device and using it for further assaults or evil activities. Through the analysis of network data and the search for irregularities,

supervised learning algorithms may be trained to recognize and stop C&C threats. Random forest, decision trees, and support vector machines (SVMs) are a few examples of these techniques. These algorithms may spot patterns since they are learning from the prior data, which may indicate an ongoing attack. SVMs may, for instance, divide network traffic into various categories like "regular" and "C&C attack" traffic. For example, a C&C attack has been located. Averting communication with the attacker's IP address or removing the infected device from the network are two safeguards that may be implemented in such a scenario. The most often compromised gadgets are shown in the following graph (Figure 1), along with their benefits (Hodge et al., 2019).

C&C Attacks in IoT

We now engage with electrical gadgets differently thanks to the IoT, which has also given fraudsters new access points. Attacks using C&C are common with the IoT. A compromised computer (bot) contacts an external adversary for malicious instructions in C&C attacks. C&C attacks include ransomware, data exfiltration, and distributed denial-of-service (DDoS). A device or network is bombarded with so many requests during a DDoS attack that it crashes. Sensitive data is sent from a compromised device to an attacker's server during data exfiltration. Data on the target device is encrypted during a ransomware attack, and the owner is kept prisoner until a ransom is paid; these attacks are illustrated in Figure 2 (Huang & Yu, 2018).

Figure 1. Most hacked devices

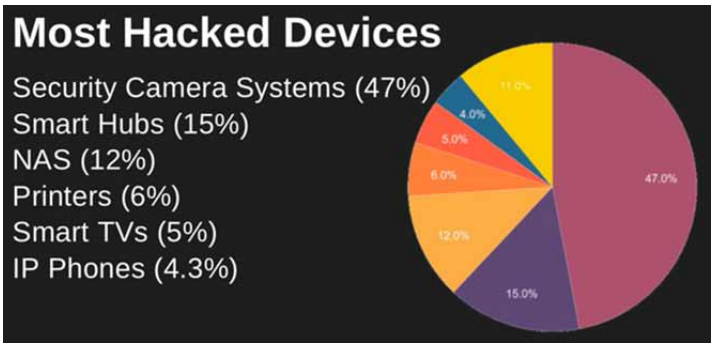
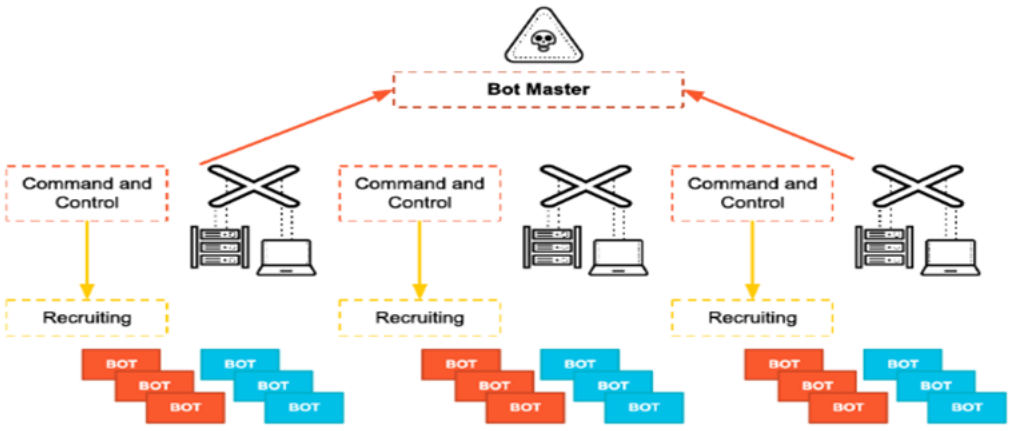


Figure 2. C&C attack architecture



A C&C attack might have disastrous financial and brand integrity ramifications. A corporation might lose a lot of money if a website or service is disrupted by a DDoS attack (Ikhsanudin et al., 2023). Trade secrets, personal information, and credit card information are just a few examples of the sensitive data types that might be exposed as a result of data exfiltration. The victim will suffer extra financial losses and reputational damage if they pay the ransom. Current techniques for detecting and guarding against C&C threats to the IoT include signature-based detection, anomaly detection, and supervised learning algorithms. Anomaly detection searches for unusual behavior patterns, whereas signature-based detection searches for known detrimental activity patterns in network data. As was previously said, supervised learning algorithms may analyze network data to find anomalies that signify active attacks.

To address these problems, researchers have suggested using phony IoT devices that mimic genuine ones in appearance and behavior. Because the false devices can establish connections with the attacker's server, security professionals can analyze the attack and develop protections. Researchers have suggested a number of machine learning techniques, such as deep learning, to enhance C&C attack detection and protection. Attacks using C&C on the IoT may have disastrous results. While there are certain techniques for identifying and countering C&C threats, they are not infallible, and attackers are always developing new techniques for evading detection (Jamali et al., 2019). A combination of multiple detection strategies, decoy devices, and machine learning algorithms may be required to enhance the detection and mitigation of C&C attacks.

Supervised Learning

Supervised learning, a subfield of machine learning, is the process of training a model to make predictions only from annotated data. In supervised learning, the model generates predictions about a target variable based on other information after the target variable has been explicitly labeled in the data. Learning under supervision seeks to develop the capacity to transform one collection of data into another. Predictive analytics, NLP, and computer vision are just a few examples of the many fields where this approach is widely used.

IoT security often makes use of supervised learning to detect and thwart possible threats. Hostile actors might compromise IoT devices due to their internet access. IoT security may be improved by supervised learning by identifying common activity patterns and highlighting anomalies. Supervised learning is a machine-learning technique that involves training a model to generate predictions from a large amount of labeled data. A labeled data collection is used in supervised learning, from which the model predicts an unlabeled target variable. Learning under supervision seeks to develop the capacity to transform one collection of data into another. Classification, regression, and anomaly detection are supervised learning-based tasks that may be completed in the context of IoT security (Khamaiseh, 2019).

Figure 3 illustrates a supervised learning technique called classification, which divides data into categories based on common traits. The categorization might be used to differentiate between normal and suspect activity in IoT devices from a security standpoint. For example, a classification model may be trained to discriminate between good and bad network information. The model is capable of comprehending average network activities, including typical data packet volume, size, and rate. The trained algorithm may then spot unusual traffic patterns that point to a forthcoming attack.

Regression, another supervised learning method, aims to predict a continuous target variable from a collection of input data. Regression may be used to predict how different circumstances will affect the operation of devices while securing the IoT. For example, a regression model may be trained to predict how many requests a web server can handle before failing. These are only a few of the factors that the model may learn to take into consideration, along with the number of requests, the number of active users, and the server's processing power. Once trained, the model can forecast how the server will respond to different loads and modify the machine's settings appropriately, as in Figure 4 (Khedr et al., 2023).

Anomaly detection is a kind of supervised learning that searches for unusual patterns in data. IoT devices may be monitored for unusual activity that can indicate an oncoming attack using anomaly

Figure 3. Classification method

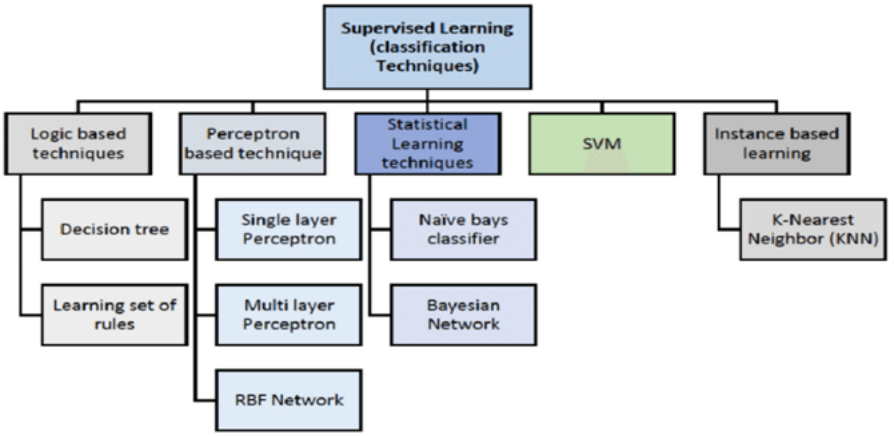
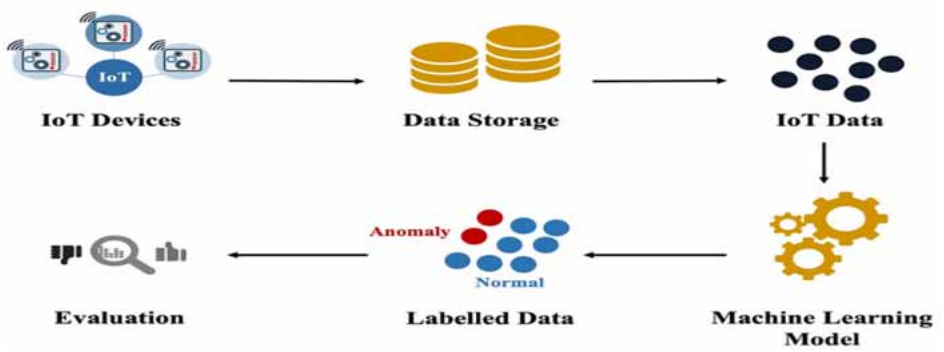


Figure 4. Anomaly detection



detection. It is possible to train anomaly detection models to identify abnormal network behavior, such as that brought on by a distributed denial-of-service attack. The model is capable of comprehending average network activities, including typical data packet volume, size, and rate. After the model has been trained, it may detect unusual network traffic patterns and raise an alert in the security division (Plageras, 2018).

Using supervised learning to protect the IoT has a number of benefits. First, supervised learning may be used to identify and neutralize cyber threats in real time. Cyber assaults may occur at any moment, making their protection essential for IoT devices. Second, by drawing on prior knowledge, supervised learning may be able to adjust to new hazards. This suggests that the model may be changed to recognize new threats. Finally, supervised learning results in a reduction in both false positives and false negatives. This suggests that the model can accurately and with few false positives detect cyber hazards.

For IoT security, supervised learning offers a lot of potential advantages, but it also has certain disadvantages. The first limitation of supervised learning is the lack of a significant quantity of labeled data. This information may be difficult to acquire in the context of IoT security due to the rarity of cyberattacks. Second, supervised learning may have problems due to overfitting. When the model is extremely intricate and overfits the training data, generalization performance falls. The computational difficulty of supervised learning is the third problem (Khashab et al., 2021). This could be challenging for IoT devices with low processor and memory capacities.

Many strategies may be used when using supervised learning techniques for IoT security to address these problems. Utilizing transfer learning, which includes leveraging parts from previously trained models, is one technique to reduce the amount of labeled data required for training. Using a model developed for one task to train a model for another is an example of transfer learning. This may assist with time and material savings in addition to improving the effectiveness of the model.

Second, by pooling the output of many models via ensemble learning, the risk of overfitting may be reduced. To get a conclusive result, ensemble learning integrates the predictions of several models trained on various independent data subsets. This may improve the model's stability and accuracy.

Finally, by removing useful characteristics from the data, feature engineering may be used to reduce the dimensionality of the input space. For the purpose of optimizing the output of the model, feature engineers choose, modify, and scale the input features. This may reduce the amount of labeled data required for training while improving the model's generalization performance.

Use Cases and Examples of How Supervised Learning Can Be Applied in IoT Security

In IoT security, supervised learning entails training models on labeled datasets to make judgments or predictions based on previously unseen data. The following are some particular use cases and illustrations of supervised learning's application to IoT security:

- Detecting intrusions: malicious activity detection in IoT networks. As an illustration, use labeled data with both normal and anomalous behavior to train a supervised learning model. After that, the model can spot departures from the learned standard behavior and sound an alarm in case there are any possible intrusions (Alsoufi, 2021).
- Anomaly detection in device behavior: In this case, it is recognizing odd behavior in specific IoT devices. For example, utilizing past data on typical device behavior, train a model. The model can then identify possible security risks by identifying anomalies like strange data transmission or unexpected communication patterns (Liu, 2020).
- Authentication of devices: assuring IoT devices' identities. To train a model that identifies the common data signatures and communication patterns of authorized devices, use supervised learning. Devices displaying unusual behavior, which could point to a compromised or unauthorized device, can then be flagged or blocked by the model (Mamdouh, 2021).
- Traffic classification: As an illustration, teach a supervised learning model to categorize various kinds of network traffic, including firmware updates, data transfers, and command and control communications. Based on the learned categories, the model can then flag or block suspicious traffic patterns (Kumar, 2021).
- Finding malware: In this scenario, the approach is determining whether IoT devices contain malicious software. For instance, utilize labeled datasets with characteristics of both malicious and benign code to train a model. In order to assist in the early detection and mitigation of security threats, the model can then analyze the code that is operating on IoT devices and classify whether it is likely to be malware (Wang, 2021).
- Security for predictive maintenance: tracking down intrusions on predictive maintenance networks. During predictive maintenance, train a model to comprehend typical device behavior. The security and dependability of maintenance procedures can then be guaranteed by the model's ability to spot anomalies that might point to a system attack (John, 2021).
- Tracking while preserving privacy: maintaining user privacy while keeping an eye on network traffic for security. Without examining each communication's content, train a supervised learning model to recognize security threats. This maintains the privacy of the data transmitted by IoT devices while enabling the detection of possible threats (Hassan, 2019).

In these use cases, supervised learning can help IoT security systems become more adept at spotting and thwarting different kinds of security threats.

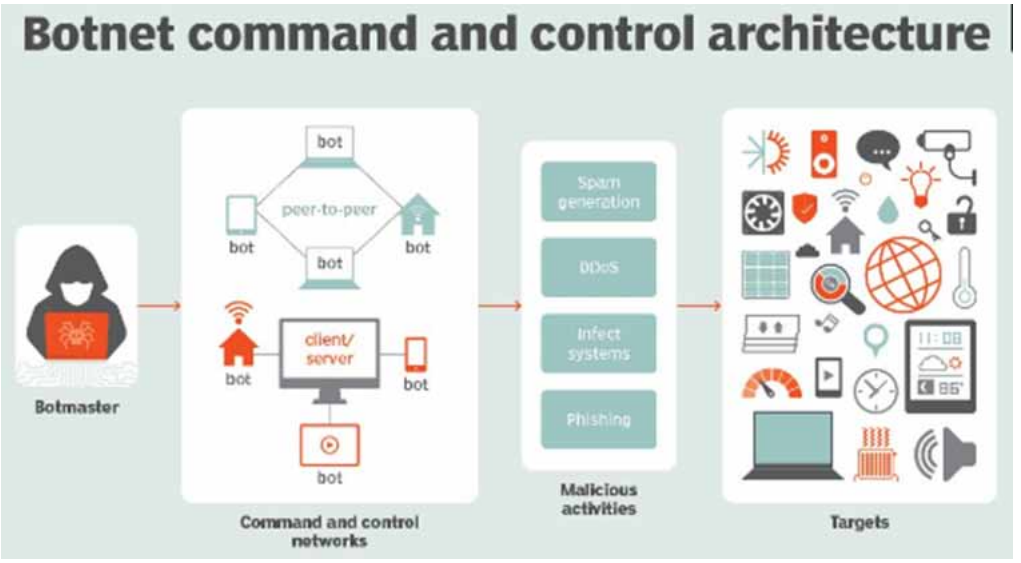
Existing Research

The term "supervised learning" refers to the method through which the system learns from labeled input. From the input information, the algorithm learns to predict the output label. Input characteristics and output labels make up the labeled data. In cybersecurity, supervised learning is often used to detect risks and create defenses. By learning the distinctions between usual and suspect network data, supervised learning may be utilized to identify and mitigate IoT C&C risks. A lot of research has been done on the use of supervised learning to identify and stop IoT C&C risks. Here, we will review some of the ground-breaking research that has been done in this area.

Many academics have studied supervised learning techniques for detecting IoT C&C attacks. The method used by Mishra and Pandya (2021) to recognize IoT botnets using deep learning is one instance (Figure 5). The strategy uses a long short-term memory (LSTM) network to model the sequences after initially using a convolutional neural network (CNN) to extract characteristics from the network traffic. The method has a detection rate of 99.98% and a false positive rate of 0.001%. Mishra et al. (2022) suggested using machine learning to analyze DNS traffic in order to find IoT botnets. Several classifiers, including decision trees, K-nearest neighbors, and random forests, are used to categorize DNS traffic as botnet or ordinary traffic. With this approach, a 99.4% success rate was achieved.

Narendraekokar et al. (2023) recommended using supervised learning to detect C&C traffic in IoT botnets. This technique uses a decision tree classifier to divide normal and botnet categories for incoming data flows. With a 0.1% false positive rate, the approach has a 99.9% detection rate. Gopal et al. (2021) described a similar deep learning-based method for recognizing C&C traffic in IoT botnets. To comprehend the cyclical nature of network activity, a multi-attention recurrent neural network (MARNN) is used. This method has a 98.5% accuracy rate and a false positive rate of 0.02%. Machine learning approaches have been widely used in IoT C&C threat detection. To uncover Hajime botnet assaults, for instance, which are notorious for their stealth and resistance to standard detection techniques, Karthika and Arockiasamy (2023) developed a decision tree-based method. The method

Figure 5. Botnet C&C architecture



employed decision trees to evaluate DNS traffic and determine if it was malicious or genuine. The trials' 99.98% detection rate and 0.001% false positive rate demonstrated the technique's accuracy.

In 2022, Reynvoet et al. did a second analysis to determine IoT C&C risks. The authors provided instructions on how to use network traffic records analysis to find C&C chats. The approach has a detection rate of 98.5% and a false positive rate of 0.47%, properly classifying traffic as C&C or non-C&C. It has also been tried to use deep learning models for IoT C&C threat detection. For instance, Karim and Razzaque (2019) suggested using a deep-belief network (DBN) to recognize Mirai botnet attacks. To identify communications between Mirai command and control, the DBN looked at packet length and direction. With only a 0.2% false positive rate throughout their tests, the scientists were able to identify 99.7% of the occurrences.

Negera et al. (2022) recommended utilizing a combination of deep Q-network (DQN) and DBN to recognize and stop Mirai botnet attacks. The DQN analyzed network traffic to find C&C discussions, while the DBN reduced botnet activity by filtering out hazardous packets. In their testing, the authors achieved a 99.9% detection rate and a 99.8% mitigation rate. Machine learning and deep learning techniques have also been employed to mitigate IoT C&C threats. For instance, Mohammed and Alheeti (2021) proposed a method using a decision tree classifier to detect and halt illicit communications associated with Mirai botnet attacks. The method examined data moving via a network and used a decision tree to categorize packets as Mirai-related or not. In their tests, the authors lowered the danger by 97%, demonstrating the effectiveness of their approach. It is important to recognize C&C concerns, but it s also important to take precautions against them. Numerous research projects have focuised on using supervised learning approaches to defend against IoT C&C threats. In order to combat IoT botnets, Vasques and Gondim (2020) suggested a deep reinforcement learning-based strategy. The most effective method for reducing botnet traffic is found using a DQN. By up to 99.9%, the technique decreased botnet traffic.

Using SDN, Zagrouba and AlHajri (2022) presented a machine learning-based approach for minimizing IoT botnets. A support vector machine (SVM) classifier is used to categorize network traffic as botnet or normal. The classifier changes the flow rules in the SDN controller to lessen botnet traffic. Using this method, up to 97% of botnet traffic was stopped. Additionally, Saravanan et al. (2023) proposed a deep learning strategy based on DQN and DBN for preventing and removing IoT botnets. We were able to reduce botnet traffic by up to 98.7 percent by using this method.

Critical Analysis of Existing Research

According to the studies mentioned above, supervised learning techniques may successfully detect and stop C&C threats on the IoT. However, there are a number of limitations and challenges that must be solved. The majority of research has been on detecting and thwarting certain IoT botnets, such as Mirai and Hajime. But when new botnet variations emerge, each with its own characteristics and attack strategies, it becomes difficult to develop standardized methods for detection and prevention.

Second, a number of studies used a variety of features to detect and classify network traffic. For instance, Sharma and Singh (2023) only took packet length and direction into account while assessing DNS traffic. These traits could be useful in detecting certain assault types, but they might not be sufficient to recognize more sophisticated attack types. Finally, some researchers employed labeled datasets to train their algorithms. However, labeled datasets could be difficult to locate, particularly for new and emerging threats. Unsupervised learning techniques could be more effective in certain situations, even when labeled data might not always be accessible. It has shown great promise in detecting and stopping C&C attacks on the IoT using supervised learning techniques. The articles examined in this article benefit from a variety of supervised learning techniques, including decision tree classifiers, deep learning models, and reinforcement learning techniques. There are still challenges to overcome despite the significant progress that has been accomplished. They include the development of novel botnet architectures, the accessibility of labeled datasets, and the need for larger feature sets. Therefore, researchers must endeavor to enhance supervised learning techniques in order to recognize and stop different IoT C&C risks in the future.

However, the literature review studies in the field of IoT have been illustrated in Table 1. This table shows the results of these studies.

Table 1. Literature review summary

Research Papers Titles	Published Date	Summary	Method	Contribution to the Project	Results
The Internet of Things: A survey (Atzori, 2010)	2010	This presentation surveys the Internet of Things's foundations, technologies, and uses.	Literature review	IoT security challenges can be better comprehended with this background knowledge of IoT architecture and related technologies.	Identified cybersecurity threats and mitigation approaches
Internet of Things (IoT) security: A review (Dey, 2020)	2020	This study provides a comprehensive analysis of the dangers and difficulties posed by the Internet of Things and a range of potential countermeasures.	Literature review	Knowing the dangers and difficulties of IoT security aids in detecting and preventing attacks.	Surveyed the Internet of Things (IoT)
Cybersecurity threats and their mitigation approaches using machine learning—A review (**Ahsan, 2022**)	2022	The paper reviews cybersecurity threats and mitigation approaches using machine learning techniques.	Literature review	It helps to identify and prevent IoT attacks by explaining the current state of cybersecurity risks and mitigation strategies using machine learning algorithms.	Developed a novel intrusion detection system for IoT networks
A novel deep learning-based intrusion detection system for IoT networks, (Awajan, 2023)	2023	This paper introduces an IDS for IoT networks that uses deep learning to spot intrusions.	Experimental study	It introduces a unique IDS for IoT networks that employ deep learning techniques for attack detection and mitigation.	Improved production quality, safety, and sustainability
IoT Network Attack Detection Using Supervised Machine Learning (Tyagi, 2021)	2021	The study suggests identifying attacks on IoT networks using supervised machine learning.	Experimental study	It presents a machine learning-based approach for detecting IoT network attacks, which can be used to detect and mitigate IoT attacks.	Developed a DDoS attack detection system using machine learning
Mitigating dos attacks in IoT using supervised and unsupervised algorithms – A survey (Gopal, 2021)	2021	This paper provides a comprehensive overview of the current supervised and unsupervised methods for protecting the Internet of Things from denial-of-service assaults.	Literature review	It explains how supervised and unsupervised algorithms are currently being used to reduce the impact of denial-of-service attacks on the Internet of Things.	Explored different algorithms for DoS attack mitigation
Cyber threat intelligence for IoT using machine learning (Mishra, 2022)	2022	The article suggests using a machine learning-based strategy for cyber threat intelligence in the Internet of Things.	Literature review	To detect and prevent IoT-based assaults, it introduces a machine learning-based strategy for cyber threat intelligence in the IoT.	Reviewed IoT security challenges and solutions
Review of Botnet attack detection in SDN-enabled IoT using machine learning (Negera, 2022)	2022	In this study, we look at how machine learning can be used to spot botnet attacks in SDN-enabled Internet of Things networks.	Literature review	It explains how machine learning may be used to spot botnet assaults in SDN-enabled IoT, which can then be mitigated.	Developed a model for detecting IoT network attacks using supervised ML
Detecting and mitigating jamming attacks in IoT networks using self-adaptation (Reynvoet, 2022)	2022	This research recommends a self-adaptive method for monitoring and protecting Internet of Things (IoT) networks from jamming assaults.	Experimental study	The paper introduces a self-adaptive method for protecting Internet of Things networks from jamming assaults.	Discussed the vision, applications, and challenges of IoT

continued on following page

Table 1. Continued

Research Papers Titles	Published Date	Summary	Method	Contribution to the Project	Results
A machine learning-based attack detection and mitigation using a secure SaaS framework (Reddy, 2022)	2022	The research suggests a secure SaaS platform using machine learning for attack detection and mitigation.	Experimental study	IoT attacks can be detected and prevented with the help of this paper, which proposes a machine learning-based solution to attack detection and mitigation that uses a secure SaaS framework.	Reviewed IoT security attacks and challenges
A survey on machine learning techniques for cybersecurity in the last decade	2020	The study provides a decade-long overview of machine-learning approaches to cybersecurity.	Literature review	Knowing the current state of the art in machine learning techniques for cybersecurity is useful for detecting and preventing attacks against the Internet of Things.	Explored cyber threat intelligence for IoT using ML
A comparative analysis of machine learning techniques for IoT intrusion detection (Vitorino, 2022)	June 15, 2022	In this study, we examine the relative merits of the decision tree, the random forest, and the support vector machine when detecting intrusions into the Internet of Things (SVM). To assess the efficacy of each method, the authors employ a dataset that features both innocuous traffic and a wide variety of attacks, such as Command-and-Control (C&C) attacks.	Literature review	This paper may be useful in deciding the machine learning technique for this purpose.	Reviewed security challenges for the Internet of Things
DDoS attack detection system using semi-supervised machine learning in SDN (Etman, 2021)	2021	The study proposed a DDoS attack detection system using semi-supervised machine learning in SDN. The system can achieve high accuracy and reduce false positives.	Semi-supervised machine learning	The paper discusses the application of machine learning in detecting DDoS attacks, which can benefit my project on detecting and mitigating IoT C&C attacks.	Reviewed botnet attack detection using machine learning
Detecting and mitigating jamming attacks in IOT networks using self-adaptation (Reynvoet, 2022)	2022	The study proposed a framework for detecting and mitigating jamming attacks in IoT networks. The framework uses self-adaptation to identify and mitigate jamming attacks.	Self-adaptation	The paper discusses a different approach to mitigating attacks in IoT networks, which can be useful in my project.	Developed a secure SaaS framework for attack detection and mitigation
A deep learning approach for DDoS attack detection using supervised learning (Tekleselassie, 2021)	2021	The study proposed a deep learning approach to detect DDoS attacks. The proposed model achieved high accuracy and reduced false positives.	Deep learning using supervised learning	The paper discusses the application of supervised learning in detecting DDoS attacks, which can benefit my project on detecting and mitigating IoT C&C attacks.	Developed a method for detecting and mitigating jamming attacks in IoT
Attack and anomaly detection in IOT networks using supervised machine learning approaches (Tyagi, 2021)	2021	The study proposed a supervised machine learning approach to detect attacks and anomalies in IoT networks. The proposed model achieved high accuracy and reduced false positives.	Supervised machine learning	The paper discusses the application of machine learning in detecting attacks and anomalies in IoT networks, which can benefit my project.	Reviewed machine learning techniques for cybersecurity

continued on following page

Table 1. Continued

Research Papers Titles	Published Date	Summary	Method	Contribution to the Project	Results
Detecting Amazon bot reviewers using unsupervised and supervised learning (Wood, 2022)	2022	The study proposed a method to detect Amazon bot reviewers using unsupervised and supervised learning. The proposed model achieved high accuracy and identified the bot reviewers accurately.	Unsupervised and supervised learning	Although not directly related to my project, the paper discusses the application of machine learning in detecting fraudulent activities, which can be useful in developing an approach for detecting and mitigating IoT C&C attacks.	Developed a deep learning approach for DDoS attack detection
Machine Learning-based Attacks Detection and Countermeasures in IoT	2022	To identify and stop assaults on Internet of Things (IoT) gadgets, this article suggests using machine learning. The authors employ a dataset that contains both innocuous traffic and diverse attacks, emphasizing numerous different sorts of attacks, including C&C attacks. An anti-malware traffic-blocking countermeasure is also proposed.	The authors propose a machine learning-based approach to detect and counteract attacks in IoT devices.	This paper has the potential to shed light on how machine learning can be used to prevent C&C threats in IoT devices and offer a workable method for filtering out harmful data.	Developed a model for attack and anomaly detection in IoT networks

Identification of Research Gaps

Many concerns remain unresolved despite the vast literature on IoT C&C threats and supervised learning in cybersecurity. First, although identifying IoT C&C risks has received a lot of attention, effective mitigation strategies have received less focus. Additionally, the effectiveness of supervised learning for detecting and reducing IoT C&C risks has not been thoroughly examined in earlier studies on the subject. Instead, many investigations have concentrated on certain threat types, such as malware or phishing. The majority of supervised learning models used in earlier research were trained and evaluated using publicly accessible datasets, which may not accurately reflect real-world scenarios.

DISCUSSION AND ANALYSIS

The review of the literature underlines the need for more research to close the knowledge gaps. IoT C&C threat detection technologies are crucial, but future research should also concentrate on developing efficient countermeasures. Experts in the sector should also consider how well-supervised learning can detect and stop IoT C&C attacks. Future research should also use real-world datasets to train and evaluate supervised learning models in order to validate their precision and effectiveness in real-world conditions. The most recent supervised learning techniques, such as deep learning and reinforcement learning, may potentially be the subject of future investigations. These approaches have been successful in other cyber fields, and they might improve the way supervised learning models identify and stop C&C threats on the IoT.

The literature review for this research paper provides readers with an introduction to IoT C&C attacks, their categories, and the need to take precautions to avoid them. The importance

of supervised learning in recognizing and combating cyberattacks like IoT C&C threats is underlined in this discussion as well. There are still a number of research gaps in this area, so future work should focus on creating IoT C&C attack mitigation strategies, assessing the effectiveness of supervised learning specifically for C&C attacks, using real-world datasets to train and test supervised learning models, and exploring advanced supervised learning techniques. The results of this study have important ramifications for academics, cybersecurity professionals, and IoT security.

The role of supervised learning in preventing and responding to C&C attacks against the IoT is well covered in the literature review in this research. The evaluation emphasizes the need to take precautions against IoT C&C threats since they constitute a severe danger to the security of IoT devices and networks and may jeopardize customer and business data. The review recognizes the importance of supervised learning for cybersecurity as well as its ability to deter and respond to attacks using command and control on the IoT. However, there are a few open scientific questions that need further research (Shukla et al., 2023). Because it sets the background and points out areas that need more investigation, the literature review is crucial. The paper emphasizes the need for further investigation into the use of real-world datasets for supervised learning model training and testing, the invention of innovative supervised learning methodologies, and the development of effective IoT C&C threat mitigation measures.

The literature review establishes the foundation for the investigation, making it a crucial part of the research report. A thorough analysis of the literature may make it easier to comprehend the state of the field's research as well as its shortcomings. The study topic, the research questions, and the research methodology are all influenced by the literature review. In order to evaluate the status of the subject, identify any knowledge gaps, and propose prospective future study topics, IoT security studies must undertake an extensive literature analysis. As IoT security evolves quickly, the literature review is useful for keeping academics abreast of the most recent advancements (Ye & Liu, 2022). Additionally, the review of the literature reveals areas that need further study, as well as those in which the use of previously created tools and procedures may improve IoT security.

CONCLUSION

In conclusion, this survey paper on supervised learning for C&C attack detection in IoT devices presents several key findings and contributions. First, the study explores the effectiveness of supervised learning in enhancing IoT security by autonomously identifying patterns indicative of C&C threats in real-time. It emphasizes the advantages and drawbacks of this approach, addressing considerations such as the necessity for well-labeled datasets, resource constraints of IoT devices, and ethical implications related to data security.

Second, the paper provides a comprehensive analysis of the current state of the art in the field, summarizing prior research and highlighting relevant results. By doing so, it offers valuable insights into the strengths and weaknesses of existing approaches, aiding researchers in understanding the landscape and informing future directions for exploration.

Furthermore, the survey paper identifies research gaps, guiding future efforts and encouraging exploration of untried directions in the realm of supervised learning for C&C attack detection in IoT. This contribution is particularly beneficial for researchers seeking to expand the knowledge base and contribute to advancements in the field. For practitioners, the survey consolidates earlier research to assist in comprehending and implementing security solutions for IoT deployments. The critical evaluation of prior initiatives offers practical advice for decision-makers, helping them navigate the selection and implementation of security measures to safeguard their IoT ecosystems.

Last, the study emphasizes the ethical aspects of IoT security, stressing the importance of aligning security measures with moral principles and cultural norms. This consideration benefits policymakers by providing insights into the ethical dimensions of implementing security measures in the rapidly evolving IoT landscape. In summary, this survey paper serves as a valuable resource for researchers, practitioners, and policymakers alike. It contributes to the existing knowledge base, guides future research efforts, aids in practical decision-making for security implementations, and underscores the ethical considerations essential for policymakers shaping regulations and policies in the IoT domain.

AUTHOR NOTE

On behalf of all authors, the corresponding author states that there is no conflict of interest.

Data Availability Statement: The original contributions presented in the study are included in the article/supplementary material; further inquiries can be directed to the correspondence author.

REFERENCES

Abuagoub, A. M. (2022). IoT security evolution: Challenges and countermeasures review. *International Journal of Communication Networks and Information Security*, *11*(3). Advance online publication. doi:10.17762/ijcnis.v11i3.4272

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using machine learning—A review. *Journal of Cybersecurity and Privacy*, *2*(3), 527–555. doi:10.3390/jcp2030027

Al-Qerem, A., Alauthman, M., Almomani, A., & Gupta, B. B. (2020). IoT transaction processing through cooperative concurrency control on fog–cloud computing environment. *Soft Computing*, *24*(8), 5695–5711. doi:10.1007/s00500-019-04220-y

Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. *Applied Sciences (Basel, Switzerland)*, *11*(18), 8383. doi:10.3390/app11188383

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of things: A survey. *Computer Networks*, *54*(15), 2787–2805. doi:10.1016/j.comnet.2010.05.010

Awajan, A. (2023). A novel deep learning-based intrusion detection system for IoT networks. *Computers*, *12*(2), 34. doi:10.3390/computers12020034

Cioffi, R., Travaglioni, M., Piscitelli, G., Petrillo, A., & De Felice, F. (2020). Artificial intelligence and machine learning applications in smart production: Progress, trends, and directions. *Sustainability (Basel)*, *12*(2), 492. doi:10.3390/su12020492

Cuadra-Sánchez, A., & Aracil, J. (2015). *Traffic anomaly detection*. Elsevier.

Dey, N., Mahalle, P. N., Shafi, P. M., Kimabahune, V. V., & Hassanien, A. E. (2020). *Internet of things, smart computing and technology: A roadmap ahead*. Springer Nature. doi:10.1007/978-3-030-39047-1

Etman, M. A. (2021). *DDoS attack detection system using semi-supervised machine learning in SDN*. 10.32920/ryerson.14657868.v1

Gangolli, A., Mahmoud, Q. H., & Azim, A. (2022). A machine learning based approach to detect fault injection attacks in IoT software systems. *2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. doi:10.1109/SMC53654.2022.9945117

Gopal, S., Poongodi, C., Nanthiya, D., Snega Priya, R., Saran, G., & Sathya Priya, M. (2021). Mitigating dos attacks in IoT using supervised and unsupervised algorithms – A survey. *IOP Conference Series. Materials Science and Engineering*, *1055*(1), 012072. doi:10.1088/1757-899X/1055/1/012072

Gupta, B. B., & Tewari, A. (2020). Evolution of internet of things (IoT). *A beginner's guide to internet of things security*, 1-9. 10.1201/9781003001126-1

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems*, *97*, 512–529. doi:10.1016/j.future.2019.02.060

Hodge, C., Hauck, K., Gupta, S., & Bennett, J. C. (2019). *Vehicle cybersecurity threats and mitigation approaches*. 10.2172/1559930

Huang, H., & Yu, H. (2018). *Compact and fast machine learning accelerator for IoT devices*. Springer.

Ikhsanudin, M., Suryani, V., & Pahlevi, R. R. (2023). DDoS attack detection on MQTT protocol using semi-supervised DBSCAN and support vector machine model. *2023 11th International Conference on Information and Communication Technology (ICoICT)*. doi:10.1109/ICoICT58202.2023.10262594

Jamali, M. A., Bahrami, B., Heidari, A., Allahverdizadeh, P., & Norouzi, F. (2019). *Undefined*. Springer.

John, J., Ghosal, A., Margaria, T., & Pesch, D. (2021). DSLs and middleware platforms in a model-driven development approach for secure predictive maintenance systems in smart factories. *Leveraging applications of formal methods, verification and validation: 10th international symposium on leveraging applications of formal methods, ISoLA 2021, Rhodes, Greece, October 17–29, 2021 Proceedings*, *10*, 146–161.

Kara, M., Laouid, A., Hammoudeh, M., AlShaikh, M., & Bounceur, A. (2022). Proof of chance: A lightweight consensus algorithm for the internet of things. *IEEE Transactions on Industrial Informatics*, *18*(11), 8336–8345. doi:10.1109/TII.2022.3168747

Kara, M., Karampidis, K., Papadourakis, G., Laouid, A., & AlShaikh, M. (2023a, April). A Probabilistic Public-Key Encryption with Ensuring Data Integrity in Cloud Computing. In *2023 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO)* (pp. 59-66). IEEE.

Kara, M., Laouid, A., Bounceur, A., Hammoudeh, M., & Alshaikh, M. (2023b). Perfect Confidentiality through Unconditionally Secure Homomorphic Encryption Using OTP With a Single Pre-Shared Key. *Journal of Information Science & Engineering, 39*(1).

Karim, M. R., & Razzaque, M. A. (2019). *Hands-on deep learning for IoT*. Academic Press.

Karthika, P., & Arockiasamy, K. (2023). Simulation of SDN in mininet and detection of DDoS attack using machine learning. *Bulletin of Electrical Engineering and Informatics*, *12*(3), 1797–1805. doi:10.11591/eei.v12i3.5232

Khamaiseh, S. Y. (2019). *Detection and countermeasure of saturation attacks in software-defined networks*. Academic Press.

Khashab, F., Moubarak, J., Feghali, A., & Bassil, C. (2021). DDoS attack detection and mitigation in SDN using machine learning. *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*. doi:10.1109/NetSoft51509.2021.9492558

Khedr, W. I., Gouda, A. E., & Mohamed, E. R. (2023). FMDADM: A multi-layer DDoS attack detection and mitigation framework using machine learning for Stateful SDN-based IoT networks. *IEEE Access : Practical Innovations, Open Solutions*, *11*, 28934–28954. doi:10.1109/ACCESS.2023.3260256

Khedr, W. I., Gouda, A. E., & Mohamed, E. R. (2023). P4-HLDMC: A novel framework for DDoS and ARP attack detection and mitigation in SD-IoT networks using machine learning, stateful P4, and distributed multi-controller architecture. *Mathematics*, *11*(16), 3552. doi:10.3390/math11163552

Kumar, R., Swarnkar, M., Singal, G., & Kumar, N. (2021). IoT network traffic classification using machine learning algorithms: An experimental analysis. *IEEE Internet of Things Journal*, *9*(2), 989–1008. doi:10.1109/JIOT.2021.3121517

Laouid, A., AlShaikh, M., Lalem, F., Bounceur, A., Euler, R., Bezoui, M., & Tari, A. et al. (2018, June). A distributed security protocol designed for the context of internet of things. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems* (pp. 1-5). doi:10.1145/3231053.3231079

Liu, Y., Garg, S., Nie, J., Zhang, Y., Xiong, Z., Kang, J., & Hossain, M. S. (2020). Deep anomaly detection for time-series data in industrial IoT: A communication-efficient on-device federated learning approach. *IEEE Internet of Things Journal*, *8*(8), 6348–6358. doi:10.1109/JIOT.2020.3011726

Mamdouh, M., Awad, A. I., Khalaf, A. A., & Hamed, H. F. (2021). Authentication and identity management of IoHT devices: Achievements, challenges, and future directions. *Computers & Security*, *111*, 102491. doi:10.1016/j.cose.2021.102491

Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 59353–59377. doi:10.1109/ACCESS.2021.3073408

Mishra, S., Albarakati, A., & Sharma, S. K. (2022). Cyber threat intelligence for IoT using machine learning. *Processes (Basel, Switzerland)*, *10*(12), 2673. doi:10.3390/pr10122673

Mohammed, M. M., & Alheeti, K. M. (2021). Evaluating machine learning algorithms to detect and classify attacks in IoT. *2021 International Conference on Communication & Information Technology (ICICT)*. doi:10.1109/ICICT52195.2021.9568472

Narendraekokar, V. H., Durbha, S. S., Michalas, A., & Nagarhalli, T. P. (2023). Intelligent approaches to cyber security. CRC Press.

Negera, W. G., Schwenker, F., Debelee, T. G., Melaku, H. M., & Ayano, Y. M. (2022). Review of botnet attack detection in SDN-enabled IoT using machine learning. *Sensors (Basel)*, *22*(24), 9837. doi:10.3390/s22249837 PMID:36560204

Othman, T. S., Koy, K. R., & Abdullah, S. M. (2023). Intrusion Detection Systems for IoT Attack Detection and Identification Using Intelligent Techniques. *Networks, 5*, 6.

Plageras, A. P., Psannis, K. E., Stergiou, C., Wang, H., & Gupta, B. B. (2018). Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings. *Future Generation Computer Systems*, *82*, 349–357. doi:10.1016/j.future.2017.09.082

Reddy, S., & Shyam, G. K. (2022). A machine learning based attack detection and mitigation using a secure SaaS framework. *Journal of King Saud University. Computer and Information Sciences*, *34*(7), 4047–4061. doi:10.1016/j.jksuci.2020.10.005

Reynvoet, M., Gheibi, O., Quin, F., & Weyns, D. (2022). Detecting and mitigating jamming attacks in IoT networks using self-adaptation. *2022 IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion (ACSOS-C)*. doi:10.1109/ACSOSC56246.2022.00019

Saravanan, V., Sreelatha, P., Atyam, N. R., Madiajagan, M., Saravanan, D., & Sultana, H. P. (2023). Design of deep learning model for radio resource allocation in 5G for massive iot device. *Sustainable Energy Technologies and Assessments*, *56*, 103054. doi:10.1016/j.seta.2023.103054

Sharma, A., & Singh, U. K. (2023). Cloud computing security through detection & Mitigation of zero-day attack using machine learning techniques. SSRN *Electronic Journal*. 10.2139/ssrn.4358061

Shoba Bindu, C., & Sasikala, C. (2018). Security in ubiquitous computing environment: Vulnerabilities, attacks and defenses. *Studies in Big Data*, 101-127. 10.1007/978-3-030-01566-4_5

Shukla, P., Krishna, C. R., & Patil, N. V. (2023). Eiot-ddos: Embedded classification approach for IoT traffic-based DDoS attacks. *Cluster Computing*. Advance online publication. doi:10.1007/s10586-023-04027-5

Sivabalan, S., & Radcliffe, P. J. (2017). Detecting IoT zombie attacks on web servers. *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*. doi:10.1109/ATNAC.2017.8215358

Tekleselassie, H. (2021). A deep learning approach for DDoS attack detection using supervised learning. *MATEC Web of Conferences, 348*, 01012. doi:10.1051/matecconf/202134801012

Tsukerman, E. (2020). *Designing a machine learning intrusion detection system*. 10.1007/978-1-4842-6591-8

Tyagi, H., & Kumar, R. (2021). Attack and anomaly detection in IoT networks using supervised machine learning approaches. *Revue d'Intelligence Artificielle*, *35*(1), 11–21. doi:10.18280/ria.350102

Uday Karthick, C. K., & Manimegalai, R. (2021). A novel threat modeling and attack analysis for IoT applications. *Security of Internet of Things Nodes*, 263-279. 10.1201/9781003127598-11-11

Vasques, A. T., & Gondim, J. J. (2020). Amplified reflection DDoS attacks over IoT reflector running CoAP. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. doi:10.23919/CISTI49556.2020.9140882

Vitorino, J., Andrade, R., Praça, I., Sousa, O., & Maia, E. (2022). A comparative analysis of machine learning techniques for IoT intrusion detection. *Foundations and Practice of Security*, 191-207. 10.1007/978-3-031-08147-7_13

Wang, H., Zhang, W., He, H., Liu, P., Luo, D. X., Liu, Y., Jiang, J., Li, Y., Zhang, X., Liu, W., Zhang, R., & Lan, X. (2021). An evolutionary study of IoT malware. *IEEE Internet of Things Journal*, *8*(20), 15422–15440. doi:10.1109/JIOT.2021.3063840

Wood, B., & Slhoub, K. (2022). Detecting Amazon bot reviewers using unsupervised and supervised learning. *2022 IEEE World AI IoT Congress (AIIoT)*. doi:10.1109/AIIoT54504.2022.9817207

Yagoub, M. A., Laouid, A., Bounceur, A., & Alshaikh, M. (2019, July). An intelligent cloud data protection technique based on multi agent system using advanced cryptographic algorithms. In *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems* (pp. 1-7). doi:10.1145/3341325.3342012

Ye, J., & Liu, B. (2022). A deep learning-based system for IoT intrusion detection. *International Conference on Neural Networks, Information, and Communication Engineering (NNICE 2022)*. doi:10.1117/12.2639322

Zagrouba, R., & AlHajri, R. (2022). Machine learning based attacks detection and countermeasures in IoT. *International Journal of Communication Networks and Information Security*, *13*(2). Advance online publication. doi:10.17762/ijcnis.v13i2.4943

Muath AlShaikh has been a Ph.D. holder in computer science since 2016, University of Bretagne Occidentale, France. He received his master's degree in computer science in 2010 from Utara University in Malaysia and his BSc in computer science in 2006 from AlBalqa University, Jordan. He is affiliated with the Lab-STICC / UMR CNRS 6283, SFIIS team of the University of Bretagne Occidentale, France. He has been an associate professor with the Computer Science Department, Saudi Electronic University, KSA. His research interests include homomorphic, cyber security, watermarking, cryptology, information security and image processing, and computer vision.

Waleed Alsemaih completed his bachelor's degree in information technology and computing in 2008 and completed a master's degree in cyber security in 2023.Currently, he is GRC manager whose role involves overseeing and implementing GRC initiatives and working closely with stakeholders to ensure adherence to regulatory requirements and best practices.

Sultan Alamri received a master's degree in information technology from the School of Engineering and Mathematical Sciences, La Trobe University, Australia, in 2010, and the PhD degree from the Faculty of Information Technology, Monash University, Australia, in 2014. He is currently a full professor with the College of Computing and Informatics, Saudi Electronic University, Saudi Arabia. Sultan is a senior member IEEE, data scientist, and researcher. His research interests include geospatial maps, GIS, data engineering, machine learning, computational geometry, and spatial databases.

Qusai Ramadan is a postdoctoral software engineer at Koblenz University, specializing in software engineering with a focus on model-security engineering. He earned his PhD in computer science from Koblenz-Landau University in 2020, presenting a novel model-based methodology for data protection in complex systems. Before his current role, Dr. Ramadan served as a dedicated research assistant within the same research group from 2015 to 2019. His academic journey extends across international borders, including a lecturer position at Najran University (Saudi Arabia) from 2010 to 2012. Dr. Ramadan received his Master of Science in IT from Utara University of Malaysia in 2010 and his Bachelor of Science in computer science from Al al-Bayt University (Jordan) in 2008.