OULUN YLIOPISTO
UNIVERSITY of OULU

Internet of Things security with machine learning techniques: A Systematic Literature Review.

University of Oulu
Degree programme in Information Processing Science
Master's Thesis
Kenneth Mutai
June 2019

Abstract

The Internet of Things (IoT) technologies are beneficial for both private and businesses. The growth of the technology and its rapid introduction to target fast-growing markets faces security challenges. Machine learning techniques have been recently used in research studies as a solution in securing IoT devices. These machine learning techniques have been implemented successfully in other fields. The objective of this thesis is to identify and analyze existing scientific literature published recently regarding the use of machine learning techniques in securing IoT devices.

In this thesis, a systematic literature review was conducted to explore the previous research on the use of machine learning in IoT security. The review was conducted by following a procedure developed in the review protocol. The data for the study was collected from three databases i.e. IEEE Xplore, Scopus and Web of Science. From a total of 855 identified papers, 20 relevant primary studies were selected to answer the research question. The study identified 7 machine learning techniques used in IoT security, additionally, several attack models were identified and classified into 5 categories.

The results show that the use of machine learning techniques in IoT security is a promising solution to the challenges facing security. Supervised machine learning techniques have better performance in comparison to unsupervised and reinforced learning. The findings also identified that data types and the learning method affects the performance of machine learning techniques. Furthermore, the results show that machine learning approach is mostly used in securing the network.

Keywords
Machine learning, algorithms, Internet of things, security, systematic literature review

Supervisor
Prof. Harri Oinas-Kukkonen
Dr. Xiuyan Shao

Foreword

First and foremost, I would like to express my sincere gratitude to my supervisors Prof. Harri Oinas-Kukkonen and Dr. Xiuyan Shao for their guidance throughout the process of writing this thesis. Their feedback proved helpful especially when I felt trapped and faced with a number of challenging issues.

Also, I want to express my gratitude to my family and friends who has always been with me and encourage me to complete my studies. Thesis work is always challenging and at times frustrating but their support and encouragement made it easier.

Kenneth Mutai
Oulu, 4th June 2019.

Abbreviations

ML	Machine Learning
SVM	Support Vector Machine
ANN	Artificial Neural Network
NN	Neural Network
KNN	K- Nearest Neighbor
RF	Random Forest
RFID	Radio Frequency Identification
ROC	Receiver Operating Characteristics
WSNs	Wireless Sensor Networks
IoT	Internet of Things
FQDN	Fully Qualified Domain Name
DNS	Domain Name Service
DNSSEC	Domain Name Service Security Extension
DoS	Denial of Service
DDoS	Distributed Denial of Service
RF	Radio Frequency
PCA	Principle Component Analysis

Contents

1. Introduction

The Internet of Things (IoT) are internet enabled devices embedded with wireless sensor networks which form a network of devices that provide advance and intelligent services (Restuccia, D'Oro, & Melodia, 2018). IoT devices communicate and interact over the internet with the connected devices through a standard communication protocol and can be monitored and controlled remotely to perform a desired functionality. This has eventually transformed human-to-human communication and human-to-machine communication to machine-to-machine communication (Giri, Dutta, Neogy, Dahal, & Pervez, 2017). The field of IoT has transpired as a field of incredible growth, impact and potential. As a result, the technological advancement has led to the development of smart environments in which heterogeneous smart devices with RFID, mobile, cloud computing, wireless network connection and sensor technologies enable shared communication between the devices hence creating smart applications such as smart homes, e-health and smart cities (Giri et al., 2017).

The application of IoT devices is predicted to grow in the near future, this significance is evident in their application and use in everyday lives to perform various tasks such as automating our homes. The ever increasing consumer demand and emerging application are among other leading factors that has led to the increase in the use of IoT which has recently gained more attention from both academia and industry (Samaila, Neto, Fernandes, Freire, & Inácio, 2018). With the simultaneous evolution of technologies, the use of these devices are envisioned to increase by extending internet connection to almost every useful physical object. Consequently, the number of the devices connected to the internet will also increase creating a huge network (Cañedo & Skjellum, 2016). There are quite a number of sectors positively impacted by this technological trend, among them includes health care, manufacturing processing, electricity processing, agriculture, and security (Giri et al., 2017).

The increase has however led to generation of huge data as the interconnected devices collect and share data over the internet which can be analyzed and monetized (Giri et al., 2017). Despite the boost for IoT growth from advancing technologies and creation of new innovative business models, challenges regarding security and privacy are on the rise too and are not given as much attention as they deserve (Samaila, Neto, Fernandes, Freire, & Inácio, 2018). Ensuring the safety of sensitive data stored in the devices or in-transit should be a major concern, especially with the rise of the use of IoT devices which tend to broaden the service of attack, for instance, a single device with a weak or no security connected to the internet can create an entry point for an attacker which can lead to a

larger attack. Real-time attacks are on the rise as the number of edge devices which serves as entry point to a network increases (Samaila et al., 2018). For instance, wearable devices such as smart watches that collect health data from the user and sends it to a Smartphone has to have a secure connection to avoid privacy information leakage. Therefore, the solutions to security issues should not only focus on a single device but has to involve the entire IoT ecosystem. Furthermore, as the use of IoT expands due to its undeniable benefits to the users, the existing security issues will also magnify if necessary measures relating to security issues are not taken into consideration (F. Restuccia et al., 2018).

Wireless networks are known to be susceptible to a number of attacks such as intrusion, Denial of Service (DoS), botnets, jamming, spoofing, unauthorized router access, among others (Mendez Mena, Papapanagiotou, & Yang, 2018). With IoT devices heavily relying on wireless networks, it makes them vulnerable to these kinds of attack, eventually compromising the confidentiality, integrity and availability of data, authenticity, authorization, privacy and non-repudiation (Samaila et al., 2018). Ensuring information security within the IoT ecosystem is challenging especially with the current available solutions, mainly, majority of IoT devices have constrained resources such as limited storage, memory and processing power in order to run complex security defense systems (Xiao, Wan, Lu, Zhang, & Wu, 2018). With highly heterogeneous components, naive security configurations, weak encryption verification (Sun, Li, Alam Bhuiyan, Wang, & Li, 2019) leave the devices insecure hence vulnerable to attacks due to weak security defense. Therefore, the introduction of machine learning as a new security paradigm can address this unique challenges facing the IoT ecosystem which the current security solutions may not be able to provide an effective solution.

Leveraging the ability of Machine Learning (ML) techniques in securing IoT devices could be a solution to the challenges facing IoT devices. ML techniques have been demonstrated to be a success in classifying problems in a number of areas, for example, in health monitoring, speech recognition, spam and fraud detection, computer networks, among others (Li, Palmieri, & Xiang, 2019; M. Mamdouh, M. A. I. Elrukhsi, & A. Khattab, 2018). The success of ML in solving complex classification problems is attributed by its ability to provide general framework to models proven to be too complex or dynamic to be summarized mathematically therefore earning its popularity (Restuccia et al., 2018). With the complexities in IoT environment, for instance, several number of devices and unstructured data collected from the devices can present huge security risk. By diversifying risks, ML techniques can provide security solutions due to their ability in classification of complex data. Network-based solutions identify devices so as to allow access to a network, monitor incoming and outgoing traffic and create a profile that determines normal behavior and abnormal behavior. ML techniques such as anomaly detection, intrusion, malware detection, access control, among others have been studied.

In summary, undoubtedly the impact of the application of IoT on daily activities cannot be underestimated and the challenges regarding information security and privacy can hardly be avoided. Currently, both network and device-based solutions still face some challenges, therefore, they are not effective enough in ensuring the security of IoT devices and therefore raises concern. A number of studies have been conducted on the new solutions from both technical and regulatory perspectives, new solutions such as anomaly and malware detection based on ML technique promise a better future but still not enough. Therefore in this thesis, through a Systematic Literature Review (SLR) a study is conducted to identify what are the most used ML techniques in ensuring the security of IoT devices.

The structure of this thesis is as follows: Section 2 gives a description of the background of this thesis; Section 3 presents the SLR and describes the procedure followed in performing the review; Section 4 presents the results of the review; the answers to the research questions are discussed in Section 5; Finally, Section 6 provides the conclusion of the thesis.

2. Background and Related work

This chapter explains the background of security in IoT and ML techniques, describing the key concepts focusing on network security in IoT devices. Section 2.1 presents the overview of IoT environment on security and privacy issues. Section 2.2 explains the characteristics of machine learning techniques used in IoT security and section 2.3 discusses related studies on this topic.

2.1 Overview of IoT Environment

The structure of IoT systems makes it a high demand technology domain due to its heterogeneous essence, dynamics, intelligence, mobility and undefined parameters. However, these characteristics also makes these systems vulnerable to attacks (Mendez Mena et al., 2018). Different instances of security issues in IoT devices includes technological, ethical and privacy concerns (Mendez Mena et al., 2018). Moreover, the challenge facing these devices are limited resources in terms of amount of storage and memory available, and low processing capability, the majority of security solutions available rely heavily on encryption which demands high performing devices to run complex encryption and decryption algorithms, which does not fit the resource-constrained IoT devices. Also the heavy dependency of IoT devices on wireless networks for communication faces security challenges known currently to affect wireless networks such as intrusion (Mendez Mena et al., 2018). Therefore, security within the IoT devices is complex because it is dependent on external components for its functionality.

2.1.1 Security Issues in IoT

Device identification

The identification of devices in a network is important especially in an IoT environment. This enables the properties of the devices to be known. For instance, Domain name service (DNS) enables the identification of a host on the internet and the host's property can be known through fully qualified domain name (FQDN), hence similar structures can be applied in object identification in IoT. The challenge in object identification in IoT is ensuring the integrity of the records used in naming architecture. DNS cache poisoning and man-in-the-middle are common attacks that can compromise naming architecture. The existing solutions such as domain name system security extensions (DNSSEC) requires devices with high computational and communication overhead, therefore, this solution may not be suitable for IoT device (Z. Zhang et al., 2014).

Authentication and Authorization
Traditional authentication and authorization within IoT devices is a challenge. Due to the high number of devices, the use of usernames and passwords for authentication and access control for authorization is cumbersome for key management (M. Shahzad & M. P. Singh, 2017). The use of weak password for authentication or unchanged password from default values is common despite the efforts of creating awareness.

Lightweight cryptosystems and security protocols
Although lightweight cryptosystems and security protocols may be helpful to the resource constrained IoT devices such as sensor nodes it is still not suitable for such kind of devices. Suitable cryptosystems such as public-key cryptosystems have higher security but this also comes with high computational overhead as compared to other cryptosystems such as symmetric-key cryptosystems. Therefore with the computational overhead still high it still remains a challenge for IoT devices with limited resources. (Gupta & Quamara, 2018)

Software vulnerability
Due to the market demands and attempts in making the first entry to the market, the majority of companies do not focus on security as a priority. This is often considered as an add-on, therefore releasing the product to the market with vulnerabilities. Security mechanisms such as intrusion detection systems or antivirus software require a fair amount of computational power of which in the case of some IoT devices it might not be applicable (Sommer & Paxson, 2010).

The attempts of securing IoT devices is an ongoing process. There are different approach on how to view security issues. (Mamdouh et al., 2018) classified security attacks in IoT as follows; goal-oriented attack which threatens the confidentiality; performer-oriented attacks and layer oriented attack. Security threats within the IoT environment can also occur on multiple layers such as interface layer, service layer, network layer and sensing layer, therefore, to ensure the safety of IoT systems the protection should be applicable at every layer (Moh & Raju, 2018). For instance, network, physical, and software attacks as well as privacy leakages (Xiao et al., 2018).

2.1.2. Privacy Issues in IoT

The privacy concerns are common within the IoT ecosystem (Moh & Raju, 2018). Majority of the devices collect personal data such as name, date of birth, payment information, health data, address and personal activities. The use of cloud services for data storage requires the devices to communicate by sending unencrypted data to the cloud service, for instance when using a home network, there can be a risk of exposing data in case there is any misconfiguration within the IoT system. According to (Ziegeldorf, Morchon, &

Wehrle, 2014) privacy threats were categorized into several categories namely; Identification: which is a threat associated with identifier such as names, date of birth of an individual; Localization and tracking category is a threat that collects individual recording of location within a certain time and space, activities such as work schedules or vacation plans data can be fetched from IoT sensors; Profiling, this categorizes an individual into a group using data collected from IoT devices, this could lead to price discrimination, social engineering or erroneous automatic decisions; Privacy-violation and presentation category is a threat of communicating private information to an unwanted audience; The lifecycle transition category can occur during upgrade where data is backed up and restored, the process mixed up where the wrong data goes to a wrong devices which leads to privacy violation; Inventory attack category focus on smart things which has the ability to be queried. For instance, an attacker can query devices and compile an inventory of devices on a specific location and finally linkage category is a threat that combines data about a subject from different sources and contexts.

2.2 Machine Learning Techniques

Machine learning is a field of study where algorithms and statistical models are used in a computer system to perform specific tasks without using explicit instruction. These algorithms and statistical models learn from the experience when performing a certain task (Perez, Astor, Abreu, & Scalise, 2017). Machine learning has been used extensively to analyze data in IoT (Moh & Raju, 2018). There are various types of algorithms within machine learning that can learn from the data collected (Cañedo & Skjellum, 2016), the difference depends on their approach to learn, the input and output data type and the intended task or problem to solve, algorithms such as nearest neighbors, neutral networks, k-means are a few examples. The selection on the type of algorithm to use for learning often relies on the amount of data required to train, training time, forecast accuracy and speed. Therefore, depending on the approach of learning, these algorithms can be categorized as follows: supervised, unsupervised and reinforcement learning.

2.2.1 Supervised Learning

Supervised learning technique is a task driven that develops a mathematical model of sets of data based on both input and desired output. This learning technique uses labeled sets of data to train the algorithm of which in the end the best function that describes the input data is selected. Therefore, known inputs and their corresponding outputs are provided for learning, eventually these information helps the machine to identify the output for a supplied input (Mamdouh et al., 2018). For instance, labelling an IoT device network traffic for identification purposes can utilize techniques such as Support Vector Machine (SVM), Naive Bayes, K-Nearest Neighbor (K-NN), and Neural Network (NN) to develop classification or regression models. (Xiao et al., 2018) Classification models are used

when the outputs are restricted to a certain category or class of sets of values while regression are used when the expected output has numerical value within a range. IoT devices can apply K-NN in network and malware detection (Xiao et al., 2018).

2.2.2 Unsupervised Learning

Unsupervised learning technique uses unlabeled data in training the algorithm which eventually detects the pattern and can describe a model (Xiao et al., 2018). In this case the input data enables the algorithm to mine for rules, detect patterns and perhaps summarize and group points eventually giving meaning and better understanding, this is because there is no output given. Clustering and association models are the main types of unsupervised learning algorithms. In clustering, a set of data is grouped together by identifying commonalities of the same group or groups that are similar to each other. Principal Component Analysis (PCA) and K-means are a few of the algorithms used.

2.2.3 Reinforcement Learning

Reinforcement learning technique allows algorithms to learn continuously from their environment experience and have the ability to determine an ideal behavior (Xiao et al., 2018). There are no known inputs with corresponding output. For instance, within IoT devices, algorithms such as Q-learning can enable these devices to choose security protocols and key parameters against various attacks. The algorithm interacts with the surrounding dataset for learning (M. Mamdouh et al., 2018). Q-learning has been used to improve performance in malware detection and authentication. Machine learning key tasks for instance includes the discovery of pattern in an existing data, detecting outliers, predicting values and feature extraction. This task is important to IoT security. (Moh & Raju, 2018) ML algorithms utilize this task. Table 1 shows the different machine learning algorithms used in each use case.

Table 1. Categorization of machine learning solution for IoT security.

Use Case	**Machine Learning Algorithm**
Pattern discovery	● K-means ● DBSCAN
Discovery of unusual data points	● SVM ● RF ● PCA ● KNN ● Naive Bayes
Prediction of values and categories	● Linear Regression ● Support Vector Regression ● CART ● FFNN
Feature extraction	● PCA ● CCA

Evaluation matrix

The performance of a machine learning algorithm is evaluated using several matrices such as classification matrices which includes classification accuracy, confusion matrix, area under receiver operating curve (ROC curve), logarithmic loss and regression matrices. For instance, among other models confusion matrix is often used to graphically visualize the performance of a machine learning model. The main criteria for classifying the results are true positive and true negative. This is the case where the entries are classified correctly has either belongs to positive or negative class respectively. The other criteria are false negative and false positive where the entries belonging to negative and positive class are identified incorrectly. As a result other performance can be derived from the classification such as accuracy which measures the percentage of correctly identified entries by the model; error rate which measures the percentage incorrectly classified entries; sensibility gives the percentage of entries belonging to a positive class that were identified correctly; specificity measures the percentage of entries of a negative class that were identified correctly; precision measures the percentage of hits over the entries of the positive class that were classified as belonging to the positive class (Perez et al., 2017; Vinayakumar et al., 2019).

Table 2. Machine learning solution for IoT security.

Attacks	**Security Technique**	**Machine learning algorithms**	**Performance**
DoS	Secure IoT offloading Access control	Neural network Q-learning	Detection Accuracy Root-mean error
Jamming	Secure IoT offloading	Q-learning DQN	Energy consumption SINR
Spoofing	Authentication	Q-learning Dyna-Q SVM DNN Distributed Frank-Wolfe	Average error rate Detection rate Classification accuracy False alarm rate Miss detection rate
Intrusion	Access control	SVM Naive Bayes K-NN Neural network	Classification accuracy False positive rate Detection rate Root mean error
Malware	Malware detection Access control	Q/Dyna-Q/PDS Random forest K-nearest neighbors	Classification accuracy Detection accuracy Detection latency
Eavesdropping	Authentication	Q-learning Nonparametric Bayesian	Proximity passing rate Secrecy data rate

The summary from Table 2 above shows various scenarios where machine learning techniques are implemented on IoT devices. Several methods can be applied to a single attack. The difference in the results from the evaluation matrix can be used to select the best method that has the best performance on a specific task.

2.3 Related Work

Studies covering the area of security in IoT devices using machine learning algorithms has majorly focused on individual attack models and used different machine learning techniques. For example, Intrusion detection has largely been focused in a number of studies. The methodology used in the majority of the previous study has been experimental, barely any review have been conducted so far. Therefore, this leaves a gap where a comprehensive review on existing literature where ML algorithms are reviewed with the goal of either identifying the most used algorithm and what could be done to improve their performance. Moreover, the new developments in this field has been growing up recently and the studies have to keep up with the trend.

In their recent study Hussain. F. et al., (2019) mentioned the current solution facing the IoT networks and the possible solution for the challenges identified by the use of ML and deep learning. In their discussion they mentioned the current use of machine learning and deep learning in solving several security problems in IoT networks. In specific they reviewed the security requirements in IoT devices, the attack vectors and the security solutions that are currently in use. In addition, they also identified the gaps that requires ML and deep learning approaches. In spite of the systematic review on IoT security solutions with ML solutions, the focus was not on evaluating the performance of an individual ML technique but rather the application of ML and deep learning (DL) techniques on various security challenges.

(Xiao et al., 2018) in their paper focused on data privacy. The attack models they focused on were authentication, access control, secure offloading, and malware detection, basically their review was on how artificial intelligence enhances security in IoT devices and also the challenges facing ML-based approaches as an IoT security solution that needed to be addressed. Their focus was on specific security issues on IoT devices and their ML solutions. This approach then leaves out other ML techniques that might not fall under the selected IoT security challenges as their solutions. Moreover, this study shows the vulnerabilities within the IoT environment when comparing the number of attack models studied in this study.

Fotios. Z. et al., (2019) reviewed the use of machine learning in IoT application. But their focus was on smart transportation such as route optimization, packing, street lights, and accident prevention/detection etc. Their review focuses on the application of ML techniques and IoT applications in improving transportation by creating intelligent transportation system. Although their approach included the combination of ML techniques and IoT devices their focus was not security but generally improving services which this thesis is focusing on.

Therefore, the contribution of this study is to conduct a systematic literature review on the implementation of machine learning algorithms in securing IoT devices. Identifying the most used ML technique in IoT will enable the understanding of what circumstances these techniques perform best and what could be done to improve their performance. In addition, it also shows the direction in which current research is focusing on and why those sections are creating concern for researchers. Within the IoT environment, there are several layers that are vulnerable to a number of security challenges. For instance, physical layer, network layer, transport layer and application layer and ML approach could be applied more on layers such as network layer rather than physical layer. The challenges facing security in IoT devices are unique to the traditional security solutions. The IoT devices differs based on the functionality, this result in difference in data type collected from the sensors of which has to be processed differently.

3. Systematic Literature Review

This chapter discusses the procedures of conducting the SLR for this thesis. First, an overview of the research method is presented and the key stages are discussed. Then, following the stages of SLR, each stage is further elaborated in-depth accordingly.

3.1 Overview of Systematic Literature Review

Kitchenham & Charters (2007) defined that "A systematic literature review is a means of identifying, evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomenon of interest". The research for this thesis has been carried out according to the SLR guidelines provided by Kitchenham & Charters (2007). Literature review process has to follow a predefined search strategy. SLR is divided into three main phases: planning the review, conducting the review and finally reporting the review.

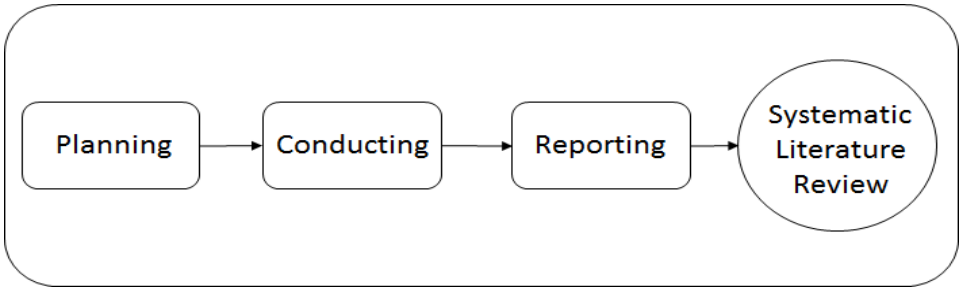


Figure 1. Systematic literature review process (Rai et al., 2015)

The planning phase mainly consists of three stages, namely: the identification of the need for a review, specification of the research questions and then followed by the development of a review protocol where appropriate keywords and search strings are selected. The conducting phase includes a number of stages, they are: search strategy that focuses on identifying primary studies resources, selection criteria which involves inclusion and exclusion to obtain potentially relevant primary studies for the review, quality assessment and data extraction. Finally, reporting phase comprises of specification of dissemination mechanism, formatting the main report and evaluation of the report. The aim of these phases is to obtain reliable and valid results. A detailed process of an SLR is further depicted in the Figure 2 below, based on Kitchenham & Charters (2007).

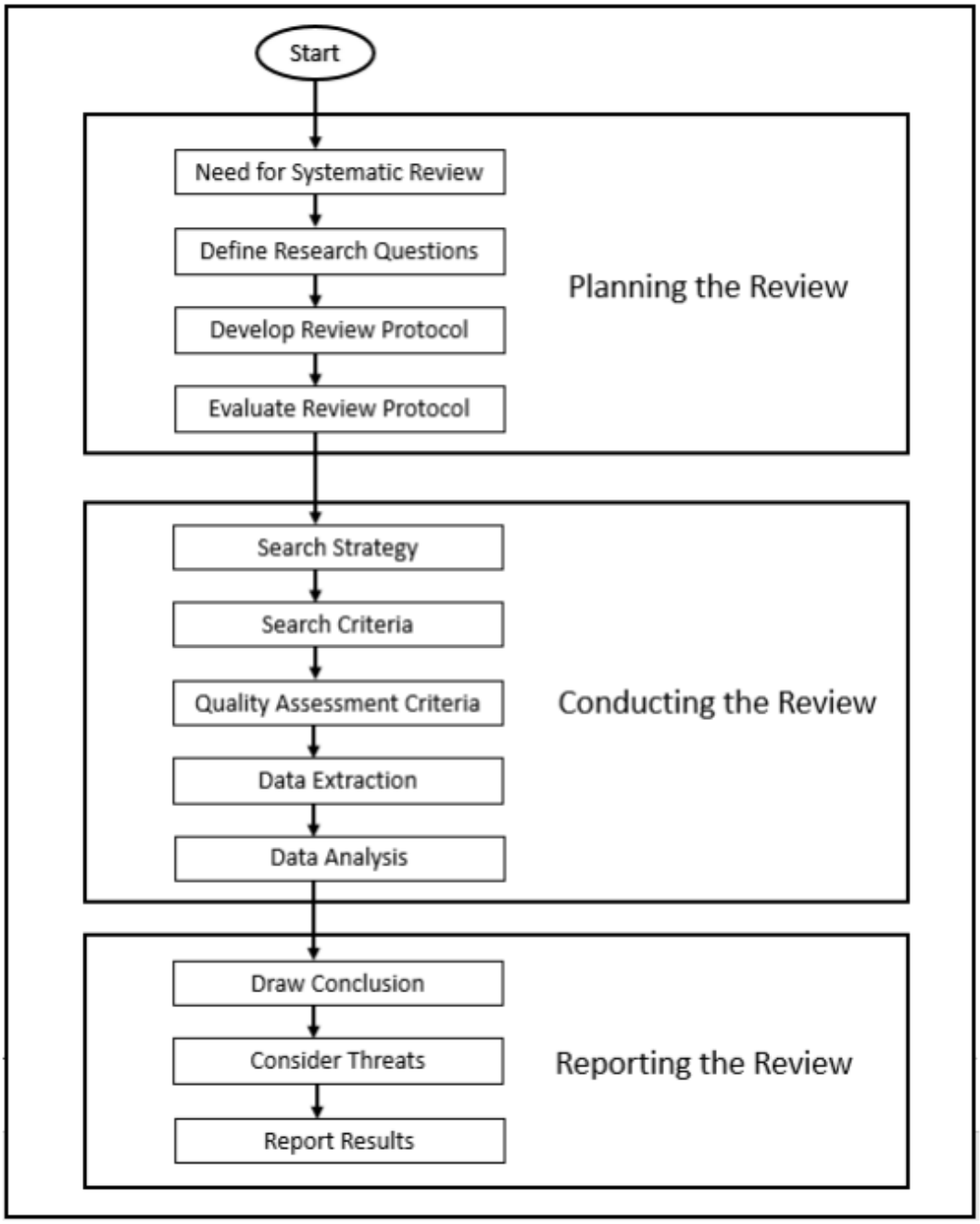


Figure 2. Steps that are followed for SLR (Kitchenham & Charters, 2007).

3.2 Planning the Review

The planning phase as mentioned earlier consists of steps of guidelines to be followed in the process of conducting the review. The first step in the planning phase of the review is the identification of the need for the review, thereafter, the specification of the research question then the development of a review protocol. The main steps associated with planning the review are explained in the following subsections, adopted from Kitchenham & Charters (2007).

3.2.1 Identification of the need for Systematic Review

The need for undertaking a systematic review is to summarize the existing literature on the use of ML techniques for securing IoT devices. Further studies are needed to explore the application of ML in IoT security. Therefore to accomplish this SLR is needed to extract and analyze ML techniques employed in securing IoT devices.

3.2.2 Research Question

The following research questions are defined and intended to be answered through this thesis:

RQ1: What is currently known about machine learning techniques in securing IoT devices?

RQ2: What are the machine learning techniques commonly used in IoT security in the existing literature?

The research questions are formed with the aim of studying machine learning techniques as a solution to IoT security issues based on the existing literature. The purpose of the first research question (RQ1) is to identify what is known regarding the use of ML techniques as a security solution in IoT devices. Issues relating to utilization of machine learning techniques on improving the security of IoT devices will be answered in RQ1. The second research question (RQ2) aims to identify different ML algorithms used in IoT security. The relevant information regarding the usage of machine learning in IoT security from each primary study are also extracted.

3.2.3 Developing Review Protocol

The review protocol specifies a set of procedures that has to be followed while conducting a systematic review (Kitchenham & Charters, 2007). The goal is to describe a detailed plan that will enable the collection of relevant study material for answering the research questions. The other importance of the predefined review process is to reduce the

possibility of the biases of the researcher. The guidelines for conducting SLR review process adapted from Kitchenham & Charters (2007) provides a structure for developing the protocol. In addition, it is recommended that the review protocol should be evaluated by an expert. Appendix A presents the review protocol for this study.

3.2.4 Search Strategy

The goal of search strategy is to find as many suitable studies that relates to the research questions. Kitchenham (2004) mentioned the importance of unbiased search strategy for primary studies, therefore, to achieve this, the search strategy is applied on several electronic databases to extract primary study papers. In order to get an idea about the quantity of the articles in this field, a pilot search is performed.

Pilot Search

The importance of performing a pilot search as proposed by Kitchenham & Charters (2007) helps in identifying potential studies by following the review protocol which defines the search string and the resources that are used. A pilot search was performed on Google Scholar for this study in order to get an overall idea on the available number of literatures. The reason Google Scholar is chosen for the pilot search is because it has literature with diverse fields of study. The pilot search was performed with a default search options on Google Scholar using the input keyword 'machine learning in Internet of Things Security' without the quotes.

A result of 396,000 were found, this included articles, books, magazines, chapter, patents, citations etc. Then, the keyword was modified by inserting quotes around the keywords and the results was 0. This indicates that "machine learning technique in internet of things security" as a single concept brought no interest yet, hence, it does not provide articles for this search. Upon refining the search results further with the word 'machine learning' added along with 'internet of things security' both with quotes provided a results of 897 papers. Next, the addition of the word 'technique' to the previous search string without quotes gave a result of 290,000. Therefore, the outcome indicated that separate keyword provided more search results than a single search term. This also showed that there are considerable amount of literature on this topic.

Based on the results from the pilot search, the strings were further modified by adding various search phrases, synonyms and related terms for each concept and applied to the advanced search options in the selected database. Google Scholar searches a number of resources such as articles, books, theses, abstract, PowerPoint etc. which may not be related to information security. Hence, the search keywords are applied to a few databases which are considered to include the majority of the studies in the information security discipline so as to get more precise and relevant results for the study. The selected database included IEEE Xplore, Web of Science and Scopus.

Refining criteria was applied at the database to get more related studies on the topic. The criteria included selection by year (articles published between 2016 and 2019), subject area (Information science and security, machine learning) and language (English). The results of the search in each database are presented below in Table 3.

Table 3. The results from pilot search.

Search Keywords	**Database**	**Result (First hit)**	**Result (After applying selection criteria)**
(machine learning) AND (internet of things) AND (security)	IEEE Xplore	334	25
	Scopus	342	17
	Web of Science core collection	178	23
Total		854	65

The addition of synonyms and related terms to each keyword resulted into a more relevant and related studies. Learning the results from the pilot search, additional search criteria was defined when applying the search for the actual string. This also consist the advanced search option which included search operators (such as OR, AND) that were applied to the selected database. The actual search string and database are discussed below.

Search Strings & Database

The main goal of a search string is to identify suitable sources which are closely related to the field of study and help in answering the research question of the study. Three scientific databases were used for acquiring relevant studies related to the research questions in this study. In addition to handling advanced search queries, another reason for selecting these databases is their coverage and use in the domain of information security. The search string is thereafter applied to each of the following databases; IEEE Xplore, Scopus and Web of Science, all the three database contained a number of peered reviewed articles collection with a few containing full text.

3.2.5 Selection Criteria

The selection criteria as previously described in the review protocol gives the procedure that enables the identification and selection of relevant primary study material from the

searched results. The aim of the selection criteria is to be inclusive to all retrieved papers which are related to ML techniques in IoT security. The selection of relevant materials based on the selection criteria are inclusion, exclusion, and quality assessment criteria which are designed based on the research question of this study. The inclusion, exclusion and quality assessment criteria are presented below as follows:

Inclusion Criteria

The following inclusion criteria were applied to this study:

- The material should be written in English
- The material should be available in full text
- The material should be published between the year 2016 and 2019
- The material directly answers one or more research question of the study
- The material should focus on IoT security and machine learning techniques

Exclusion Criteria

The following exclusion criteria were applied for this study:

- Not in English
- Duplicate articles
- Papers written before 2016
- Studies that do not focus on machine learning techniques and IoT security.
- Not peer-reviewed scientific papers (i.e. presentation, blog posts, etc.)
- Studies related to established companies

Quality Assessment

Beside the general inclusion and exclusion criteria, in SLR it is considered crucial to assess the quality of the primary studies. Kitchenham & Charters (2007) mentioned that the quality assessment criteria as an instrument that is used to provide more additional and detailed information already gathered from the inclusion and exclusion criteria on the weight of individual studies when synthesizing the results. Furthermore, quality assessment help in guiding and determining the strength of inference and interpretation of the findings from primary studies. Each study is evaluated for quality assessment, the measurement is based on questions from a checklist. Although there is no agreed definition of quality (Kitchenham & Charters, 2007) the checklist is applied in order to reduce biases and to assess the quality.

Therefore, to assess the quality of the primary studies and to reduce the bias quality criteria checklist was applied. A total of five questions were created to assess the quality. The structure of the checklist questions are formulated in a way that ensures that the selected papers address the research questions. All papers that satisfy the selection criteria were selected for the review. The selected papers were studied and analyzed to answer the research question. The questions that were used to evaluate the quality of the

paper are presented in Table 4.

Table 4. Checklist for quality assessment (Sheuly, 2013).

Quality checklist questions	Yes or No
Does the paper mention the objective clearly?	
Are the results defined clearly in the paper? Are the results helpful to answer the research question?	
Does the paper clearly mention about IoT security?	
Does the paper clearly mention about machine learning in IoT security?	
Does the paper describe clearly the research methodology used?	

3.3 Conducting the Review

The actual literature review is the execution of each step as described in the review protocol. The database and the search strings were identified from which thereafter the SLR is performed. The search string were applied on the selected database as described in the search strategy. Upon obtaining the relevant papers for primary study, selection criteria is applied to check the relevance of the paper, this includes the quality check to identify whether the quality criteria is met.

After the quality assessment, the selected primary studies are studied and analyzed thoroughly to extract data which are stored in a defined data extraction form. Thereafter, the information from the primary studies is accurately stored and synthesized later in order to present the results of the reviewed primary studies. The analysis of the extracted data from the selected studies provide the answer to the proposed research question for this study. During the process of conducting a literature review the search process and the results are documented in sufficient detail for readers so as to be able to go through the thoroughness of the search and to be transparent, replicable and possible to further reanalyze.

3.3.1 Selection Process

The selection process is a multistage process that involves several stages that facilitate and ensure that any relevant papers are included for the study. This process describes the actual implementation for selecting the literature by applying the search strategy in

respect to the review protocol. The process of selecting papers for this study is presented in appendix B. This provides a guideline in ensuring the selection of the papers. In order to obtain primary studies for this review, the search string was applied to the selected database. The final search phrase was:

> (Machine learning* OR machine learning technique*machine learning algorithms*OR machine learning methods) AND (Internet of Things* OR IoT) AND (Security*OR security issues*OR security challenges*OR cybersecurity)

The results of the tailored search strings according to the syntax requested by each of the three scientific databases are presented in Table 5 below. A total of 855 articles were obtained using the search string.

Table 5. Selected database and results for this study.

Database	**Number of Papers**	**Number of Papers Excluded at the database**	**Remaining number of papers**	**Duplicates**	**Total**
IEEE Xplore	335	315	25	25	78
Scopus	342	301	41		
Web of Science	178	141	37		
Total	855	757	103		

The selection of the papers from the database was the next step. This step utilizes the individual database refining technique, for instance filtering by subject area, publication year, document type and language. Regarding the topic of this study, information technology and computer science subject areas are considered. The publications between 2016 and 2019 are also included in the search. Besides that, document type such as conference publications, journals and magazines, articles, conference review, books, chapters and articles in the press are included in the search. Therefore, as a result 757 papers are excluded and a total of 103 papers are selected for further selection.

Inclusion and exclusion criteria was applied to list of papers in order to remove the irrelevant papers. Through the analysis of the title, abstract and keywords of each paper, and with the implementation of the exclusion criteria, irrelevant paper were identified and excluded. A total number of 20 papers matched the exclusion criteria, hence excluded from the study and the remaining paper proceeded for inclusion criteria. The search

results of individual database are presented in appendix C., the excluded papers majorly consisted of papers that did not focus on the topic. For instance, non-peered review papers.

The next step was inclusion criteria, which further narrowed down the selected papers emphasizing their relevance to the goal of this study. During the application of inclusion criteria, the abstract of each paper was reviewed in-depth with the intent of matching with the guidelines of inclusion criteria. This resulted to a selection of 58 papers. The basis to include a paper was that it should clearly state its focus on machine learning techniques, IoT and security issues. For example, papers with the focus on machine learning data analysis were excluded at this stage.

Finally, quality assessment criteria was applied as the last step in the selection process so as to ensure that the selected papers were the most relevant in the view of answering the research questions in this study. This process involved reading the full-text of the paper. The relevant study papers were selected after reading through the entire paper. As a result, a total of 20 primary studies were chosen and were considered for the final review.

3.3.2 Data Extraction Strategy

The data extraction strategy was used to gather all the information necessary to address the research questions. Through reading the full-text of each of the selected materials, relevant data was extracted. The goal of the extraction process was to extract and record relevant data for primary studies. Therefore, an excel sheet was prepared for data extraction and recording according to the category of each primary paper. The following data were extracted from the selected primary studies.

- The primary information about the paper, this includes author(s), title, publication, year, and keywords.
- The machine learning algorithms used in IoT security
- The attack models that uses machine learning techniques

3.3.3 Data Analysis

According to Kitchenham & Charters (2007), data analysis implies that the results of the primary studies are examined and summarized. Therefore, in this thesis to analyze the extracted data quantitative data analysis approach was used. A quantitative data analysis focuses on integrating studies comprising of natural language results and conclusions, more importantly where different researchers may have used terms and concepts with subtly different meaning (Kitchenham & Charters, 2007). Therefore, for this thesis this

technique was used to answer both RQ1 and RQ2.

During the data extraction process from each primary study, the main concepts related to machine learning techniques and IoT security issues are identified based on original author's term. In order to enable and facilitate comparisons across different studies and to ensure efficient extraction of findings of the research questions the main concept were organized in a tabular form. In summary, the data analysis is achieved through the following; identification of machine learning techniques, documentation of set of reported machine learning techniques and elaboration of gaps.

3.4 Reporting the Review

The final stage of a SLR involves reporting the results of the review. The results of the systematic review are written. The relevant primary studies were selected of which thereafter the data is extracted into a form. The collected data is synthesized using appropriate data synthesis technique and finally the results are reported in the following chapter.

4. Results

This Chapter presents the results of the SLR process as discussed in the previous chapter. Having passed the selection criteria, a total of 20 primary studies were selected from the initial selection of 248 studies. The next section are presented as follows, Section 4.1 describes the overview of the studies and section 4.2 presents the analysis of the results.

4.1 Overview of the Results

The following subsection discusses the overview of the selected primary studies with major classification. The primary studies varies in their research approach by focusing on different security issues and solutions on the devices network. Each primary study has been assigned a unique study ID for easy referencing in this SLR. The list of primary studies is attached to the appendix D.

4.1.1 Publication Trend

The selected primary studies were not limited to a specific period of publication, actually all the papers were recent. However, the results have shown that the selected papers happened to have been between the year 2016 and 2019. The distribution of papers published on machine learning techniques in securing IoT devices are presented in Figure 3.

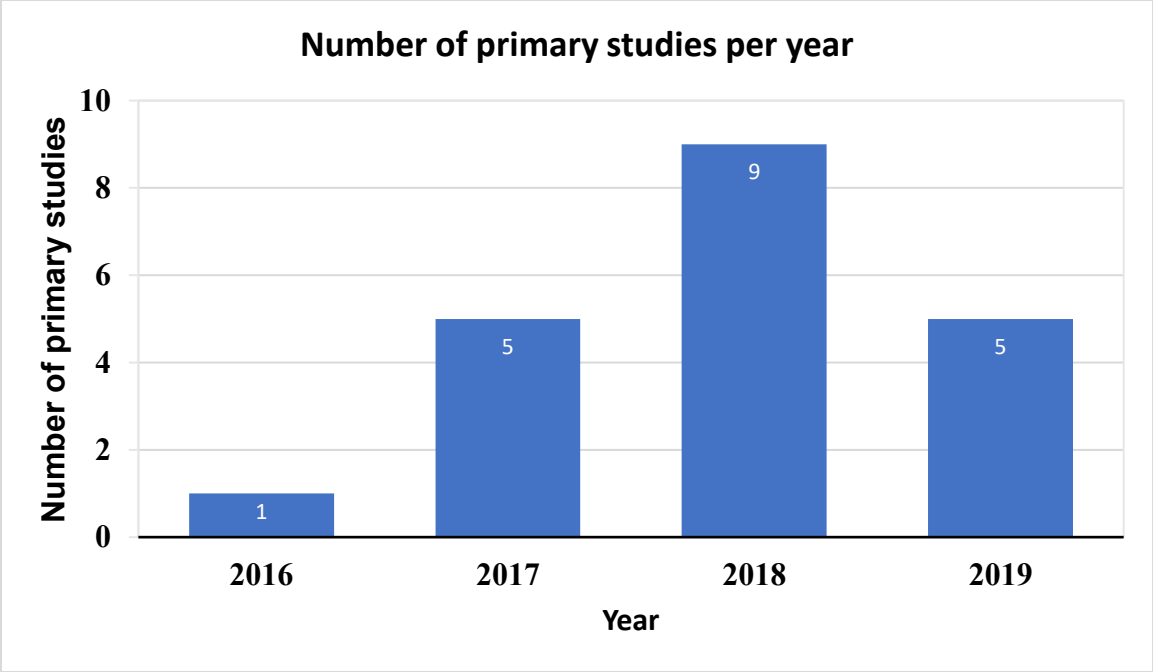


Figure 3. Publication distribution by year.

From the distribution of the studies, there was a significant increase in the number of studies published 2018. In 2019, there is a decrease in the number of papers, but this is because the search date of the systematic literature review procedure was conducted on March 2019. Therefore, from the distribution of the studies it can be argued that there is a growing interest in the area of IoT security specifically where machine learning techniques are implemented as a solution.

4.1.2 Research Focus

The primary studies were categorized into groups based on the research focus of the paper. The categories are intrusion detection, malware detection, authentication, anomaly detection and others. The 'other' category included papers that could neither be classified into the mentioned categories above but could be between the boundaries of IoT security and machine learning approach. The studies that mentioned ML techniques in IoT security were taken into consideration. The classification of the primary studies based on the research focus are shown in Figure 4.

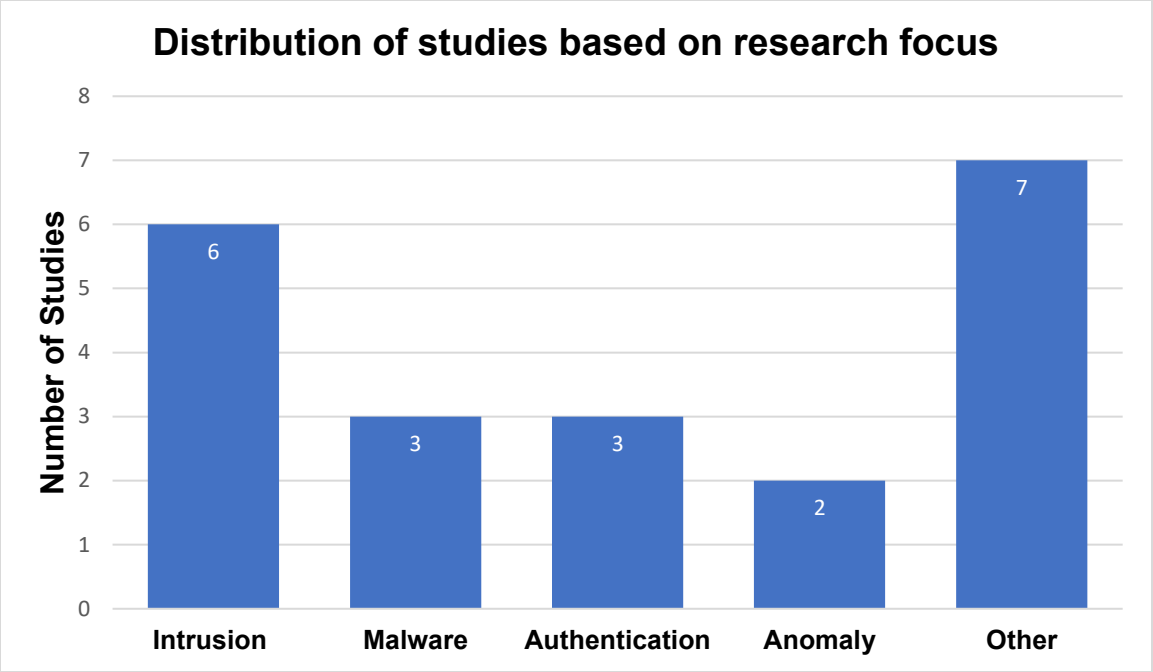


Figure 4. Distribution of primary studies based on research focus

Intrusion detection: The category includes ML techniques used to monitor network traffic within the IoT environment for malicious activity or policy violation. 6 out of 20 primary studies indicated that their research area is focused on network security. For instance, study [P9] provided a lightweight attack detection strategy for IoT devices. The conventional intrusion detection method such as signature-based intrusion detection are does not have the capability to withstand security threats due to the growth, complexity and ambiguity of IoT devices. This study utilized machine learning technique in their simulation by using supervised learning method SVM to detect adversary attempts to inject unnecessary data into the IoT network. SVM was used as a classifier in the training phase, the features from a training datasets containing labeled samples were extracted and later used to train the classifier. Later, the trained classifier is used to classify unobserved datasets. This approach protects the network from attacks such as DoS. The results were satisfactory in terms of classification accuracy and detection time. Study [P17] has a focus on securing medical devices by using ML features to profile the devices accurately and observing for its abnormal behavior. DT was used classification algorithm. During the training phase DT was used to create a normal profile of a device network, additionally, new sets of features which were developed specifically for security attributes were included in the learning model. The features selected mainly focused on the typical usage of the medical device. The features includes the type of action, time of action, number of action occurrences, time interval since last occurrences, signal strength indicator, the day when the device was accessed and the location of the device. Study

[P13] in their experiment has also focuses on securing network edge for IoT devices by utilizing ML classifiers to develop a fog assistant Intrusion detection and prevention system. Recurrent neural network (RNN), Multi-Layer Perceptron (MLP) and alternate decision tree (ADT) classifiers were used in parallel. RNN and MLP focused on monitoring the traffic, the output identified whether the traffic behavior was normal or under attack. In case of an attack ADT classifier determines the type of the attack.

Malware detection: The category mentioned ways in which IoT devices are protected from malicious software programs that can cause damage to device or infiltrate to the data within the device. 3 primary studies focused on detecting malware in IoT devices using machine learning techniques. Study [P1] has a focus on detecting ransomware attack on IoT devices. Their approach used ML technique to monitor the power consumption patterns on android devices as a way of identifying and classifying ransomware attacks and non-malicious applications. KNN, NN, SVM and RF were used as classifiers. Considering the power usage sequence as time-series data and with Dynamic Time Warping (DTW) used to classify distance based time-series for distance measure, ML classifier such as KNN was used to simulate the distance. Samples were aligned together based on the distance in between. Study [P10] also focused on android devices by implementing and analyzing the use malicious app detection tool. This approach consisted of ML techniques in monitoring the behavior of system functions to identify abnormal behavior. Study [P11] approach to IoT security on android devices testing framework. It demonstrated the use of machine learning techniques on Android malware detection system and more importantly tested and compared various machine learning algorithms on their implementation process for evaluation.

Authentication: The category includes ways in which IoT devices are identified and verified to grant access control. 3 out of 20 primary studies has a research focus on enhancing authentication within the IoT environment using machine learning. Study [P2] has a focus on authentication of the IoT devices wireless nodes by utilizing RF communication framework on the wireless transmitter and utilized ML to detect on the receiver. ANN was trained with pseudo-random bit-streams to help in detecting data variability in evaluation stage. This approach allows real-time authentication of wireless nodes. Study [P4] also focus on authentication by using wearable brainwave headsets to collect brainwave reactions from the user. The brainwave data collected features were thereafter extracted using ML approach so as to serve as authentication tokens. Study [P6] describes the authentication of IoT devices through their radio frequency by using Permutation Entropy (PE) and Dispersion Entropy (DE) statistical features. The application of ML classifiers namely; SVM, KNN and DT had a little improvement on the accuracy in identification of the device.

Anomaly detection: The category includes way in which identification of rare items, events or observations that differs significantly from the normal behavior of a device within a network. Study [P8] experimented the use machine learning techniques in securing IoT systems. The study investigated the use ML technique in network gateway to detect anomalies in the data from the edge devices, by training the network to detect invalid data points. Their approach was not focused on specific area of IoT devices such as authentication or access control but the IoT system as a whole by monitoring the system behavior. In the training phase NN classifier used data samples as training data and to learn the healthy state of a system. At the testing phase NN was able to determine valid and invalid hence predicting invalid data points successfully.

Other: The category includes way in which a number of ways in which the security of IoT systems are implemented using machine learning techniques. The studies in this category were not group into the above categories because there focus could be grouped into an independent group. 7 out of 20 primary studies were in this category. Study [P3] has a focus on the use of ML techniques in implementing a smart trust management method to automatically assess the IoT resource trust and evaluate services provider attributes. [P12] in the efforts of detecting potential insider threat utilized the user's social media to analyze sentiments posted. ML techniques were used to find possible malicious insider. Also, [P14] demonstrated the use of ML in monitoring IoT network traffic behaviors to detect Distributed Denial of Service (DDoS). Study [P16] focused on detecting phishing websites. Their approach on improving existing phishing detection technique included the use of ML to aggregate and analysis on page layout in order to determine page layout similarity, hence detecting phishing pages. Study [P20] experimented on identifying unknown operating systems.
All of the primary studies were related to the use machine learning techniques in securing IoT devices, which was fundamental to the research questions (machine learning techniques in IoT security). Therefore, this indicates that the selected primary studies has a high relevance and strong contribution to answer the research questions.

4.2 Analysis of Results

The following section discusses the results of SLR related to the type of machine learning algorithms used in securing IoT devices and IoT attack models. The two aspects are most relevant in relation to the research question of this thesis.

4.2.1 Analysis of machine learning algorithms

The list of primary studies along with the used machine learning algorithms are presented in table 10. Based on the collected data from the primary studies, this study indicates that SVM is the most widely used machine learning algorithms in securing IoT devices.

Table 6. Frequency of ML techniques and primary studies.

Machine learning algorithm	**Frequency**	**Reference**
Support Vector Machine (SVM)	11	[P1] [P3] [P4] [P5] [P6] [P7] [P9] [P12] [P14] [P19] [P20]
Neural Network (NN)	10	[P1] [P2] [P3] [P5] [P7] [P8] [P11] [P13] [P14] [P15]
Decision tree (DT)	9	[P6] [P7] [P10] [P11] [P12] [P13] [P14] [P17] [P20]
Random Forest (RF)	3	[P1] [P11] [P14]
Naïve Bayes	6	[P3] [P4[P7]] [P10] [P12] [P18]
K-nearest neighbors (KNN)	3	[P1] [P6] [P7] [P14]
K-means	2	[P5] [P12]

There are other machine learning algorithms which were identified from the primary studies includes; Neural Network (NN), Decision Tree (DT), Naive Bayes, Random Forest (RF), K-nearest neighbors (KNN), and K-means. A majority of the primary studies used more than one ML algorithms in their study. A few studies used one ML algorithms in the studies [P2], [P8], [P9], [P10], [P15], [P17], [P8] and [P19]. The list of machine learning algorithms reported in individual primary study is presented in the list in Appendix E.

Park et al. [P12] in their study made a comparison between supervised and unsupervised learning algorithms in detecting malicious insider, based on the results they concluded that supervised learning had a higher accuracy rate based on evaluation matrix in the detection malicious insider threat. The complexity of the algorithm has a direct impact on the performance and accuracy [P9], in supervised learning the dataset simple because they are controlled and does not require complex algorithm. Moreover, the comparison within the both supervised ML technique show varying results. For instance, within

supervised learning DT had the highest accuracy rate followed by SVM, linear and Naive Bayes respectively. [P11] also made a similar comparison and evaluated their results on their accuracy, precision and recall.

Support Vector Machine

SVM is a supervised learning technique that generates input and output mapping functions from a set of labelled training data. The functions used for learning in this learning technique are either classification or regression. Primary studies indicated that SVM is the common machine learning algorithm used in IoT security. A total of 11 studies discussed the SVM approach in IoT security ([P1] [P3] [P4] [P5] [P6] [P7] [P9] [P12] [P14] [P19] [P20]). One of the reasons for its popularity is its efficient in performance [P9]. In comparison to other algorithms as mentioned in [P19] it can overcome noise and also work with little or no prior training, also SVM do not have additional feature selection properties that is why it takes less training and testing times [P9]. However, according to [P14] the results from their experiment indicated that SVM detection with linear kernel performed poorly as compared to DT and KNN. This shows that difference in data type affects the performance of the ML technique. In this primary studies SVM was widely used in intrusion detection and authentication as ML technique of choice.

Neural Network

Neural network is a model used in deep learning. Deep learning is a subfield of ML which used algorithms inspired by the structure and function of the brain's neural networks and has input, hidden and output layers. The number of primary studies that focused on ANN were [P8] and [P2]. [P15] mainly focused their studies on DNN which is a still ANN but with multiple layers between input layer and output layer. [P8] addressed the issues of anomaly detection within the IoT system with neural network. Their approach was to train the network to detect invalid data point. On their study [P2] used ML in enhancing IoT security through authentication of wireless nodes. 8 primary studies mentioned the use of neural networks which includes ANN and RNN [P1], [P3], [P5], [P7], [P11], [P13], [P14], [P19]. The algorithms were either combined with other algorithms such as [P19] where they used SVM and neural network to guarantee wireless communication or as a comparison of with the other algorithms, for instance, [P11] compared NN, LR, DT, RF and ET in testing malware detection system in IoT systems.

Decision Tree

A total of 9 out of 20 primary studies in ML techniques have used DT algorithm. DT algorithm is a supervised learning which has also taken attention of several authors alongside SVM and ANN. For instance, DT has been explored in several cases regarding the security in IoT systems. Primary studies [P17] [P11] [P14] [P13] [P10] [P12] mentioned the use of DT in intrusion detection while [P6] [P20] mentioned the use of DT in identification of unknown operating system type in IoT and physical layer authentication

of IoT wireless devices.

[P17], compared the performance of DT with SVM and K-means in their study when experimenting these ML algorithms on determining attacks targeting medical devices. In their conclusion, DT had the highest detection rate, low false positive rate first training and prediction speed compared to SVM and K-means. However, they also mentioned that there was a failure of the algorithm to detect and provide similar results as previously shown if the attacker is familiar with the device and know the schedules and the data patterns. [P12], evaluated and compared both supervised and unsupervised learning in detecting potential malicious insider. DT had the highest accuracy overall, also supervised learning perform better in detecting the threats compared to unsupervised learning.

Naive Bayes

Naive Bayes is among one of the ML algorithms used in securing IoT devices. This algorithm is commonly used in categorizing word-based documents such as spam [P18]. Six primary studies [P3] [P7] [P10] and [P18] explains that the implementation of security in IoT devices used Naive Bayes. [P18] describes that the accuracy of Naive Bayes is at least high with the amount of training data that is required to estimate input values. It is also suitable for an environment where feature space dynamically changes. [P10] compared Naive Bayes and DT algorithms in detecting malicious mobile malware in android application with an inclusion of Androidetect system. Androidetect system is a tool that automates the detection malicious application. The results from their experiment proved that the combination of ML algorithms and Androidetect system has a better detection rate of malicious application.

[P3][P7][P12] in their experiment also made comparison of Naive Bayes with other ML algorithms. The comparison SVM, Naive Bayes, NN, KNN from [P3] in detecting on-off attack on IoT devices by using smart trust management method showed that Naive Bayes had high in precision rate and recall but not the favorite in F1-score. Moreover, according to [P7] the results from their testing data showed that Naive Bayes had the least time to train compared with SVM and ANN which takes time to train. The reason for the least training time is that Naive Bayes uses primitive operations. On the other hand, [P12] explains that low detection accuracy in Naive Bayes as compared to DT, SVM and Linear is as a result of the data type that was used in this study.

Random Forest

Random forest is an integrated learning where a number of sample input are selected from the original training set through the bootstrapping resampling technique [P11].

According to [P11], RF was among the algorithms used in adversarial samples on android malware detection system for IoT systems. From their performance result RF accuracy was high in comparison to NN, DT and LR. [P1] in their experiment also compared RF with NN, SVM and KNN in detecting crypto-ransomware in IoT networks. The analysis of their performance of classifying algorithms concluded that RF had the second highest detection, accuracy, precision rate and F-measure behind KNN. [P14] compared RF with KNN, SVM, DT and NN when experimenting the detection of DDoS in IoT consumer devices. The test set accuracy from all the algorithms were higher with just a small difference with SVM which was the lowest.

4.2.2 Analysis of Security Issues

There are several security issues identified from 20 primary studies. The security issues are categorized into five categories, it includes intrusion detection, malware detection, anomaly detection, authentication and other. The categorization is based on the research focus, presented in section 4.1.2.

Intrusion detection

Intrusion in computer network security refers to the activities where outside entities attempts to infiltrate a network to gain access to a device in order to steal information [P5]. Intrusion detection systems has been used before but with the new age of IoT new challenges arise for instance, the majority of IoT devices have limited resources run complex security solutions hence the systems are no longer effective. A lightweight intrusion detection system as mentioned in [P9] seem to provide a solution that could benefit IoT devices, it uses machine learning algorithms in detecting attempts that inject unnecessary data into a network and [P17] focusing on securing medical devices. With the nature of IoT systems which consists of various devices that generate a large volume of data it tends to overwork intrusion detection systems, therefore, to improve the detection rate various machine learning algorithms are combined [P19], forming hybrid systems with better performance [P15].

Malware detection

Malware attacks results into loss of sensitive information, disruption of regular operations or even direct or indirect financial loss, for example ransomware. The solution presented for this kind of attacks are using ML techniques in identifying patterns of specific feature behavior to distinguish malware from a non-malicious application [P1]. Malicious detection tools based on ML approach improve the detection rate by combining system function in Android devices [P10].

Anomaly detection

The behaviors that seem unusually or as not intended tend to raise alarm especially when it refers to security issues within the IoT, therefore, the ability to detect anomalies is important and even better if it is known earlier before causing any damage. [P8] approached this security issue by detecting anomalies in the data sent through a gateway devices from the edge devices. Gateway devices connects edge devices to the internet while edge devices has a single purpose such as collecting the temperature data. The anomaly detection method focuses on identifying the abnormal behaviour of the device.

Authentication

Authentication in IoT devices is a challenge due to the nature of the devices, hence traditional methods of authentication does not apply. For example IoT devices lack functional user interface where user can interact. For this case new ways of authentication is required so as to gain access to the system securely. Several ML learning techniques were used to obtain accurate classification on radio frequency fingerprinting identification and authentication [P6]. Study [P2] further improved the radio frequency authentication by including a real time network-based framework to authenticate wireless nodes through wireless transmitters and receivers. This approach of wireless node authentication eliminates key-based identification of IoT nodes also, it is a low cost secure authentication since it does not require additional hardware for the transmitter.

5. Discussion

This section of the thesis discusses the findings of the SLR and answer the research questions defined earlier.

RQ1: What is currently known about machine learning techniques in securing IoT devices?

The use of ML techniques in securing IoT devices is still at an early stage. The number of IoT devices have been on the rise, it can be argued that the combination of ML and IoT security has recently gotten attention from the industry and academia. ML algorithms have been used as a solution on various attack models. This approach has mostly focused on network security. Intrusion detection systems, and authentication are few examples where machine learning algorithms have been largely used in IoT security.

IoT devices pose a security challenge to existing security measures due to their heterogeneous nature. For instance, IoT systems consist of different types of devices, methods of communication, types of data, various resource level of devices and perhaps system configuration. As a result, this increases the attack surface. With the ability of ML algorithms to deal with complex data structures, scalability and big data it is suitable for implementation in IoT security.

Based on the analysis of the primary studies, SVM is identified as the most popular machine learning technique used in IoT security. SVM in most cases had a better performance based on the evaluation matrix as compared to other ML techniques. The performance of the algorithm is affected by the structure of the data. Other techniques that are also used in securing IoT devices are NN, DT, Naive Bayes, RF, KNN and K-means. It is important also to mention that the results of the performance can vary depending on the data type.

Despite the measure of the ML technique based on the performance it is difficult to conclude that an individual technique is better than the rest because within the IoT environment there are different devices and components. For instance, SVM has a better performance in authentication but performs poorly on Intrusion detection of which NN performs best. Therefore, there are quite a number of differences that makes it difficult to make a conclusion on a specific ML technique.

RQ2: What are the machine learning algorithms commonly used in IoT security in the existing literature?

The primary study shows that there are 7 different ML algorithms that are used in IoT security. The algorithms consist of supervised and unsupervised learning methods. Supervised learning methods are more efficient in detection rate as compared to unsupervised learning. The output data in supervised learning is known and therefore the input data is mapped based on the desired output and this makes these algorithms to have better performance in terms of detection accuracy and training time. In comparison to the unsupervised learning where the output data has unknown parameters and therefore the ML algorithm has to harvest rules to process the input data. Unfortunately there was no ML learning technique based on reinforced learning in the primary studies selection for this thesis.

The most commonly used algorithms in IoT security includes SVM, ANN, DT, RF, Naive Bayes, KNN and K-means. The SLR also reveals that ML algorithms can be combined in order to improve the performance. The performance metrics, data type and training time are considered the most important when selecting an appropriate algorithm.

SVM is the commonly used ML technique in this study. It was used in intrusion detection and authentication. NN was the second method of choice, DT, RF, Naive Bayes, KNN and K-means followed as other methods used in this study. Generally, ML technique approach was used more on securing the IoT network. The WSNs in IoT facilitates the communication, for instance, these devices have limited resources such as memory and since they rely on cloud services for storage, wireless communication is crucial to run the functionality of the devices, therefore the same feature that enables the functionality of the devices can also be a point of attack. The IoT environment creates a challenge for traditional security solutions, therefore with the application of ML techniques in ensuring the security of IoT there is a significant improvement in IoT security.

6. Conclusion

The results show that the use of machine learning in securing IoT devices is a new and interesting research topic. The growth in the use of IoT devices in today raises concerns about security and privacy. Due to the nature of IoT environments such as heterogeneity, the majority of these devices are still vulnerable to different forms of attack. ML approach in securing IoT devices through the network is considered a promising solution at the moment. Security issues in IoT still remains a challenge as it involves quite a number of stakeholders.

The performance of ML algorithm is evaluated based on the evaluation matrix. The duration of the training time depends on the ML techniques used for example if supervised or unsupervised learning method is used. Besides the technique, data type also affects the training time and the evaluation matrix. Complex data type take more time to process and may result in low accuracy detection rate. Other evaluation matrix includes accuracy detection, precision, F1-score, true positive, false positive ROC curve.

The results show an increased interest in the use of ML techniques as a solution to IoT security. The publication trend indicates that the publications on the topic have recently increased. The research focus classification also shows that practitioners are more interested in network security in IoT devices. Wireless sensor networks are the main building block of IoT devices, it enables data transfer that supports the functionality of the device. The networks are prone to various types of security threats.

Studies have shown that there is scarcity of studies on ML techniques in IoT security. There is still much to be explored relating to this topic. Furthermore, not only network layer but also physical, data link, transport and application layers should be given attention because the mentioned layers can create an entry point for an attacker to interrupt or destroy the whole system. IoT devices has a wide range of attacks. The number of analyzed papers and novelty of the field of study is still not enough to draw a decisive conclusion and make a prediction about the future.

6.1 Study Limitation & Validity Threats

This SLR was conducted in a systematic way to cover all possible studies related to the use of machine learning techniques in securing IoT devices. The main limitation to this study relates to conducting the search. The list of limitations of the SLR that should be taken into consideration are given below.

- The review did not include books and magazines about machine learning in IoT

devices
- The review only included papers that were in three databases: IEEE, Scopus and Web of Science.
- The only reviewed papers were those available in full-text.

Validity threat is one common factor that can negatively impact the accuracy of the research. This gives the reason to ensure that these threats are identified and handled so as to make sure the review results are reliable and can be transferred to others. The threats to validity in this study were categorized into the following categories: Investigation bias, publication bias, threats to study selection and data extraction.

Investigator bias.
The review was conducted by an individual person, there is a tendency of threats to validity as compared to a study conducted by several researchers. Therefore, to reduce this bias, the author of this study executed some task more than once to ensure the quality of the work.

Publication bias
The common bias in systematic reviews is publication bias (Kitchenham & Charters 2007). This is because it is often most likely positive results are published than negative results. This bias can still be observed in this study of which a few included studies failed to produce reliable results on the implementation of ML in IoT security. Despite the biases, the majority of the studies were successfully implemented and therefore it cannot be considered as a major threat as this bias matches the aim of this study which is identifying most used ML techniques in IoT rather than analyzing individual techniques used in IoT security. Although the search keywords in this SLR may have covered a wide range on ML and IoT security some papers may have used different names to refer to the subject of this study.

Threats of study selection
The review protocol defined the search strategy, this enabled the author to cover as much studies as possible. The inclusion/exclusion helped in minimizing the threat in the selection of primary studies. The pilot search was performed to formulate the search string of which the actual search followed thereafter. The search string was applied on well-known databases in the field of information processing science. The titles and abstracts of each study were read more than once so as to select the right studies, this method was helpful in minimizing the threats to study selection. In addition, the use of wide search string on multiple databases helped in reducing the risk of excluding relevant primary studies and it covered the majority of publications in the field.

Threats to data extraction process and results

The data extraction phase is another threat to validity. The data extraction process was designed during the creation of review protocol. The process assisted in recording of relevant information from the primary studies. The bias related to data extraction process was minimized with the implementation of this procedure.

6.2 Future Work

In this SLR, the use of ML techniques in IoT security are explored based on the existing literature. There is still scarcity of studies in this field, more studies are needed to strengthen the results of this study. Further studies with rigor research approach and with the focus on ML technique in IoT security is recommended. For future research, it could be important to find new algorithms that have more effective performance, also creating and testing hybrid models for better detection rate. This will enable the performance of IoT security solutions to be more effective and efficient.

Also, with the technological advancements could impact the performance of ML because most of the ML learning techniques rely on these technologies, for instance, the introduction of 5G could also create an impact especially with higher internet speed and the complex security encryptions moved to the cloud services which are not suitable for IoT devices could benefit in securing the IoT devices. Despite the success in embracing ML techniques in securing IoT devices it is also important to note that attackers are often sophisticated and could also shift their focus in using ML to launch attacks, this approach can be devastating to IoT devices.

References

Reference to the primary studies are listed alphabetically after the main references list.

F. Restuccia, S. D'Oro, & T. Melodia. (2018). Securing the internet of things in the age of machine learning and software-defined networking. *IEEE Internet of Things Journal, 5*(6), 4829-4842. doi:10.1109/JIOT.2018.2846040

Giri, A., Dutta, S., Neogy, S., Dahal, K., & Pervez, Z. (2017). Internet of things (IoT): A survey on architecture, enabling technologies, applications and challenges. Paper presented at the *Proceedings of the 1st International Conference on Internet of Things and Machine Learning,* Liverpool, United Kingdom. 7:1-7:12. doi:10.1145/3109761.3109768 Retrieved from http://doi.acm.org/10.1145/3109761.3109768

Gupta, B. B., & Quamara, M. (2018). An overview of internet of things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience, 0*(0), e4946. doi:10.1002/cpe.4946

Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2019). Machine learning in IoT security: Current solutions and future challenges. *ArXiv Preprint arXiv:1904.05735,*

Kitchenham, B. (2004). Procedure for undertaking systematic reviews. Computer Science Depart-ment, Keele University (TRISE-0401) and National ICT Australia Ltd (0400011T. 1), Joint Technical Report

Kitchenham, B., & Charters, B. (2007). Systematic literature reviews in software engineering – A systematic literature review. Tech. Rep. EBSE, Keele University and Durham University Joint Report, Staffordshire, UK.

J. Cañedo, & A. Skjellum. (2016). Using machine learning to secure IoT systems. Paper presented at the *2016 14th Annual Conference on Privacy, Security and Trust (PST),* 219-222. doi:10.1109/PST.2016.7906930

L. Xiao, X. Wan, X. Lu, Y. Zhang, & D. Wu. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Processing Magazine, 35*(5), 41-49. doi:10.1109/MSP.2018.2825478

Li, J., Palmieri, F., & Xiang, Y. (2019). *Special issue on security and privacy in machine learning* doi:https://doi.org/10.1016/j.ins.2019.03.045 "

M. Mamdouh, M. A. I. Elrukhsi, & A. Khattab. (2018). Securing the internet of things and wireless sensor networks via machine learning: A survey. Paper presented at the *2018 International Conference on Computer and Applications (ICCA),* 215-218. doi:10.1109/COMAPP.2018.8460440

M. Moh, & R. Raju. (2018). Machine learning techniques for security of internet of things (IoT) and fog computing systems. Paper presented at the *2018 International Conference on High Performance Computing & Simulation (HPCS),* 709-715. doi:10.1109/HPCS.2018.00116

M. Shahzad, & M. P. Singh. (2017). Continuous authentication and authorization for the internet of things. *IEEE Internet Computing, 21*(2), 86-90. doi:10.1109/MIC.2017.33

Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective, 27*(3), 162-182. doi:10.1080/19393555.2018.1458258

Mohamad Noor, M. b., & Hassan, W. H. (2019). *Current research on internet of things (IoT) security: A survey* doi:https://doi.org/10.1016/j.comnet.2018.11.025

Rai, R., Sahoo, G., & Mehfuz, S. (2015). Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration. SpringerPlus, 4(1), 197.

R. Sommer, & V. Paxson. (2010). Outside the closed world: On using machine learning for network intrusion detection. Paper presented at the *2010 IEEE Symposium on Security and Privacy,* 305-316. doi:10.1109/SP.2010.25

Samaila, M. G., Neto, M., Fernandes, D. A. B., Freire, M., & Inácio, P. R. M. (2018). Challenges of securing internet of things devices: A survey. *Security and Privacy, 1*(2), e20. doi:10.1002/spy2.20

Sun, P., Li, J., Alam Bhuiyan, M. Z., Wang, L., & Li, B. (2019). *Modeling and clustering attacker activities in IoT through machine learning techniques* doi:https://doi.org/10.1016/j.ins.2018.04.065

Z. Zhang, M. C. Y. Cho, C. Wang, C. Hsu, C. Chen, & S. Shieh. (2014). *IoT security: Ongoing challenges and research opportunities* doi:10.1109/SOCA.2014.58

Zantalis, F., Koulouras, G., Karabetsos, S., & Kandris, D. (2019). A review of machine learning and IoT in smart transportation. *Future Internet, 11*(4) doi:10.3390/fi11040094

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the internet of things: Threats and challenges. *Security and Communication Networks, 7*(12), 2728-2742. doi:10.1002/sec.795

Primary Studies

Azmoodeh, A., Dehghantanha, A., Conti, M., & Choo, K. R. (2018). Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *Journal of Ambient Intelligence and Humanized Computing, 9*(4), 1141-1152. doi:10.1007/s12652-017-0558-5

B. Chatterjee, D. Das, S. Maity, & S. Sen. (2019). RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning. *IEEE Internet of Things Journal, 6*(1), 388-398. doi:10.1109/JIOT.2018.2849324

Caminha, J., Perkusich, A., & Perkusich, M. (2018). A smart trust management method to detect on-off attacks in the internet of things. *Security and Communication Networks,* , UNSP 6063456. doi:10.1155/2018/6063456

Chiu, W., Su, C., Fan, C., Chen, C., & Yeh, K. (2018). Authentication with what you see and remember in the internet of things. *Symmetry-Basel, 10*(11), 537. doi:10.3390/sym10110537

D. Perez, M. A. Astor, D. P. Abreu, & E. Scalise. (2017). Intrusion detection in computer networks using hybrid machine learning techniques. Paper presented at the *2017 XLIII Latin American Computer Conference (CLEI),* 1-10. doi:10.1109/CLEI.2017.8226392

G. Baldini, R. Giuliani, G. Steri, & R. Neisse. (2017). Physical layer authentication of internet of things wireless devices through permutation and dispersion entropy. Paper presented at the *2017 Global Internet of Things Summit (GIoTS),* 1-6. doi:10.1109/GIOTS.2017.8016272

I. Kotenko, I. Saenko, & A. Branitskiy. (2018). Framework for mobile internet of things security monitoring based on big data processing and machine learning. *IEEE Access, 6*, 72714-72723. doi:10.1109/ACCESS.2018.2881998

J. Cañedo, & A. Skjellum. (2016). Using machine learning to secure IoT systems. Paper presented at the *2016 14th Annual Conference on Privacy, Security and Trust (PST),* 219-222. doi:10.1109/PST.2016.7906930

Jan, S. U., Ahmed, S., Shakhov, V., & Koo, I. (2019). Toward a lightweight intrusion detection system for the internet of things. *Ieee Access, 7*, 42450-42471. doi:10.1109/ACCESS.2019.2907965

L. Wei, W. Luo, J. Weng, Y. Zhong, X. Zhang, & Z. Yan. (2017). Machine learning-based malicious application detection of android. *IEEE Access, 5*, 25591-25601. doi:10.1109/ACCESS.2017.2771470

Liu, X., Du, X., Zhang, X., Zhu, Q., Wang, H., & Guizani, M. (2019). Adversarial samples on android malware detection systems for IoT systems. *Sensors, 19*(4), 974. doi:10.3390/s19040974

Mao, J., Bian, J., Tian, W., Zhu, S., Wei, T., Li, A., & Liang, Z. (2018). *Detecting phishing websites via aggregation analysis of page layouts* doi:https://doi.org/10.1016/j.procs.2018.03.053

Park, W., You, Y., & Lee, K. (2018). Detecting potential insider threat: Analyzing insiders' sentiment exposed in social media. *Security and Communication Networks,* , UNSP 7243296. doi:10.1155/2018/7243296

Q. Shafi, A. Basit, S. Qaisar, A. Koay, & I. Welch. (2018). Fog-assisted SDN controlled framework for enduring anomaly detection in an IoT network. *IEEE Access, 6*, 73713-73723. doi:10.1109/ACCESS.2018.2884293

R. Doshi, N. Apthorpe, & N. Feamster. (2018). Machine learning DDoS detection for consumer internet of things devices. Paper presented at the *2018 IEEE Security and Privacy Workshops (SPW),* 29-35. doi:10.1109/SPW.2018.00013

R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, & S. Venkatraman. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access, 7*, 41525-41550. doi:10.1109/ACCESS.2019.2895334

S. Gao, & G. Thamilarasu. (2017). Machine-learning classifiers for security in connected medical devices. Paper presented at the *2017 26th International Conference on Computer Communication and Networks (ICCCN),* 1-5. doi:10.1109/ICCCN.2017.8038507

T. Cho, H. Kim, & J. H. Yi. (2017). Security assessment of code obfuscation based on dynamic monitoring in android things. *IEEE Access, 5*, 6361-6371. doi:10.1109/ACCESS.2017.2693388

Tian, Q., Li, J., & Liu, H. (2019). A method for guaranteeing wireless communication based on a combination of deep and shallow learning. *Ieee Access, 7*, 38688-38695. doi:10.1109/ACCESS.2019.2905754

Xuan, S., Man, D., Yang, W., Wang, W., Zhao, J., & Yu, M. (2018). Identification of unknown operating system type of internet of things terminal device based on RIPPER. *International Journal of Distributed Sensor Networks, 14*(10), 1550147718806707. doi:10.1177/1550147718806707

Appendix A: Structure of the Review Protocol

1. Background of the study

2. Research questions

3. Search strategy

    a. Search strings
    b. Pilot Search
    c. Searched in selected databases

4. Study selection criteria

    a. Inclusion criteria
    b. Exclusion criteria

5. Study selection process

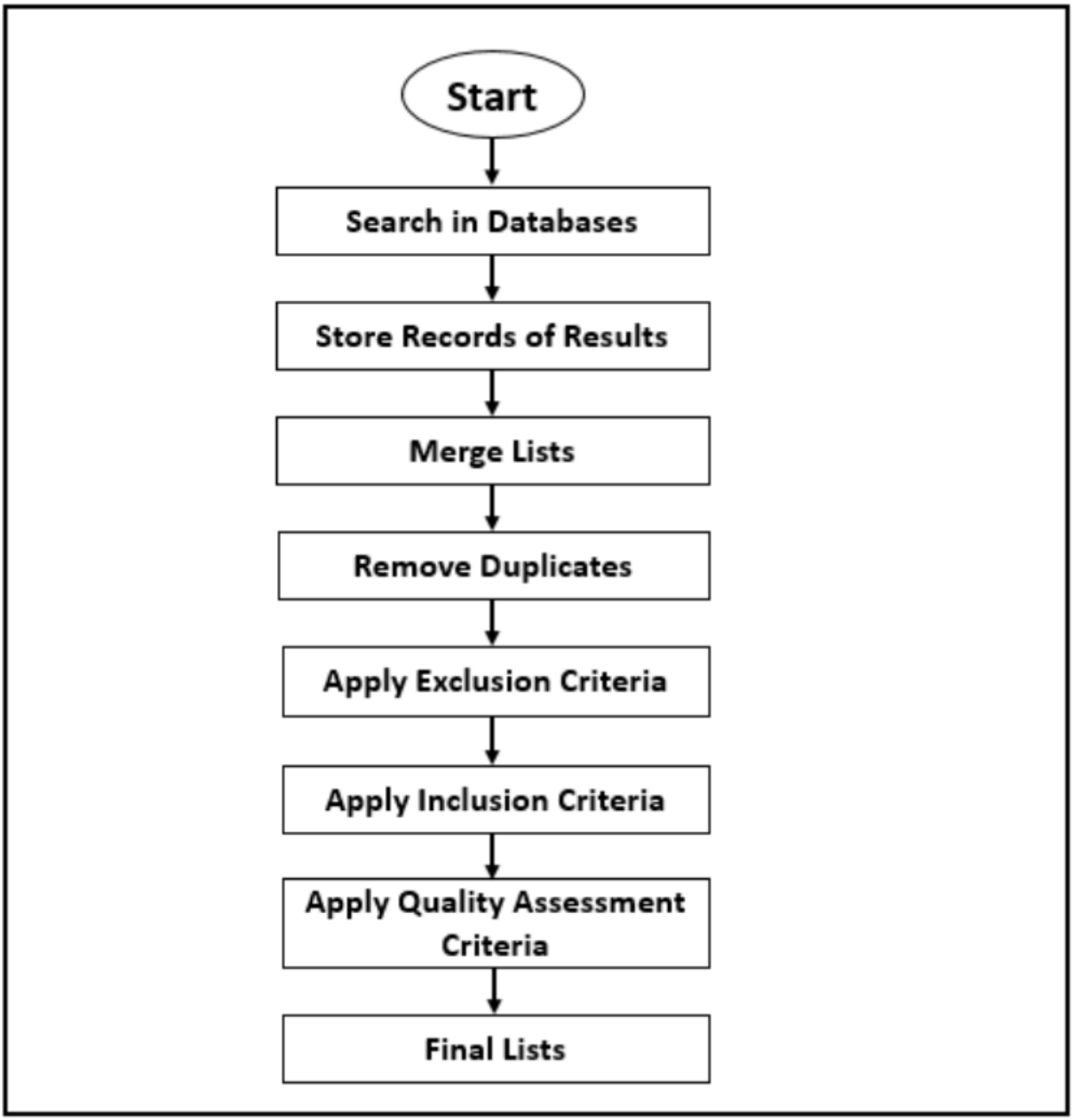
6. Duplicate removal

7. Study quality assessment

8. Data extraction strategy

9. Data synthesis extraction

Appendix B: The workflow of selecting primary studies.



Appendix C: Search Results

IEEE

Keywords	Results before screening	Results after screening
(machine learning AND internet of things AND security)	335	25

Scopus

Keywords	Results before screening	Results after screening
(machine learning AND internet of things AND security)	342	41

Web of science

Keywords	Results before screening	Results after screening
(machine learning AND internet of things OR IoT AND security)	178	37

Appendix D: List of Primary Studies and ID

Authors(s)	Title	Study ID
Azmoodeh, A., Dehghantanha, A., Conti, M., & Choo, K. R. (2018).	Detecting crypto-ransomware in IoT networks based on energy consumption footprint	[P1]
B. Chatterjee, D. Das, S. Maity, & S. Sen. (2019)	RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning	[P2]
Caminha, J., Perkusich, A., & Perkusich, M. (2018).	A smart trust management method to detect on-off attacks in the internet of things	[P3]
Chiu, W., Su, C., Fan, C., Chen, C., & Yeh, K. (2018)	Authentication with what you see and remember in the internet of things	[P4]
D. Perez, M. A. Astor, D. P. Abreu, & E. Scalise. (2017)	Intrusion detection in computer networks using hybrid machine learning techniques	[P5]
G. Baldini, R. Giuliani, G. Steri, & R. Neisse. (2017).	Physical layer authentication of internet of things wireless devices through permutation and dispersion entropy	[P6]
I. Kotenko, I. Saenko, & A. Branitskiy. (2018).	Framework for mobile internet of things security monitoring based on big data processing and machine learning	[P7]
J. Cañedo, & A. Skjellum. (2016).	Using machine learning to secure IoT systems	[P8]

Jan, S. U., Ahmed, S., Shakhov, V., & Koo, I. (2019).	Toward a lightweight intrusion detection system for the internet of things	[P9]
L. Wei, W. Luo, J. Weng, Y. Zhong, X. Zhang, & Z. Yan. (2017)	Machine learning-based malicious application detection of android	[P10]
Liu, X., Du, X., Zhang, X., Zhu, Q., Wang, H., & Guizani, M. (2019)	Adversarial samples on android malware detection systems for IoT systems	[P11]
Park, W., You, Y., & Lee, K. (2018).	Detecting potential insider threat: Analyzing insiders' sentiment exposed in social media	[P12]
Q. Shafi, A. Basit, S. Qaisar, A. Koay, & I. Welch. (2018)	Fog-assisted SDN controlled framework for enduring anomaly detection in an IoT network	[P13]
R. Doshi, N. Apthorpe, & N. Feamster. (2018)	Machine learning DDoS detection for consumer internet of things devices	[P14]
R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, & S. Venkatraman. (2019)	Deep learning approach for intelligent intrusion detection system	[P15]
Mao, J., Bian, J., Tian, W., Zhu, S., Wei, T., Li, A., & Liang, Z. (2018)	Detecting phishing websites via aggregation analysis of page layouts.	[P16]
S. Gao, & G. Thamilarasu. (2017).	Machine-learning classifiers for security in connected medical devices	[P17]
T. Cho, H. Kim, & J. H. Yi. (2017)	Security assessment of code obfuscation based on dynamic monitoring in android things	[P18]
Tian, Q., Li, J., & Liu, H. (2019)	A method for guaranteeing wireless communication based on a combination of deep and shallow learning	[P19]

Xuan, S., Man, D., Yang, W., Wang, W., Zhao, J., & Yu, M. (2018)	Identification of unknown operating system type of internet of things terminal device based on RIPPER	[P20]

Appendix E: Machine learning algorithms used

Study ID	**Used machine learning algorithms**
[P1]	support vector machine (SVM) neural network (NN) random forest (RF) K-nearest neighbors (KNN)
[P2]	artificial neural network(ANN),
[P3]	support vector machine(LSVM) neural network (NN) naïve Bayes
[P4]	support vector machine(SVM) naïve Bayes
[P5]	support vector machine (SVM), neural network (NN) K-means
[P6]	support vector machine(SVM) decision tree(DT) K-nearest neighbor(KNN),
[P7]	principal component analysis(PCA) support vector machine(SVM) K-nearest neighbor(KNN) Gaussian naïve Bayes(GNB) artificial neural network(ANN) decision tree(DT)

[P8]	artificial neural network (ANN)
[P9]	support vector machine (SVM)
[P10]	Naive bayes decision tree (DT)
[P11]	neural network (NN) logistic regression (LN) decision tree (DT) random forest (RF) extreme tree(ET)
[P12]	support vector machine(SVM) naïve Bayes linear decision tree (DT) K-means expectation maximization (EM) density based spatial clustering of application with noise(DBSCAN)
[P13]	recurrent neural network (RNN) alternate decision tree (ADT)
[P14]	K-nearest neighbors (KNN) support vector machine(LSVM) decision tree (DT) random forest (RF) neural network (NN)
[P15]	deep neural network (DNN)
[P16]	Support Vector Machine (SVM)

	Decision Tree (DT)
[P17]	decision tree(DT)
[P18]	Naive Bayes
[P19]	support vector machine (SVM)
[P20]	support vector machine (SVM), decision tree (DT)

Appendix F: Frequency of used ML techniques

Machine learning algorithm	**Frequency**	**Reference**
Support Vector Machine (SVM)	11	[P1] [P3] [P4] [P5] [P6] [P7] [P9] [P12] [P14] [P19] [P20]
Neural Network (NN)	10	[P1] [P2] [P3] [P5] [P7] [P8] [P11] [P13] [P14] [P15]
Decision tree (DT)	9	[P6] [P7] [P10] [P11] [P12] [P13] [P14] [P17] [P20]
Random Forest (RF)	3	[P1] [P11] [P14]
Naïve Bayes	6	[P3] [P4[P7]] [P10] [P12] [P18]
K-nearest neighbors (KNN)	3	[P1] [P6] [P7] [P14]
K-means	2	[P5] [P12]