IDENTIFYING NETWORK TRAFFIC BOTNET FOR INTERNET OF THINGS USING MACHINE LEARNING ALGORITHMS

AMIRHOSSEIN REZAEI

UNIVERSITI TEKNOLOGI MALAYSIA

IDENTIFYING NETWORK TRAFFIC BOTNET FOR INTERNET OF THINGS USING MACHINE LEARNING ALGORITHMS

AMIRHOSSEIN REZAEI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia

AUGUST 2021

DEDICATION

In honor of my beloved father. Hossein Rezaei. You left fingerprints of grace on our lives. You shan’t be forgotten. Also, my supportive mother and sisters.

ACKNOWLEDGEMENT

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my main supervisor, Profesor Dr. Shamsul Bin Sahibuddin for her continuous support and valuable feedbacks that enabled me to achieve the research milestones within the required time-frame. I am thankful also to my co-supervisors Dr. Saiful Adli Bin Ismail and Dr. Suriayati Chuprat for their continuous support and valuable feedbacks in reviewing, improving and evaluating my research. Also, I am grateful to every member of my family and friends who stood by me with kind and love during the Ph.D. journey.

I am also indebted to Universiti Teknologi Malaysia (UTM) for funding my Ph.D study. Librarians at UTM, Cardiff University of Wales and the National University of Singapore also deserve special thanks for their assistance in supplying the relevant literatures.

My fellow postgraduate student should also be recognised for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family member.

ABSTRACT

The Internet of Things (IoT) is one of the latest technologies in the field of telecommunication. However, security of the network is a prominent challenge in IoT. Among the security risks, a Botnet has been identified to cause a significant threat to the network. A Botnet is a network of private computers infected with malicious software and being controlled as a group without the owners' knowledge. The Botnet is normally used to send spam, steal data, and carry out Distributed Denial of Service attack. It also allows the attacker to access the devices and their connections. The master (owner) organized the Botnet by using Command and Control (C&C) software. One of the method of detection is Ensemble Learning method, which is a technique of Machine Learning. Ensemble Learning models use several models of the same kind for classifying or regressing the output. The idea behind such a technique is to use several weak predictors together to create a strong predictor. There are several types of research on the detection of Botnet using Machine Learning methods. However, each method has its limitations such as real-time monitoring, timely detection, and adaptability to new threats. Among all studies that have been reviewed, none of them explained why they choose specific methods for detecting Botnet. Also, they focus on a specific type of Botnet or specific operating systems and devices. Hence, this study aims to improve the Network Traffic Botnet identification through features reduction and ensemble learning methods, and to identify the best machine learning method to detect the Botnet in IoT networks. This is achieved by first finding the best of supervised learning, unsupervised learning, and regression learning methods. Then used the two best of them in the Ensemble Learning method for achieving the best possible result. To validate the accuracy of the proposed model, 790745 normal domain names and 199772 malicious domain names have been collected from 3 different sources. To ensure the method is not overfitting, the cross-validation technique was used. All machine learning algorithms that have been used in this study are developed in Python 3 on the same computer for equalization of speed. It is found that the proposed model is the best in the matter of accuracy achieved 100% and reduce the number of features from 204 to only 20 by combining the two best of the machine learning methods: Decision Tree and Artificial Neural Networks. This Ensemble Learning method is useful for identifying Botnet and Bots during communication in IoT networks.

ABSTRAK

Internet of Things (IoT) adalah salah satu teknologi terkini dalam bidang telekomunikasi. Walau bagaimanapun, keselamatan rangkaian adalah cabaran utama dalam IoT. Di antara risiko keselamatan, Botnet telah dikenal pasti menyebabkan ancaman yang signifikan terhadap rangkaian. Botnet adalah rangkaian komputer peribadi yang dijangkiti perisian berbahaya dan dikawal dalam satu kelompok tanpa pengetahuan pemiliknya. Botnet biasanya digunakan untuk mengirim spam, mencuri data, dan melakukan Serangan Penafian Perkhidmatan. Ini juga membolehkan penyerang mengakses peranti dan rangkaiannya. Pemilik Botnet mengatur Botnet dengan menggunakan perisian Arahan dan Kawalan. Salah satu kaedah pengesanan adalah kaedah Pembelajaran *Essemble*, iaitu teknik Pembelajaran Mesin. Model Pembelajaran *Ensemble* menggunakan beberapa model yang sama untuk mengklasifikan atau merosotkan dapatan. Idea di sebalik teknik tersebut adalah menggunakan beberapa peramal yang lemah bersama-sama untuk membina peramal yang kuat. Terdapat beberapa jenis penyelidikan mengenai pengesanan Botnet menggunakan kaedah Pembelajaran Mesin. Walau bagaimanapun, setiap kaedah mempunyai batasan seperti pemantauan masa nyata, pengesanan tepat pada masanya, dan kemampuan menyesuaikan diri dengan ancaman baru. Di antara semua kajian yang telah dikaji, tidak ada yang menjelaskan mengapa mereka memilih kaedah khusus untuk mengesan Botnet. Mereka juga memfokus pada jenis Botnet atau sistem operasi dan peranti tertentu. Oleh itu, kajian ini bertujuan untuk meningkatkan pengenalan *Network Traffic Botnet* melalui kaedah pengurangan ciri dan Pembelajaran *Ensemble*, dan untuk mengenal pasti kaedah Pembelajaran Mesin yang lebih baik untuk mengesan Botnet dalam rangkaian IoT. Hal ini dapat dicapai dengan mencari kaedah pembelajaran terarah, pembelajaran tidak diarah dan kaedah pembelajaran regresi. Kemudian gunakan dua yang terbaik dalam kaedah Pembelajaran *Ensemble* bagi mencapai hasil yang terbaik. Untuk mengesahkan ketepatan model yang dicadangkan, 790745 nama domain normal dan 199772 nama domain berbahaya telah dikumpulkan dari 3 sumber yang berbeza. Untuk mengelakkan sesuatu kaedah berlebihan, teknik pengesahan silang digunakan. Semua algoritma Pembelajaran Mesin yang telah digunakan dalam kajian ini dibangunkan di Python 3 pada komputer yang sama untuk memastikan kelajuan yang sama. Hasil kajian menunjukkan bahawa model yang dicadangkan adalah yang terbaik dalam mencapai hal 100% ketepatan, dan mengurangkan bilangan ciri daripada 204 ke hanya 20 dengan menggabungkan dua kaedah Pembelajaran Mesin terbaik: Pohon Keputusan dan Rangkaian Neural Buatan. Kaedah Pembelajaran *Ensemble* ini berguna untuk mengenal pasti Botnet dan Bot semasa komunikasi dalam rangkaian IoT.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IoT	-	Internet of Things
DDoS	-	Distributed denial of service
C&C	-	Command and Control
IDS	-	Intrusion Detection System
kNN	-	k- Nearest Neighbors
GBM	-	Gradient Boosting Machines
SVM	-	Support Vector Machine
ANN	-	Artificial Neural Networks
DBSCAN	-	Density-based spatial clustering of applications with noise
GMM	-	Gaussian Mixture Model
LAC	-	Learning Automata based Clustering
AP	-	Affinity Propagation
RFID	-	Radio Frequency Identification
NFC	-	Field Communication
WSAN	-	Wireless Sensor and Actuator Networks
PKI	-	Public key infrastructure
MCC	-	Mobile Cloud Computing
Bots	-	Infected devices
Zombie	-	Infected devices
P2P	-	peer to peer
OWASP	-	Open Web Application Security Projects
ELM	-	Extreme Learning Machine
HMM	-	Hidden Markov Model
DTN	-	Delay tolerant network
AC	-	Accounting centre
6LowPAN	-	IPv6 over Low Power Wireless Personal Area Networks
RPL	-	Routing over Low Power and Lossy Networks
BLSTM-RNN	-	Bidirectional Long Short-Term Memory Recurrent Neural Network
IRC	-	Internet Relay Chat

DHT	-	Distributed has tag
DGA	-	Domain Generation Algorithm
DPI	-	Deep packet inspection
NN	-	Neural Network
JI	-	Jaccard index
AUC	-	Area Under the ROC Curve
OC-SVM	-	The One-Class Support Vector Machine
PPV	-	Positive predictive value
FPR	-	False positive rate
TPR	-	True positive rate
ACC	-	Accuracy
RMSE	-	The Root Mean Square Error
TP	-	True Positive
TN	-	True Negative
FP	-	False Positive
FN	-	False Negative

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

One of the new technologies in the field of telecommunication is the Internet of Things (IoT). IoT is the physical objectives of network, vehicles, devices, buildings and other items which are embedded with things such as electronics, sensors, software as well as connectivity of network, the IoT allows those objects to collect and exchange data (Roy et al., 2015). In this era of new technology, IoT is the next major step, which carries great changes in the functionality of business. It is expected of that number of devices and their functions that are connected to the IoT, will be increased in the future. (Stergiou et al., 2016).

The IoT has a high impact on users' daily lives and potentially on users' behaviour. The most recognizable factors of the IoT are being visible both in indoor and in the working fields as detecting a private could user. Apart from that, the IoT can also play a leading role in other areas such as, smart homes, e-health, assisted living, and enhanced learning. Secondly, users of business could also see the impact of the IoT particularly in logistics, automation and industrial manufacturing, intelligent transportation, and business management (Alsmirat et al., 2016).

The IoT includes three main parts; the things or objects, communication networks that connect things, and the systems of computers using data steaming from/to things. Generally, IoT is a kind of network of physical things that are set up with electronics, software, sensors, and the connectivity which activates them. The exchange of data by operators, manufacturers, and some other connected devices allow for greater value services (Batalla and Krawiec, 2014).

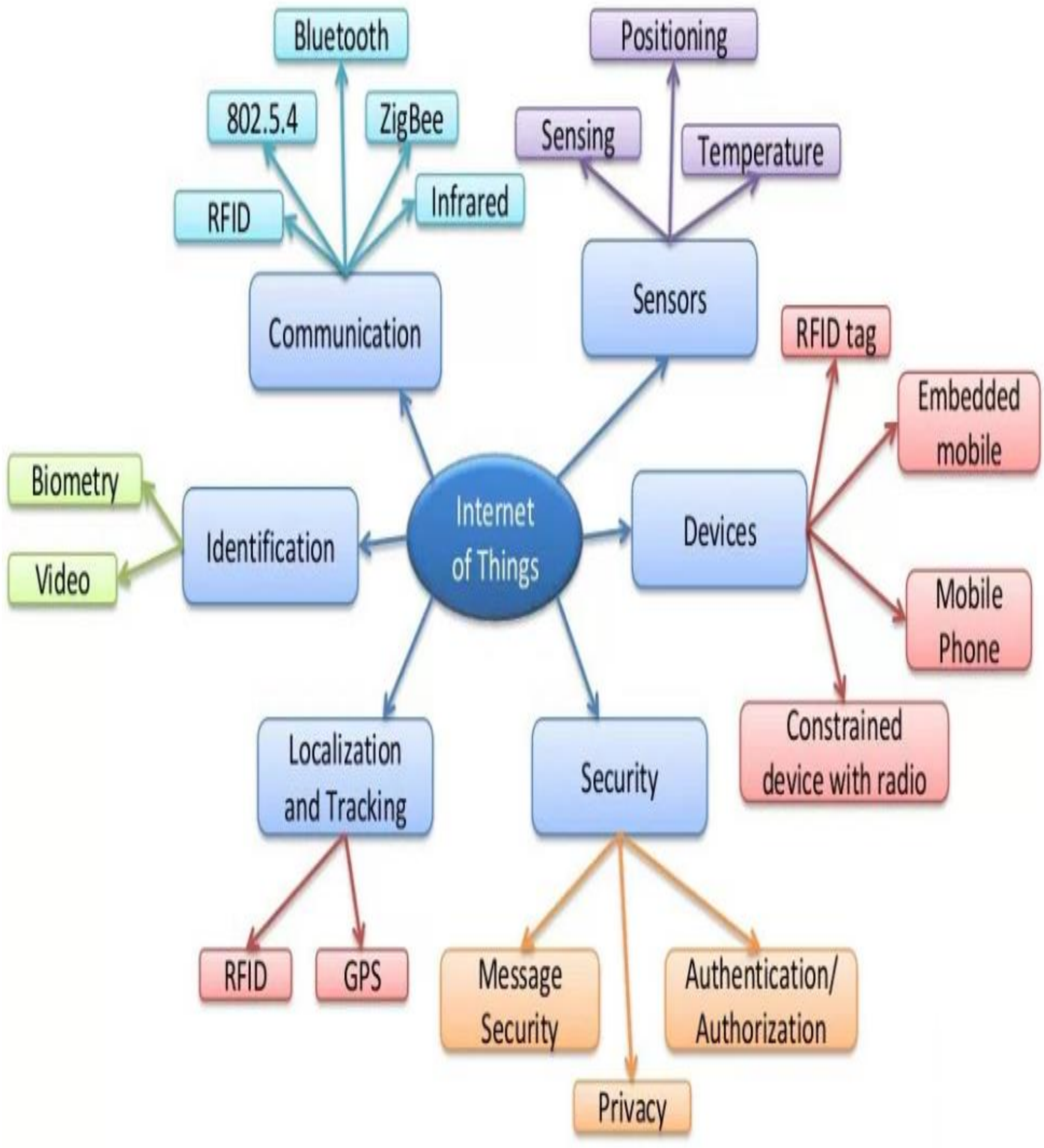

Figure 1.1 The Connectivity of the Internet of Things (Batalla and Krawiec, 2014)

The performance of cloud service can be found in a wide variety of applications such as in health care sector, electronic governance, production facilities, network services and also in the monitoring of numerous parameters to maintain optimality and so on (Georgia et al., 2016).

On the other hand, cloud computing is another new technology which is growing fast and becoming the part that connects to IoT for storage and on demand.

The current tendency for handling big data and rapid delivery of services based on customers demands have affected a quick migration of nearly all computing facilities to cloud networks. The accuracy of any computing system depends on the incremental number of input samples and the choices given to the computing core unit (Bruno and Nurchis, 2013).

Due to cloud computing can handle big data and rapid delivery of services based on customers' demands. On the other hand, the challenges on IoT's devices in a matter of energy source and memory can be solved by using cloud computing. Therefore, cloud computing is related to IoT network and it has to be concerned about cloud computing to understanding better on IoT challenges.

Furthermore, with the rising conversion of new appliances and tools with the latest technology, there is a presented demand for gradation and measurement standards for collating new research discoveries in the market. The measurements used need be accurate and quick enough to keep up with the computing section and the core used in the services of cloud. The arrival of IoT has enhanced the value in terms of the accuracy and correctness of measurements of data, due to the inputs from multiple sources as they are also unified in the cloud (Hongming et al., 2017).

IoT and Cloud computing are two dissimilar technologies which have already become a part of our lives. A higher usage and adoption rate for both technologies are expected to be an important part of the future of internet (Botta et al., 2016).

According to Botta et al. (2016), it was found that IoT and cloud computing have achieved their popularities in recent years. The number of research papers discussing IoT and cloud computing (both individually) has increased since 2008 Additionally, previous studies looking into both technologies have also increased. Figure 1.3 shows research and interest trends on IoT and cloud.

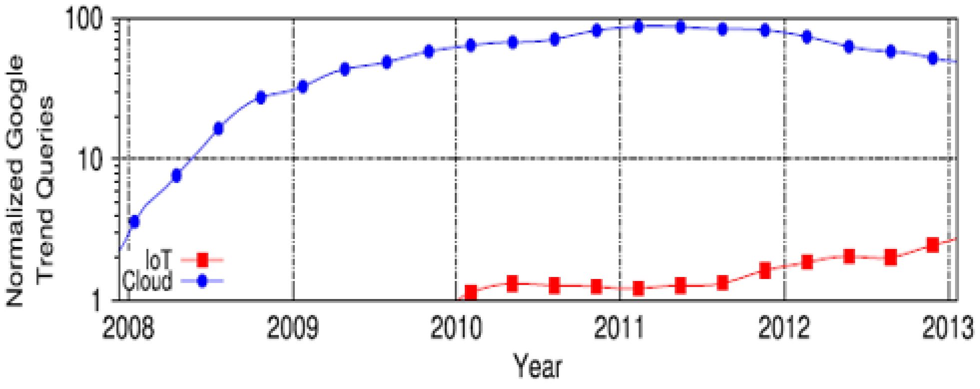

Figure 1.2 Research and Interest Trends on IoT and Cloud.(Botta et al., 2016)(a).

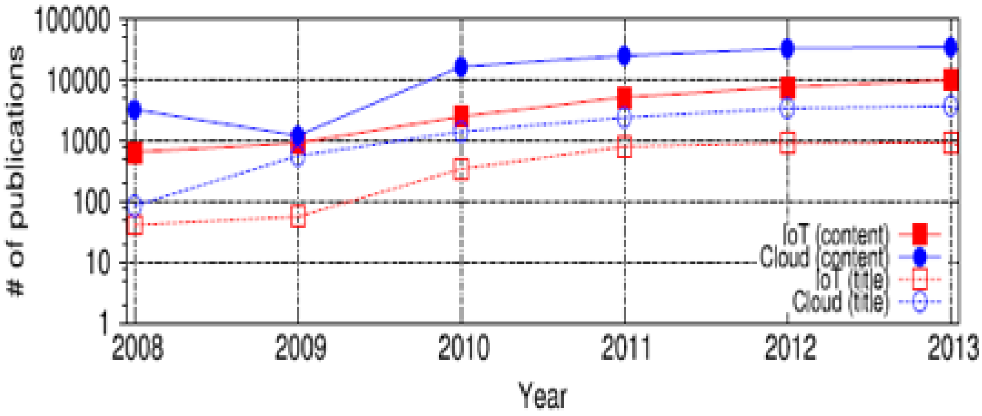

Figure 1-2 Research and Interest Trends on IoT and Cloud.(Botta et al., 2016)(b).

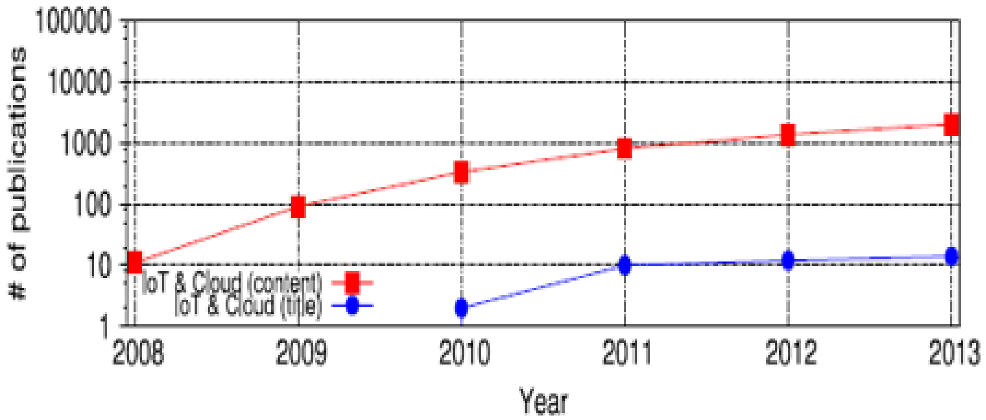

Figure 1-2 Research and Interest Trends on IoT and Cloud.(Botta et al., 2016)(c).

The IoT has been an interesting topic to study as it is concerned with an actual being in the physical world connected to the virtual unit in the cyber world. Physical and also digital units are improved by processing, sensing, and self-adapting abilities to achieve interface during special addressing system. The IoT comes with added security challenges, similar other Internet technologies, such as the Radio Frequency Identification (RFID), Near Field Communication (NFC), and Wireless Sensor and Actuator Networks (WSAN). Numerous problems can particularly in areas such as the system architecture, standard, and other human concerns (Mohd et al., 2017).

There are security issues that should be taken into consideration. When dealing with security issues, questions such as ‘How do we verify malicious IoT devices?’, ‘How do we create a suitable security framework for intelligent applications of things?’, ‘How do we maintain an equilibrium among high security requests of things and also supporting hardware limitations of foundations?’ may arise. An ultimate question that should be asked is ‘How can the society safely participate in both physical and cyber worlds via inter communication?’.

These kinds of important barriers are able to manipulate the improvement of the future IoT. Beside the disclosure of huge information is also susceptible to potential vulnerabilities from robust attackers. Moreover, limited sources involving heterogeneous networks and sensor nodes, channels of connection and interfaces, bandwidth, storage, and energy, may persuade single model design too. In the direction of the general IoT researches on its architecture form, standard, communication protocol, as well as management of network have been explored in previous studies (Mohd et al., 2017).

On the subject of the special security of the IoT, a number of open problems such as a Botnet, distributed denial of service attacks (DDoS) attacks, cryptographic algorithms, access control, authentication protocols, and governance frameworks may occur. Much of the research have focused on particular communication methods such as the WLAN or RFID, comprehensive cryptographic mechanisms such as key management, and useful applications such as supply chain management and multimedia traffic (Mohd et al., 2017).

The security frameworks in usual networks could present merits for security protection of the IoT. Nevertheless, the security problem to the future of the IoT is a difficult technical problem involving multidimensional subject that merges the data security, security in the network, infrastructure security, and management security. Generally, the present methods only offer solutions for a particular communication technique or software and might be lacking in universality for a complex system (Mohd et al., 2017).

The research and development of the IoT over the last decade has been observed. As demonstrated in Figure 1.4, Gartner approximated that by 2016 there will be 6.4 billion connected devices using it. The world residents are assumed to reach 7.6 billion by 2020 which means that there would be nearly 3 devices linked to IoT for every person in the world (Sicari et al., 2015). Connected things, such as implantable medical devices and transportations, play vital roles in our routine lives. Therefore, powerful security requests for the IoT have turned into a necessity. To cope with the massive use of the IoT, confidentiality, integrity, and authentication are among the major security issues that need to be addressed (Chi et al., 2017).

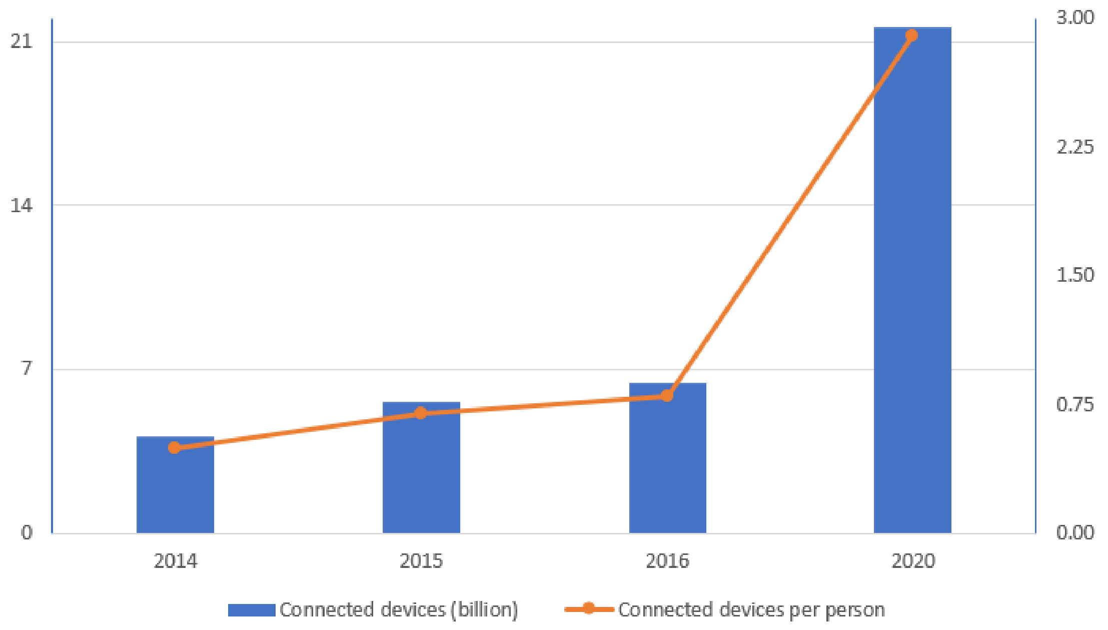

Figure 1.3 The Number of Connected Devices in IoT (Chi et al., 2017).

It could be challenging to create applications for the IoT due to several reasons; high difficulty of distributed computing, the lack of overall guidelines and frameworks involving communication at the low level for simpler implementation at the high level, the use of different programming languages used, and the numerous protocols of communication. All these aspects require developers who are capable of managing the foundation and handling both the hardware and software layers via protecting all functional and non-functional requirements of the software (Ammar et al., 2018).

1.2 Background of the Problem

This section will review challenges in IoT security, Botnet, Botnet detection techniques, and Machine Learning techniques researches that have been done recently.

1.2.1 Internet of Things Security

The advantages of being everywhere and the growing reputation of IoT have made devices of IoT a strong boosting platform for cyber-attacks. This increases the intensity and numerous repetitions of security events involving IoT devices. They have obviously become a new fragile link in the chain of security of recent computer networks. IoT devices could be the weak point of desktop systems. However, what they lack in computing of abilities they make up for in statistics. Furthermore, due to being regularly connected to the internet and also apparently infiltrated by faults in several situations of simple outcome configurations of security, they become an easy target for attackers.

The Internet of Things (IoT) is becoming more popular. Computing services now require a vast volume of data storage as well as processing. The resource constraints due to the unique characteristics of IoT including short range communication, and self-organization have resulted in the outsourcing use of the cloud as a storage. This brings up a chain of new challenges in the security and privacy threats of the IoT (Zhou et al., 2017).

The IoT comprise of electronics software and sensors embedded within physical objects that allow things to be controlled remotely. The present network infrastructure facilitates direct integration among computer communication networks as well as the physical world, which will significantly help improve, efficiency and accuracy to benefit the economy (Li et al., 2011). For that reason, the IoT has been extensively applied in a range of applications for instance in building automation, energy management medical healthcare systems, environment monitoring, and transportation.

Nevertheless, because of the limitations of resources in the IoT devices, they continuously represent active and extremely complex computation closely related to the IoT users' privacy. The IoT users must not be exposed to compromised and malicious IoT users within malicious cloud servers. Hence, the major concern now lies on how to effectively protect the privacy protective of the IoT in the cloud (Sheng et al., 2013).

The IoT has been creating a new situation that malware could be using to create strong Botnet. One of the newly discovered pieces of Linux malware is Mirai that has been used for roping devices of IoT into Botnet. Mirai could gain shell access using the default password of telnet or accounts of SSH. After it takes access to the account, it could generate delayed processes, install other malware on the system and even delete files. The infected devices that are secretly under control of Mirai also await commands for striking in the form of DDoS attack. The massive internet outage in October 2016 was affected by the DDoS attack using compromised IoT devices running the Mirai malware (Yuchen et al., 2017).

This section explained an overview of security in the Internet of Things problems that in detail will be described in chapter 2 section 2.2.

1.2.2 Botnet

Botnet are groups of connected, malware-tainted hosts (bots) that can be managed by a remote attacker. They are prominent threats in cybersecurity, regularly utilized for purposes ranging from distributed denial-of-service attacks and click-fraud to email spam and cryptocurrency mining (Smominru, 2018). According to ongoing estimates, Botnet control billions of infected hosts worldwide and are responsible for 70 percent of all spam (Jaiswal and Shivraj, 2013).

A group of infected devices (bots) is called Botnet which is remotely controlled via a bot master over and done with C&C (Command and Control) channel. They are used to accomplish different kinds of attacks for example DDoS, credential theft, spam, phishing, and so on. Each member communicates to each other, which are between the bot and bot master.

A Botnet can be categorized as centralized and decentralized Botnet. Bots from time to time contact the server the C&C for receiving commands in centralized Botnet. HTTP and IRC are examples of communication protocols that can be used. However, in a decentralized Botnet which is also called peer to peer (P2P), receiving the command directly from C&C server to the only one of the bots. Afterward, the bot is in charge of handing the message to other bots which will then be passed to other bots. Overnet, HTTP2P, and Kademlia are some of the communication protocols that were used in Botnet (Alejandre et al., 2017).

According to the EU Cybersecurity (2015), studied on the historical data on cyber-attacks, a Botnet were the sources of these kind of attacks in most of the cases. These Botnets are essentially zombies or bots (infected devices) with malware (malicious software), designed with some level of control over the zombies (Kamluk, 2017). The number of zombies contained within the framework of a Botnet normally varies from numerous to a few thousand bots. The biggest observed networks include millions of zombies. These armies of zombies permit a lot of attacks without the users' knowledge. Maintenance a Botnet has low cost and also it requires more knowledge of bot to grow the popularity of a Botnet for attackers (Kasprzyk et al., 2017).

On the other hand, one of the sources of income for large groups of cybercriminals is a Botnet which allow them to make huge profits from illegal actions. For instance, the DNS Changer which contains more than four millions zombies, was used to insert advertisements which generated a USD 14 million income within five years of operations, while Storm which has approximately five millions zombies, was used for sending SPAM, made a USD 3.5 million income per year. Furthermore, the risk of Botnet will be increased extremely by considering an opportunity of the present network of Botnet to create this type of cyber-attacks (Kijewski , 2013).

Currently, Botnet has become the technical backbone for supporting cyber-attacks like setting up DDoS attacks, stolen personal data, and sending spam emails (Antonakakis et al., 2012). Recently, most zombies are based on DGAs (Domain Generation Algorithms) to generate a meeting point with their C&C server (Schiavoni et al., 2014). A usual DGA includes several seeds that operate integer, current time and date to create a list of nominee domains. That list has changed during the time of attack, making it challenging for law agencies to verify and shut down a Botnet. Old-styled solutions consist of blacklisting and also reverse engineering (Zhou et al., 2013). Nevertheless, blacklisting is not enough to provide protection against the fluxing of domains. On the other hand, reverse engineering takes a lot of time, requires a sample of the malware and is not possible in most hands-on applications (Yadav et al., 2012).

While Botnet have existed for a long time, they proceed to develop and get complex. More up to date Botnet frequently encrypt their packets, differ their control protocols, and use peer to peer topologies rather than centralized ones to improve their robustness (Jaiswal and Shivraj, 2013). Along these lines, generally utilized signature-based (Roberto et al., 2010), heuristic-based (Kazuya et al., 2010), and content-based (Timothy et al., 2008) techniques for identifying Botnet are rendered ineffective and are less generalizable, making recognition of previously unseen or newer Botnet difficult.

What makes the problem even more complex is the recent trend towards stealthy and more resilient Botnet architectures, which depart from traditional centralized architectures and allow Botnets to avoid detection and remain in the system for extended periods of time. Botnets can achieve resilience by either anti-signature or architectural stealth. Anti-signature stealth involves the ability to manipulate the characteristics of bot-generated traffic to mask features that could be observed by signature-based detectors. On the other hand, architectural stealth means the ability to establish an overlay network that minimizes the exposure of malicious traffic to detectors. For these reasons, Botnets have recently received considerable attention from both the industry and the research community (Sweeney, 2014).

This section explained an overview of security in Botnet and bots problems that in detail will be described in chapter 2 section 2.3.

1.2.3 Botnet Identification Techniques

Botnet detection has got a substantial focus from industry and academia. Figure. 1.5 shows the classification of botnet detection techniques which are classified into Signature-based and Anomaly-based (Manmeet et al., 2019).

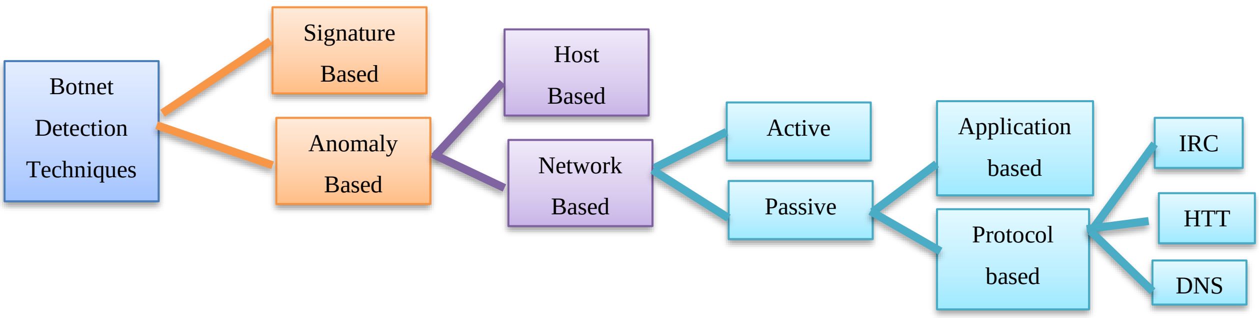

Figure 1.4 Botnet Detection Techniques.

Scalability is one of the most important challenges that Botnet detection methods face and is, therefore, the main focus of many of the most recent studies in the big data sphere [Singh et al., 2014: Soltanaghaei and Kharrazi, 2015: Kwon et al., 2016].

On the other hand, anomaly-based detection techniques, as are common in intrusion detection frameworks, show potential for identifying previously unseen or fresher Botnet. There are two broad anomaly-based methodologies found in researches. One methodology trains on nominal or non-malicious network traffic, and classify any traffic outside of the nominal range as Botnet activity (Sudipta et al., 2017). The other methodology trains on various kinds of Botnet traffic and identifies similarly malicious Botnet traffic (Sebastian et al., 2014).

Standard packet level or flow level statistics, such as payload length, the mean number of bytes per packet, and flow duration, are analyzed using machine-learning techniques such as supervised classification or clustering (Matija and Jens, 2014).

However, the flow characteristics are often characteristic of specific protocol-based Botnets and are not generalizable to newer Botnet varieties.

Graph-based methods are relatively new to Botnet detection (Shishir et al., 2010; Jing and Ioannis, 2015). These methods ignore the sequential nature of the data and focus on the graphical structure of the communication using centralized graph measurements. However, they often do not lend themselves well to a really useful tool, as they require access to all data at once to build graph models.

One promising approach to Botnet detection and mitigation is the Moving Target Defense (MTD), a novel and game-changing approach to cyber defense that is part of the broader trend towards Adaptive Cyber Defense (ACD). MTD has the potential to create asymmetrical uncertainty, providing the defender with a tactical advantage over the attacker (Jajodia et al., 2011).

Using antivirus software and a firewall to protect the host is not enough to prevent it from becoming infected with Botnet malware. In addition, even if it can be stopped by the C&C server, the infected host (bot) can be re-launched for a future attack. In this case, is needed host-based detection to remove the bot program from the host. Various studies have been conducted in the field of host-based detection techniques (Etemad and Vahdani, 2012: Huang, 2013).

Flow-based attributes extracted from the network traces were similar to NetFlow features such as bytes-per-packet, bytes-per-flow, and bytes per second. Botnet detection techniques using flow analysis have emerged in the last few years. There are several network traffic flow detection techniques that have been proposed in recent years. Anomaly detection can be done through mining-based detection techniques that are used to extract unexpected patterns of network traffic. It can, therefore, detect abnormal traffic even if the packets are encrypted. Many of the techniques used were flow analysis (W.H.Liao and C.C.Chang, 2010: Zhao et al., 2013: Hung and Sun, 2018: Alauthaman et al., 2018).

There are several techniques provided for detecting Botnet however, either their accuracy is not high enough, or they are for some specific types of devices and attacks. Chapter 2 section 2.4 will explain the summary of Botnet detection techniques that have been reviewed in this study.

1.2.4 Machine Learning Techniques

The Intrusion Detection system classification (IDS) is divided into three. One of them is Anomaly based, which it has two separate classes: Host based and Network based. Network based is split into two different types of monitoring: 1- active monitoring and 2- passive monitoring. Passive monitoring works in two layers which are protocol and application. One of the techniques used for detecting Botnet is Machine Learning which is classified under the application layer or generally under the IDS class.

One of the subsections of Artificial Intelligence in the field of computer science is Machine learning. Machine learning is the repeated use of statistical methods to give the ability of learning to computers via data without being clearly programmed for example a gradual improvement of performance on one specific task (Samuel, 2000).

Generally, Machine learning has three kinds of algorithms which are (Sunil, 2017):

a) Supervised Learning:

Supervised Learning which is also called the Classification method is a type of algorithm that includes the target, dependent variable or outcome variable that is to be forecasted from a given set of analysts or independent variables. Therefore, it can generate the function that maps inputs to wanted outputs using those set of variables. Until the model reaches the desired level of accuracy on training data, the training process will be continued. Some examples of Supervised Learning are: Regression, Random Forest, Decision Tree, KNN, and Logistic Regression.

b) **Unsupervised Learning:**

Unsupervised Learning which is also called the Clustering method does not have any dependent variable or outcome variable for forecasting. This is used to cluster population into several groups that are widely used for consumers in separate groups for particular intervention. Some examples of Unsupervised Learning are K means and Apriori algorithm.

c) **Reinforcement Learning:**

In this algorithm, the machine will be trained to make specific decisions. This works in the way that the machine is exposed to the environment where it trains itself repeatedly using trial and error. This machine learns from experiences in the past and then tries to capture the best possible knowledge to make accurate decisions in business. One example of Reinforcement Learning is the Markov Decision Process.

There are several different types of machine learning algorithms which will be highlighted in the chapter 2 section 2.5.1 particularly those which are commonly used and those which can be applied to almost any data problem.

One of the recent technologies that attracted significant attention in the community of security is machine learning. Furthermore, it delivers a meaning to battle DGA and to find the related structure of malware. The machine learning can be divided into two techniques; unsupervised and supervised learning.

An unsupervised learning technique domain into clusters to take advantage of the statistical powers of every group (Woodbridge et al., 2016). They found that this kind of approach takes a lot of time and needs several hours to generate domain clusters in order to create good simplification abilities. In some exciting cases, the statistical powers cannot be extracted because of the limited availability of zombies particularly those that are connected to the same DGA in the initiative networks (Zhang et al., 2016).

A supervised learning technique does not depend on statistical powers to expose DGAs. It functions straight on the raw domains and also their semantic characteristics. In another research, it was noted that others have established a system that utilizes large-scale, passive DNS analysis techniques to detect domains engaging in a malicious activity called "EXPOSURE", whereby the decision tree C4.5 will be created using elements that are pulled out from the traffic of DNS (Bilge et al., 2011). Other studies made use of ELM (Extreme Learning Machine) to categorize benign from malicious domains (Shi et al., 2017) while others accomplished one separate HMM (Hidden Markov Model) for every DGA. An HMM will be given input to the domain also categorizes whether the input will be mechanically created (Antonakakis et al., 2012). A Long Short-Term Memory (LSTM) network creates a ninety percent detection rate with 1.10000 FP (false positive) rate (Woodbridge et al., 2016). ELM, C4.5, LSTM, and HMM seemed to be acceptable mechanisms for the detection of DGA in existing frameworks. Nonetheless, there has been little attempt to evaluate them on a realistically huge methods such as SVM (Support Vector Machine), Recurrent SVM, Bidirectional LSTM, and CNN+LSTM, all of which have not been validated in this application domain (Tang, 2013;Zhang et al., 2013; Kim et al., 2016;Graves and J. Schmidhuber, 2005).

In all studies that have been done (refer to chapter 2 section 2.5.2), there is no explanation of why they selected those specific method(s) also none of them could achieve 100% accuracy of detection furthermore, most the studies focus on a specific type of Botnet attack or specific target which includes the type of devices and the type of OSs. Moreover, to decide in this field which of higher FP (False Alarm) or higher FN (Missed Alarm) is more vulnerable, it is depends on in which industries this method going to be used. For example, if using in the hospital which related to a patient's life then higher FN is more vulnerable while if using in the military service then higher FP is more vulnerable. In conclusion, there is not a method that can cover all kinds of Botnet attacks as well as different devices with different OS with the achievement of 100% detection which in detail will be discussed in chapter 2.

1.3 Statement of the Problem

As discussed in Section 1.2, a Botnet attack is one of the major threats to IoT that has been used for DDoS attacks, stealing data, sending spam, and also giving hackers access to the devices and device's connection. Research on the detection of Botnet using supervised and/or unsupervised machine learning methods has been done the details will discuss in chapter 2 however, each method has its limitation such as real-time monitoring, timely detection, and adaptability to new threats which this study will be addressing them as for real-time monitoring, the proposed method can be run in real-time for detecting and disconnecting Botnet from the network. For timely detection, by reducing the number of features and testing which ML method is faster. For adaptability of new threats, the dataset used in this research is collected from several different types of Botnet to ensure it is not trained base on some specific characteristic of some Botnet or devices.

On supervised learning methods, the statistical foundation is hypothesis representation; it concerns with the relationship between the features "x" and target "y" that should be defined by the selection of features as well as by accepting some detailed knowledge about what that behavior looks like in order to accurately represent the behavior of bots. Detecting bots based on some known and specific characteristics has been used in supervised learning methods. The accuracy of supervised learning methods can be effective against bot traffic which seeks to cover up itself among legitimate traffic by giving some specific characteristics of the malicious traffic. However, in most supervised learning methods, they have a common trend and are separate from specific perceptions about bot traffic revealed in the featured space. Therefore, supervised learning methods perform very poorly. Supervised learning techniques might overcome the secret nature of bots. Supervised learning techniques worked for cases whereby some specific characteristics are known. More details regarding the different methods and techniques that have been used to detect the Botnet are presented in Chapter 2.

On the other hand, unsupervised learning techniques are generally used for targeting behavioral patterns that are not specific to any kind of bots. The aim of previous studies that utilized unsupervised learning techniques is to capture the group’s activity via a bot in a Botnet. The relationship between samples is the main concern of unsupervised learning methods because it is able to recognize samples that appear. However, being too concerned with the similarities of samples may result in a high rate of false positives due to bots trying to cover up their activities. Selecting the correct number of features will lead to; firstly, achieve high accuracy of detection secondly, reducing the time duration of running the machine learning method, and lastly reduce overfitting possibility. Therefore, the number of features for training the machine learning algorithm is critical.

1.4 Research Questions

The main aim of this study is to improve Network Traffic Botnet identification through features reduction and ensemble learning methods by first reducing the number of features using several techniques for analyzing them such as scatter plot, histogram, Spectral Clustering, and dendrogram. After finalizing the features, this study will examine several different Machine Learning methods to find out which one is the best. In the end, evaluating the most suitable Machine Learning algorithm for detecting Botnet in IoT.networks.

This led this research to the research questions listed below:

RQ 1: What is the most efficient machine learning algorithm for Botnet detection in IoT networks?

RQ 2: How to minimize the feature sets that can effectively represent Botnet attacks in IoT networks?

RQ 3: How to evaluate the most suitable machine learning algorithm for detecting Botnet in IoT networks?

1.5 Research Objectives

The main objectives of this research are:

RO 1: To identify the most efficient machine learning algorithms for Botnet detection in IoT networks.

RO 2: To increase the efficiency of detection of Botnet attacks in IoT networks by feature reduction sets.

RO 3: To increase the accuracy of detecting Botnet in IoT networks by evaluating the most suitable machine learning algorithm.

1.6 Research Scope

As mentioned in Section 1.3, different machine learning methods include regression, supervised, and unsupervised learning methods have their advantages and disadvantages in detecting Botnet in the IoT networks. This research focused on firstly, discovering the most efficient existing machine learning algorithms. Secondly, minimizing the feature sets that can effectively represent. And lastly, evaluating the most suitable machine learning algorithm for detecting Botnet in IoT networks.

This research covers all type of attacks which can be used on different types of Botnet attacks such as the distributed denial of service attack (DDoS attack), steal data, send spam, and allow an attacker to access the device and its connection during communications between IoT and cloud computing.

1.7 Significance of the Study

Since the IoT keeps growing on a daily basis, the security of IoT becomes more challenging and important. One of the recent challenges in this area is a Botnet and bots. On the other hand, machine learning is one of the techniques that has been used for detecting a Botnet and bots on the networks and has few advantages compared to other methods such as the speed of detection and the accuracy of detection. This research will study Botnet during the communication between IoT devices for detecting infected devices and Botnet by using machine learning techniques that can detect and disable Botnet from IoT networks whit a minimum number of features needed for detection as well as to increase the percentage of accuracy without overfitting the method.

1.8 Structure of the Thesis

This study started with reviewing previous studies that have been done for identifying Botnet and bots in the Internet of Things network and researching several different techniques that have been used in this matter. After finding the gaps, this study determines the aim of this research. The next step is to be collecting and gathering the datasets that need to be used in this study. After setting up the datasets, the process of selecting the features and minimizing them will start by using several different analyzing techniques.

The next step is to examine the datasets with selected features in different Machine Learning methods and rank them based on the accuracy and the duration of detection. After that, this study will create different experiments based on combining each two of those Machine Learning methods that have a result higher than the threshold to create all different possibilities of Ensemble Learning methods.

After getting the results of all experiments, this study will divide the data into training and testing which this research has done it 3 times then it will use the Cross-Validation technique to ensure this method is not overfitting. In the end, this study will rank all the experiments to find out the most suitable machine learning algorithm for detecting Botnet in IoT networks.

In summary, chapter 1 discussed an overview of identifying the Botnet and bot in the IoT networks by explaining the background of the problem in IoT security, Botnet, Botnet Identification techniques, and Machine Learning techniques. After that, explain the problem statement and research questions as well as research objectives. Then it presented the research scope and significance of this study. In the end, it provided the structure of this study by explaining each step.

Chapter 2 will review previous studies that have been done in IoT, the security of IoT, Botnet in IoT, Botnet Identification, Botnet IDS classification, and Machine Learning detection techniques.

Chapter 3 will discuss research design and procedure, operational framework, data sources, experimental setup, instrumentation and data analysis, assumptions and limitations, research planning and schedule, and proposed plan.

Chapter 4 will talk about several Machine learning algorithms based on chapter 2 selected the most well-known methods for detecting Botnet included; supervised learning, unsupervised learning, and regression learning methods for identifying Botnet in IoT.

Chapter 5 will examine the way to use both of the best methods of selected Machine Learning methods by combining each two of them to optimize the detection of Botnet in the Internet of Things (IoT) for increasing the security of the IoT network against the infected Botnet and bots.

Chapter 6 will explain the selected Ensemble Learning methods in detail and concluding remarks then talk about the contributions of this study after that will talk about the limitation of this study. In the end, will talk about the future direction of this research.

1.9 Summary

There are several techniques provided for detecting Botnet however, either their accuracy is not high enough, or they are for some specific types of devices and attacks.

On the other hand, The Software Engineering Body of Knowledge (SWEBOK) is an international standard. SWEBOK specifying a guide to the generally accepted software engineering body of knowledge. The SWEBOK Guide has been created through cooperation among several professional bodies and members of the industry and is published by the IEEE Computer Society (IEEE). The standard can be accessed freely from the IEEE Computer Society. In late 2013, SWEBOK V3 was approved for publication and released. In 2016, the IEEE Computer Society kicked off the SWEBOK Evolution effort to develop future iterations of the body of knowledge.

In addition, previous studies do not categorize detecting Botnet in IoT network proposals under study according to their nature or Knowledge Area (KA) within the field of software engineering.

After reviewing recent studies on the detecting of Botnet in the Internet of Things which in detail will explain in chapter 2 several gaps have been detected. Such as, there is not a method that can apply to different types of Botnet as well as various devices with different OSs (i.e. only detecting for Android devices). In all studies that have been done, the accuracy of detection of Botnet is not high enough that can be reliable on them. Therefore, there is standardization and minimization of the number of features requirements for detecting Botnet.

This chapter discussed an overview of identifying the Botnet and bot in the IoT networks by explaining the background of the problem in IoT security, Botnet, Botnet Identification techniques, and Machine Learning techniques. After that, explain the problem statement and research questions as well as research objectives. Then it presented the research scope and significance of this study. In the end, it provided the structure of this study by explaining each step.

REFERENCES

Abdulghani Ali Ahmed, Waheb A. Jabbar, Ali Safaa Sadiq, and Hiran Patel (2020). Deep learning-based classification model for botnet attack detection. Journal of Ambient Intelligence and Humanized Computing.

Abdullah, Abdollah, M.Noh, Z.Mas' ud, Selamat, R.Yusof, and M.Melaka, (2013). *Revealing the criterion on botnet detection technique.* IJCSI International Journal of Computer Science Issues, vol. 10, no. 2, pp. 208–215, 2013.

Abdullah, R. S., A. MF, N. ZA, M. Z. Mas' Ud, S. SR, and R. Yusof (2013). Revealing the Criterion on Botnet Detection Technique. IJCSI International Journal of Computer Science Issues 10 (2), pp 208–215.

Abraham B, Mandyay A, Bapaty R, Alaliz F, Brown DE, Veeraraghavan M (2018). A comparison of machine learning approaches to detect botnet traffic. IEEE.

Abu Rajab, M., J. Zarfoss, F. Monrose, and A. Terzis (2006). A Multifaceted Approach to Understanding the Botnet Phenomenon. Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, Rio de Janeriro, Brazil, 41–52. ACM.

Abu Rajab, M., Zarfoss, J., Monrose, F., (2006). *Amultifaceted approach to understanding the botnet phenomenon*. Proc. 6th ACM SIGCOMM Conf. on Internet Measurement, p.41-52.

Abu-Alia A (2015). *Detecting domain flux botnet using machine learning techniques*. Qatar University, College of Engineering.

Adat, and Gupta, (2017). Security in Internet of Things: issues,challenges, taxonomy,and architecture. Telecommun.Syst. (2017).

Ahmad Karim, Rosli Salleh, Muhammad Khurram Khan, (2016). *SMARTbot: A Behavioral Analysis Framework Augmented with Machine Learning to Identify Mobile Botnet Applications*. Journal PLOS, https://doi.org/10.1371/journal.pone.0150077.

Aiello, M., M. Mongelli, and G. Papaleo (2014a). DNS Tunneling Detection through Statistical Fingerprints of Protocol Messages and Machine Learning. International Journal of Communication Systems 28(14): 1987–2002.

Aiello,M.,M.Mongelli, and G. Papaleo (2014b). Supervised Learning Approaches withMajority Voting for DNS Tunneling Detection. International Joint Conference SOCO’14-CISIS’14-ICEUTE’14, Bilbao, Spain: 463–472. Springer.

Akinrolabu, Agrafiotis, and Erola (2018). The challenge of detecting sophisticated attacks: Insights from soc analysts. in: Proceedings of the 13th International Conference on Availability, Reliability and Security, ACM, 2018, p. 55.

Akoglu, H. Tong, and D. Koutra (2015). Graph based anomaly detection and description: a survey. Data Min. Knowl. Discov. 29 (3) (2015) 626–688.

Akoglu, M. McGlohon, and C. Faloutsos (2010). OddBall: spotting anomalies in weighted graphs, in: Advances in Knowledge Discovery and Data Mining. 14th Pacific-Asia Conference, PAKDD 2010, Hyderabad, India, June 21–24, 2010. Proceedings. Part II, 2010, pp. 410–421.

Al Fuqaha A , Guizani M , Mohammadi M , Aledhari M , Ayyash M (2015). *Internet of things: a survey on enabling technologies, protocols, and applications.* IEEE Commun Surveys Tutorials 2015;17(4):2347–76.

Al Shorman A, Faris H, and Aljarah I (2019). Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection. J Ambient Intell Humaniz Comput.

Alauthaman, N. Aslam, L. Zhang, R. Alasem, and M. A. Hossain (2018). A P2P Botnet detection scheme based on decision tree and adaptive multilayer neural networks. Neural Computing and Applications, vol. 29, no. 11, pp. 991–1004, 2018.

Alauthman, Aslam, Alkasassbeh, Khan, AL-qerem, and Raymond Choo (2019). An efficient reinforcement learning-based Botnet detection approach. Journal of Network and Computer Applications, Elsevier.

Albanese M., Jajodia S., and Venkatesan S. (2018). Defending from stealthy botnets using moving target defenses. IEEE Secur. Priv. 2018, 16, pp. 92–97.

Alexander J.A.M.van Deursen, and Karen Mossberger (2018). *Any Thing for Anyone? A New Digital Divide in Internet‐of‐Things Skills*, Policy & Internet, Wiley Online Library, Volume 10, Issue 2, Pages 122-140, February 2018.

Alhanahnah, M., Lin, Q., and Yan, Q. (2018). Efficient signature generation for classifying cross-architecture IoT malware. In: Conference on Communications and Network Security (CNS). IEEE, pp. 1–9 (2018).

Almomani A. (2018). Fast-flux Hunter: A System for Filtering Online Fast-flux Botnet. Neural Computing and Applications 29 (7): pp 483–493. doi:10.1007/s00521-016-2531-1.

Almomani A., M. Alauthman, F. Albalas, O. Dorgham, and A. Obeidat (2018). An Online Intrusion Detection System to Cloud Computing Based on Neucube Algorithms. International Journal of Cloud Applications and Computing (IJCAC) 8 (2): pp 96–112. doi:10.4018/IJCAC.

Al-Nawasrah, A., A. Al-Momani, F. Meziane, and M. Alauthman (2018). Fast Flux Botnet Detection Framework Using Adaptive Dynamic Evolving Spiking Neural Network Algorithm. Proceedings, the 9th International Conference on Information and Communication Systems (ICICS 2018), Irbid, Jordan. IEEE.

Alpcan, T. and Ba¸sar, T. (2006). An intrusion detection game with limited observations. In: Proceedings of the 12th International Symposium on Dynamic Games and Applications (ISDG 2006), Sophia-Antipolis, France, July 2006.

Alqatawna and Faris (2017). Toward a Detection Framework for Android Botnet. in 2017 International Conference on New Trends in Computing Sciences (ICTCS), 2017: IEEE, pp.197-202.

Alsmirat, Jararweh, Obaidat, and Gupta (2016). Internet of surveillance: a cloud supported large-scale wireless surveillance system. Springer, Volume 73, Issue 3, pp 973–992.

Altaher A., S. Ramadass, A. Meulenberg, M. Abdat, and A. Ali (2012). Combined Behavior-and Signature-Based Internet Worm Detection System. International Information Institute (Tokyo). Information 15: 4213.

Alzahrani and Ghorbani (2015). Real-time signature-based detection approach for sms botnet. in 2015 13th Annual Conference on Privacy, Security and Trust (PST), 2015: IEEE, pp. 157-164.

Amaal Al Shorman, Hossam Faris, and Ibrahim Aljarah (2019). Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection. Journal of Ambient Intelligence and Humanized Computing, Springer Nature 2019.

Ammar, Russello, and Crispo (2017). *Internet of Things: A survey on the security of IoT frameworks*.ELSEVIER, Journal of Information Security and Applications 38 pp. 8–27.

Ammar, Russello, and Crispo (2018). *Internet of Things: A survey on the security of IoT frameworks*. Elsevier Journal of Information Security and Applications Volume 38, pp8–27.

Anchit Bijalwan (2020). Botnet Forensic Analysis Using Machine Learning. Hindawi, Security and Communication Networks, Volume 2020, Article ID 9302318.

Andrew Whitmore, Anurag Agarwal, and Li Da Xu (2015). *The Internet of Things—A survey of topics and trends*, Springer, Information Systems Frontiers, Volume 17, Issue 2, Pages 261–274, April 2015.

Angrishi K (2017). Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. arXiv preprint arXiv:1702.03681.

Antonakakis, April, Bailey, Bernhard, Bursztein, Cochran, Durumeric, Halderman, Invernizzi, and Kallitsis (2017) Understanding the mirai botnet. In: USENIX security symposium, pp 1092–1110.

Antonakakis, Perdisci, Nadji, Vasiliglou, Abu-Nimeh, Lee, and Dagon, (2012*). From trow away trafficc to bots: detecting the Rise of DGA-Based Malware*. The 21st USENIX Security Symposium 12.

Anuradha D. Biradar and B. Padmavathi (2020). BotHook: A Supervised Machine Learning Approach for Botnet Detection Using DNS Query Data. Lecture Notes in Electrical Engineering 570, Springer Nature Singapore Pte Ltd. 2020.

Aris, Sema F.Oktug, and Thiemo Voigt (2018). *Security of Internet of Things for a Reliable Internet of Services.* Springer Link, Autonomous Control for a Reliable Internet of Services pp 337-370.

Aristidis Likas, Nikos Vlassis, and Jakob J. Verbeekb (2003).*The global k-means clustering algorithm.* ELSEVIER, Pattern Recognition, Volume 36, Issue 2, pp 451-461.

Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, and Zaharia, (2010). *A view of cloud computing.* Communication of the ACM Volume 53, Issue 4, pp50–58.

Ashok and Narendra (2019). An Architecture for Analysis of Mobile Botnet Detection Using Machine Learning. Springer Nature Singapore, ICACDS 2019, CCIS 1045, pp. 127–139.

Aswini and Vinod (2015). Towards the detection of android malware using ensemble features. J Inf Assur Secur 10(1).

Athirah Zaffira Binti Majit, Palaniappan Shamala, Cik Feresa Mohd Foozy, Chuah Chai Wen, and Muruga Chinniah (2020). Android Botnet Detection by Classification Techniques. Springer Nature Switzerland AG 2020, pp. 109–120.

Azmoodeh A., Dehghantanha A., and Choo K.K.R. (2018). Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning. IEEE Trans. Sustain. Comput. 4(1), 88–95 (2018).

B.Choi, S.K.Choi, and K.Cho (2013). Detection of mobile botnet using vpn. in:Innovative Mobile and Internet Services in Ubiquitous Computing(IMIS). 2013 Seventh International Conferenceon,IEEE.pp.142–148.

B.Samani, H.Jazi, N.Stakhanova, and A.Ghorbani (2014). Towards effective feature selection in machine learning-based botnet detection approaches. CNS 247–255doi:10.1109/CNS.2014.6997492.

Babak, Roberto, Andrea, and Kang (2014). Peerrush: Mining for unwanted p2p trac. Journal of Information Security and Applications 19 (3) (2014) pp. 194-208.

Bacon, Pasquier, Papagiannis,Singh, Eyers, and Pietzuch,(2014*). Information flow control for secure cloud computing.* IEEE Trans. Netw.Serv.Manage., vol. 11, no. 1, Mar. 2014.

Bacon, Singh, Trossen, Pavel, Bontozoglou, Vastardis, Yang, Pennington, Clarke, and Jones (2012). *Personal and social communication services for health and lifestyle monitoring*. in Proc. 1st Int. Conf. Global Health Challenges (Global Health'12).

Barford, and Yegneswaran, (2007). *An inside look at botnets. In: Malware Detection*. Springer, p.171-191.

Barsamian, A.V., (2009). Network Characterization for Botnet Detection Using Statistical-Behavioral Methods. Master Thesis, Dartmouth College.

Barthakur, P., Dahal, M., Ghose, M.K., (2013). An efficient machine learning based classification scheme for detecting distributed command & control traffic of P2P botnets. p.9.

Batalla and Krawiec (2014). Conception of ID layer performance at the network level for Internet of Things. Springer, Volume 18, Issue 2, pp 465–480.

Beigi, E.B., Jazi, H.H., Stakhanova, N., and Ghorbani, A.A.(2014). Towards effective feature selection in machine learning-based botnet detection approaches. In:

Proceedings of the IEEE Conference on Communications and Network Security (IEEE CNS 2014), pp. 247–255. IEEE, San Francisco, October 2014.

BEIGI, H. JAZI, N. STAKHANOVA AND A. GHORBANI, (2014). *Towards Effective Feature Selection in Machine Learning-Based Botnet Detection Approaches*. IEEE Conference on Communications and Network Security (CNS), Oct 29-31, 2014, San Francisco, CA.

Belgiu and Dragut (2016). Random forest in remote sensing: a review of applications and future directions. ISPRS J Photogramm Remote Sens 114: pp. 24–31.

Benson and Chandrasekaran (2017). *Sounding the Bell for Improving Internet (of Things) Security.* IoTS&P '17 Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Pages 77-82.

Bertino (2016). *Data Security and Privacy in the IoT*. Proc. 19th Int'l Conf.Extending Database Technology (EDBT16).

Bertino and Islam (2017). *Botnets and Internet of Things Security.* IEEE Computer Society, Volume 50, Issue 2, pp 76-79.

Bijalwan, Chand, E. S. Pilli, and C. Rama Krishna (2016). Botnet analysis using ensemble classifier. Perspectives in Science, vol. 8, pp. 502–504.

Bilge, D. Balzarotti, W. Robertson, E. Kirda, and C. Kruegel (2012). *Disclosure: detecting botnet command and control servers through large-scale netflow analysis*. In Proceedings of the 28th Annual Computer Security Applications Conference, ser. ACSAC '12. New York, NY, USA: ACM, 2012, pp. 129–138.

Bilge, Kirda, Kruegel, and Balduzzi, (2011). EXPOSURE: Finding Malicious Domains Using Passive DNS.

Binkley and Singh, (2006). *An algorithm for anomalybased botnet detection*. Proc. USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop, p.43-48.

Binsalleeh, Ormerod, Boukhtouta, Sinha, Youssef, Debbabi, and Wang, (2010). On the analysis of the zeus botnet crimeware toolkit. in: Eighth Annual International Conference on Privacy Security and Trust (PST), 2010, pp. 31-38.

Blasing, L. Batyuk, A.-D. Schmidt, S. A. Camtepe, and S. Albayrak, (2010). An android application sandbox system for suspicious software detection. in

Malicious and unwanted software (MALWARE), 2010 5th international conference on, pp. 55–62, 2010.

Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre (2008). Fast unfolding of communities in large networks. J. Stat. Mech 2008 (10) (2008) P10008.

Borgohain T., Kumar U., Sanyal S. (2015). *Survey of security and privacy issues of internet of things.* arXiv:150102211.

Botta, Walter de Donato, Valerio Persico, and Antonio Pescapé (2016). *Integration of Cloud computing and Internet of Things: A survey*. Elsevier Future Generation Computer Systems Volume 56, pp684–700.

Bouij-Pasquier I , El Kalam AA , Ouahman AA , De Montfort M (2015). *A security framework for internet of things.* In: International conference on cryptology and network security. Springer; p. 19–31.

Breiman L (2001). Random forests. Machine Learning. Springer, 45 (1): pp. 5–32.

Bruno and Nurchis (2013). *Robust and efficient data collection schemes for vehicular multimedia sensor Network.* IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks"Madrid, Spain, pp. 1–10, June 2013.

Bruno Bogaz Zarpelao, Rodrigo Sanches Miani, Claudio Toshio Kawakani, and Sean Carlisto deAlvarenga (2017). *A survey of intrusion detection in Internet of Things*. ELSEVIER, Journal of Network and Computer Applications 84 (2017) 25–37.

C.Catania and G.Garino (2012). Automatic network intrusion detection - Current techniques and open issues. Computers & Electrical Engineering 38 (5) (2012) 1062–1072. doi:10.1016/j.compeleceng.2012.05.013.

C.Guntuku, P.Narang, and C.Hota (2013). Real-time Peer-to-Peer Botnet Detection Framework based on Bayesian Regularized Neural Network. arXiv.orgarXiv:1307.7464v1.

C.Kolias, G.Kambourakis, A.Stavrou, and M.Voas (2017). DDoS in the IoT - Mirai and Other Botnets. IEEE Computer 50 (7) pp 80–84. doi:10.1109/MC.2017.201.

C.Lin, Y.Chen, and C.Hung (2014). Botnet Detection Using Support Vector Machines with Artificial Fish Swarm Algorithm. J. Applied Mathematics 2014 (4) 1–9. doi:10.1155/2014/986428.

C.Wu, S.Sheng, and X.Dong (2018). Research on visualization systems for ddos attack detection. in: 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE, 2018, pp. 2986-2991.

Cadenas, M. C. Garrido, R. Martinez, and P. P. Bonissone (2012). Extending information processing in a fuzzy random forest ensemble. Soft Computing, vol. 16, pp. 845–861.

Canedo, Skjellum, Cyber, and Ginn (2016). *Using Machine Learning to Secure IoT Systems*. IEEE, 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand Dec 2016.

Carlos Ansotegui, Meinolf Sellmann, Kevin Tierney (2018). *Self-configuring Cost-Sensitive Hierarchical Clustering with Recourse.* Springer, Principles and Practice of Constraint Programming pp 524-534.

Carroll, Merwe, and Kotzé, (2012). *Securing Virtual and Cloud Environments*. In I. Ivanov; et al. Cloud Computing and Services Science, Service Science: Research and Innovations in the Service Economy. Springer Science+Business Media.

Chao Yang, Robert Harkreader, and Guofei Gu (2013). Empirical evaluation and new design for fighting evolving Twitter spammers. IEEE TIFS 8, 8 (2013).

Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos (2014). *Context Aware Computing for The Internet of Things: A Survey*, IEEE Communications Surveys & Tutorials, Volume 16, Issue 1, Pages 414-454, May 2014.

Chen and Le (2017). Hey, you, keep away from my device: remotely implanting a virus expeller to defeat Mirai on IoT devices. UbiComp (2017) 1–15.

Chen, K., Wang, P., and Lee, Y., (2015). Finding unknown malice in 10 seconds: mass vetting for new threats at the Google-Play scale. USENIX Security, vol. 15.

Chen, Luo, Yin, Xiao, Au, and Tang (2017). *CloudBot: Advanced mobile botnets using ubiquitous cloud technologies.* Elsevier,Pervasive and Mobile Computing journal, pp. 270-285.

Chi Cheng, rongxing Lu, Albrecht Petzoldt, and Tsuyoshi Takagi (2017). *Securing the Internet of Things in a Quantum World.* IEEE Communications magazine.

Ching-Hsiang Hsu, Chun-Ying Huang, and Kuan-Ta Chen (2010). *Fast-flux bot detection in real time.* Springer RAID 2010: Recent Advances in Intrusion Detection pp 464-483.

Choi, S.-K. Choi, and K. Cho (2013). Detection of mobile botnet using VPN. in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 142–148, 2013.

Chowdhury, M. Khanzadeh, R. Akula, F. Zhang, S. Zhang, H.R. Medal, M. Marufuzzaman, and L. Bian (2017). Botnet detection using graph-based feature clustering. J. Big Data 4 (2017) 14.

Christian Grimme, Dennis Assenmacher, and Lena Adam (2018). Changing Perspectives: Is It Sufficient to Detect Social Bots?. In SCSM.

Christian Kater and Robert Jäschke (2016). You shall not pass: detecting malicious users at registration time. In ACM WebSci Workshops.

Cimpanu and Catalin (Aug 30, 2016). *There's a 120,000-Strong IoT DDoS Botnet Lurking Around*. Softpedia. http://news.softpedia.com/news/there-s-a120-000-strong-iot-ddos-botnet-lurking-around-507773.shtml

Cinzia Bernardeschi, Francesco Mercaldo, Vittoria Nardone, and Antonella Santone (2019). Exploiting Model Checking for Mobile Botnet Detection. 23rd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, ScienceDirect, Procedia Computer Science 159 (2019) pp 963–972.

Clayton Allen Davis, Onur Varol, Emilio Ferrara, Alessandro Flammini, and Filippo Menczer (2016). BotOrNot: A System to Evaluate Social Bots. In ACM WWW Companion.

Cremonini, and Riccardi, (2009). The Dorothy project: an open botnet analysis framework for automatic tracking and activity visualization. IEEE European Conf. on Computer Network Defense, p.52-54.

CSA Corporate Members (2015). *Cloud Security Alliance (CSA).*The 2015 CSA APAC Congress will be held December 1st-3rd in Guangzhou, China, Available: http://www.cloudsecurityalliance.org/

Curtin RR, Gardner AB, Grzonkowski S, Kleymenov A, Mosquera A (2018). Detecting DGA domains with recurrent neural networks and side information. arXiv preprint arXiv: pp. 1810.02023.

D.Hoang, and C.Nguyen (2018). Botnet Detection Based On Machine Learning Techniques Using DNS Query Data. Future Internet 10 (5) 43. doi:10.3390/fi10050043.

D.M.J.Tax (2001) One-class classification. TU Delft, Delft University of Technology, 2001.

Dagon, D., C. C. Zou, and W. Lee (2006). Modeling Botnet Propagation Using Time Zones. NDSS 6: pp 2–13. San Diego, California, USA.

Damopoulos, G. Kambourakis, S. Gritzalis, and S. O. Park (2014). Exposing mobile malware from the inside (or what is your mobile app really doing?). Peer--Peer Netw. Appl., vol. 7, no. 4, pp. 687–697, 2014.

Daniele Ucci, Leonardo Aniello, and Roberto Baldoni (2019). Survey of machine learning techniques for malware analysis, ELSEVIER, Computers & Security, Volume 81, Pages 123-147, March 2019.

Das, Samburaj (2015). *Linux.Wifatch: Vigilante Hacker Infects Routers with Malware to Fight Bad Malware.* October 2015. https://hacked.com/linux-wifatch vigilante-hacker-infects-routers-malware-fight-bad-malware/

Derhamy H , Eliasson J , Delsing J , Priller P (2015). *A survey of commercial frame-works for the internet of things.* In: 2015 IEEE 20th conference on emerging technologies & factory automation (ETFA). IEEE; 2015. p. 1–8.

Descher, M., et al. (2009). *Retaining data control to the client in infrastructure clouds*. International Conference on Availability, Reliability and Security, IEEE, pp. 9-16, 2009.

Dhaya MA and Ravi R (2020). Multi feature behavior approximation model based efficient botnet detection to mitigate financial frauds. J Ambient Intell Humaniz Comput.

Doshi and Noah (2018). Machine Learning DDoS Detection for Consumer Internet of Things Devices. IEEE Security and Privacy Workshops (SPW) pp 1–7.

Doshi, Apthorpe, and Feamster (2018). *Machine Learning DDoS Detection for Consumer Internet of Things Devices.* arXiv preprint arXiv:1804.04159, 2018. Cornell University.

Doshi, R., Apthorpe, N., and Feamster, N. (2018). Machine learning DDoS detection for consumer internet of things devices. In: IEEE Security and Privacy Workshops, pp. 29–35.

Dotsev, Sermyagin, Shakhin, Reyer, Wimmers, Brem, Zinovieva (2018). *PSXIV-4 Breed purity of Holstein bulls born in Russia and imported from different countries.* Journal of Animal Science, Volume 96, Issue suppl_3, Pages 142–143.

E.Anthi, L.Williams, and P.Burnap (2018). Pulse: an adaptive intrusion detection for the internet of things. in: Living in the Internet of Things: Cybersecurity of the IoT - 2018, Institution of Engineering and Technology, 2018, pp. 1–5. doi:10.1049/cp.2018.0035.

Edwards and Profetis, (2016). *Hajime:Analysis of a Decentralized Internet Worm for IoT Devices*. Rapidity Networks; 16 Oct. 2016; security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf.

Elaheh Biglar Beigi, Hossein Hadian Jazi, Natalia Stakhanova, and Ali A. Ghorbani, (2014). *Towards effective feature selection in machine learning-based botnet detection approaches.* IEEE Conference on Communications and Network Security.

Eleonora Borgia (2014). *The Internet of Things vision: Key features, applications and open issues*, ELSEVIER, Computer Communications, Volume 54, Pages 1-31, 1 Dec 2014.

Ellen Messmer (2010). *Are security issues delaying adoption of cloud computing?.* Network World website: https://www.networkworld.com/article/2245986/saas/cloud-computing-security-challenges-unite-hosting-providers--security-specialists.html

Enck, M. Ongtang, and P. McDaniel (2009). On lightweight mobile phone application certification. in Proceedings of the 16th ACM CCS, pp. 235–245, 2009.

Eslahi, M. Yousefi, M. V. Naseri, Y. M. Yussof, N. M. Tahir, and H. Hashim (2016). Cooperative network behaviour analysis model for mobile Botnet detection. in Computer Applications & Industrial Electronics (ISCAIE), 2016 IEEE Symposium on, pp. 107–112, 2016.

Eslahi, R. Salleh, and N. B. Anuar (2012). MoBots: A new generation of botnets on mobile devices and networks. in IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), pp. 262–266, 2012.

Etemad and Vahdani (2012). Real-time botnet command and control characterization at the host leve. in Proceedings of the Sixth International Symposium on Telecommunications, pp. 1005–1009, Tehran, Iran, November 2012.

EU Cybersecurity, (2015). *The report on the state of cyber security in Poland for the year 2014*. www.bsa.org/EUcybersecurity

Faris Al-Zoubi AM, Heidari AA, Aljarah I, Mafarja M, Hassonah MA, and Fujita H (2019). An intelligent system for spam detection and identification of the most relevant features based on evolutionary random weight networks. Inf Fusion 48:67–83.

Faris H, Aljarah Im and Al-ShboulB (2015). Optimizing feedforward neural networks using krill herd algorithm for e-mail spam detection. In:2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT). IEEE, pp 1–5.

FarisH, Aljarah I, and Al-ShboulB(2016). Ahybrid approach based on particle swarm optimization and random forests for e-mail spam filtering. In: International conference on computational collective intelligence. Springer, pp 498–508.

Fedynyshyn G., Chuah M.C., and Tan G. (2011). Detection and classification of different botnet C&C channels. In: Calero, J.M.A., Yang, L.T., M´armol, F.G., Garc´ıa Villalba, L.J., Li, A.X., Wang, Y. (eds.) ATC 2011. LNCS, vol. 6906, pp. 228–242. (2011). https://doi.org/10.1007/978-3-642-23496-5 17

Feily, M., Shahrestani, A., Ramadass, S., (2009). *A survey of botnet and botnet detection*. IEEE 3rd Int. Conf. on Emerging Security Information, Systems and Technologies, p.268-273.

Fernando A.Teixeira, Fernando M.Q.Pereira, Hao-Chi Wong, José M.S.Nogueira, and Leonardo B.Oliveira (2019). *SIoT: Securing Internet of Things through distributed systems analysis*, ELSEVIER, Future Generation Computer Systems, Volume 92, Pages 1172-1186, March 2019.

Fortinet threat-report-q3 (2018). [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2018.pdf. [Accessed: 23-Feb-2020].

Francisco Villegas Alejandre, Nareli Cruz Cortes, and Eleazar Aguirre Anaya, (2017). *Feature selection to detect botnets using machine learning algorithms.* International Conference on Electronics, Communications and Computers (CONIELECOMP).

Francisco Villegas Alejandre, Nareli Cruz Cortés, and Eleazar Aguirre Anaya (2017). *Feature selection to detect botnets using machine learning algorithms.* IEEE Feb 2017 International Conference on Electronics, Communications and Computers (CONIELECOMP) Colula, Mexco.

Francois, S. Wang, and T. Engel (2011). Bottrack: tracking botnets using netflow and pagerank. in: International Conference on Research in Networking, Springer, 2011, pp. 1–14.

Frank and Harrell (2015). *Ordinal Logistic Regression*. Springer, Regression Modeling Strategies pp 311-325.

Fremantle and Scott, (2015*). A security survey of middleware for the Internet of Things*. PeerJ PrePrints, vol. 3, Jul. 2015, Art. no. e1521.

Fremantle P , Scott P (2017) . *A survey of secure middleware for the internet of things*. Peer J Comput Sci 2017;3:e114.

G. Gu, J. Zhang, and W. Lee (2008). BotSniffer: Detecting Botnet Command and Control Channels in network traffic. the Computer Sciences Commons, and the Engineering Commons, 2008.

G. Gu, P. Porras, V. Yegneswaran, M. Fong, W. Lee (2007). BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation. 16th USENIX Security Symposium, 2007.

G. Gu, Ro. Perdisct, J. Zhang, and W. Lee (2008). BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection. USENIX Association, 17th USENIX Security Symposium, 2008.

G.Gu, J. Zhang, and W. Lee, (2008). *BotSniffer: Detecting botnet command and control channels in network traffic.* Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08).

G.Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, (2007). *Bothunter: Detecting malware infection through ids-driven dialog correlation.* Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium. USENIX Association, 2007, p. 12.

Galar, A. Fernandez, E. Barrenechea, H. Bustince, and F. Herrera (2012). A review on ensembles for the class imbalance problem: bagging-, boosting-, and hybrid-based approaches. IEEE Transactions on Systems, Man, and Cybernetics, Part C, vol. 42, no. 4, pp. 463–484.

Garg, A. K. Singh, A. K. Sarje, and S. K. Peddoju (2013). Behaviour analysis of machine learning algorithms for detecting P2P botnets. in Proceedings of the 15th international conference on Advanced computing technologies (ICACT), Rajampet, India, September 2013.

Georgia L. Harris and Maria Isabel Pena (2016). *A Review and Survey of Metrology Outreach Efforts*. In Post-Secondary Education. J. Meas. Sci.Volume 11, Issue 1, pp 37–51.

Girei, Shah, and Shahid (2016). An enhanced botnet detection technique for mobile devices using log analysis. in 2016 22nd International Conference on Automation and Computing (ICAC), 2016: IEEE, pp. 450-455.

Graves and Schmidhuber (2005). Frame wise phoneme classification with bidirectional LSTM and other neural network architectures. Neural Networks 18.5, pp 602-610

Gregory Maus, (2017). A Typology of Socialbots (Abbrev.). In ACM WebSci.

Grizzard, J., Sharma, V., Nunnery, C., (2007). *Peer-to-peer botnets: overview and case study*. Proc. 1st USENIX Workshop on Hot Topics in Understanding Botnets, p.1.

Gu G., P. A. Porras, V. Yegneswaran, M. W. Fong, and W. Lee (2007). BotHunter: Detecting Malware Infection through IDS-Driven Dialog Correlation. Usenix Security 7, pp 1–16.

Gu, G., Porras, P., Yegneswaran, V., Fong, M., and Lee, W. (2007). BotHunter: detecting malware infection through IDS-driven dialog correlation. In: Proceedings of the 16th USENIX Security Symposium (USENIX Security 2007), pp. 167–182. USENIX Association, August 2007.

Gu, Perdisci, Zhang, Lee (2008). BotMiner: clustering analysis of network traffic for protocol- and structure-independent botnet detection. in: Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA, 2008, pp. 139–154.

Guofei Gu, Phillip Porras, Vinod Yegneswaran, Martin Fong and Wenke Lee (2007). BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation. 16th USENIX Security Symposium, (2007).

H.Kim, J.Smith, and G.Shin (2008). Detecting energy-greedy anomalies and mobile malware variants. MobiSys 239doi:10.1145/1378600.1378627.

H.Tran, C.Dang, H.Nguyen, P.Vo, and T.Vu (2019). Multi-confirmations and dns graph mining for malicious domain detection. in: Intelligent Computing-Proceedings of the Computing Conference, Springer, 2019, pp. 639-653.

Haddadi and Zincir (2016). Benchmarking the effect of flow exporters and protocol filters on botnet traffic classification. IEEE Syst. J. 10(4), pp. 1390–1401.

Haddadi F. and Zincir Heywood A.N. (2017). Botnet behaviour analysis: How would a data analytics-based system with minimum a priori information perform? Int. J. Netw. Manag. 2017, 27, e1977.

Haddadi, F., Morgan, J., et al. (2014). *Botnet behaviour analysis using ip flows: with http filters using classifiers.* 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 7–12.

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

Hallman, Bryan, and Palavicini (2017). IoDDoS the internet of distributed denial of sevice attacks. researchgate.net. URL https://www.researchgate.net/profile/Roger_Hallman2/publication/316455478_IoDDoS_-_The_

Hassanzadeh, R. Nayak, and D. Stebila (2012). Analyzing the effectiveness of graph metrics for anomaly detection in online social networks. in: Web Information Systems Engineering - WISE 2012 - 13th International Conference, Paphos, Cyprus, November 28–30, 2012. Proceedings, 2012, pp. 624–630.

Hayate Takase et al. (2019). A prototype implementation and evaluation of the malware detection mechanism for IoT devices using the processor information. International Journal of Information Security, pp. 1–11.

Hilton (2016).*Dyn Analysis Summary Of Friday October 21 Attack*. http://hub.dyn.com/dyn-blog/dyn-analysis-summary-of-friday-october-21-attack

Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos (2017). *IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges*. IEEE Internet of Things Journal Volume 4, Issue 1, pp75-87.

Hoover and Miller (2016). *Decision tree machine learning*. https://patents.google.com/patent/US20160155070A1/en

Huang (2013). Effective bot host detection based on network Failure models. Computer Networks, vol. 57, no. 2, pp. 514–525, 2013.

Hung and Sun, (2018). A botnet detection system based on machine-learning using flow-based features. in Proceedings of the SECURWARE 2018: @e Twelfth International Conferenc on Emerging Security Information, Italy, September 2018.

Huseynov and Kim (2014). *Unsupervised hadoop-based p2p botnet detection with threshold setting.* Department of Computer Science, Korea Advanced, Institute of Science and Technology.

Huseynov K, Kim K, Yoo PD (2014) *Semi-supervised botnet detection using ant colony clustering*. SCIS 2014. In: The 31th symposium on cryptography and information security Kagoshima. The Institute of Electronics, Information and Communication Engineers, Japan.

HUSEYNOV, K. KIM and P. YOO, (2014). *Semi-supervised Botnet Detection Using Ant Colony System*. 31th Symposium on Cryptography and Information Security, Kagoshima, Japan, Jan. pp. 21-24.

Huseynov, Kim, and Yoo (2014). Semi-supervised botnet detection using ant colony clustering. In: Proceedings of Symposium on Cryptography and Information Security (SCIS), pp. 1–7 (2014).

Huy-Trung Nguyen, Quoc-Dung Ngo, and Van-Hoang Le (2019). A novel graph-based approach for IoT botnet detection. International Journal of Information Security, Springer-Verlag GmbH Germany, part of Springer Nature 2019.

Huy-Trung Nguyen, Quoc-Dung Ngo, Doan-Hieu Nguyen, and Van-Hoang Le (2019). PSI-rooted subgraph: A novel feature for IoT botnet detection using classifier algorithms. ICT Express Journal, Elsevier.

I. Kotenko, I. Saenko, F. Skorik, and S. Bushuev(2015). *Neural network approach to forecast the state of the internet of things elements*. In Soft Computing and Measurements(SCM), 2015 XVIII International Conference on, pages133–135, May 2015.

Ianelli, N and Hackworth, A., (2005). *Botnets as a vehicle for online crime*. CERT Coordination Center, 1(1):28.in security - A survey. CoRR, vol. abs/1611.03186, http://arxiv.org/abs/1611.03186

Igor Popov (2017). Malware detection using machine learning based on word2vec embedding of machine code instruction. presented at the Siberian Symposium on Data Science and Engineering (SSDSE), 2017, pp. 1–4.

Iliofotou, H. chul Kim, M. Faloutsos, M. Mitzenmacher, P. Pappu, and G. Varghese (2011). Graption: a graph-based P2P traffic classification framework for the internet backbone. Comput. Netw. 55 (8) (2011) 1909–1920.

Ionut and Camelia (2016). *Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things*. IEEE, 12th International Conference on Intelligent Computer Communication and Processing (ICCP).

J.He, Y.Yang, X.Wang, and Z.Tan (2017). Adaptive traffic sampling for P2P botnet detection. Int. Journal of Network Management 27 (5) e1992. doi:10.1002/nem.1992.

J.Roosmalen, E.Vranken, and D.Eekelen (2018). Applying deep learning on packet flows for botnet detection. SAC 1629–1636doi:10.1145/3167132.3167306.

Jadhav S., Dutia S., Calangutkar K., Oh T., Kim Y.H., and Kim J.N. (2015). Cloud-based android botnet malware detection system. in: Advanced Communication Technology (ICACT). 2015 17th International Conference on, IEEE. pp. 347–352.

Jadhav, Dutia, Calangutkar, T.Oh, H.Kim, and N.Kim (2015). Cloud-based Android botnet malware detection system. in 2015 17th International Conference on Advanced Communication Technology (ICACT), 2015: IEEE, pp. 347-352.

Jaime Lynn Speiser, Bethany J.Wolf, Dongjun Chung, Constantine J.Karvellas, David G.Koch, Valerie L.Durkalski (2019). *BiMM forest: A random forest method for modeling clustered and longitudinal binary outcomes*. Elsevier, Chemometrics and Intelligent Laboratory Systems, Volume 185, 15 February 2019, Pages 122-134.

Jaiswal and Shivraj Bajgude (2013). Botnet technology. In 3rd International Conference on Emerging Trends in Computer and Image Processing (ICETCIP’2013), pages 169–175, 2013.

Jajodia, S., Ghosh, A.K., Swarup, V., Wang, C., and Wang, X.S. (2011). Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. Advances in Information Security, vol. 54. Springer, New York (2011).

Jakob Ziegier, Hubert Gattringer, Andreas Mueller (2018). *Classification of Gait Phases Based on Bilateral EMG Data Using Support Vector Machines*. 2018 7th IEEE International Conference on Biomedical Robotics and Biomechatronics (Biorob).

Jameel Qadri, Thomas M. Chen, and Jorge Blasco (2016). A review of significance of energy-consumption anomaly in malware detection in mobile devices. Intl. Journal on Cyber Situational Awareness, Vol. 1, No. 1.

Jankowski, Ritchie, Bellini, Covello, and Costa, (2014).*The Internet of Things: Making Sense of the Next Mega-Trend.* Goldman Sachs, New York, Tech. Rep., 2014.

Jatinder Singh, Thomas Pasquier, Bacon, and Hajoon(2016). *Twenty Security Considerations for Cloud-Supported Internet of Things.* IEEE JOURNAL, VOL. 3, NO. 3.

Javier Álvarez Cid-Fuentes, Claudia Szabo, and Katrina Falkner (2018). *An adaptive framework for the detection of novel botnets,* ELSEVIER, Computers & Security, Volume 79, Pages 148-161, November 2018.

Javier Velasco-Mata, Eduardo Fidalgo, Victor Gonzalez-Castro, Enrique Alegre, and Pablo Blanco-Medina (2019). Botnet Detection on TCP Traffic Using Supervised Machine Learning. Springer Nature Switzerland AG 2019, pp. 444–455.

Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami (2013). *Internet of Things (IoT): A vision, architectural elements, and future directions,* ELSEVIER, Future Generation Computer Systems, Volume 29, Issue 7, Pages 1645-1660, Sep 2013.

Jerkins (2017). *Motivating a Market or Regulatory Solution to IoT Insecurity with the Mirai Botnet Code.* 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC) 9-11 Jan 2017 Las Vegas, NV, USA.

Jiang, Nagra, and Ahammad (2016). Sok: Applying machine learning. https://arxiv.org/abs/1611.03186

Jing L., X. Yang, G. Kaveh, D. Hongmei, and Z. Jingyuan (2009). Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures. EURASIP Journal on Wireless Communications and Networking 2009, 11.

Jing Wang and Ioannis Paschalidis (2014). Botnet detection using social graph analysis. 2014 52nd Annual Allerton Conference on Communication, Control, and Computing, Allerton 2014.

Jing, L., Yang, X., Kaveh, G. (2009). *Botnet: classification, attacks, detection, tracing, and preventive measures.* EURASIP J. Wirel. Commun. Network., 2009: p.1-11.

Jing, Q., Vasilakos, A.V., Wan, J., (2014). *Security of the Internet of Things: perspectives and challenges.* Wirel. Netw. Volume 20, 8, PP 2481–2501.

John Peurifoy, Yichen Shen, Li Jing, Yi Yang, Fidel Cano-Renteria, Brendan G. DeLacy, John D. Joannopoulos (2018). *Nanophotonic particle simulation and inverse design using artificial neural networks*. Science Advances 01 Jun 2018, Vol. 4, no. 6.

Jung B., Kim T., Im E.G. (2018). Malware classification using byte sequence information. In: Proceedings of the Conference on Research in Adaptive and Convergent Systems. ACM, pp. 143–148 (2018).

Kadir A.F.A., Stakhanova N., and Ghorbani A.A. (2015). Android botnets: What urls are telling us. in: International Conference on Network and System Security, Springer. pp. 78–91.

Kadir, Andi Fitriah Abdul, Natalia Stakhanova, and Ali Akbar Ghorbani (2015). Android botnets: What urls are telling us. International Conference on Network and System Security. Springer, Cham, 2015.

Kai-Cheng Yang, Onur Varol, Clayton A Davis, Emilio Ferrara, Alessandro Flammini, and Filippo Menczer (2019). Arming the public with AI to counter social bots. Human Behavior and Emerging Technologies (2019).

Kamal Alieyan, Ammar Almomani, Mohammed Anbar, Mohammad Alauthman, Rosni Abdullah, and B. B. Gupta (2019). DNS rule-based schema to botnet detection. Enterprise Information Systems (Online) Journal, Enterprise Information Systems, DOI: 10.1080/17517575.2019.1644673.

Kambourakis, Kolias, and Stavrou (2017). The Mirai botnet and the IoT Zombie Armies. in: 2017 IEEE Military Communications Conference (MILCOM), IEEE, 2017, pp. 267–272. doi:10.1109/MILCOM.2017.8170867.

Kambourakisa, Kolias, and Stavrou (2017). *The Mirai Botnet and the IoT Zombie Armies*. IEEE, Milcom 2017 Track 3 - Cyber Security and Trusted Computing.

Kamluk (2017). *Botnet business.* Kaspersky Lab:

Kapil Sinha, Arun Viswanathan, and Julian Bunn (2019). TRACKING TEMPORAL EVOLUTION OF NETWORK ACTIVITY FOR BOTNET DETECTION. arXiv:1908.03443, Cornell University.

Karasaridis, Rexroad, and Hoeflin (2016). Wide-Scale Botnet Detection and Characterization. https://www.usenix.org/legacy/events/hotbots07/tech/full_papers/karasaridis/karasaridis.pdf.

Karim, A., R. B. Salleh, M. Shiraz, S. A. A. Shah, I. Awan, and N. B. Anuar (2014). Botnet Detection Techniques: Review, Future Trends and Issues. Journal of Zhejiang University SCIENCE C 15: pp 943–983. doi:10.1631/jzus.C1300242.

Karim, R. Salleh, M. K. Khan, A. Siddiqa, and K.-K. R. Choo (2016). On the analysis and detection of mobile botnet applications. J. Univers. Comput. Sci., vol. 22, no. 4, pp. 567–588, 2016.

KARIM, Rosli Bin SALLEH, Muhammad SHIRAZ, Syed Adeel Ali SHAH, Irfan AWAN, Nor Badrul ANUAR (2014). *Botnet detection techniques: review, future trends, and issues*. Journal of Zhejiang University-SCIENCE C (Computers & Electronics).

Karim, S. A. A. Shah, and R. Salleh (2014). Mobile botnet attacks: a thematic taxonomy. in New Perspectives in Information Systems and Technologies, Volume 2, Springer, pp. 153–164, 2014.

Karim, Salleh, Khurram Khan, Siddiqa, and Raymond Choo (2016) *On the analysis and detection of mobile botnet applications*. J Univ Comput Sci 22(4):567–588.

Kasprzyk, Paz, and Tarapata (2017*). Modeling and simulation of botnet based cyber-threats.* EDP Sciences, MATEC Web of Conferences 125, 03013.

Kazuya Kuwabara, Hiroaki Kikuchi, Masato Terada, and Masashi Fujiwara (2010). Heuristics for detecting botnet coordinated attacks. In Proceedings of the 4th International Workshop on Advances on Information Security (WAIS2010), pages 603–607, 02 2010.

Khalil, K., Qian, Z., Yu, P., Krishnamurthy, S., and Swam, A. (2016). Optimal monitor placement for detection of persistent threats. In: Proceedings of the IEEE Global Communications Conference (IEEE GLOBECOM 2016). IEEE, Washington, DC, December 2016.

Khan , Khan, Zaheer, and Khan S (2012). *Future internet: the internet of things architecture, possible applications and key challenges*. In: Frontiers of information technology (FIT), 2012 10th international conference on. IEEE; 2012. p. 257–60.

Khattak, S., N. Ramay, K. Khan, A. Syed, and S. Khayam (2013). A Taxonomy of Botnet Behavior, Detection, and Defense.

Khehra G, Sofat S (2018) BotScoop: scalable detection of DGA based botnets using DNS traffic. In: 9th ICCCNT 2018, 10–12 July 2018, IISC, Bengaluru, India.

Kijewski A, (2013). *Secure 2013 CERT Polska vs botnets*. https://www.secure.edu.pl/repository/2013/prezentacje/D1_1715_A_Kijewski

Kim, H., Claffy, K.C., Fomenkov, M., Barman, D., Faloutsos, M., and Lee, K. (2008). Internet traffic classification demystified: myths, caveats, and the best practices. In: Proceedings of the 2008 ACM CoNEXT Conference, pp. 11:1–11:12.

Kim, Jernite, Sontag, and Alexande, (2016). *Character-Aware Neural Language models.* Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence (AAAI-16).

Kirubavathi and Anitha (2016). Botnet detection via mining of traffic flow characteristics. Comput. Electr. Eng. 50, 91–101 (2016)

Kirubavathi Venkatesh and Anitha Nadarajan (2012). HTTP botnet detection using adaptive learning rate multilayer feed-forward neural network. In: Askoxylakis, I., P¨ohls, H.C., Posegga, J. (eds.) WISTP 2012. LNCS, vol. 7322, pp. 38–48. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30955-7 5

Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas (2017).*DDoS in the IoT:Mirai and Other Botnets*. THE IEEE COMPUTER SOCIETY, Volume 50, Issue 7, pp 80-84.

Kolias, Kambourakis, Stavrou, and Voas (2017). Ddos in the iot: mirai and other botnets. Computer 50(7):80–84.

Kovacs (2015). *Developers of Mysterious Wifatch Malware Come Forward* .https://www.securityweek.com/developers-mysterious-wifatchmalware-come-forward

Kovatsch, Ostermaier, and Mayer, (2012). *Moving application logic from the firmware to the cloud: Towards the thin server architecture for the Internet of Things*. in Proc. 6th Int. Conf. Innov.Mobile Internet Serv. Ubiq.Comput(IMIS), 2012.

Kozik and Choras (2017). Pattern Extraction Algorithm for NetFlow-Based Botnet Activities Detection. Security and Communication Networks 2017 1–10. doi:10.1155/2017/6047053.

Kresimir Popovic , Zeljko Hocenski, (2010).*Cloud computing security issues and challenges*. In The Third International Conference on Advances in Humanoriented and Personalized Mechanisms, Technologies, and Services, 2010, pp.344-349.

Kugisaki, Y., Kasahara, Y., Hori, Y., (2007). *Bot detection based on traffic analysis*. IEEE Int. Conf. on Intelligent Pervasive Computing, p.303-306.

Kumar JS and Patel DR (2014). *A survey on internet of things: security and privacy issues*. Int J Comput Appl 2014;90(11).

Kwon, J. Lee, H. Lee, and A. Perrig (2016). PsyBoG: A Scalable Botnet Detection Method for Large-scale DNS Traffic. Computer Networks.

L.Li, J.Liu, L.Cheng, S.Qiu, W.Wang, X.Zhang, and Z.Zhang (2018). CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Trans. Intell. Transp. Syst. 19 (7) (2018) 2204–2220, doi: 10.1109/TITS.2017.2777990.

Lagraa, J. François, A. Lahmadi, M. Miner, C.A. Hammerschmidt, and R. State (2017). Botgm: unsupervised graph mining to detect botnets in traffic flows. in: 1st Cyber Security in Networking Conference, CSNet 2017, Rio de Janeiro, Brazil, October 18–20, 2017, 2017, pp. 1–8.

Leo Breiman (2001). *Random Forests. Springer, Machine Learning,* October 2001, Volume 45, Issue 1, pp 5–32.

Leon Böck, Emmanouil Vasilomanolakis, Jan Helge Wolf, and Max Mühlhäuser (2019). *Autonomously detecting sensors in fully distributed botnets*, ELSEVIER, Computers & Security, Volume 83, Pages 1-13, June 2019.

Letteri, Massimo Del Rosso, Pasquale Caianiello, and Dajana Cassioli (2018). Performance of Botnet Detection by Neural Networks in Software-Defined Networks. at semanticscholar.org, https://pdfs.semanticscholar.org/09a6/105db6de932ef5986a2d75d56d2233ddb66a.pdf.

Letteri, Rosso, Caianiello, and Cassioli (2018). Performance of Botnet Detection by Neural Networks in Software-Defined Networks. ITASEC. https://dblp.org/rec/conf/itasec/LetteriRCC18

Leverett, (2011). *Quantitatively assessing and visualising industrial system attack surfaces*. M.S. thesis, Dept. Comput. Lab., Univ. Cambridge, Cambridge, U.K., 2011.

Li Z., A. Goyal, Y. Chen, and V. Paxson (2009). Automating Analysis of Large-scale Botnet Probing Events. In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, pp 11–22. ACM.

Li, C., W. Jiang, and X. Zou (2009). Botnet: Survey and Case Study. Innovative Computing, Information and Control (ICICIC), 2009 Fourth International

Conference, Kaohsiung, Taiwan,1184–1187. IEEE. doi:10.1136/hrt.2008.156208.

Li, Goyal, and Chen (2008). Honeynet-Based Botnet Scan Traffic Analysis. Springer Science+Business Media, LLC 2008.

Li, Lu, Liang, Shen, Chen, and Lin, (2011). *Smart Community: An Internet of Things Application.* IEEE Commun. Mag., vol. 49, no. 11, 2011.

Lin and Chen (2012). Class-imbalanced classifiers for high-dimensional data. Briefings in Bioinformatics, vol. 14, no. 1, pp. 13–26.

Lin and Li, (2013). Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks. IEEE Trans. Vehic. Tech., vol.62, no. 7, 2013.

Lina Ni, Chao Li, Xiao Wang, Honglu Jiang, Jiguo Yu (2018). *DP-MCDBSCAN: Differential Privacy Preserving Multi-Core DBSCAN Clustering for Network User Data*. IEEE Access, Volume. 6, Page(s): 21053 - 21063.

Liu, L., Chen, S., Yan, G, (2008). BotTracer: executionbased bot-like malware detection. In: Information Security. Springer Berlin Heidelberg, p.97-113.

Livadas C., Walsh R., Lapsley D., and Strayer W.T. (2006). Using machine learning techniques to identify botnet traffic. In: Proceedings. 2006 31st IEEE Conference on Local Computer Networks, pp. 967–974, November 2006

Livadas, Walsh, Lapsley, and Strayer (2006). Usilng machine learning technliques to identify botnet traffic. in: Proceedings. 2006 31st IEEE Conference on Local Computer Networks, 2006, pp. 967–974.

Lotfollahi, Zade, Siavoshani, and Saberian (2017). Deep Packet - A Novel Approach For Encrypted Traffic Classification Using Deep Learning. CoRR cs.LG. http://arxiv.org/abs/1709.02656v3

Lu, Zhu, Lin, Fan, and Shen,(2010). *Pi: A Practical Incentive Protocol for Delay Tolerant Networks.* IEEE Trans. Wireless Commun., vol. 9, no. 4, Apr. 2010.

Luca Scrucca and Adrian E. Raftery (2018). *clustvarsel: A Package Implementing Variable Selection for Gaussian Model-Based Clustering in R*. Journal of Statistical Software, Volume 84, Issue 01.

Luigi Atzori, Antonio Iera, and Giacomo Morabito (2010). *The Internet of Things: A survey,* ELSEVIER, Computer Networks, Volume 54, Issue 15, Pages 2787-2805, 28 Oct 2010.

M. Ali, R. Dhamotharan, E. Khan, S.U. Khan, A.V. Vasilakos, K. Li, A.Y. Zomaya, SeDaSC: *secure data sharing in clouds*. IEEE Syst. J. (2015), http://dx.doi.org/10.1109/JSYST.2014.2379646.

M.Antonakakis, T.April, M.Bailey, M.Bernhard, E.Bursztein, J.Cochran, Z.Durumeric, A.Halderman, L.Invernizzi, M.Kallitsis, D.Kumar, C.Lever, Z.Ma, J.Mason, D.Menscher, C.Seaman, N.Sullivan, K.Thomas, and Y.Zhou (2017). Understanding the Mirai Botnet. USENIX Security Symposium.

M.Donno, N.Dragoni, A.Giaretta, and A.Spognardi (2018). DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. Security and Communication Networks 2018 (4) 1–30. doi:10.1155/2018/7178164.

M.Feily, A.Shahrestani, and S. Ramadass, (2009). *A survey of botnet and botnet detection*. Emerging Security Information, Systems and Technologies, SECURWARE. Third International Conference on. IEEE, 2009, pp. 268–273.

M.Feily, A.Shahrestani, and S.Ramadass (2009). A survey of botnet and botnet detection. in: Third International Conference on Emerging Security Information, Systems and Technologies., 2009, pp. 268-273.

M.Lyu, D.Sherratt, A.Sivanathan, H.Gharakheili, A.Radford, and V.Sivaraman (2017). Quantifying the reflective DDoS attack capability of household IoT devices. ACM, New York, New York, USA, 2017. doi:10.1145/3098243.3098264.

M.Ring, S.Wunderlich, D.Scheuring, D.Landes, and A.Hotho (2019). A survey of network-based intrusion detection data sets. Computers & Security, ScienceDirect, Volume 86, September 2019, Pages 147-167.

M.Singh, M.Singh, and S.Kaur (2019). Issues and challenges in dns based botnet detection: A survey. Computers & Security, ScienceDirect,Volume 86, September 2019, Pages 28-52.

Mahesh Banerjee and Dr. S. D. Samantaray (2019). Network Traffic Analysis Based IoT Botnet Detection Using Honeynet Data Applying Classification Techniques. International Journal of Computer Science and Information Security (IJCSIS), Vol. 17, No. 8, August 2019.

Mahesh Banerjee, Bhavna Agarwal, and S. D. Samantaray (2019). An Integrated Approach for Botnet Detection and Prediction Using Honeynet and Socialnet Data. International Conference on Intelligent Computing and Smart Communication 2019, Springer, page 423-431.

Mahmoud, Yousuf, Aloul, and Zualkernan (2015) *Internet of things (iot) security: Current status, challenges and prospective measures.* In 2015 10th International Conference for Internet Technology and Secured Transactions(ICITST), pages 336–341, Dec 2015.

Maimo LF, Celdran AH, Perez MG, Clemente FJG, and Perez GM (2019). Dynamic management of a deep learning-based anomaly detection system for 5G networks. J Ambient Intell Humaniz Comput 10(8): pp. 3083–3097.

Manadhata, P.K., Wing, J.M.(2011). An attack surface metric. IEEE Trans. Softw. Eng.37(3), pp 371–386.

Manmeet Singh, Maninder Singh, and Sanmeet Kaur (2019). Issues and challenges in DNS based botnet detection: A survey. Computers & Security, sciencedirect, Elsevier.

Maria Habib, Ibrahim Aljarah, Hossam Faris and Seyedali Mirjalili (2019). Multi-objective Particle Swarm Optimization for Botnet Detection in Internet of Things. Algorithms for Intelligent Systems, Springer Nature Singapore Pte Ltd., pp 203-229.

Marzano, Alexander, Fonseca, Fazzion, Hoepers, Steding-Jessen, Chaves, Cunha, Guedes, and Meira (2018). The evolution of bashlite and mirai iot botnets. In: 2018 IEEE symposium on computers and communications (ISCC). IEEE, pp 00813–00818.

Massimiliano Albanese, Sushil Jajodia, Sridhar Venkatesan, George Cybenko, and Thanh Nguyen (2019). Adaptive Cyber Defenses for Botnet Detection and Mitigation. Springer Nature Switzerland AG 2019, pp 156-205.

Masters, Greg (2016). *Millions of IoT devices enlisted into DDoS bots with Bashlite malware.* SC Magazine. Retrieved 21 October 2016. https://www.scmagazine.com/millions-of-iot-devices-enlisted-into-ddosbots-with-bashlite-malware/article/530241/

Masud, J. Gao, L. Khan, J. Han, and B. Thuraisingham (2008). Mining concept-drifting data stream to detect peer to peer botnet traffic. Tech. Report UTDCS-05-08, University of Texas at Dallas, Richardson, Texas.

Masud, T. Al-khateeb, L. Khan, B. Thuraisingham, and K. Hamlen, (2008). *Flow-based identification of botnet traffic by mining multiple log files*. in Distributed Framework and Applications, 2008. DFmA 2008. First International Conference on, oct. 2008, pp. 200 –206.

Matias D. Cattaneo, Michael Jansson, Whitney K. Newey (2018). *Inference in Linear Regression Models with Many Covariates and Heteroscedasticity*. Journal of the American Statistical Association.Volume 113, 2018 - Issue 523.

Matija Stevanovic and Jens Myrup Pedersen (2014). An efficient flow-based botnet detection using supervised machine learning. In 2014 International Conference on Computing, Networking and Communications, ICNC 2014, pages 797–801, 02 2014.

McCarty, B., 2003. *Botnets: big and bigger*. IEEE Secur. Priv., 1(4):87-90.

McDermott, Farzan Majdani, and Andrei V. Petrovski (2018). *Botnet Detection in the Internet of Things using Deep Learning Approaches*. IEEE, International joint conference on neural networks 2018 (IJCBB), Rio de Janeiro, Brazil.

McKay, B. Pendleton, J. Britt, and B. Nakhavanit (2019). Machine learning algorithms on botnet traffic: ensemble and simple algorithms. in Proceedings of the 3rd International Conference on Compute and Data Analysis, pp. 31–35, Kahului, HI, USA.

Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Breitenbacher D, Shabtai A, Elovici Y (2018). N-baiot: Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Comput 13(9): pp. 12–22.

Meng and Spanoudakis (2015). MBotCS: A mobile botnet detection system based on machine learning. in International Conference on Risks and Security of Internet and Systems, 2015: Springer, pp. 274-291.

Meng Jiang, Peng Cui, Alex Beutel, Christos Faloutsos, and Shiqiang Yang (2016b). Inferring lockstep behavior from connectivity pattern in large graphs. KAIS 48, 2 (2016).

Meng Jiang, Peng Cui, Alex Beutel, Christos Faloutsos, and Shiqiang Yang (2016a). Catching Synchronized Behaviors in Large Networks: A Graph Mining Approach. ACM TKDD 10, 4 (2016).

Michele Mazza, Stefano Cresci, Marco Avvenuti, Walter Quattrociocchi, and Maurizio Tesconi (2019). RTbust: Exploiting Temporal Patterns for Botnet Detection on Twitter. WebSci 2019, June 30–July 3, 2019, Boston, MA, USA.

Middleton, Tully, and Kjeldsen, (2013). *Forecast: The Internet of Things, Worldwide*. Gartner, 2013 [Online].

Miller and Busby-Earle, (2016). *The role of machine learning in botnet detection*. Journal of Cyber Security, Vol 4, pp 1–32.

Ming Fan et al., (2016). Frequent Subgraph based Familial Classification of Android Malware. presented at the IEEE 27th International Symposium on Software Reliability Engineering.

Mirsky Y, Doitshman T, Elovici Y, Shabtai A (2018). Kitsune: an ensemble of autoencoders for online network intrusion detection. arXiv preprint arXiv :18020 9089.

Mohammad Hasanzadeh-Mofrad and Alireza Rezvanian (2018). *Learning Automata Clustering*. Journal of Computational Science, Volume 24, January 2018, Pages 379-388.

Mohan VS, Vinayakumar R, Soman KP, Poornachandran P (2018). Spoof Net: syntactic patterns for identification of ominous online factors. In: IEEE Security and PrivacyWorkshops, pp. 258–263.

Mohd. Abdul Sattar, Mohammed Anwaruddin, and Mohd. Anas Ali (2017). *A review on Internet of Things-Protocols Issues*. IJIREEICE Vol 5, Issue 2, P91-97.

Mongkolluksamee, Visoottiviseth, and Fukuda (2018). Robust Peer to Peer Mobile Botnet Detection by Using Communication Patterns. in Proceedings of the Asian Internet Engineering Conference, 2018: ACM, pp. 38-45.

Montgomery, Peack, and Vining (2012). *Introduction to linear regression analysis. John Wiley&Sons*.https://books.google.com.my/books?hl=en&lr=&id=0yR4KUL4VDkC&oi=fnd&pg=PR13&dq=Linear+Regression&ots=p5nqAdkQwg&sig=-vSqbbMv9z1PmuhShv7Apx6DbRo&redir_esc=y#v=onepage&q=Linear%20Regression&f=false

Moodi M and Ghazvini M (2019). A new method for assigning appropriate labels to create a 28 Standard Android Botnet Dataset (28-SABD). J Ambient Intell Humaniz Comput 10(11): pp. 4579–4593.

Moon, Kim, Hur, and Kim (2012). Detection of botnets before activation: an enhanced honeypot system for intentional infection and behavioral observation of malware. Special Issue: Next Generation Communication and Network Security, Volume5, Issue10, Pages 1094-1101, October 2012.

Moran Baruch and Gil David (2018). *Domain Generation Algorithm Detection Using Machine Learning Methods*. Cyber Security: Power and Technology, 2018 - Springer pp 133-161.

Mousavi, Khansari, and Rahmani (2019). A Fully Scalable Big Data Framework for Botnet Detection Based on Network Traffic Analysis. Information Sciences, Elsevier.

Muncaster (2017). *Mirai-Busting Hajime Worm Could Be Work of White Hat*. https://www.infosecuritymagazine.com/news/mirai-busting-hajime-worm-could/

N.Kumar, J.Madhuri, and M.ChanneGowda (2017). Review on security and privacy concerns in Internet of Things. in: 2017 International Conference on IoT and Application (ICIOT), IEEE, 2017, pp. 1–5. doi:10.1109/ICIOTA.2017.8073640.

Namazifar and Pan (2015). *Research spotlight: detecting algorithmically generated domains.Cisco*. http://blogs.cisco.com/security/talos/detecting-dga.

Narang, Ray, Hota and Venkatakrishnan, (2014). *Peer-Shark: Detecting Peer-to-Peer Botnets by Tracking Conversations*. IEEE Security and Privacy Workshops (SPW), May 17-18, 2014, SanJose, CA.

Narang, Reddy, and Hota (2013). Feature selection for detection of peer-to-peer botnet traffic. In: Proceedings of the 6th ACM India Computing Convention, Compute 2013, pp. 16:1–16:9. ACM, New York (2013).

Nataraj L., Karthikeyan S., Jacob G., and Manjunath B.S. (2011). Malware images: visualization and automatic classification. In: Proceedings of the 8th International Symposium on Visualization for Cyber Security. ACM, pp. 4–11 (2011).

Nazemi Gelian, H. Mashayekhi, and Y. Mashayekhi (2019). A self-learning stream classifier for flow-based botnet detection. International Journal of Communication Systems, vol. 32, pp. 1–15.

Nechaev B. and A. Gurtov (2013). Classification of Botnet Detection Techniques. Oberheide, J., M. Karir, and Z. M. Mao. 2007. “Characterizing Dark Dns Behavior.” In Detection of Intrusions and Malware, and Vulnerability Assessment, edited by M. Hämmerli B., and Sommer R., 4579, pp 140–156. Berlin, Heidelberg: Springer.

Ngu, Mario Gutierrez, Vangelis Metsis, and Surya Nepal (2017). *IoT Middleware: A Survey on Issues and Enabling Technologies*.IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 1, FEBRUARY 2017.

Nguyen Vo, Kyumin Lee, Cheng Cao, Thanh Tran, and Hongkyu Choi (2017). Revealing and detecting malicious retweeter groups. In IEEE/ACM ASONAM.

Nguyen, Cao, and Nguyen l-G (2015). *DGA botnet detection using collaborative filtering and density-based clustering.* SoICT 2015 Proceedings of the sixth international symposium on information and communication technology. New York.

Nikan Chavoshi, Hossein Hamooni, and Abdullah Mueen (2016). DeBot: Twitter Bot Detection via Warped Correlation. In IEEE ICDM.

Nogueira A., Salvador P., and Blessa F. (2010). A botnet detection system based on neural networks. In: 2010 Fifth International Conference on Digital Telecommunications, pp. 57–62, June 2010

O.Elish, Helmy, and Imtiaz Hussain (2013). Empirical Study of Homogeneous and Heterogeneous Ensemble Models for Software Development Effort Estimation. Mathematical Problemsin Engineering, Hindawi Publishing Corporation, Volume 2013, ArticleID312067.

Oberheide, J., M. Karir, and Z. M. Mao (2007). Characterizing Dark Dns Behavior. In Detection of Intrusions and Malware, and Vulnerability Assessment. edited by M. Hämmerli B., and Sommer R., 4579, pp 140–156. Berlin, Heidelberg: Springer.

Oberheide, Karir, and Mao, (2007). Characterizing dark DNS behavior. In: Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, p.140-156.

Ohm, (2010). Broken promises of privacy: Responding to the surprisingfailure of anonymization. UCLA Law Rev., vol. 57, no. 6, Aug. 2010.

Omar Y. Al-Jarrah, Omar Alhussein, Paul D. Yoo, Sami Muhaidat, Kamal Taha, Kwangjo Kim, (2016). *Data Randomization and Cluster-Based Partitioning for Botnet Intrusion Detection.* IEEE TRANSACTIONS ON CYBERNETICS, VOL. 46, Issue. 8, pp. 1796 - 1806.

P.Bazydlo, K.Lasota, and A.Kozakiewicz (2017). Botnet Fingerprinting - Anomaly Detection in SMTP Conversations. IEEE Security & Privacy 15 (6) 25–32. doi:10.1109/MSP.2017.4251116.

Pa YMP, Suzuki S, Yoshioka K, Matsumoto T, Kasama T, Rossow C (2015). Iotpot: analysing the rise of IoT compromises. EMU 9:1.

Padal, Hou, Shin, Zhu, Uysal, Wang, Singhal, and Merchant (2009). *Automated control of multiple virtualized resources.* Proceedings of the 4th ACM European conference on Computer systems, pp. 13–26. ACM.

Pajouh, Dehghantanha, Khayami, and Choo (2018). Intelligent os x malware threat detection with code inspection. Journal of Computer Virology and Hacking Techniques 14 (3) (2018) 213-223.

Panimalar P. and K. Rameshkumar (2014). A Review on Taxonomy of Botnet Detection. Advances in Engineering and Technology (ICAET), 2014 International Conference, Nagapattinam, India, pp 1–4. IEEE.

Patrick Diebold, Andreas Hess and Giinter Schafer (2005). A Honeypot Architecture for Detecting and Analyzing Unknown Network Attacks. Kommunikation in Verteilten Systemen (KiVS), Springer, pp 245-255 (2005).

Paul Szoldra (2016). *Inside the Internet of Things village at DefCon.* http://www.businessinsider.com/iot-villagedefcon-2016-8

Pavani and Mridula(2016). *Equitable Machine Learning Algorithms to Probe Over P2P Botnets*. Springer, Proceedings of the 4th International Conference on Frontiers pp 13-21.

Paxton, Ahn, and Chu, (2007). *Towards practical framework for collecting and analyzing network-centric attacks.* IEEE Int. Conf. on Information Reuse and Integration, p.73-78.

Pedro Domingos (2012). *A few useful things to know about machine learning.* Communications of the ACM, Volume 55 Issue 10, October 2012, ACM New York, NY, USA, pp 78-87.

Pekta and Acarman (2017). Effective feature selection for Botnet detection based on network flow analysis. In: researchgate.net, URL: https://www.researchgate.net/profile/Abdurrahman_Pektas/publication/320243609_EFFECTIVE_FEATURE_SELECTION_FOR_BOTNET_DETECTION_BASED_ON_NETWORK_FLOW_ANALYSIS/links/59d72e33458515db19ca943d/EFFECTIVE-FEATURE-SELECTION-FOR-BOTNET-DETECTION-BASED-ON-NETWORK-FLOW-ANALYSIS.pdf

Pham and Dacier, (2011). *Honeypot trace forensics: the observation view point matters*. Fut. Gener. Comput. Syst., 27(5):539-546.

Pham, V.-H., and M. Dacier (2011). Honeypot Trace Forensics: The Observation Viewpoint Matters. Future Generation Computer Systems 27 (5): 539–546. doi:10.1016/j.future.2010.06.004.

Pia S.de Boer, Alexander J.A.M.van Deursen, and Thomas J.L.van Rompay (2019). *Accepting the Internet-of-Things in our homes: The role of user skills*, ELSEVIER, Telematics and Informatics, Volume 36, Pages 147-156, March 2019.

Puri, R., (2003). Bots & Botnet: an Overview. SANS Institute.

Qiao Su, Yanhui Zhu, Yalin Jia, Ping Li, Fang Hu, Xingyong Xu (2018*). Sedimentary Environment Analysis by Grain-Size Data Based on Mini Batch K-Means Algorithm.* Geofluids Volume 2018, Article ID 8519695, 11 pages.

Qiao, Y., Yang, Y., He, J., (2012). *Detecting parasite P2P botnet in eMule-like networks through quasi-periodicity recognition*. Information Security and Cryptology-ICISC, p.127-139.

R.Perdisci, J. Zhang, W. Lee et al., (2008). *Botminer: Clustering analysis of network traffic for protocol-and structure-independent botnet detection*. USENIX Security Symposium, 2008, pp. 139–154.

Rahbarinia and Perdisci (2013). *Peerrush: Mining for unwanted p2p traffic*. Dept. of Computer Science, University of Georgia. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment pp. 62-82. Springer Berlin Heidelberg.

Ramachandran and, Feamster, (2006). *Understanding the network-level behavior of spammers*. ACM SIGCOMM Comput. Commun. Rev., 36(4):291-302.

Ramachandran, Feamster, and Dagon, (2006). *Revealing botnet membership using DNSBL counterintelligence*. Proc. 2nd USENIX Steps to Reducing Unwanted Traffic on the Internet, p.49-54.

Raza Hasan, Sellappan Palaniappan, Abdul Rafiez Abdul Raziff, Salman Mahmood, Kamal Uddin Sarker (2018). *Student Academic Performance Prediction by using Decision Tree Algorithm*. 4th International Conference on Computer and Information Sciences (ICCOINS).

Riaz Ullah Khan, Xiaosong Zhang, Rajesh Kumar, Abubakar Sharif, Noorbakhsh Amiri Golilarz, and Mamoun Alazab (2019). An Adaptive Multi-Layer Botnet Detection Technique Using Machine Learning Classifiers. Appl. Sci. 2019, 9, 2375; doi:10.3390/app9112375.

Roberto Perdisci, Wenke Lee, and Nick Feamster (2010). Behavioral clustering of http-based malware and signature generation using malicious network traces. In Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation, NSDI'10, pages 26–26, Berkeley, CA, USA, 2010. USENIX Association.

Roman, Lopez, and Najera, (2011). *Securing the Internet of Things*. Computer, vol. 44, no. 9, 2011.

Roy, Bose, and Sarddar (2015). *A Fog-Based DSS Model for Driving Rule Violation Monitoring Framework on the Internet of Things* . International Journal of Advanced Science and Technology, Vol.82, pp.23-32.

Ruixi Yuan, Zhu Li, Xiaohong Guan, and Li Xu (2010). *An SVM-based machine learning method for accurate internet traffic classification*. Springer, Information Systems Frontiers, Vol 12,Issue 2, pp 149-156.

S.Asri and B.Pranggono (2015). Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure. Wireless Personal Communications 83 (3) 2211–2223. doi:10.1007/s11277-015-2510-3.

S.Han and E.Im (2012). A Survey on P2P Botnet Detection. Vol. 120 of Lecture Notes in Electrical Engineering, Springer Netherlands, 2012, book section 56, pp. 589-593.

S.Saad, I.Traore, A.Ghorbani, B.Sayed, D.Zhao, W.Lu, J.Felix, and P.Hakimian, (2011). *Detecting p2p botnets through network behavior analysis and machine learning*. Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on. IEEE, 2011, pp. 174–180.

Saad, S., et al. (2011). Detecting P2P botnets through network behavior analysis and machine learning. In: 2011 Ninth Annual International Conference on Privacy, Security and Trust, pp. 174–180, July 2011

Saad, Traore, Ghorbani, Sayed, Zhao, Lu, Felix, and Hakimian, (2011*). Detecting p2p botnets through network behavior analysis and machine learning*. in Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on, july 2011, pp. 174 –180.

Saiyan Saiyod1, Youksamay Chanthakoummane, Nunnapus Benjamas, Nattawat Khamphakdee and Jirayus Chaichawananit (2016). Improving Intrusion Detection on Snort Rules for Botnet Detection. Information Science and Applications (ICISA) 2016 Springer, pp 765-779.

Samaila, Neto, Fernandes, Freire, In´acio, (2017). *Security challenges of the Internet of Things*. In: Batalla, J.M., Mastorakis, G., Mavromoustakis, C.X., Pallis, E. (eds.) Beyond the Internet of Things. IT, pp.53–82. Springer.

Samani, Jazi, Stakhanova, and Ghorbani (2014). Towards effective feature selection in machine learning-based botnet detection approaches. In: 2014 IEEE Conference on Communications and Network Security, pp. 247–255.

Samani, Jazi, Stakhanova, and Ghorbani, (2014). Towards effective feature selection in machine learning-based botnet detection approaches. in: IEEE Conference on Communications and Network Security, CNS 2014, San Francisco, CA, USA, October 29–31, 2014, 2014, pp. 247–255.

Samuel, (2000). *Some studies in machine learning using the game of checkers*. IEEE, IBM Journal of Research and Development, Vol 44,Issue 1.2, pp 206-226.

Sangho Lee and Jong Kim (2014). Early filtering of ephemeral malicious accounts on Twitter. Computer Communications 54 (2014).

Sangita Baruah (2019). Botnet Detection: Analysis of Various Techniques. Proceedings of International Conference on Computational Intelligence & IoT (ICCIIoT), ELSEVIER.

Sangkatsanee, P., Wattanapongsakorn, N., and Charnsripinyo, C. (2011). Practical real-time intrusion detection using machine learning approaches. Comput. Commun. 34(18), pp. 2227–2235.

Sapello, Constantin Serban, Ritu Chadha, Rauf Izmailov (2017). *Application of Learning Using Privileged Information(LUPI): Botnet Detection*. IEEE 2017 26th International Conference on Computer Communication and Networks (ICCCN) Vancouver, BC, Canada.

Satoh A, Nakamura Y, Nobayashi D, Ikenaga T (2018) Estimating the randomness of domain names for DGA bot callbacks. IEEE Commun Lett 22(7).

Schiavoni, Maggi, Cavallaro, and Zenero, (2014). *Phonix: DGA-based botnet tracking and intelligence.* International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA).

Schick, Shane (October 6, 2015). *Linux.Wifatch: The Router Virus That May Be Secretly Defending You From Other Malware*. Security Intelligence. Archived from the original on 7 December 2017. https://securityintelligence.com/news/linux-wifatch-the-router-virusthat-may-be-secretly-defending-you-from-other-malware/

Schiller, Binkley, and Harley, (2011). *Botnets—the Killer Web APP*. Syngress, Rockland.

Schmidt et al (2009). Static analysis of executables for collaborative malware detection on android. in 2009 IEEE International Conference on Communications, pp. 1–5, 2009.

Schmidt, S., Alpcan, T., Albayrak, S¸., Ba¸sar, T., and Mueller, A. (2008). A malware detector placement game for intrusion detection. In: Lopez, J., H¨ammerli, B.M. (eds.) CRITIS 2007. LNCS, vol. 5141, pp. 311–326. Springer, Heidelberg (2008).

Schneier (2016). *Lessons From the Dyn DDoS Attack*. https://securityintelligence.com/lessons-from-the-dyn-ddos-attack/,

Scott and Spaniel (2016).*Rise of the Machines, The DYN Attack was just a Practice Run.* http://icitech.org/icit-publication-the-rise-of-the-machines-the-dyn-attack-was-just-a-practice-run/

Sebastian Garcia, Martin Grill, Jan Stiborek, and Alejandro Zunino (2014). An empirical comparison of botnet detection methods. computers & security, 45:100–123, 2014.

Selim Yilmaz and Sevil Sen (2019). Early Detection of Botnet Activities Using Grammatical Evolution. Springer Nature Switzerland AG 2019.

Sen, (2011). *Privacy Preservation Technologies in Internet of Things. Proc*. Int'l. Conferenc. Emerging Trends in Mathematics, Technology, and Management, 2011.

Seshadri Rao Chinta, Vinod BabuPolinati and P. N. Srinivas (2018). Detecting Bots inside a Host using Network Behavior Analysis. International Journal of Computer Applications (0975 – 8887) Volume 180 – No.47, June 2018.

Shahrooz Shahrivartehrani and ShadilAkimi Bin Zainal Abidin Dionaea (2016). Honeypot Implementation and Malware Analysis in Cloud Environment. Journal of Computing Technologies and Creative Content 1(1), 1-5, August 2016.

Sheng, Yangy, Yuz, Vasilakos, McCanny, and Leung, (2013). *A Survey on the IETF Protocol Suite for the Internet of Things: Standards, Challenges, and Opportunities*. IEEE Wireless Commun., vol. 20, no. 6, 2013.

Shenghua Liu, Bryan Hooi, and Christos Faloutsos (2017). HoloScope: Topologyand-Spike Aware Fraud Detection. In ACM CIKM.

Shenghua Liu, Bryan Hooi, and Christos Faloutsos (2018). A Contrast Metric for Fraud Detection in Rich Graphs. IEEE TKDE (2018).

Shi, Gong, and Juntao, (2017). Malicious Domain Name Detection Based on Exreme Machine Learning. Neural Processing Lettrs pp 1-11.

Shishir Nagaraja, Prateek Mittal, Chi-Yao Hong, Matthew Caesar, and Nikita Borisov (2010). Botgrep: Finding p2p bots with structured graph analysis. In Proceedings of the 19th USENIX Conference on Security, USENIX Security'10, pages 7–7, Berkeley, CA, USA, 2010. USENIX Association.

Shogo Maeda, Atsushi Kanai, Shigeaki Tanimoto, Takashi Hatashima, and Kazuhiko Ohkubo (2019). A Botnet Detection Method on SDN using Deep Learning. IEEE International Conference on Consumer Electronics (ICCE).

Silva, R. M. Silva, Pinto, and Salles, (2013). *Botnets: A survey.* Computer Networks, vol. 57, no. 2, pp. 378 – 403.

Silva, S. S., R. M. Silva, R. C. Pinto, and R. M. Salles (2013). Botnets: A Survey. Computer Networks 57 (2): pp 378–403. doi:10.1016/j.comnet.2012.07.021.

Sina Hojjatinia, Sajad Hamzenejadi, and Hadis Mohseni (2020). Android Botnet Detection using Convolutional Neural Networks. 28th Iranian Conference on Electrical Engineering (ICEE2020).

Singh, Guntuku, Thakur, Hota (2014). Big data analytics framework for peer-to-peer botnet detection. Network 3:0 (Elsevier).

Singh, S. C. Guntuku, A. Thakur, and C. Hota (2014). Big data analytics framework for peer-to-peer botnet detection using random forests. Information Sciences 278 (2014) 488–497.

Smominru. https://www.cyber.nj.gov/threat-profiles/botnet-variants/smominru, Feb 2018.

Soltanaghaei and Kharrazi (2015). Detection of fast-flux botnets through DNS traffic analysis. Scientia Iranica. Transaction D, Computer Science & Engineering, Electrical 22 (6) (2015) 2389.

Somayeh Esmaeili and Hamid Reza Shahriari (2019). PodBot: A New Botnet Detection Method by Host and Network-Based Analysis. 27th Iranian Conference on Electrical Engineering (ICEE2019).

Sommer and Paxson (2010). *Outside the closed world: On using machinelearning for network intrusion detection.* IEEE Symposium on Security and Privacy (SP), May 2010 Berkeley/Oakland, CA, USA.

Sonar and Upadhyay (2016). *An Approach to Secure Internet of Things Against DDoS.* Singapore: Springer Singapore, 2016, pp. 367–376.

Spreitzenbarth, D. Arp, M. Hubner, H. Gascon, and K. Rieck (2014). DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket. in NDSS, 2014.

Stalmans, and Irwin (2011). A framework for DNS based detection and mitigation of malware infections on a network. IEEE Information Security South Africa, p.1-8.

Stavroulakis and Stamp (2010). *Handbook of Information and commnication Ssecurity*. Springer Hcidelherg Dordrecht London New Yok. e ISBN 9782612041174.

Stefano Cresci, Marinella Petrocchi, Angelo Spognardi, and Stefano Tognazzi (2019). On the capability of evolved spambots to evade detection via genetic engineering. Online Social Networks and Media 9 (2019).

Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angelo Spognardi, and Maurizio Tesconi (2018). Social Fingerprinting: detection of spambot groups through DNA-inspired behavioral modeling. IEEE TDSC 15, 4 (2018).

Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angelo Spognardi, and Maurizio Tesconi (2016). DNA-inspired online behavioral modeling and its application to spambot detection. IEEE Intelligent Systems 31, 5 (2016).

Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angelo Spognardi, and Maurizio Tesconi (2015). Fame for sale: Efficient detection of fake Twitter followers. Decision Support Systems 80.

Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angelo Spognardi, and Maurizio Tesconi (2017). The Paradigm-Shift of Social Spambots: Evidence, Theories, and Tools for the Arms Race. In ACM WWW Companion.

Stephanie Ding and Julian Bunn (2017). Machine Learning for Cybersecurity: Network-based Botnet Detection Using Time Limited Flows. https://curj.caltech.edu/2018/07/11/machine-learning-for-cybersecurity-network-based-botnet-detection-using-time-limited-flows/?share=google-plus-1&nb=1

Stergiou, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta (2016). *Secure integration of IoT and Cloud Computing.* Elsevier pp. 964-975.

Stevanovic and Pedersen (2014). *An efficient flow-based botnet detection using supervised machine learning. Department of Electronic Systems*. Aalborg University. In Computing, Networking and Communications (ICNC), 2014 International Conference on p797–801 (IEEE).

Stevanovic and Pedersen, (2013). *Machine learning for identifying botnet network traffic.* Aalborg University, Tech. Rep., 2013.

Stinson and Mitchell (2007). *Characterizing bots' remote control behavior*. In: Detection of Intrusions and Malware,and Vulnerability Assessment. Springer, p.89-108.

Stinson, E., Mitchell, J.C. (2008). Towards systematic evaluation of the evadability of bot/botnet detection methods. In: Proceedings of the 2nd USENIX Workshop on Offensive Technologies. USENIX Association, San Jose, July 2008.

Stone-gross B et al. (2009). Your botnet is my botnet: analysis of a botnet takeover. 97; 2009. pp. 635–47.

Strayer, Lapsely, Walsh, and Livadas (2008). *Botnet detection based on network behaviour. in Botnet Detection,* ser. Advances in Information Security, W. Lee, C. Wang, and D. Dagon, Eds. Springer, 2008, vol. 36, pp. 1–24.

Su J., Vasconcellos D., Prasad S., Sgandurra D., Feng Y., and Sakurai K. (2018). Lightweight classification of IoT malware based on image recognition. In: 2018 42nd Annual Computer Software and Applications Conference (COMPSAC). IEEE, pp. 664–669 (2018).

Su SC (2015). *Detecting p2p botnet in software defined network*. Institute of Network Engineering College of Computer Science National Chiao Tung University. http://ndltd.ncl.edu.tw/cgi-bin/gs32/gsweb.cgi/login?o=dnclcdr&s=id=%22103NCTU5726023%22.&searchmode=basic

Subashini and Kavitha, (2010). *A survey on security issues in service delivery models of cloud computing*. Journal of Network and Computer Applications, vol. 99.

Sudipta Chowdhury, Mojtaba Khanzadeh, Ravi Akula, Fangyan Zhang, Song Zhang, Hugh Medal, Mohammad Marufuzzaman, and Linkan Bian (2017). Botnet detection using graph-based feature clustering. Journal of Big Data, 4(1):14, May 2017.

Sunil Ray (2017). *Essentials of Machine Learning Algorithms (with Python and R Codes).* Analytics Vidhya, SEPTEMBER 9, 2017, https://www.analyticsvidhya.com/blog/2017/09/common-machine-learning-algorithms

Suzan Almutairi, Saoucene Mahfoudh, Sultan Almutairi, and Jalal S. Alowibdi (2020). Hybrid Botnet Detection Based on Host and Network Analysis. Hindawi Journal of Computer Networks and Communications Volume 2020, Article ID 9024726, 16 pages.

Suzuki S., Pa Y.M.P., Yoshioka K., Matsumoto T., Kasama T., and Rossow C. (2016). IoTPOT: a novel honenypot for revealing current IoT threats. J. Inf. Process. 24, 522–533 (2016).

Swati Khandelwal,(2016). *New iot botnet malware discovered; infecting more devices worldwide*. http://thehackernews.com/2016/10/linux-irciot-botnet.html, 2016.

Sweeney, P.J.(2014). Designing effective and stealthy botnets for cyber espionage and interdiction: finding the cyber high ground. Ph.D. thesis, Thayer School of Engineering, Darthmouth College, August 2014.

Taedong Kim and Stephen J. Wright (2018). *PMU Placement for Line Outage Identification via Multinomial Logistic Regression*. IEEE Transactions on Smart Grid. Volume. 9 , Issue. 1.

Tang, (2013). Deep Lerning using linear support vector machines. arXiv preprint arXiv: 1306.0239.

Tansettanakorn C., Thongprasit S., Thamkongka S., and Visoottiviseth V. (2016). Abis: a prototype of android botnet identification system. in: Student Project Conference (ICT-ISPC). 2016 Fifth ICT International, IEEE. pp. 1–5.

Tariq and Baig (2017). Machine Learning Based Botnet Detection in Software Defined Networks. International Journal of Security and Its Applications, 11(11): pp. 1–12, 2017.

Tarunpreet Bhatia and A.K.Verma (2017). Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues. Springer Science+Business Media New York 2017.

Thangapandiyan and Anand (2016). An efficient botnet detection system for P2P botnet. in: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET, IEEE, 2016, pp. 1217–1221. doi:10.1109/WiSPNET.2016.7566330.

Tian, Fang, Liu, and Lei (2016). *Detecting malicious domains by massive dns traffic data analysis.* In 2016 8th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC),vol. 01, Aug 2016, pp. 130–133.

Timothy Strayer, David Lapsely, Robert Walsh, and Carl Livadas (2008). Botnet Detection Based on Network Behavior. pages 1–24. Springer US, Boston, MA, 2008.

Timothy Strayer, Robert Walsh, Carl Livadas, and David Lapsley (2006). Detecting Botnets with Tight Command and Control. Proceedings. 2006 31st IEEE Conference on Local Computer Networks.

Tognazzi, Stefano Cresci, Marinella Petrocchi, and Angelo Spognardi (2018). From Reaction to Proaction: UnexploredWays to the Detection of Evolving Spambots. In ACM WWW Companion.

Tong Li, Jin Li, Zheli Liu, Ping Li, Chunfu Jia (2018). *Differentially private Naive Bayes learning over multiple data sources.* Elsevier, Information Sciences, Volume 444, May 2018, Pages 89-104.

Tran D, Mac H, Tong V, Tran HA, Nguyen LG (2018). A LSTM based framework for handling multiclass imbalance in DGA botnet detection. Neurocomputing 275: pp. 2401–2413.

Trend Micro, 2006. *Taxonomy of Botnet Threats*. Technical Report.

Vania J., A. Meniya, and H. Jethva (2013). A Review on Botnet and Detection Technique. International Journal of Computer Trends and Technology 4 (1): pp 23–29.

Vania, Meniya, and Jethva (2013). *A review on botnet and detection technique*. International Journal of Computer Trends and Technology, Vol 4, issue 1, pp. 23–29.

Vikas B (2015). Internet of things (iot): A survey on privacy issues and security 2015.

Vinayakumar R, Poornachandran P, Soman KP (2018c). Scalable framework for cyber threat situational awareness based on domain name systems data analysis. In: Big data in engineering applications, pp. 113–142.

Vinayakumar R, Soman KP, Poornachandran P (2018b). Detecting malicious domain names using deep learning approaches at scale. J Intell Fuzzy Syst 34(3): pp. 1355–1367.

Vinayakumar R, Soman KP, Poornachandran P, Mohan VS, Kumar AD (2019). ScaleNet: scalable and hybrid framework for cyber threat situational awareness based on DNS, URL, and Email data analysis. J Cyber Secur Mobil 8(2): pp. 189–240.

Vinayakumar R, Soman KP, Poornachandran P, Sachin Kumar S (2018a). Evaluating deep learning approaches to characterize and classify the DGAs at scale. J Intell Fuzzy Syst 34(3):pp. 1265–1276.

Vinayakumar, Soman, Poornachandran, Alazab, and Alireza (2019). DBD: Deep Learning DGA-Based Botnet Detection. Springer Nature Switzerland AG 2019.

W.H.Liao and C.C.Chang (2010). Peer to peer botnet detection using data mining scheme. in Proceedings of the International Conference on Internet Technology and Applications, pp. 1–4, Wuhan, China, August 2010.

W.Wu, J.Alvarez, C.Liu, and M.Sun (2018). Bot detection using unsupervised machine learning. Microsystem Technologies 24 (1) (2018) pp. 209-217.

W.Xue, C.Luo, G.Lan, R.K.Rana, W.Hu, and A.Seneviratne, (2017). Kryptein a compressive-sensing-based encryption scheme for the internet of things. IPSN (2017) 169–180.

Wang and Paschalidis (2014). Botnet detection using social graph analysis. in: 52nd Annual Allerton Conference on Communication, Control, and Computing, Allerton 2014, Allerton Park & Retreat Center, Monticello, IL, September 30, –October 3, 2014, 2014, pp. 393–400.

Wang K., Huang C.Y., Lin S.J., and Lin Y.D. (2011). A fuzzy pattern-based filtering algorithm for botnet detection. Comput. Netw. 55(15), 3275–3286 (2011)

Wang S., Yan Q., Chen Z., Yang B., Zhao C., and Conti M. (2018). Detecting android malware leveraging textsemantics of network flows. IEEE Trans. Inf. Forensics Secur. 2018, 13, pp. 1096–1109.

Wang X, Guo N, Gao F, and Feng J (2019). Distributed denial of service attack defence simulation based on honeynet technology. J Ambient Intell Humaniz Comput.

Wang, B., Li, Z., and Li, D., (2010). *Modeling connections behavior for web-based bots detection*. 2nd IEEE Int. Conf. on e-Business and Information System Security, p.1-4.

Wang, Li, and Harry (2017). Cluster and cloud computing framework for scientific metrology in flow control. Springer Science+Business Media, pp 1–10.

Wang, Liu, Pitsilis, and X.Zhang (2018). Abstracting massive data for lightweight intrusion detection in computer networks. Inf. Sci. 433–434 (2018) 417–430.

Wang, M.Zhao, and J.Wang (2019b). Effective android malware detection with a hybrid model based on deep autoencoder and convolutional neural network. J. Ambient Intell. Hum. Comput. 10 (8) (2019) 3035–3043.

Wang, M.Zhao, Z.Gao, G.Xu, H.Xian, Y.Li, and X.Zhang (2019a). Constructing features for detecting android malicious applications. issues, taxonomy and directions. IEEE Access 7 (2019) 67602–67631, doi: 10.1109/ACCESS.2019.2918139.

Wang, Ruigang Liang, Xiaokang Liu, Yingjun Zhang, Kai Chen, and Jin Li (2017). *An Inside Look at IoT Malware.* Springer ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume 202,pp 176-186.

Wang, X.Zhang, and S.Gombault (2009). Constructing attribute weights from computer audit data for effective intrusion detection. J. Syst. Softw. 82 (12) (2009) 1974–1981.

Wang, Y.He, J.Liu, and S.Gombault (2015). Constructing important features from massive network traffic for lightweight intrusion detection. IET Inf. Secur. 9 (6) (2015) 374–379.

Wei Wang, Yaoyao Shang, Yongzhong He, Yidong Li, and Jiqiang Liu (2020). BotMark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors. Information Sciences, ScienceDirect, Elsevier.

Wei Wu, Jaime Alvarez, Chengcheng Liu, and Hung‑Min Sun (2018). *Bot detection using unsupervised machine learning*. Springer-Verlag Berlin Heidelberg, Microsyst Technol (2018) 24:209–217.

Wellman, M.P. and Prakash, A. (2014). Empirical game-theoretic analysis of an adaptive cyber-defense scenario (preliminary report). In: Poovendran, R., Saad, W. (eds.) GameSec 2014. LNCS, vol. 8840, pp. 43–58. Springer, Cham (2014).

Winkler, (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham, MA USA: Syngress. pp. 187, 189.

Woodbridge, Anderson, Ahuja, and Grant, (2016). *Predicting Domain Generation Algorithms with Long Short-Term Memory Networks*. arXiv preprint arXiv:161100791.

Woosub Jung, Hongyang Zhao, Minglong Sun, and Gang Zhou (2020). IoT Botnet Detection via Power Consumption Modeling. Smart Health Volume 15, Science Direct, ELSEVIER, March 2020.

X.Li, J.Wang, and X.Zhang, (2017). Botnet Detection Technology Based on DNS. Future Internet 9 (4) 55. doi:10.3390/fi9040055. URL http://www.mdpi.com/1999-5903/9/4/55.

X.Li, L. Wang, and E. Sung (2008). AdaBoost with SVM-based component classifiers. Engineering Applications of Artificial Intelligence, vol. 21, no. 5, pp. 785–795.

X.Liu, J.Liu, S.Zhu, W.Wang, and X.Zhang (2019). Privacy risk analysis and mitigation of analytics libraries in the android ecosystem. IEEE Trans. Mob. Comput. (2019), doi: 10.1109/TMC.2019.2903186.

X.Xu, N. Yuruk, Z. Feng, and T.A.J. Schweiger (2007). SCAN: a structural clustering algorithm for networks. in: Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Jose, California, USA, August 12–15, 2007, 2007, pp. 824–833.

X.Y.Liu, J. Wu, and Z.-H. Zhou (2009). Exploratory undersampling for class imbalance learning. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 39, no. 2, pp. 539–550.

Xing Chen, Li Huang, Di Xie, Qi Zhao (2018). *EGBMMDA: Extreme Gradient Boosting Machine for MiRNA-Disease Association prediction*. Cell Death & Diseasevolume 9, Article number: 3 (2018).

Xingmei, Jing, and He (2013). Research on the basic characteristics, the key technologies, the network architecture and security problems of the internet of things. In Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on, pages825–828, Oct 2013.

Xueyan Wu, Jiquan Yang, Shuihua Wang (2018). Tea category identification based on optimal wavelet entropy and weighted k-Nearest Neighbors algorithm. Springer Science+Business Media New York.

Y.Meidan, M.Bohadana, Y.Mathov, Y.Mirsky, D.Breitenbacher, A.Shabtai, and Y.Elovici (2018). N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders. arXiv.orgarXiv:1805.03409v1.

Y.Yang, L.Wu, G.Yin, L.Li, and H.Zhao (2017). A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal 4 (5) pp 1250–1258. doi:10.1109/JIOT.2017.2694844.

Y.Ye, L. Chen, D. Wang, T. Li, Q. Jiang, and M. Zhao (2009). SBMDS: an interpretable string based malware detection system using SVM ensemble with bagging. Journal in Computer Virology, vol. 5, no. 4, pp. 283–293.

Yadav, Reddy, Reddy, and Ranjan, (2012). *Detecting algorithmically generated domain-flux attacks with DNS traffic analysis*. IEEE, ACM Transactions on Networking 20.5, pp 1663-1677.

Yang, Y., Wu, L., Yin, G., Li, L., and Zha (2017).*A survey on security and privacy issues in Internet-of-Things.* IEEE Internet of Things J. 4(5), 1250–1258(2017).

Yerima SY, Sezer S, and Muttik I (2015). High accuracy android malware detection using ensemble learning. IET Inf Secur 9(6): pp. 313–320.

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, and Takahiro Kasama (2015). Christian Rossow IoTPOT:Analysing the Rise of IoT Compromises. 9th USENIX Workshop on Offensive Technologies, Audust 10-11, 2015, Washington, D.C.

Yomi Karthik Rupesh, Payman Behnam, Goverdhan Reddy Pandla, Manikanth Miryala, Mahdi Nazm Bojnordi (2018). *Acceleratingk-Medians Clustering Using a Novel 4T-4R RRAM Cell.* IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Volume: 26 , Issue: 12.

Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao (2017). *A Survey on Security and Privacy Issues in Internet-of-Things*. IEEE INTERNET OF THINGS JOURNAL,pp 2327-4662.

Yusof, Saudi, and Ridzuan (2017a). A New Android Botnet Classification for GPS Exploitation Based on Permission and API Calls. in International Conference on Advanced Engineering Theory and Applications, 2017: Springer, pp. 27-37.

Yusof, Saudi, and Ridzuan (2017b). A new mobile botnet classification based on permission and API calls. in 2017 Seventh International Conference on Emerging Security Technologies (EST), 2017: IEEE, pp. 122-127.

Z. Xu, K. Ren, S. Qin, and F. Craciun (2018). CDGDroid: Android malware detection based on deep learning using CFG and DFG. in In Proceedings of the 20th International Conference on Formal Engineering Methods, ICFEM, 2018, pp. 177–193.

Zachary Miller, Brian Dickinson, William Deitrick, Wei Hu, and Alex Hai Wang (2014). Twitter spammer detection using data stream clustering. Information Sciences 260 (2014).

Zanella, (2014). *Internet of Things for smart cities*. IEEE Internet Things J., vol. 1, no. 1, Feb. 2014.

Zarpelao, Miani, Kawakani, and Alvarenga (2017). A survey of intrusion detection in Internet of Things. J. Network and Computer Applications 84 pp 25–37. doi:10.1016/j.jnca.2017.02.009.

Zarpelo, Miani, Kawakani, de Alvarenga, (2017). *A survey of intrusion detection in Internet of Things.* J. Netw. Comput. Appl. 84, 25 – 37(2017).

Zeidanloo and Manaf, (2009). *Botnet command and control mechanisms*. 2nd IEEE Int. Conf. on Computer and Electrical Engineering, p.564-568.

Zeidanloo, H. R., M. J. Z. Shooshtari, P. V. Amoli, M. Safari, and M. Zamani (2010). A Taxonomy of Botnet Detection Techniques. Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International ConferenceChengdu, China, 2: 158–162. IEEE.

Zeidanloo, Shooshtari, Amoli, Safari, and Zamani (2010). A taxonomy of botnet detection techniques. in: 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), Vol. 2, 2010, pp. 158-162.

Zeidanloo, Shooshtari, and Amoli, (2010). *A taxonomy of botnet detection techniques*. 3rd IEEE Int. Conf. on Computer Science and Information Technology, p.158-162.

Zhang, Gharaibeh, Thanasoulas, and Papadopoulos, (2016). *Bptdigger: Detecting dga bots in a single Network.* Proceedings of IEEE International Workshop on Analysis, ndss Traffic Monitoring and Analysis

Zhang, J., Perdisci, R., Lee, W., Luo, X., and Sarfraz, U. (2014). *Building a scalable system for stealthy P2P-botnet detection*. IEEE Transactions on Information Forensics and Security, Volume 9, Issue 1, pp. 27–38.

Zhang, J., Perdisci, R., Lee, W., Luo, X., and Sarfraz, U.(2014). Building a scalable system for stealthy P2P-botnet detection. IEEE Trans. Inf. Forensics Secur. 9(1), pp 27–38.

Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K., and Shieh, S., (2014). *IoT security: ongoing challenges and research opportunities.* IEEE 7th

International Conference on Service-Oriented Computing and Applications Matsue, Japan, pp. 230–234.

Zhang, Zhao, Liu, Li, and Gong, (2013). *Recuarrent support vector machines for speech recognition.* IEEE International Conference pm Acoustics, Speech and Signal Processing (ICASSP).

Zhao, D., Traore, I., Sayed, B., Lu, W., Saad, S., Ghorbani, A., and Garant, D.(2013*).* *Botnet detection based on traffic behavior analysis and flow intervals*. Elsevier, SciVerse ScienceDirect, computers & security 39, pp. 2–16.

Zhao, I. Traore, and B. Sayed (2013). Botnet detection based on traffic behavior analysis and flow intervals. Computers & Security, vol. 39, pp. 2–16, 2013.

Zhao, P. P. Lee, J. Lui, X. Guan, X. Ma, and J. Tao (2012). Cloud-based push-styled mobile botnets: a case study of exploiting the cloud to device messaging service. in Proceedings of the 28th Annual Computer Security Applications Conference, pp. 119–128, 2012.

Zhao, Traore, Sayed, Lu, Saad, Ghorbani, and Garan, (2013). *Botnet detection based on traffic behavior analysis and flow intervals*. 27th IFIP International Information Security Conference, November, 2013.

Zhao, Zongqu, Junfeng Wang, and Chonggang Wang (2013). An unknown malware detection scheme based on the features of graph. Security and Communication Networks, vol. 6, pp. 239–246.

Zhauniarovich, Khalil, Yu, and Dacier (2018). A survey on malicious domains detection through dns data analysis. ACM Computing Surveys (CSUR) 51 (4) (2018) 67.

Zhi Yang, Christo Wilson, Xiao Wang, Tingting Gao, Ben Y Zhao, and Yafei Dai (2014). Uncovering social network sybils in the wild. ACM TKDD 8, 1 (2014)

Zhou, Cao, Dong, and Vasilakos (2017). Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions. IEEE Communications Magazine.

Zhou, Dong, Cao, and Vasilakos, (2015). *Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs*, IEEE Trans. Info. Forensics and Security, vol. 10, no. 6, 2015 , pp. 1299–314.

Zhou, Li, Miao, and Yin, (2013). *DGA-Based Botnet Detection Using DNS traffic*. Journal of Internet Services and Information Security, 3.3/4, pp 116-123.

Zhu, Lin, Lu, Fan, and Shen,(2009). *SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay Tolerant Networks.* IEEE Trans. Vehic. Tech., vol. 58, no. 8, Oct. 2009, pp.4628–39.

Zhu, Z., Lu, G., Chen, Y., (2008). *Botnet research survey*. 32nd Annual IEEE Int. Computer Software and Applications, p.967-972.

Zi-Jia Wang, Zhi-Hui Zhan, Ying Lin, Wei-Jie Yu, Hua-Qiang Yuan, Tian-Long Gu (2018). *Dual-Strategy Differential Evolution With Affinity Propagation Clustering for Multimodal Optimization Problems.* IEEE Transactions on Evolutionary Computationm Volume. 22 , Issue. 6.

Zissis and Lekkas, (2010). *Addressing cloud computing security issues*. Future Generation Computer Systems Vol. 28, No. 3.

Appendix A Gantt Chart for Research Plan

Task	10 September – 14 December 2018 & 18 February – 26 July 2019										
	2018				**2019**						
	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	July
Topic Research											
Planning											
Literature Review											
Research Design											
Analysis											
Development											
Implementation											
Evaluation											
Report writing											
Final Submission											
Presentation											

Appendix B List of features

src, src port, dst, dst port, original dataset, original label, event generator, event signature, event priority, ndpi risk, ndpi detected protocol, payload bytes first, packet pay size 3, C packets rst avg, packet pay size 2, dst 2 src packets rate, C packets rst min, C packets urg avg, src 2 dst packets rate, C packets fin avg, C idle time max, http response status code, packet header size 4, dst 2 src inter time std, packet header size 0, C packets rst std, pay load bytes max, src 2 dst header bytes min, C dst 2 src packets rate max, packet pay size 8, dst 2 src header bytes min, http request version, src 2 dst header bytes max, dns query type, pay load bytes avg, dst 2 src header bytes std, C dst 2 src packets rate min, C packets syn std, C src2dst packets rate max, packet header size 7, C packets syn max, C tcp retrans missions max, packets fin, src 2 dst pay bytes, packet header size 6, dst 2 src packets, inter time 10, C packets ack avg, src 2 dst header bytes, inter time 9, C idle time std, C dst 2 src pay bytes rate max, packet direction 5, C src 2 dst pay bytes max, packet direction 0, packet direction 1, inter time 7, packets rst, C packets psh min, C src 2 dst pay bytes rate avg, src 2 dst inter time std, C src 2 dst pay bytes avg, dns num answers, packet pay size 7, C number of contacts, detection completed, inter time 6, src 2 dst header bytes std, packets ack, C packets rst max, inter time 3, dst 2 src header bytes avg, C duration avg, C packets ack min, dns query class, C dst 2 src pay bytes std, C packets syn avg, C packets psh max, C src 2 dst packets rate avg, dst 2 src pay bytes min, C dst 2 src header bytes min, src 2 dst inter time max, src 2 dst pay bytes min, http method, C packets psh avg, C dst 2 src header bytes std, C packets ack std, flow use time, inter time 2, dst 2 src inter time min, C dst 2 src packets rate std, packet pay size 4, C packets ack max, C dst 2 src packets max, C src 2 dst pay bytes min, dns num queries, inter time 8, packet header size 8, src 2 dst pay bytes max, protocol, dst 2 src pay bytes max, http content type, C src 2 dst packets avg, C src 2 dst pay bytes rate std, response rel time, packet pay size 10, inter time min, packet header size 1, dns reply code, inter time avg, C packets psh std, src 2 dst header bytes avg, packet direction 9, C dst 2 src packets std, packet header size 9, src 2 dst packets, pay load bytes, packet pay size 5, http num request headers, packet header size 2, packet direction 4, packet direction 7, C tcp retransmissions min, C duration min, C dst 2 src pay bytes avg, dst 2 src pay bytes avg, C dst 2 src header bytes max, C packets syn min, packet direction 3, http num response headers, C packets fin std, C duration std, C src 2 dst header bytes max, packets syn, C dst 2 src header bytes avg, C src 2 dst pay bytes rate min, packets psh, src 2 dst pay bytes rate, C tcp retransmissions std, C idle time avg, C src 2 dst packets rate min, C src 2 dst packets max, C duration max, packet direction 6, C packets fin max, C packets urg std, C src 2 dst packets rate std, dst 2 src header bytes, pay load bytes std, C dst 2 src pay bytes rate avg, src 2 dst inter time min, flow duration, C src 2 dst pay bytes std, C src 2 dst packets min, C packets urg min, inter time 5, dst 2 src header bytes max, packet direction 10, dst 2 src inter time max, packet pay size 0, packets, inter time max, inter time std, C src 2 dst packets std, packets urg, packet direction 8, dst 2 src pay bytes rate, src 2 dst inter time avg, dns rsp type, flow idle time, packet header size 3, inter time 0, C dst 2 src pay bytes min, dst 2 src pay bytes std, C src 2 dst header bytes avg, C dst 2 src packets avg, bytes, packets without pay load, C tcp retransmissions avg, inter time 1, C src 2 dst pay bytes rate max, inter time 4, C dst 2 src pay bytes max, packet pay size 6, dst 2 src pay bytes, pay load bytes min, tcp retransmissions, C packets fin min, C dst 2 src packets rate avg, dst 2 src inter time avg, packet header size 5, packet pay size 1, packet header size 10, C dst 2 src pay bytes rate std, src 2 dst pay bytes std, C idle time min, C src 2 dst header bytes std, src 2 dst pay bytes avg, packet pay size 9, packet direction 2, C src 2 dst header bytes min, C dst 2 src packets min, C packets urg max, and C dst 2 src pay bytes rat e min.

APPENDIX C BIODATA OF THE AUTHOR

Amirhossein Rezaei has born in Tehran, IRAN in 1984, has obtained a B.Sc in Industrial management from Azad Islamic Universiti of Tehran Iran in 2008. He got his Master Degree in Computer Science (MIT) from The University of Nottingham in 2013.

LIST OF PUBLICATIONS

Journal with Impact Factor:

1. Amirhossein Rezaei. (2021). Using Ensemble Learning Technique for Detecting Botnet on IoT. *Springer, SN Computer Science*. https://link.springer.com/article/10.1007/s42979-021-00585-w.
2. Amirhossein Rezaei. (2020). Detecting Botnet on IoT by Using Unsupervised Learning Techniques. *International Journal of Computer Science and Information Security.* https://www.academia.edu/download/63299752/11_Paper_01042031_IJCSIS_Camera_Ready_pp89-10020200513-21294-1d2nl1r.pdf.
3. Amirhossein Rezaei. (2019). Identifying Botnet on IoT by Using Supervised Learning Techniques. Oriental Journal of Computer Science and Technology, Vol. 12, No 4. https://pdfs.semanticscholar.org/739a/f0fe8ea7576927cb73e7571f8b7a838fc66a.pdf.
4. Amirhossein Rezaei. (2019). Botnet on Internet of Things challenges. Open International Journal of Informatics (OIJI). https://razak.utm.my/researchweek/paris2019/.
5. Amirhossein Rezaei. (2018). Identifying Botnet on IoT and Cloud by Using Machine Learning Techniques. Open International Journal of Informatics (OIJI). http://www.i-scholar.in/index.php/Oriental/article/view/196172.