UNIVERSITI TEKNIKAL MALAYSIA MELAKA

CONSTRUCTING IoT BOTNET DETECTION MODEL BASED ON DEGREE CENTRALITY AND PATH ANALYSIS

WAN NUR FATIHAH BINTI WAN MOHD ZAKI

MASTER OF SCIENCE IN INFORMATION AND COMMUNICATION TECHNOLOGY

2023

UTeM

اونيۏرسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Faculty of Information and Communication Technology

CONSTRUCTING IoT BOTNET DETECTION MODEL BASED ON DEGREE CENTRALITY AND PATH ANALYSIS

Wan Nur Fatihah binti Wan Mohd Zaki

Master of Science in Information and Communication Technology

2023

CONSTRUCTING IoT BOTNET DETECTION MODEL BASED ON DEGREE CENTRALITY AND PATH ANALYSIS

WAN NUR FATIHAH BINTI WAN MOHD ZAKI

A thesis submitted
in fulfillment of the requirements for the degree of Master of Science
in Information and Communication Technology

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I declare that this thesis entitled “Constructing IoT Botnet Detection Model Based on Degree Centrality and Path Analysis” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ....

Name : WAN NUR FATIHAH BINTI WAN MOHD ZAKI

Date : 7/5/2023

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of Master of Science in Information and Communication Technology.

Signature :…………………………………………….

Supervisor Name : TS. DR. RAIHANA SYAHIRAH BINTI ABDULLAH

Date : 8/5/2023

DEDICATION

I've dedicated my thesis to my family, supervisor, and many friends. Three people, in particular, deserve special thanks: my beloved spouse Syafiq Muzhafar bin Abdullah, and both of my parents, Wan Mohd Zaki bin Wan Md Ali and Maziah binti Ishak. Their words of encouragement and resolve are still ringing in my ears. In addition, the support I've received from my supervisor Ts. Dr. Raihana Syahirah binti Abdullah has been invaluable throughout the process, particularly in helping me enhance my research master's dissertation. Lastly, my pals have been the most generous and supportive people I have ever met.

ABSTRACT

Internet of things (IoT) Botnet is a network of connected devices, generally smart devices with software and intelligent sensors, networked over the internet to send and receive data from other intelligent devices infected with IoT Botnet malware. The development of IoT Botnet in IoT devices has a significant impact on network security. IoT Botnet attack activities have become a major problem to mitigate since IoT Botnet is the most recent and high-profile security issue. IoT Botnet activities is challenging task in order to identify since IoT Botnet are targeting IoT devices. In addition, the current IoT Botnet detection is still not have ability to reveal patterns of IoT Botnet attacks and ignore the important recognization of IoT Botnet behaviors has resulted loss of meet the detection criteria. Thus, the focus of this research is to identify IoT Botnet behaviour, to propose an IoT Botnet attack pattern based on its behaviour, to construct an IoT Botnet detection model and to validate the selection of the IoT Botnet detection model utilising detection of the IoT Botnet attack detection criteria. In order to deal with this problem, the research methodology is essential to ensure the research is appropriately implemented by providing a systematic organization with the appropriate guideline. This research have five phases of research methodology which are study and requirement analysis, data collection, analysis and design, developing the new model and validation and testing. Furthermore, this research is constructing the IoT Botnet attack pattern based on combining the IoT Botnet life cycle and IoT Botnet behaviour through the IoT Botnet activities. Then, this research has develop IoT Botnet detection model based on graph analytics approach respectively to detect IoT Botnet attack activities. The earlier detection of IoT Botnet has been visualized by IoT Botnet attack patterns using the degree centrality and path analysis. In validation process, the result showed that the proposed IoT Botnets model has accomplished all the selection detection criterias. Therefore, it is necessary for this research to constructing IoT Botnet detection model based on degree centrality and path analysis.

MEMBINA MODEL PENGESANAN IoT BOTNET BERDASARKAN KEPUSATAN DARJAH DAN ANALISIS LALUAN

ABSTRAK

Internet benda (IoT) Botnet ialah rangkaian peranti yang disambungkan pada umumnya merupakan peranti pintar dengan perisian dan penderia pintar yang dihubungkan melalui internet bagi menghantar dan menerima data daripada peranti pintar lain yang dijangkiti perisian hasad IoT Botnet. Pembangunan IoT Botnet dalam peranti IoT mempunyai kesan yang besar terhadap keselamatan rangkaian. Aktiviti serangan IoT Botnet telah menjadi masalah utama yang perlu dikurangkan disebabkan IoT Botnet merupakan isu keselamatan yang paling terkini dan berprofil tinggi. Aktiviti IoT Botnet adalah tugas yang mencabar untuk dikenal pasti kerana IoT Botnet menyasarkan hanya peranti IoT. Di samping itu, pengesanan IoT Botnet kini masih tidak mempunyai keupayaan untuk mendedahkan paten serangan IoT Botnet dan mengabaikan fungsi penting tingkah laku Botnet IoT telah mengakibatkan kriteria pengesanan tidak dapat dipenuhi. Oleh itu, fokus kajian ini adalah untuk mengenal pasti tingkah laku IoT Botnet, mencadangkan paten serangan IoT Botnet berdasarkan tingkah lakunya, membangunkan model pengesanan IoT Botnet berdasarkan darjah kepusatan dan analisis laluan, dan mengesahkan model pengesanan Botnet IoT berdasarkan darjah kepusatan dan analisis laluan. Bagi menangani masalah ini, metodologi penyelidikan adalah penting untuk memastikan penyelidikan dilaksanakan dengan sewajarnya melalui penyediaan organisasi yang sistematik dengan garis panduan yang sesuai. Penyelidikan ini mempunyai lima fasa metodologi kajian iaitu kajian dan analisis keperluan, pengumpulan data, analisis dan reka bentuk, pembangunan model baharu serta pengesahan dan pengujian. Tambahan pula, penyelidikan ini juga membina paten serangan IoT Botnet berdasarkan kitaran IoT Botnet serta tingkah laku IoT Botnet melalui aktiviti IoT Botnet. Kemudian, penyelidikan ini telah membangunkan model pengesanan botnet IoT berdasarkan pendekatan analisis graf bagi mengesan aktiviti serangan IoT Botnet. Pengesanan awal IoT botnet telah divisualisasikan oleh paten serangan IoT Botnet menggunakan darjah kepusatan dan analisis laluan. Dalam proses pengesahan, keputusan yang ditunjukkan oleh model pengesanan IoT Botnet adalah memenuhi semua kriteria pengesanan yang ditentukan. Oleh itu, adalah perlu bagi penyelidikan ini untuk membina model pengesanan IoT Botnet berdasarkan kepusatan darjah dan analisis laluan.

ACKNOWLEDGEMENTS

In the Name of Allah, the Most Gracious, the Most Merciful.

Please allow me to thank and worship Allah the Almighty first for all I have from the beginning of time. He is my Creator and my Sustainer. Next, I'd like to express my gratitude to Universiti Teknikal Malaysia Melaka (UTeM) for providing the study environment.

My deepest gratitude goes to my main supervisor is, Ts. Dr. Raihana Syahirah Binti Abdullah, for all of her assistance, guidance, and inspiration. In addition, I will never forget her endless patience in mentoring and imparting valuable knowledge to me. Also, thanks to my co-supervisor, Dr. S.M. Warusia Mohamed S.M.M. Yassin has always guided me along the way.

The last thing I want to say is how grateful I am to my spouse, Syafiq Muzhafar bin Abdullah, for his support and encouragement throughout my life. In addition, I would like to express my sincere gratitude to my parents, Wan Mohd Zaki bin Wan Md Ali and Maziah binti Ishak, for their generous sponsorship, encouragement, unwavering support, love, and prayers. Finally, I'd like to extend my gratitude to everyone who has offered help, support, or inspiration as I began my research.

TABLE OF CONTENTS

PAGE

DECLARATION
APPROVAL
DEDICATION
ABSTRACT i
ABSTRAK ii
ACKNOWLEDGEMENTS iii
TABLE OF CONTENTS iv
LIST OF TABLES vii
LIST OF FIGURES viii
LIST OF APPENDICES x
LIST OF ABBREVIATIONS xi
LIST OF PUBLICATIONS xii

CHAPTER
1. INTRODUCTION 1
1.1 Background 1
1.2 Problem Statement 5
1.3 Research Objectives 7
1.4 Research Questions 7
1.5 Scope of Research 7
1.6 Contribution of Research 8
1.7 Thesis Outline 8

2. LITERATURE REVIEW 11
2.1 Introduction 11
2.2 Chapter Objective 11
2.3 Chapter Outline 11
2.4 Internet of Things (IoT) 13
2.4.1 IoT Component 14
2.4.2 IoT Architecture 16
2.4.3 Methods of IoT Attack 18
2.4.4 Type of IoT Malware 19
2.4.5 Analysis of IoT 22
2.5 IoT Botnet 23
2.5.1 Type of IoT Botnet malware 24
2.5.2 Attacking Behaviour 25
2.5.3 C&C Models 26
2.5.4 Rally Mechanism 28
2.5.5 Communication Protocol 28
2.5.6 Observable Activities 29
2.5.7 IoT Botnet Life Cycle 30
2.5.8 Analysis of IoT Botnet 32
2.6 Overview on IoT Botnet Detection Model 33
2.6.1 Analysis on IoT Botnet Detection Model Component 40
2.7 Graph Analytic 43
2.7.1 Component of Graph Representation 44

2.7.2 Type of Graph Analytics 44
2.7.3 Graph Representation 46
2.7.4 Proof Techniques 48
2.7.5 Analysis of Graph Analytics 50
2.8 Review on Current Technique used in IoT Botnet Detection 51
2.9 Review on Proposed IoT Botnet Detection Models 57
2.10 Summary 58

3. RESEARCH METHODOLOGY 60
3.1 Introduction 60
3.2 Chapter Objective 60
3.3 Chapter Outline 60
3.4 Research Methodology 61
3.4.1 Phase 1: Study and Requirement Analysis Phase 63
3.4.2 Phase 2: Data Collection Phase 63
3.4.3 Phase 3: Analysis and Design Phase 64
3.4.4 Phase 4: Model Development Phase 65
3.4.5 Phase 5: Validation and Testing Phase 66
3.5 IoT Botnet Environment Setup 66
3.6 Summary 69

4. ANALYSIS AND DESIGN 70
4.1 Introduction 70
4.2 Chapter Objective 70
4.3 Chapter Outline 71
4.4 Overview of Analysis Approach 71
4.4.1 Dataset Collection 72
4.4.2 IoT Botnet Analysis Environment 73
4.4.3 IoT Botnet Behaviours Analysis 81
4.4.4 IoT Botnet Attack Pattern 90
4.5 Proposed IoT Botnet Detection Model 92
4.6 Summary 93

5. IMPLEMENTATION 94
5.1 Introduction 94
5.2 Chapter Objective 94
5.3 Chapter Outline 94
5.4 Process Flow of Implementation Process 95
5.5 IoT Botnet Detection Model 96
5.5.1 Dataset 96
5.5.2 Identification Attack Pattern 97
5.5.3 Degree Centrality Analysis 98
5.5.4 Path Analysis 109
5.5.5 IoT Botnet Detected 110
5.6 Summary 110

6. TESTING AND VALIDATION 111
6.1 Introduction 111
6.2 Chapter Objectives 111

6.3 Chapter Outline 111

6.4 Testing Dataset 112

6.4.1 Testing of CTU-IoT-Malware-35 for Degree Analysis 113

6.4.2 Testing of CTU-IoT-Malware-48 for Degree Analysis 116

6.4.3 Testing of CTU-IoT-Malware-44 for Degree Analysis 118

6.4.4 Path Analysis Testing for CTU-IoT-Malware-35, CTU-IoT-Malware-48 and CTU-IoT-Malware-44 121

6.4.5 Testing of IoT Botnet Detected 122

6.5 Testing Design for Selection Detection Criteria 123

6.6 Testing Result Validation 124

6.7 Summary 128

7. CONCLUSION 129

7.1 Introduction 129

7.2 Research Summarization 129

7.3 Research Contribution 132

7.4 Research Limitation 133

7.5 Future Research 133

REFERENCES 135

APPENDICES 153

LIST OF TABLE

TABLE	TITLE	PAGE
2.1	Summary of IoT architecture	18
2.2	Method IoT attack summary	18
2.3	Summary of IoT malware types	21
2.4	Type of IoT Botnet malware	24
2.5	Type of C&C models	26
2.6	Communication protocol	29
2.7	Observable activities	30
2.8	General terminology component in IoT Botnet detection model	40
2.9	Analysis of IoT Botnet detection models	41
2.10	IoT Botnet detecion methods	53
3.1	IoT Botnet dataset	64
3.2	IoT devices in this experiment	68
3.3	List of software in this experiment	69
4.1	IoT Botnet dataset	73
4.2	A summary of IoT Botnet behaviour analysis	84
5.1	IoT Botnet implementation dataset	97
5.2	Graph degree CTU-IoT-Malware-34	100
5.3	Graph degree CTU-IoT-Malware-52	103
5.4	Graph degree CTU-IoT-Malware-43	106
5.5	Path analysis	109
6.1	IoT Botnet testing dataset	112
6.2	Graph degree CTU-IoT-Malware-35	114
6.3	Graph degree CTU-IoT-Malware-48	117
6.4	Graph degree CTU-IoT-Malware-44	119
6.5	Path analysis	122
6.6	General terminology to describe the criteria on IoT Botnet model	124
6.7	Testing validation result on IoT Botnet model criteria	125

LIST OF FIGURES

FIGURE	TITLE	PAGE
1.1	Deloitte Global analysis 1 of static technology's potential impact on industry 4.0 (Goswami et al., 2020)	2
1.2	Number of previous research on malicious activities	4
2.1	Chapter 2 outline	12
2.2	IoT component (Dorsemaine et al., 2016)	14
2.3	IoT architecture (Sikder et al., 2018)	16
2.4	Type of IoT malware	19
2.5	IoT Taxonomy	22
2.6	IoT Botnet life cycle	31
2.7	IoT Botnet taxonomy	32
2.8	Syntactic and behavioural analysis model (Said et al., 2018)	34
2.9	PSI-graph and convolutional neural network classifier (CNN) model (Nguyen, Ngo, and Le, 2018)	35
2.10	Behaviour-based deep learning framework (BDLF) model (Yuxin and Siyi, 2019)	36
2.11	BotChase bot detection system model (Daya et al., 2020)	37
2.12	Function call sequence graph (FCSG) model (Kawasoe et al., 2021)	38
2.13	IoT malware analysis model (Wu et al., 2021)	39
2.14	Component of graph representation	44
2.15	Type of graph analytics (Singh, Dutta Pramanik, and Choudhury, 2018)	44
2.16	Taxonomy of graph analytics	50
3.1	Chapter 3 outline	61
3.2	Summary of research methodology	62
3.3	Study and requirement analysis phase	63
3.4	Data collection phase	63
3.5	Analysis and design phase	64

3.6 Model development phase 65
3.7 Validation and analysis of result phase 66
3.8 IoT Botnet analysis enviroment (Sebastian Garcia, Agustin Parmisano, and Maria Jose Erquiaga, 2020) 67
4.1 Chapter 4 outline 71
4.2 Overview of analysis approach 72
4.3 Flowchart of dataset collection 72
4.4 IoT Botnet analysis environment flowchart 74
4.5 Flowchart of Virus Total and Cuckoo Sandbox analysis process 75
4.6 Virus Total report 76
4.7 File system action 77
4.8 Cuckoo Sandbox analysis report 1 78
4.9 Cuckoo Sandbox analysis report 2 78
4.10 Flowchart of Wireshark analysis process 79
4.11 Example of bot communication with C&C server 80
4.12 Flowchart of IoT Botnet behaviour analysis 81
4.13 IoT Botnet attack patterns 90
4.14 Proposed IoT Botnet detection model 92
5.1 Chapter 5 outline 95
5.2 Implementation process flow 95
5.3 IoT Botnet detection model 96
5.4 Graph CTU-IoT-Malware-34 99
5.5 Graph CTU-IoT-Malware-52 102
5.6 Graph CTU-IoT-Malware-43 106
6.1 Chapter 6 outline 112
6.2 Graph CTU-IoT-Malware-35 113
6.3 Graph CTU-IoT-Malware-48 116
6.4 Graph CTU-IoT-Malware-44 119
6.5 Flowchart of testing design 123

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Related work IoT Botnet	153

LIST OF ABBREVIATIONS

AI	-	Artificial Intelligence
C&C	-	Command & Control
CPU	-	Central Processing Unit
DDoS	-	Distributed Denial of Service
DNS	-	Domain Name System
GPS	-	Global Positioning System
HTTP	-	Hypertext Transfer Protocol
ICT	-	Information and Communication Technology
IETF	-	Internet Engineering Task Force
IoT	-	Internet of Things
IP	-	Internet Protocol
IRC	-	Internet Relay Chat
MCMC	-	Malaysian Communications and Multimedia Commission
P2P	-	Peer-to-Peer
RAM	-	Random Access Memory
WHO	-	World Health Organization

LIST OF PUBLICATIONS

1. Wan Nur Fatihah, Wan Mohd Zaki, R. S., Abdullah, W., Yassin, M., Faizal, and M. S., Rosli, 2020. Discovering IoT Botnet Detection Method : A Review. *Technology Reports of Kansai University,* 62(09), 45-58.

2. Wan Nur Fatihah, Wan Mohd Zaki, R. S., Abdullah, W., Yassin, M., Faizal, and M. S., Rosli, 2021. Constructing IoT Botnets Attack Pattern for Host Based and Network Based Platform. *International Journal of Advanced Computer Science and Applications (IJACSA),* 12(8), 1–8.

CHAPTER 1

INTRODUCTION

1.1 Background

During the worldwide breakout of the COVID-19 pandemic, reliance on technologies such as the Internet of Things (IoT), Blockchain, Artificial Intelligence (AI), Cloud Computing, and Big Data Analytics has elevated. IoT plays a significant role in mitigating the risk of coronavirus transmission by providing platforms that facilitate WHO compliance (Kamal, Aljohani and Alanazi, 2020). The IoT refers to internet-connected devices, including software and smart sensors. IoT can transmit and receive data from other devices such as smartphones, smart lamps, smart homes, smart toys, smart door locks, baby monitors and IP cameras (Wan Mohd Zaki et al., 2021). According to Wegner (2021), expenditure on IoT hardware increased by 5.4% in 2020, while expenditure on IoT infrastructure/cloud services increased by 34.7% during the same period. Consequently, the COVID-19 pandemic has significantly impacted various areas of the IoT sector. Moreover, IoT infrastructure services are expanding, indicating IoT's widespread use during the COVID-19 pandemic.

Industry 4.0 is a set of technologies that facilitate the modernisation of industry. The third annual study by Deloitte Global focused on Industry 4.0 technologies, which may be the immediate objectives of customer experience officers and have the most significant impact on various businesses (Goswami et al., 2020). Figure 1.1 depicts the potential impact of static technology on industry 4.0, particularly the Internet of Things. The Internet of Things ranks highest among AI, cloud infrastructure, and big data/analytics. It demonstrates that IoT is rapidly expanding. In addition, IoT provides essential tools for automating data collection and generating insights through sensors, networks, and analytics. IoT is the essential digital stack component for the industrial sector.

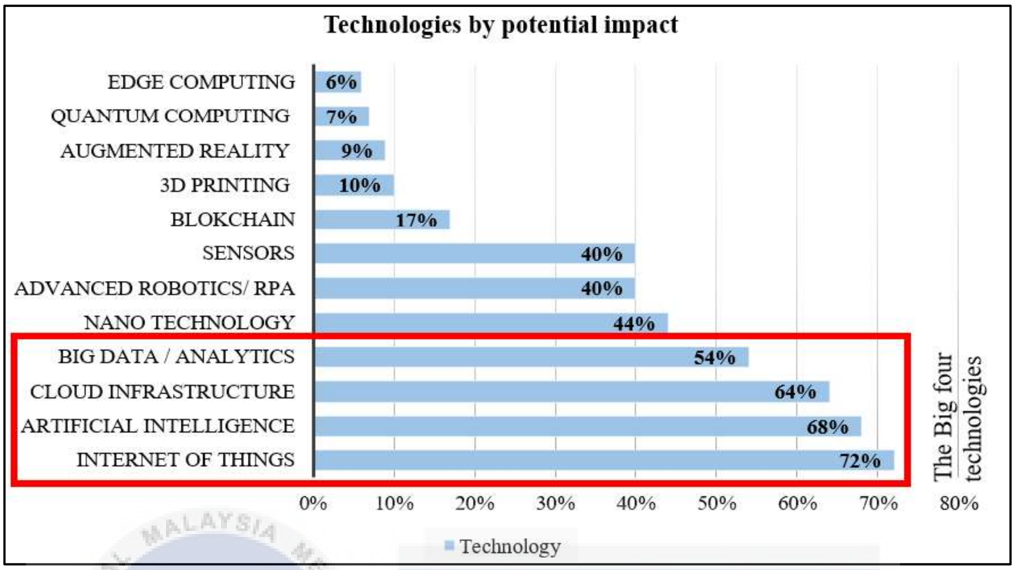

Figure 1.1: Deloitte Global analysis 1 of static technology's potential impact on industry 4.0 (Goswami et al., 2020)

The growing interest in the Internet of Things indicates that IoT development will increase throughout the year (Gartner, 2018). Typically, IoT devices are interconnection devices that can interact online (Gubbi et al., 2013; Virtual tech gurus, 2016). Most academics, such as El Beqqal and Aziz (2018), Gokhale, Bhat, and Bhat (2018), and Nawir et al. (2017), have taken the development and improvement of IoT intelligence devices seriously in response to IoT device security concerns. Thus, these interconnected devices are vulnerable to a novel attack that may exploit security flaws. For instance, IoT-based attacks are more challenging to eliminate as the number of attacks on various devices increases rapidly (Granville and Margi, 2019).

On the other hand, IoT devices are still in their infancy, with the majority of IoT devices being unsafe, and this situation has remained uncertain over the past few years (Victoria and Rønning, 2017). Thus, attackers gradually exploited these vulnerabilities to compromise vulnerable devices (Koroniotis et al., 2019). In addition, increasing the number of inappropriate IoT devices would attract the attention of cybercriminals and generate massive cyberattacks (Abouzakhar, Jones and Angelopoulou, 2017). According to Vignau, Khoury and Hallé (2019), as a result, Botnets have become the most prevalent cyber attack that infects many IoT devices.

The botnet is an abbreviation for the robot and network described by Plohmann, Gerhards-Padilla, and Leder (2011). As claimed by R. S. Abdullah et al. (2011), Alomari et al. (2012), and R. S. Abdullah et al. (2011), the Botnet has the ability to infiltrate any system of devices. It will transform from a group of hostile computers into a computer, an automater, a drone, and a zombie (2013). In contrast, the minimum number of Botnet infections is approximately 3.5 million, which could cause significant harm to the future of the Internet of Things applications (MyCERT, 2018). Therefore, researchers have numerous opportunities to investigate IoT Botnet infection in terms of available solutions for detection methods, detection sources, communication protocol, and IoT Botnet type. This available solution will make it easier for the community to acquire current information.

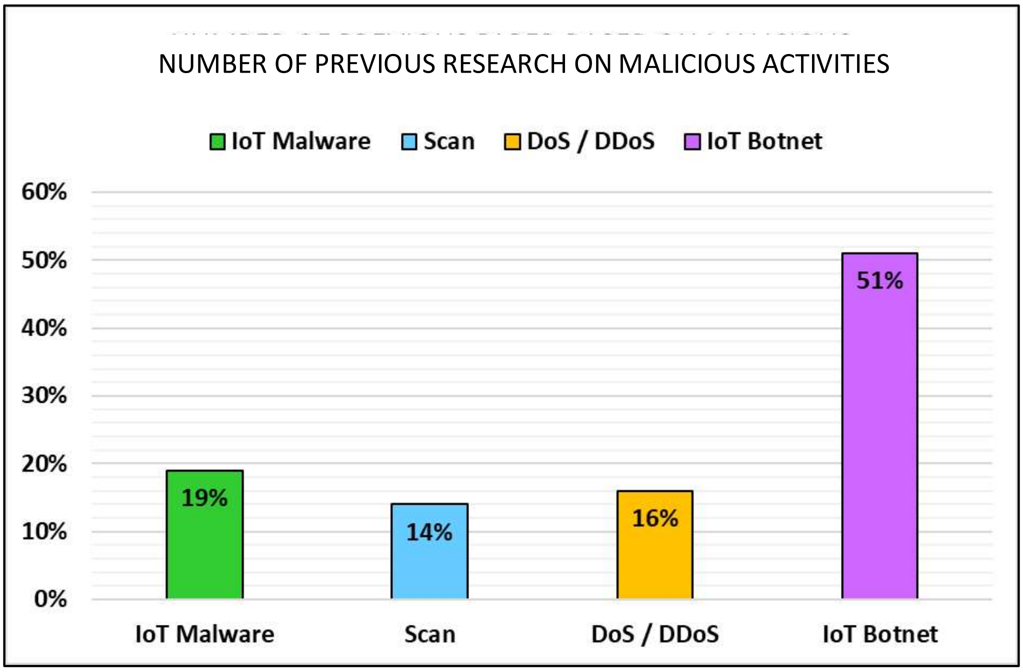

Figure 1.2: Number of previous research on malicious activities

Figure 1.2 depicts the research on malicious activities (Wazzan et al., 2021). IoT Botnet is the research of the most significant number of previous studies on IoT Malware, Scan, and DoS/DDoS. Figure 1.2 indicates that the IoT Botnet is 32% distinct from IoT Malware. This research focused on IoT Botnet because the increasing number of IoT devices has made it challenging to identify and assess the spread of malware in IoT activity. In addition, the existing IoT Botnet detection technique was flow-based, allowing malware to be automatically detected using machine learning and deep learning techniques (H. T. Nguyen et al., 2019).

IoT has enormous potential for expansion despite numerous identified problems (Gopal et al., 2018; Zhang et al., 2014). Therefore, IoT is not entirely secure, as most previous research required the development of the proper detection techniques for the new IoT Botnet attack behaviours (Wazzan et al., 2021). In addition, numerous IoT Botnet detection techniques utilise flow packet traffic, deep packet inspection, and statistical characteristics. In addition, Chowdhury et al. (2017) mentioned that the detection techniques capture the features of IoT Botnet attacks that are unique to specific links. In addition, rapid technological advancements result in an insufficient comprehension of IoT Botnet. In terms of understanding IoT Botnets, identifying new IoT Botnet behaviours and characteristics, and choosing the appropriate IoT Botnet detection techniques, the previous research has limitations in mitigating the current IoT Botnet detection. Constructing IoT Botnet Detection Model Based on Degree Centrality and Path Analysis was the primary goal of this research.

1.2 Problem Statement

Due to the growing interest in the IoT, its development is anticipated to accelerate throughout the year (Gartner, 2018). According to IoT-connected device statistics, the number of IoT-connected devices will continue to increase through 2025, presenting enormous growth potential, despite the recognition of numerous obstacles Statista (2019). In contrast, rapid technological development has resulted in insufficient IoT knowledge. IoT devices may exploit many design flaws or vulnerabilities to commit identity theft, steal data, compromise networks, or even cause physical damage. Thus, the exponential increase of IoT device utilisation provides hackers with more opportunities to exploit them.

Moreover, according to Kaspersky Lab (2018), malware attacks on Internet of Things (IoT) devices increased substantially in 2018 compared to the previous year. IoT devices have become the new Botnet platform, and Botnet hackers exploit IoT devices (Edwards and Profetis, 2016; H. T. Nguyen et al., 2019). Therefore, IoT devices are still insecure and may be responsible for several threats and viruses in recent years, particularly IoT Botnets.

Previous research by Patel and Upadhyay (2018) focused more on recognising than revealing the motivations behind an attacker's activity pattern. Understanding typical usage patterns facilitate the detection and prevention of IoT Botnet attacks. As IoT Botnets are not entirely secure, additional research is required to develop efficient detection algorithms that account for the new characteristics of IoT Botnet attacks (Hamza et al., 2020). In addition, most investigators utilised platform functionality without addressing IoT Botnet detection attacks. As a result, hackers create increasingly sophisticated IoT Botnets and improperly conduct massive attacks on IoT devices. As IoT Botnet represents an emerging threat and high-profile security breaches, IoT Botnet activity attacks remain complex.

According to H. T. Nguyen et al. (2019), modern IoT Botnet detection technology uses flow-based machine learning and deep learning for automatic detection. With the vast number of IoT devices producing voluminous amounts of data, it may be challenging to manage manually. Most IoT Botnet detection strategies rely on statistical flow/packet traffic characteristics or deep packet inspection. However, current graph-based IoT Botnet disclosure strategies have significant flaws (Chowdhury et al., 2017; Rangaswamy and Gurusamy, 2018). In addition to the overall field/subgraph topological structure, this method captures the properties of each connection's IoT Botnet effect (Chowdhury et al., 2017).

In addition, the graph theory associated with attack graphics can aid in identifying and preventing attacks before they have a negative impact on the business (Karin R. Saoub, 2021). Therefore, any technique based on graph theory can demonstrate attack activity in IoT Botnet detection. The IoT Botnet Detection using a graph model is designed to close the gap in this study. To identify the IoT Botnet attack pattern, the behaviours of IoT Botnet attacks were analysed. The IoT Botnet attack pattern is then utilised as a starting point for developing the IoT Botnet Model using a graph analytic approach. Consequently, this study expands upon the concise statement of the research issue:

"The development of IoT Botnets in IoT devices substantially impacts network security. Identifying and evaluating IoT Botnet activity that targets IoT devices is challenging. Since IoT Botnet is the most recent and high-profile security issue, defending against IoT Botnet attack activities has become a major challenge. Moreover, the current IoT