



Bahria University
Discovering Knowledge

FINAL YEAR PROJECT REPORT
RPIDS: RASPBERRY PI BASED
INTRUSION DETECTION SYSTEM FOR
INTERNET OF THINGS

By

ASMA BAIG	(43756)
HAMZA SIKANDAR	(43721)
MUHAMMAD ARSLAN	(43730)

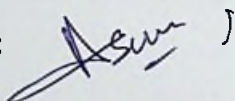
SUPERVISED BY
(MR. BILAL MUHAMMAD IQBAL)

BAHRIA UNIVERSITY (KARACHI CAMPUS)

DECLARATION

We hereby declare that this project report is based on our original work except for citations and quotations which have been duly acknowledged. We also declare that it has not been previously and concurrently submitted for any other degree or award at Bahria University or other institutions.

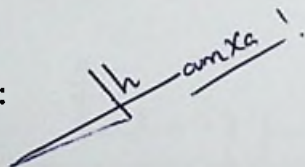
Signature:



Name : Asma Baig

Reg No.: 43756

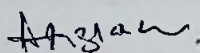
Signature:



Name : Hamza Sikandar

Reg No.: 43721

Signature:



Name : Muhammad Arslan

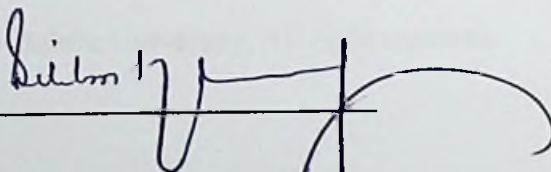
Reg No.: 43730

Date : 16th December, 2019.

APPROVAL FOR SUBMISSION

We certify that this project report entitled "RPIDS: RASPBERRY PI BASED INTRUSION DETECTION SYSTEM FOR INTERNET OF THINGS" was prepared by ASMA BAIG, HAMZA SIKANDAR & MUHAMMAD ARSLAN has met the required standard for submission in partial fulfilment of the requirements for the award of Bachelor of Computer Science (Honours) at Bahria University.

Approved by,

Signature: 

Supervisor: Mr. Bilal Muhammad Iqbal

Date : 16-12-2019

ACKNOWLEDGEMENTS

We would like to thank everyone who had contributed to the successful completion of this project. We would like to express our gratitude to our research supervisor, Mr. Bilal Muhammad Iqbal for his invaluable advice, guidance and his enormous patience throughout the development of the research.

In addition, we would also like to express our gratitude to our loving parent and friends who had helped and given me encouragement.

RPIDS: RASPBERRY PI BASED INTRUSION DETECTION SYSTEM FOR INTERNET OF THINGS

ABSTRACT

Internet of things has recently give a vast scope for making a smart and innovative environment. The major target of this project is to enhance the life of human and make it secure from vulnerabilities in the environment and make secure and give comfort to the industries, organization even the life of individual person. Thus there is a decisive need or desirable for intrusion detection system (IDS) make functioning for IoT devices to protect or mitigate IoT concerned security threads from damages the equipment's. This report explores different detections and prevention of the attacks like TCP traffic, DOS attack, DDOS, Port scanning, Back doors, CGI exploits etc. There are several tools are available to detect and automate the intrusion detection in IoT devices like snort, suricata, psense etc. we are using snort for defining rule against these attacks.

Snort has become the single most widely deployed and trusted intrusion prevention and detection technology in the world. Snort IDS is the open source security community worldwide can detect and respond to bugs, worms, malware attacks, and other security threats faster and more efficiently than other IDS engines. Furthermore, there are a wide variety of reference guides available for installing, configuring, deploying, and managing Snort IDS sensors and rule-based signatures on a network. This report presents a comprehensive survey of the IDSs designed for the IoT model, with a focus on the corresponding methods, features, and mechanisms. This report also provides deep insight into the IoT architecture, emerging security vulnerabilities, and their relation to the layers of the IoT architecture.

TABLE OF CONTENTS

DECLARATION	ii
APPROVAL FOR SUBMISSION	iii
ACKNOWLEDGEMENTS	v
ABSTRACT	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	x
LIST OF FIGURES	xi
LIST OF SYMBOLS / ABBREVIATIONS	xii
LIST OF APPENDICES	xiii

CHAPTER

1	INTRODUCTION	1
	1.1 Background	1
	1.2 Problem Statements	2
	1.3 Aims and Objectives	2
	1.4 Scope of Project	3
2	LITERATURE REVIEW	4
	2.1 Intrusion Detection System	4
	2.1.1 Type of IDS	5
	2.1.2 Types of Attacks in IDS	6
	2.2 IDS Detection Techniques	8
	2.2.1 Anomalt Based IDS	8
	2.2.2 Signature Based IDS	8

2.3	Snort	8
2.3.1	Snort Working	9
2.3.2	Snort Architecture	9
2.3.3	Snort Modules	10
2.3.4	Snort Components	11
2.3.5	Snort Operation System	13
2.3.6	Snort Ports	14
2.3.7	Snort Protocols	14
2.3.8	Snort Direction Operators	15
2.4	Internet of Things	15
2.4.1	IoT and Smart Environment	16
2.4.2	Security Challenges in IoT	17
2.4.3	IoT Weakness	17
3	DESIGN AND METHODOLOGY	18
3.1	Project Development Approach	18
3.2	Experimental Set-Up	19
3.3	Types of IDS	19
3.4	Techniques of IDS	20
3.5	Quality Factor	20
3.6	Risk Factor	22
3.7	Mitigation of Risk Strategies	22
3.8	Tools for IDS	23
3.8.1	Raspberry pi model b	23
3.8.2	ESP - 8266	24
4	IMPLEMENTATION	25
4.1	Workflow	25
4.2	Install Rasbian on Raspberry pi	26
4.3	Raspberry pi as Router	26
4.3.1	Steps for Making Raspberry Pi as a Router	26
4.4	Installation of Snort	28
4.5	Configuration of Snort	31

4.6	Making IoT Device Using ESP - 8266	31
4.7	Making IoT Device Using Raspberry Pi	32
4.8	Make Network	32
4.9	Define Rules for IDS & IPS	33
4.9.1	Local Rules	33
4.9.2	DOS Rules	34
4.9.3	DDOS Rules	37
4.9.4	Brute Force Rules	39
4.9.5	Deauth Rules	40
4.9.6	DNS Spoofing Rules	41
5	RESULTS AND DISCUSSIONS	43
5.1	Result of Brute Force	43
5.2	Result of DOS	44
5.3	Overall Processing	44
5.4	Attack Distribution of Snort	45
5.5	Discussion of Project	45
6	CONCLUSION AND RECOMMENDATIONS	49
6.1	Conclusion	49
6.2	Recommendation	50
	REFERENCES	51
	APPENDICES	53