NDDOS – TCP SYN FLOODING DETECTION USING SVM

AZWAR HAFUZA BIN MOHD NASIR

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: [NDDoS – TCP SYN Flooding detection using SVM]

SESI PENGAJIAN: [2020 / 2021]

Saya: AZWAR HAFUZA BIN MOHD NASIR

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

_____	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
_____	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)
_____	TIDAK TERHAD	

AZWAR

(TANDATANGAN PELAJAR)

Alamat tetap: 63-D, Flat Taman Kosas,

68000, Ampang Selangor

Tarikh: 10/9/2021

(TANDATANGAN PENYELIA)

TS. NOR AZMAN BIN MAT ARIFF

Nama Penyelia

Tarikh: 10/9/2021

CATATAN: * Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

NDDoS – TCP SYN Flooding detection using SVM

AZWAR HAFUZA BIN MOHD NASIR

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Networking) with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2021

DECLARATION

I hereby declare that this project report entitled

[NDDoS – TCP SYN Flooding detection using SVM]

is written by me and is my own effort and that no part has been plagiarized

without citations.

STUDENT : AZWAR HAFUZA BIN MOHD NASIR Date : 10/9/2021

I hereby declare that I have read this project report and found

this project report is sufficient in term of the scope and quality for the award of

Bachelor of Computer Science (Computer Networking) with Honours.

SUPERVISOR : _____ Date : 10/9/2021

(TS. NOR AZMAN BIN MAT ARIFF)

DEDICATION

Alhamdulillah. All praise to Allah in providing me a good surrounding upon completing this project. This dedication is for my family, my supportive members and for my supervisors Ts. Nor Azman Bin Mat Ariff for all the inspiration, motivation, support and always give the best to me while completing this project.

ACKNOWLEDGEMENTS

At first, thank you Allah for all of the blessing and moral guidance while completing this project, and also for providing me a good and supportive surrounding. Because, if I'm doing alone, I will never succeed to complete this project.

Next, greatest thank you for my supervisor. Ts. Nor Azman Bin Mat Ariff. Because always give me moral support and not tired while answering my question. If not have the right guidance and knowledge, I sure that I will never complete this project.

Lastly, thank you for my family, members, classmates and for all who help me direct indirectly upon completing this project.

ABSTRACT

Leading to Industrial Revolution (IR) 4.0, most of the services are depending on the technology. This changes also will lead to a war named cyber war. The most popular weapon that was used during cyber-attack is Denial of Service (DoS) or Distributed Denial of Service (DDoS). In order to control this problem, a good detection system must be implements in the network architecture. The purpose of doing this project is to propose a DoS TCP SYN flooding detection using machine learning algorithm specifically Support Vector Machine (SVM). In this study, a dataset that was used is gain from Canadian Institute for Cybersecurity named NSL-KDD dataset. In conclusion, hope this project will achieve its goals and can be used for all people as precaution step for securing its network.

ABSTRAK

Menuju Revolusi Perindustrian 4.0, kebanyakan servis bergantung kepada teknologi. Perubahan ini boleh membawa kepada perang disebut sebagai perang siber. Senjata yang paling terkenal yang digunakan semasa perang siber ialah serangan DoS dan juga DDoS. Untuk mengekang masalah ini, system pendeteksi yang berkesan mestilah diwujudkan dan digunakan didalam seni bina rangkaian. Tujuan menjalankan projek ini adalah untuk mencadangkan 'DoS TCP SYN flooding detection' sebagai alat pendeteksi serangan DoS yang menggunakan algoritma pembelajaran mesin lebih spesifik ialah Mesin Sokongan Vektor. Semasa penyelidikan ini, set data yang digunakan ialah daripada Institusi KeselamatanSiber Kanada bernama NSL-KDD. Sebagai konklusi, semoga projek ini akan mencapai matlamatnya dan boleh dimanfaatkan oleh semua orang sebagai langkah awal untuk menyelamatkan rangkaian mereka.

TABLE OF CONTENTS

PAGE

LIST OF TABLES

PAGE

LIST OF FIGURES

PAGE

LIST OF ABBREVIATIONS

FYP	-	**Final Year Project**
DDoS	-	Distributed Denial of Service
DoS	-	Denial of Service
HTTP	-	Hypertext Transfer Protocol
UDP	-	User Datagram Protocol
ICMP	-	Internet Control Message Protocol
TCP	-	Transmission Control Protocol
SYN	-	Synchronize
IDS	-	Intrusion Detection System
SVM	-	Support Vector Machine
HIDS	-	Host-Based Intrusion Detection System
NIDS	-	Network Intrusion Detection System
PPS	-	Packets Per Seconds
RPS	-	Request Per Seconds
SYN-ACK	-	Synchronize-Acknowledge
CPU	-	Central Processing Unit
CMD	-	Command Prompt
OS	-	Operating System
RBF	-	Radial Basis Function
CIC	-	Canadian Institute for Cybersecurity

LIST OF ATTACHMENTS

CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

Distributed Denial of Service (DDoS) are the extended for Denial of Service (DoS). As knowledge, DoS is the type of attack that require and launched by the single attacker machine. While DDoS are the combination of multiple machine that are set to be an attacker machine that will be used to perform network hack like DDoS. DDoS attack will be the high impact attack for the network because the attack is launch by many devices or machine in one single time.

The problem for DDoS attack is, sometimes owner for the attacker machine does not know that they involved in the attack because the script for DDoS attack is inserted on the malicious software or program that downloaded on the internet. There are few methods to launch the Dos or DDoS attack and the common is by launching the flood attack. Flooding attack can be categorized into several version depending on what protocol packet that attacker used for example HTTP flood, UDP flood, ICMP flood or commonly known as Ping flood or the other name is Ping of Death. The type of flood that will be discuss on this project is TCP flood. TCP flood on DDoS or DoS attack is using handshake in 3-way TCP handshake process[1].

The attack is starting on the first handshake step which is synchronize (SYN) the common name for this type of attack is called TCP SYN flood attack. In general, flow of this attack is the attacker send many requests to the server by using TCP protocol. Server will busy to respond the huge amount of request launched by attacker and it will be denied other real request due to focusing on the SYN attack request. Effect from this attack will be the serious problem because victim might having lost due to their business cannot be operated while the attacked were launched.

1.2 PROBLEM STATEMENT (PS)

Hacking nowadays become a trend as method to bringing down someone else. According to (Basyir, 2021) on his article in New Straits Time Malaysia, Malaysia have faced a huge amount of loss since 2017 due to cybercrime frauds and attack. The amount stated is RM 2.23B. The rate statistic of attack is indicated on pie chart below.

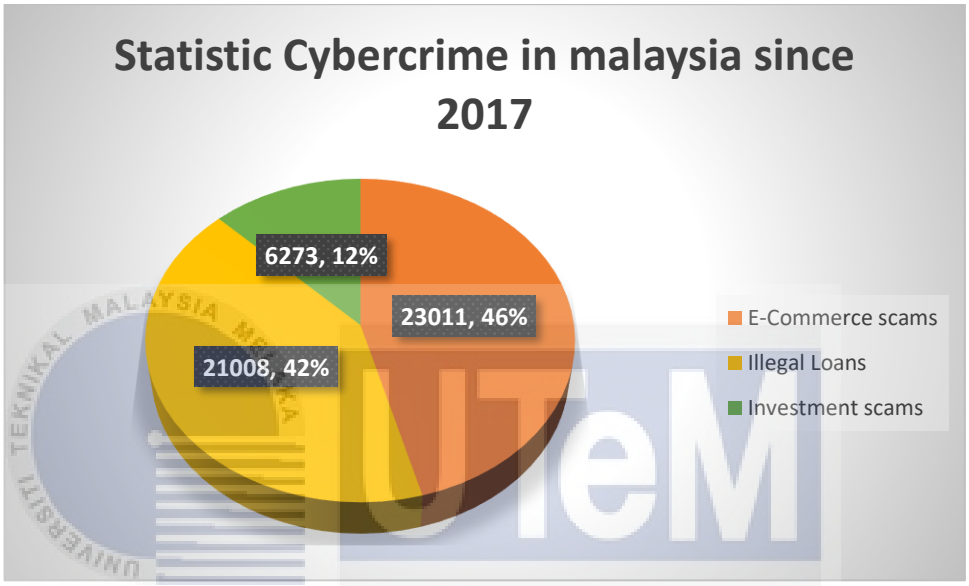

Figure 1 – Statistics cybercrime in Malaysia

This means, cyber-attack is the serious case that need a specialist expertise to solve this problem. According to figure 1. The rate shows the statistic for the scams or cybercrime fraud. But, if we deep inside the cases. In order to launch that attack, attacker also will be involved in cybersecurity threat attack such as data breach, and others network type of attack. This means, they also will have to launch the attack to the networks that relate with the Intrusion Detection System IDS. The IDS is the general terms of network attack.

As mentioned, IDS is only the term. Inside of IDS topic, there are generous of attack that widely use example phishing, deface, denial of service or Distributed denial of Service and others. If someone or some organization get stuck in this attack, they might cause a huge lost especially for a business owner or profit organization.

In general, if the e-commerce website on attack, customer might not reach the website or have been generate to another website that are set by attacker just to dropping the opponent business [(1)]. Besides, the network or traffic of the attacked network might congest and having overflow because there are several attack techniques that generate or transmit huge fake traffic towards attacked network just to prevent the opponent from succeed[(2)]. Regarding to the situation, it is recommended for a server or system have an effective technique to detect and prevent the flow of traffic in the network. Based on the problem, NDDoS – TCP SYN FLOOD DETECTION USING SVM is the best solution to prevent this problem. The problem statement (PS) for this plan is shown in Table 1.1.

PS	PROBLEM STATEMENT
PS1	Business drop cause from bad hacker launching DDOS attack to the network
PS2	Network getting slower due to congested traffic by flooding attack

Table 1 – Problem statement

1.3 PROJECT QUESTION (PQ)

There are four project questions came based on problem statement before this study. The mentioned question is summarized into table 1.2 below:

PS	PQ	PROBLEM STATEMENT
PS1	PQ1	How to classify the traffic towards network?
	PQ2	How to prevent attacker sending huge transmission on the network?
PS2	PQ1	How to detect normal transmission and fake transmission?
	PQ2	Is the machine learning algorithm can be used to measure the accuracy in detecting the spam or attack traffic towards network?

Table 2 – Project Question

1.4 PROJECT OBJECTIVE (PO)

Project objectives (PO) is the goals for this research. Table 1.3 below are the objectives on this project:

PS	PQ	PO	PROJECT QUESTION
PS1	PQ1	PO1	To study taxonomy of DoS and DDoS attack focuses on TCP SYN Flood.
	PQ2	PO2	To develop a classification system that can detect the attack towards network
PS2	PQ1		
	PQ2	PO3	To test and verify the accuracy of proposed detection method

Table 3 – Project Objective