

KLASIFIKASI SERANGAN BOTNET MENGGUNAKAN METODE

BI-DIRECTIONAL LONG SHORT-TERM MEMORY

TUGAS AKHIR

**Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer**



OLEH :

**M. Taufik
09011281823073**

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2022**

HALAMAN PENGESAHAN

TUGAS AKHIR KLASIFIKASI SERANGAN BOTNET MENGGUNAKAN METODE *BI-DIRECTIONAL LONG SHORT-TERM MEMORY*

Program Studi Sistem Komputer
Jenjang S1

Oleh

M. Taufik
09011281823073

Palembang, Desember 2022

Mengetahui,

Ketua Jurusan Sistem Komputer



Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041000

Pembimbing Tugas Akhir

4/1/23

Ahmad Hervanto, S.Kom., M.T.

NIP. 198701222015041002

AUTHENTICATION PAGE

CLASSIFICATION OF BOTNET ATTACKS USING BI-DIRECTIONAL LONG SHORT-TERM MEMORY METHOD

FINAL TASK

Submitted to Complete One of the Conditions
Obtaining Strata 1 Degree

By

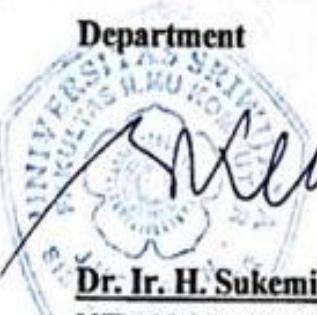
M. Taufik
09011281823073

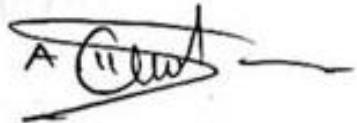
Palembang, December 2022

Acknowledge,

Head of Computer System

Supervisor

Department

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041000

4/1/23

Ahmad Heryanto, S.Kom., M.T.
NIP. 198701222015041002

HALAMAN PERSETUJUAN

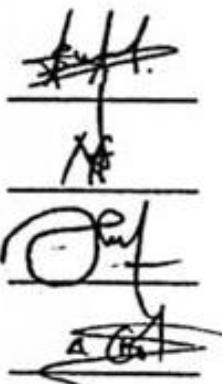
Telah diuji dan lulus pada :

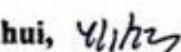
Hari : Jum'at

Tanggal : 23 Desember 2022

Tim Penguji :

1. Ketua : **Sarmayanta Sembiring, S.SI, M.T.**
2. Sekretaris : **Nurul Afifah S.Kom, M.Kom.**
3. Penguji : **Ahmad Fali Oklilas S.T, M.T.**
4. Pembimbing : **Ahmad Heryanto S.Kom, M.T.**



Mengetahui, 

Ketua Jurusan Sistem Komputer



NIP. 196612032006041000

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : M. Taufik

NIM : 09011281823073

Judul : Klasifikasi Serangan Botnet Menggunakan Metode *Bi-Directional Long Short-Term Memory*

Hasil Pengecekan Software iThenticate/Turnitin : 4%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.



Palembang, Desember 2022



M. Taufik
NIM.09011281823073

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Alhamdulillahirobbil'alamin, Segala puji dan syukur atas kehadiran ALLAH SWT Tuhan semesta alam, karena berkat Rahmat dan Karunia-Nya lah sehingga penulis dapat menyelesaikan penyusunan Tugas Akhir ini yang berjudul **"Klasifikasi Serangan Botnet Menggunakan Metode *Bi-Directional Long Short-Term Memory*".**

Dalam penyusunan laporan ini penulis menampilkan penjelasan tentang proses daripada klasifikasi serangan Botnet hingga menampilkan hasil dan data akhir yang didapatkan. Penulis berharap agar laporan ini dapat menjadi manfaat untuk orang banyak serta menjadi menjadi bacaan yang menarik sehingga menjadi sumber referensi penelitian lain yang mengambil tema penelitian bidang Networking.

Penulisan Tugas Akhir ini merupakan syarat akhir untuk memenuhi sebagian kurikulum dan syarat kelulusan pada Jurusan Sistem Komputer, Universitas Sriwijaya.

Pada kesempatan ini penulis mengucapkan terima kasih kepada banyak pihak yang telah memberikan bantuan, dorongan, motivasi, semangat dan bimbingan dalam penyusunan Skripsi ini :

1. ALLAH SWT Tuhan semesta alam.
2. Kedua orang tua Fogi Hafana S.E dan Nurtapipa S.H yang telah sangat membantu.
3. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Sutarno, S.T., M.T. selaku Dosen Pembimbing Akademik
6. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing Skripsi yang telah berkenan memberikan saran dan masukan selama pembuatan skripsi ini.

7. Bapak Ahmad Fali Oklilas, S.T., M.T. selaku dosen Pengaji Skripsi yang telah memberikan perbaikan skripsi yang bersifat membangun.
8. Hanna Pertiwi dan Tri Putri yang telah mendukung dalam masa-masa pembuatan skripsi ini.
9. Jumhadi, Dimas, Agung yang telah membantu dalam pembuatan program Skripsi.
10. Rekan seperjuangan kuliah Farhan, Imam, Realdi.
11. Rekan eldas Furqon, Alifah, Indah, Valen, Arif, Ades, Novi, Tedi, Hana
12. Rekan Sistem Komputer B 2018 Indralaya, Diko, Yudha, Rafii, Jepi, Bima, Caezar, Anjar, Daffa, Alif, Rani, Berbi, Rahma, Nia, Prazna.
13. Saudara Ayuk dan Adik.

Dalam penyusunan Skripsi ini penulis menyadari sepenuhnya bahwa skripsi ini belum masuk dalam kata sempurna, oleh karena itu penulis mengharapkan saran dan kritik dari semua pihak yang berkenan demi laporan yang lebih baik lagi.

Akhir kata penulis harap semoga Skripsi ini dapat bermanfaat serta dapat memberikan pengetahuan dan wawasan bagi semua pihak yang membutuhkannya.

Palembang, Desember 2022



M. Taufik

NIM.09011281823073

**CLASSIFICATION OF BOTNET ATTACKS USING
BI-DIRECTIONAL LONG SHORT-TERM MEMORY METHOD**

M. TAUFIK (09011281823073)

*Computer Engineering Department, Computer Science Faculty, Sriwijaya
University*
Email : mrtaufik06@gmail.com

ABSTRACT

Botnet attacks have become a major threat on the internet in recent years. Because a botnet is a collection of programs in which there is malware, both of which are connected to each other within the scope of the internet network, which can communicate with a collection of similar malware bot programs to do work that is detrimental and targets the intended victim. There are three objectives in this research, among others, to build a model of the Bi-Directional LSTM method for the ability to classify botnet attacks on the CIC-IDS 2018 dataset. Second, apply PCA feature selection to optimize the classification of botnet attacks. And thirdly Knowing the results of the classification performance of Botnet attacks seen from the results of accuracy, specificity, recall, precision. Therefore, to overcome the previous problem, the deep learning method was used. The Deep Learning method used is the BI-Directional LSTM method which is a branch of LSTM which has the advantage of having two layers, namely the forward layer and the backward layer so that it allows additional information enhancement and improves memory capabilities. This research has three benefits, including applying the Bi-Directional Long Short-Term Memory method for classifying Botnet attacks. The second is to optimize the Bi-Directional Long Short Term Memory method so as to get a high accuracy value. The third is to find out the performance of Bi-Directional Long Short-Term Memory results to classify Botnet attacks. This research was conducted by training the 2018 CIC-IDS dataset on machine learning with the provision of tuning hyperparameters and comparing results with different ratios of training data and test data so that the best evaluation results were obtained with an accuracy value of 99.82% accuracy, 99.76% precision, 99.89 recall. %, and a specificity of 99.82%.

Keywords : Botnet, LSTM, Bi-Directional LSTM, PCA, CIC-IDS-2018 Datasets

Head of Computer System



Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041000

Supervisor

Ahmad Hervanto, S.Kom., M.T.
NIP. 198701222015041000

**KLASIFIKASI SERANGAN BOTNET MENGGUNAKAN METODE
BI-DIRECTIONAL LONG SHORT-TERM MEMORY**

M. TAUFIK (09011281823073)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : mrtaufik06@gmail.com

ABSTRAK

Serangan Botnet telah menjadi ancaman yang besar di internet dalam beberapa tahun kebelakang. Karena Botnet merupakan sekumpulan program-program yang didalamnya terdapat malware yang mana keduanya saling terhubung dalam satu ruang lingkup jaringan internet yang dapat berkomunikasi dengan kumpulan program-program malware bot sejenisnya guna melakukan suatu pekerjaan yang bersifat merugikan dan menyasar ke korban yang dituju. Terdapat tiga tujuan dalam Penelitian ini antara lain untuk Membangun model metode Bi-Directional LSTM untuk kemampuan klasifikasi serangan Botnet pada dataset CIC-IDS 2018. Kedua Menerapkan seleksi fitur PCA untuk pengoptimalan klasifikasi serangan botnet. Dan ketiga Mengetahui hasil dari performa klasifikasi serangan Botnet dilihat dari hasil akurasi, spesifitas, recall, presisi. Oleh karena itu untuk mengatasi masalah sebelumnya digunakan metode deep learning. Adapun metode Deep Learning yang dipakai adalah memakai metode BI-Directional LSTM yang merupakan cabang dari LSTM yang memiliki kelebihan memiliki 2 lapisan yaitu lapisan forward dan lapisan backward sehingga memungkinkan peningkatan informasi tambahan dan meningkatkan kemampuan memori. Dalam penelitian ini memiliki tiga manfaat antara lain Menerapkan metode Bi-Directional Long Short-Term Memory untuk klasifikasi serangan Botnet. Kedua guna Mengoptimalkan metode Bi-Directional Long Short Term Memory sehingga mendapatkan nilai akurasi yang tinggi. Ketiga guna Mengetahui performa hasil Bi-Directional Long Short-Term Memory untuk mengklasifikasi serangan Botnet. Penelitian ini dilakukan dengan mentraining dataset CIC-IDS 2018 pada machine learning dengan ketentuan melakukan tuning hyperparameter serta melakukan perbandingan hasil dengan variasi rasio data training dan data uji yang berbeda sehingga didapatkan hasil evaluasi terbaik dengan nilai akurasi akurasi 99.82%, presisi 99.76%, recall 99.89%, dan spesifitas 99.82%.

Kata Kunci : Botnet, LSTM, *Bi-Directional LSTM*, PCA, Dataset CIC-IDS-2018

Ketua Jurusan Sistem Komputer



Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041000

Pembimbing Tugas Akhir

Ahmad Heryanto, S.Kom., M.T.

NIP. 198701222015041002

DAFTAR ISI

HALAMAN PENGESAHAN	i
AUTHENTICATION PAGE	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PERNYATAAN.....	iv
KATA PENGANTAR.....	v
ABSTRACT	vii
ABSTRAK.....	viii
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	xii
DAFTAR TABEL.....	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan.....	4
1.5 Manfaat.....	4
1.6 Metodologi Penelitian	4
1.7 Sistematika Penulisan.....	5
BAB II TINJAUAN PUSTAKA.....	7
2.1 Pendahuluan	7
2.2 Botnet	11
2.3 Dataset CSE- CIC – IDS 2018	11
2.4 Confusion Matrix.....	17
2.5 Principal Component Analysis	20

2.6	Artificial Intelligence.....	22
2.7	Machine Learning.....	23
2.8	Deep Learning	23
2.9	Recurrent Neural Network	24
2.10	Long Short Term Memory.....	27
2.11	Bi-Directional Long Short Term Memory	29
BAB III METODOLOGI PENELITIAN	33	
3.1	Pendahuluan	33
3.2	Kerangka Kerja.....	33
3.3	Perangkat Digunakan.....	35
3.4	Skenario Eksperimen.....	35
3.5	Skenario Riset.....	37
3.6	Persiapan Dataset.....	38
3.7	Dataset Botnet	39
3.8	Seleksi Fitur PCA.....	44
3.9	Klasifikasi BI-Directional LSTM.....	45
3.10	Tahapan BI-Directional LSTM dalam Mengolah Data.....	46
3.11	Validasi Hasil	49
3.12	Perbandingan Seleksi Fitur.....	49
BAB IV HASIL DAN ANALISIS	52	
4.1	Pendahuluan	52
4.2	Hasil Ekstraksi Dataset.....	52
4.3	Seleksi Fitur PCA.....	53
4.4	Hyperparameter BI-Directional LSTM	54
4.4.1	Tuning Hyperparameter BI-Directional LSTM	54
4.4.2	Hyperparameter utama	58

4.5	Hasil Klasifikasi	59
4.6	Validasi Hasil Klasifikasi	61
4.6.1	Validasi Hasil Rasio Data 50:50	62
4.6.2	Validasi Hasil Rasio Data 60:40	66
4.6.3	Validasi Hasil Rasio Data 70:30	71
4.6.4	Validasi Hasil Rasio Data 80:20	76
4.6.5	Validasi Hasil Rasio Data 90:10	80
4.7	Validasi Hasil BACC dan MCC	85
4.8	Validasi Hasil BACC dan MCC	86
BAB V KESIMPULAN DAN SARAN		88
5.1	Kesimpulan.....	88
5.2	Saran	88
DAFTAR PUSTAKA		89

DAFTAR GAMBAR

Gambar 2.1 Topologi Dataset CSE-CIC-IDS 2018	12
Gambar 2.2 Confusion Matrix	17
Gambar 2.3 PCA Matriks X.....	21
Gambar 2.4 Visualisasi Struktur RNN	24
Gambar 2.5 Model RNN	25
Gambar 2.6 Forward pass dan Backward pass RNN	26
Gambar 2.7 Ilustrasi blok LSTM dan memory cell units	28
Gambar 2.8 (a) forward pass dan (b) backward pass pada LSTM	29
Gambar 3.1 Kerangka Kerja	34
Gambar 3.2 Skenario eksperimen serangan Botnet	36
Gambar 3.3 Diagram Serangan Botnet	37
Gambar 3.4 Skenario riset Botnet	38
Gambar 3.5 dataset CSE-CIC-IDS 2018 Botnet.....	39
Gambar 3.6 Flowchart Seleksi Fitur	45
Gambar 3.7 Flowchart Klasifikasi BI-Directional LSTM	46
Gambar 3.8 Flowchart Tahapan BI-Directional LSTM	47
Gambar 3.9 Flowchart Proses BI-Directional LSTM pada dataset.....	48
Gambar 3.10 Tanpa PCA dan Tuning Hyperparamteter.....	50
Gambar 3.11 Dengan PCA dan Tuning Hyperparameter	51
Gambar 4.1 Hasil Ekstraksi Data	53
Gambar 4.2 Hasil Klasifikasi rasio data 50:50.....	60
Gambar 4.3 Hasil Klasifikasi	61
Gambar 4.4 Grafik loss rasio data 50:50.....	62
Gambar 4.5 Grafik Akurasi rasio data 50:50	63
Gambar 4.6 Matriks Konfusi rasio data 50:50	64
Gambar 4.7 Precission Recall Curve rasio data 50:50.....	65
Gambar 4.8 ROC Curve rasio data 50:50	66
Gambar 4.9 Grafik loss rasio data 60:40.....	67
Gambar 4.10 Grafik akurasi rasio data 60:40	67
Gambar 4.11 Matriks Konfusi rasio data 60:40	68

Gambar 4.12 Precision Recall Curve rasio data 60:40	69
Gambar 4.13 ROC curve rasio data 60:40	70
Gambar 4.14 Grafik loss rasio data 70:30.....	71
Gambar 4.15 Grafik akurasi rasio data 70:30	72
Gambar 4.16 Matriks Konfusi rasio data 70:30	73
Gambar 4.17 Precision Recall Curve rasio data 70:30	74
Gambar 4.18 ROC curve rasio data 70:30	75
Gambar 4.19 Grafik loss rasio data 80:20.....	76
Gambar 4.20 Grafik akurasi rasio data 80:20	76
Gambar 4.21 Matriks Konfusi rasio data 80:20	77
Gambar 4.22 Precision Recall Curve rasio data 80:20	79
Gambar 4.23 ROC curve rasio data 80:20	80
Gambar 4.24 Grafik loss rasio data 90:10.....	81
Gambar 4.25 Grafik akurasi rasio data 90:10	81
Gambar 4.26 Matriks konfusi rasio data 90:10	82
Gambar 4.27 Precision Recall Curve rasio data 90:10	83
Gambar 4.28 ROC curve rasio data 90:10	84
Gambar 4.29 Hasil BACC dan MCC	87

DAFTAR TABEL

Tabel 2.1 Rujukan Penelitian Terdahulu.....	7
Tabel 2.2 Fitur Dataset CSE-CIC-IDS 2018.....	13
Tabel 2.3 Matriks Konfusi	18
Tabel 2.4 Perbandingan LSTM dan BI-Directional LSTM	31
Tabel 3.1 Spesifikasi Perangkat Keras	35
Tabel 3.2 Spesifikasi Perangkat Lunak	35
Tabel 3.3 Atribut Fitur Ekstraksi	40
Tabel 4.1 Seleksi Fitur Data PCA	54
Tabel 4.2 Tuning Hyperparameter Unit Node	55
Tabel 4.3 Tuning Hyperparameter Dropout.....	55
Tabel 4.4 Tuning Hyperparameter Fungsi Aktivasi.....	56
Tabel 4.5 Tuning Hyperparameter Learning Rate	57
Tabel 4.6 Tuning Hyperparameter Batch Size	57
Tabel 4.7 Tuning Hyperparameter Epoch.....	58
Tabel 4.8 Hyperparameter utama.....	59
Tabel 4.9 Hasil performa Klasifikasi rasio data 50:50.....	64
Tabel 4.10 Hasil performa Klasifikasi rasio data 60:40.....	69
Tabel 4.11 Hasil performa Klasifikasi rasio data 70:30.....	73
Tabel 4.12 Hasil performa Klasifikasi rasio data 80:20.....	78
Tabel 4.13 Hasil performa Klasifikasi rasio data 90:10.....	83
Tabel 4.14 Hasil Validasi BACC dan MCC	86

BAB I

PENDAHULUAN

1.1 Latar Belakang

Serangan Botnet telah menjadi ancaman yang besar di internet. Karena Botnet merupakan sekumpulan program-program yang didalamnya terdapat malware yang mana keduanya saling terhubung dalam satu ruang lingkup jaringan internet yang dapat berkomunikasi dengan kumpulan program-program malware bot sejenisnya guna melakukan suatu pekerjaan yang bersifat merugikan dan menyasar ke korban yang dituju. Bot paling canggih saat ini menggunakan *Domain Generation Algorithms* (DGA) yang berfungsi menghasilkan domain dalam jumlah besar secara acak dan memilih subset guna terhubungnya komunikasi dengan server *Command and Control* (C&C)[1][2]. Penggunaan DGA untuk menghindari *Blacklist*, dan juga guna menghindari sistem keamanan[1]. Perbaikan dalam menangani kasus mengenai serangan Botnet telah banyak dilakukan dalam kurun waktu beberapa tahun belakangan, hal ini menyebabkan penelitian tentang serangan botnet merupakan bukanlah sebuah hal yang baru. Berikut ini merupakan beberapa penelitian-penelitian terdahulu yang mengambil topik yang sama dengan penelitian ini yaitu membahas tentang serangan Botnet.

Pada penelitian sebelumnya [3] dengan membahas judul mengenai Deteksi serangan Botnet pada jaringan IoT. Pada penelitian ini menggunakan metode CNN-LSTM dan memakai dataset N-Balot yang didapat dari archive.ics.uci.edu. Dengan pemakaian metode CNN-LSTM pada penelitian ini, percobaan dilakukan pada beberapa alat IoT antara lain seperti pada Bel Pintu dengan presisi 71%-75%, recall 0 untuk memindai serangan, sedangkan untuk TCP *flood attacks* menghasilkan presisi 53%, dengan menghasilkan akurasi 99%. Pada alat thermostat mendapatkan presisi 52%, Pada percobaan alat baby detection dengan metode CNN-LSTM mendapatkan hasil presisi 67%, recall 0 untuk pemindai serangan dan presisi 54% untuk TCP *flood attack*. Dan pada percobaan alat Kamera keamanan mendapatkan presisi dan recall 100% namun menghasilkan akurasi rendah

pada memindai serangan dan TCP *flood attacks*. Dari keseluruhan alat-alat IoT yang berbeda, model CNN-LSTM mempunyai kemampuan deteksi serangan botnet dengan performa optimal.

Pada penelitian berikutnya [1] dengan mengambil tema pemanfaatan kerangka kerja LSTM untuk menyeimbangkan multikelas dalam deteksi botnet. Penelitian ini memakai dataset dari dua sumber yaitu Alexa top 100000 dan OSINT DGA. Pada penelitian ini penerapan kerangka kerja LSTM untuk deteksi serangan Botnet mendapatkan hasil performa yang berbeda di setiap class adapun untuk class biasa akurasi 92.5% sedangkan class kecil 80%. Adapun presisi sebesar 60% dan recall 53%.

Pada penelitian lainnya [4] dengan tema deteksi serangan botnet menggunakan metode ANN. Pada penelitian ini memakai dataset CTU-13. Dan pemanfaatan metode *Artificial Neural Network* (ANN) pada peneliti ini mendapatkan hasil akurasi yang cukup besar melebihi 95%.

Pada penelitian [5] yang membahas tentang klasifikasi serangan botnet pada jaringan IoT. Pada penelitian ini memakai dataset N-Baiot yang berformat data pcap dan kemudian dilakukan ekstraksi data untuk klasifikasi dengan menggunakan tiga metode antara lain *Decision Tree* (DT), *Random forest* (RF) dan *k-Nearest Neighbor* (k-NN) . Pada penelitian ini melakukan dua klasifikasi yaitu klasifikasi Binary merupakan data dibagi menjadi dua benign dan malware yang menghasilkan akurasi metode k-NN 90,25%, metode DT 93% , Dan RF 95,30%. Sedangkan pada bagian klasifikasi Multiclass yang berarti lebih dari dua kategori yaitu benign, mirai, bashlite, tori, menghasilkan akurasi sebesar 95% untuk metode DT, metode RF 97% dan metode k-NN 87%.

Dari beberapa penelitian terdahulu yang telah ditampilkan , Terdapat kelemahan dan kekurangan dari Hasil akurasi, presisi dan recall masih terbilang rendah, sehingga terdapat kekurangan pada hasil presisi sebesar 60% dan recall 53%[1]. Dan juga kekurangan lainnya penelitian terdahulu belum menggunakan fitur ekstraksi. Adapun kekurangan lainnya yaitu hasil akurasi dari beberapa penelitian masih belum cukup besar dengan menghasilkan akurasi class besar 92,5% dan class kecil 80%[1]. Dan kelemahan dari

penelitian-penelitian sebelumnya yaitu hasil yang dihasilkan masih berbentuk dalam multiclass atau class yang berbeda bukan hasil dalam satu class utama baik dari akurasi, presisi, dan recall [1][3][5]. Dengan demikian, dari kelemahan dan kekurangan diatas untuk peningkatan akurasi, presisi dan recall yang lebih besar dan akan menghasilkan hasil berupa satu class utama baik akurasi, presisi, dan recall maka pada penelitian ini penulis akan menggunakan metode Bi-Directional LSTM.

Untuk meningkatkan hasil akurasi, presisi, recall dari satu class utama. Penulis mengambil tema mengenai Klasifikasi serangan Botnet menggunakan metode *Bi-Directional Long Short-Term Memory* (LSTM) dengan memakai dataset CSE-CIC-IDS2018 dari website University of New Brunswick Canada yang berbentuk format pcap yang kemudian diekstraksi menjadi format csv .

1.2 Rumusan Masalah

Berdasarkan dari beberapa penjelasan penelitian terdahulu yang telah dibahas, terdapat permasalahan yang menjadi acuan penulis untuk memperbaiki permasalahan tersebut dan dijadikan sebagai rumusan masalah antara lain :

1. Bagaimana menerapakan model metode Bi-Directional LSTM dapat menangani klasifikasi serangan Botnet pada dataset CIC-IDS-2018?
2. Bagaimana penggunaan fitur ekstraksi *Principal Component Analysis* (PCA) bisa diimplementasikan dengan baik dan tidak seperti pada penelitian sebelumnya yang tidak memakai fitur ekstraksi?
3. Bagaimana metode BI-Directional LSTM dapat menghasilkan penggeraan validasi terhadap nilai akurasi, presisi, recall yang lebih besar dari penelitian sebelumnya begitu juga spesifitas, dan F1-Score?

1.3 Batasan Masalah

Adapun batasan masalah dari pembuatan Skripsi ini antara lain :

1. Penelitian ini akan membahas tentang topik Klasifikasi serangan Botnet.

2. Dataset yang digunakan pada penelitian ini memakai dataset CSE- CIC-IDS2018 didapat dari website University of New Brunswick Canada.
3. Penerapan metode Bi-Directional LSTM pada penelitian ini supaya dapat diimplementasikan pada penanganan klasifikasi serangan Botnet.

1.4 Tujuan

Adapun Tujuan yang akan dicapai dari pembuatan skripsi ini antara lain :

1. Membangun model metode Bi-Directional LSTM untuk kemampuan klasifikasi serangan Botnet pada dataset CIC-IDS 2018.
2. Menerapkan seleksi fitur PCA untuk pengoptimalan klasifikasi serangan botnet.
3. Mengetahui hasil dari performa klasifikasi serangan Botnet dilihat dari hasil akurasi, spesifitas, recall, presisi.

1.5 Manfaat

Adapun manfaat dari pembuatan skripsi ini antara lain :

1. Menerapkan metode Bi-Directional Long Short-Term Memory untuk klasifikasi serangan Botnet.
2. Mengoptimalkan metode Bi-Directional Long Short Term Memory sehingga mendapatkan nilai akurasi yang tinggi.
3. Mengetahui performa hasil Bi-Directional Long Short-Term Memory untuk mengklasifikasi serangan Botnet.

1.6 Metodologi Penelitian

Adapun Metodologi yang akan digunakan pada pembuatan skripsi ini antara lain:

1. Tahap Pertama (Persiapan data)

Pada tahap ini melakukan pengumpulan dataset yang akan digunakan kemudian melakukan pembelajaran dan pemahaman terhadap data yang akan diolah sehingga kebutuhan untuk topik penelitian dapat terpenuhi.

2. Tahap Kedua (Studi Pustaka dan Literatur)

Pada tahap ini penulis akan mencari informasi-informasi dengan mengumpulkan jurnal, paper, maupun pencarian internet yang membahas tentang skema serangan Botnet dan penjelasan Bi-Directional LSTM yang berkenaan tentang pembuatan skripsi ini.

3. Tahap Ketiga (Pengujian)

Pada tahap ini membangun rancangan model yang terstruktur untuk tahapan klasifikasi serangan Botnet dengan mentraining dataset guna mendapatkan hasil yang diharapkan.

4. Tahap Keempat (Analisis dan Kesimpulan)

Pada tahap terakhir ini setelah mendapatkan hasil dari klasifikasi serangan Botnet kemudian melakukan analisis pada klasifikasi yang telah dilakukan sebelumnya dan menarik kesimpulan pada pembuatan skripsi ini.

1.7 Sistematika Penulisan

Adapun Sistematika penulisan pada skripsi ini untuk menjelaskan isi dari setiap sub bab antara lain :

BAB I. PENDAHULUAN

Dalam bab I , menjelaskan tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat serta sistematika penulisan dari pembahasan topik skripsi ini yaitu Klasifikasi serangan Botnet dengan metode Bi-Directional LSTM.

BAB II. TINJAUAN PUSTAKA

Dalam bab II, menampilkan literature review yang berhubungan tentang pembahasan teori serangan Botnet, metode Bi-Directional LSTM dan teori-teori lainnya yang berkaitan dengan skripsi ini.

BAB III. METODOLOGI

Dalam bab III, menjelaskan tahapan proses penelitian yang dilakukan secara terstruktur dengan menampilkan tahapan-tahapan pada persiapan dataset Botnet, kemudian penerapan metode Bi-Directional LSTM guna memenuhi tujuan dari pembuatan sripsi ini.

BAB IV, HASIL DAN ANALISIS

Dalam bab IV, menampilkan hasil yang telah didapatkan dari tahapan yang telah dilakukan, serta untuk melihat performa sistem kemudian melakukan analisis dari metode Bi-Directional LSTM.

BAB V, KESIMPULAN DAN SARAN

Dalam bab V, menampilkan kesimpulan yang ditarik dari hasil tahapan pembahasan yang telah didapatkan dan menampilkan beberapa saran masukan untuk penelitian lebih lanjut.

DAFTAR PUSTAKA

- [1] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, “A bidirectional LSTM deep learning approach for intrusion detection,” *Expert Syst. Appl.*, vol. 185, no. July, p. 115524, 2021, doi: 10.1016/j.eswa.2021.115524.
- [2] H. Alkahtani and T. H. H. Aldhyani, “Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications,” *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/3806459.
- [3] N. Gupta, V. Jindal, and P. Bedi, “LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system,” *Comput. Networks*, vol. 192, no. April, p. 108076, 2021, doi: 10.1016/j.comnet.2021.108076.
- [4] D. Tran, H. Mac, V. Tong, H. A. Tran, and L. G. Nguyen, “A LSTM based framework for handling multiclass imbalance in DGA botnet detection,” *Neurocomputing*, vol. 275, pp. 2401–2413, 2018, doi: 10.1016/j.neucom.2017.11.018.
- [5] Y. Sung, S. Jang, Y. S. Jeong, and J. H. (James J.). Park, “Malware classification algorithm using advanced Word2vec-based Bi-LSTM for ground control stations,” *Comput. Commun.*, vol. 153, no. January, pp. 342–348, 2020, doi: 10.1016/j.comcom.2020.02.005.
- [6] P. S. Muhuri, P. Chatterjee, X. Yuan, K. Roy, and A. Esterline, “Using a long short-term memory recurrent neural network (LSTM-RNN) to classify network attacks,” *Inf.*, vol. 11, no. 5, pp. 1–21, 2020, doi: 10.3390/INFO11050243.
- [7] D. Wu, Z. Jiang, X. Xie, X. Wei, W. Yu, and R. Li, “LSTM Learning with Bayesian and Gaussian Processing for Anomaly Detection in Industrial IoT,” *IEEE Trans. Ind. Informatics*, vol. 16, no. 8, pp. 5244–5253, 2020, doi: 10.1109/TII.2019.2952917.
- [8] A. A. Ahmed, *Botnet detection using a feed-forward backpropagation artificial neural network*, vol. 888. Springer International Publishing, 2019.
- [9] A. Muslim, A. B. Mutiara, R. Refianti, C. M. Karyati, and G. Setiawan, “Comparison of accuracy between long short-term memory-deep learning and multinomial logistic regression-machine learning in sentiment analysis on twitter,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, pp. 747–754, 2020, doi: 10.14569/ijacsa.2020.0110294.
- [10] M. M. Salim, S. K. Singh, and J. H. Park, “Securing Smart Cities using LSTM algorithm and lightweight containers against botnet attacks,” *Appl. Soft Comput.*, vol. 113, p. 107859, 2021, doi: 10.1016/j.asoc.2021.107859.
- [11] H. T. Nguyen, Q. D. Ngo, and V. H. Le, “A novel graph-based approach for IoT botnet detection,” *Int. J. Inf. Secur.*, vol. 19, no. 5, pp. 567–577, 2020, doi: 10.1007/s10207-019-00475-6.

- [12] P. P. Avi, J. S. Komputer, F. I. Komputer, and U. Sriwijaya, “DELINASI SINYAL ELEKTRODIAGRAM MULTI-LEAD MENGGUNAKAN METODE LONG SHORT-TERM MEMORY BERBASIS EKSTRAKSI FITUR CONVOLUTIONAL NEURAL NETWORK - Sriwijaya University Repository,” 2022, [Online]. Available: <https://repository.unsri.ac.id/65083/>.
- [13] P. P. Lid and S. Planning, *PRINCIPAL COMPONENTS ANALYSIS (PCA)** Xln 1, vol. 19, no. 3. 1993.
- [14] M. Qiao and H. Li, “Application of PCA-LSTM model in human behavior recognition,” *J. Phys. Conf. Ser.*, vol. 1650, no. 3, 2020, doi: 10.1088/1742-6596/1650/3/032161.
- [15] M. Aamir and S. M. Ali Zaidi, “Clustering based semi-supervised machine learning for DDoS attack classification,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 4, pp. 436–446, 2021, doi: 10.1016/j.jksuci.2019.02.003.
- [16] Y. Zhang, “Artificial intelligence governance capability association model based on closed-loop control theory,” vol. 2020, pp. 1063–1067, 2020, doi: 10.1109/ITAIC49862.2020.9338966.
- [17] S. S. Panwar, P. S. Negi, L. S. Panwar, and Y. P. Raiwani, “Implementation of machine learning algorithms on cicids-2017 dataset for intrusion detection using WEKA,” *Int. J. Recent Technol. Eng.*, vol. 8, no. 3, pp. 2195–2207, 2019, doi: 10.35940/ijrte.C4587.098319.
- [18] J. Effendi, “Otomatisasi Delineasi Sinyal Elektrokardiogram Menggunakan Metode Long Short-Term Memory Berbasis Ekstraksi Fitur Convolutional Neural Network 1-Dimensi,” Universitas Sriwijaya, 2020.
- [19] D. Jia *et al.*, “An Electrocardiogram Delineator via Deep Segmentation Network,” *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS*, pp. 1913–1916, 2019, doi: 10.1109/EMBC.2019.8856987.
- [20] P. Ongsulee, “Artificial intelligence, machine learning and deep learning,” *Int. Conf. ICT Knowl. Eng.*, pp. 1–6, 2018, doi: 10.1109/ICTKE.2017.8259629.
- [21] A. Malali, S. Hiriyannaiah, G. M. Siddesh, K. G. Srinivasa, and N. T. Sanjay, “Supervised ECG wave segmentation using convolutional LSTM,” *ICT Express*, vol. 6, no. 3, pp. 166–169, 2020, doi: 10.1016/j.icte.2020.04.004.
- [22] M. U. Kim and H. Jong Yang, “RNN-Based Node Selection for Sensor Networks with Energy Harvesting,” *9th Int. Conf. Inf. Commun. Technol. Converg. ICT Converg. Powered by Smart Intell. ICTC 2018*, pp. 1316–1318, 2018, doi: 10.1109/ICTC.2018.8539707.
- [23] P. Zhao and X. Yang, “Opportunistic routing for bandwidth-sensitive traffic in wireless networks with lossy links,” *J. Commun. Networks*, vol. 18, no. 5, pp. 806–817, 2016, doi: 10.1109/JCN.2016.000109.

- [24] A. Darmawahyuni, S. Nurmaini, and Sukemi, “Deep Learning with Long Short-Term Memory for Enhancement Myocardial Infarction Classification,” *Proc. 2019 6th Int. Conf. Instrumentation, Control. Autom. ICA 2019*, no. August 2019, pp. 19–23, 2019, doi: 10.1109/ICA.2019.8916683.
- [25] A. Sherstinsky, “Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) network,” *Phys. D Nonlinear Phenom.*, vol. 404, no. March, pp. 1–43, 2020, doi: 10.1016/j.physd.2019.132306.
- [26] Muhammad Gerald Rizky, “Analisis Perbandingan Metode LSTM dan BiLSTM Untuk Klasifikasi Sinyal Jantung Phonocardiogram,” pp. 1–63, 2021, [Online]. Available: <https://repository.dinamika.ac.id/id/eprint/5962/1/17410200021-2021-UNIVERSITAS DINAMIKA.pdf>.
- [27] A. Peimankar and S. Puthusserypady, “DENS-ECG: A deep learning approach for ECG signal delineation,” *Expert Syst. Appl.*, vol. 165, 2021, doi: 10.1016/j.eswa.2020.113911.
- [28] Ö. Yildirim, “A novel wavelet sequences based on deep bidirectional LSTM network model for ECG signal classification,” *Comput. Biol. Med.*, vol. 96, no. March, pp. 189–202, 2018, doi: 10.1016/j.combiomed.2018.03.016.
- [29] Y. Karyadi, “Prediksi Kualitas Udara Dengan Metoda LSTM, Bidirectional LSTM, dan GRU,” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 1, pp. 671–684, 2022, doi: 10.35957/jatisi.v9i1.1588.
- [30] S. Schiavoni, F. Maggi, L. Cavallaro, and S. Zanero, “Phoenix: DGA-based botnet tracking and intelligence,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8550 LNCS, pp. 192–211, 2014, doi: 10.1007/978-3-319-08509-8_11.
- [31] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, and S. Nõmm, “MedBIoT: Generation of an IoT botnet dataset in a medium-sized IoT network,” *ICISSP 2020 - Proc. 6th Int. Conf. Inf. Syst. Secur. Priv.*, no. Icissp 2020, pp. 207–218, 2020, doi: 10.5220/0009187802070218.