KOMPARASI PADA KLASIFIKASI TRAFIK SERANGAN *MALWARE BOTNET* DENGAN METODE *SUPPORT VECTOR MACHINE* (SVM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

MEUTIA ZAMIEYUS
09011181722018

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

HALAMAN PENGESAHAN

KOMPARASI PADA KLASIFIKASI TRAFIK SERANGAN *MALWARE BOTNET* DENGAN METODE *SUPPORT VECTOR MACHINE* (SVM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

MEUTIA ZAMIEYUS
09011181722018

Indralaya, Juni 2021

Mengetahui, 8/7/21

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 17 Juni 2021

Tim Penguji :

1. Ketua Sidang	: Ahmad Fali Oklilas, M.T.	(.....)
2. Sekretaris Sidang	: Tri Wanda Septian, S.Kom., M.Sc.	(.....)
3. Penguji Sidang	: Ahmad Heryanto, M.T.	(.....)
4. Pembimbing	: Deris Stiawan, M.T., Ph.D.	(.....)

Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Meutia Zamieyus

Nim : 09011181722018

Program Studi : Sistem Komputer

Judul Penelitian : Komparasi Pada Klasifikasi Trafik Serangan *Malware Botnet* Dengan Metode *Support Vector Machine* (SVM)

Hasil Pengecekan *Software iThenticate Turnitin* : 9%

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

Demikian surat pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, Juni 2021

Meutia Zamieyus

Nim. 09011181722018

HALAMAN PERSEMBAHAN

"Don't Give Up"

"Allahumma Yassir Wala Tu'assir"

"Man Jadda Wa Jadda"

"Sesungguhnya sesudah kesulitan itu ada kemudahan. Maka apabila kamu telah selesai dari suatu urusan, kerjakanlah dengan sungguh-sungguh urusan yang lain, dan hanya kepada Tuhanmulah hendaknya kamu berharap (Q.S Asy-Syarh : 6 - 8)"

"Tugas Akhir ini kupersembahkan untuk kedua orang tua ku tercinta, kedua saudaraku dan keluarga besar yang senantiasa memberikan semangat serta do'a yang tidak pernah putus sehingga semua nya dapat berjalan lancar"

"Terimakasih teruntuk diri sendiri (Meutia Zamieyus, S.Kom)"

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas kehadirat Allah Subhanahu Wata'ala yang telah melimpahkan rahmat dan karunia-Nya, serta memberikan nikmat iman, beserta kesehatan jasmani maupun rohani sehingga penulis dapat menyelesaikan Tugas Akhir ini yang berjudul **"Komparasi Pada Klasifikasi Trafik Serangan *Malware Botnet* dengan Metode *Support Vector Machine* (SVM)"**.

Penulis menyadari dalam proses penyelesaian Tugas Akhir ini tidak terlepas dari bimbingan, do'a dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis akan mengucapkan rasa syukur dan terima kasih kepada yang terhormat :

- Allah Subhanahu Wata'ala yang telah memberikan nikmat iman, dan kesehatan jasmani maupun rohani sehingga penulis dapat menyelesaikan Tugas Akhir ini.
- Orang Tua yang tersayang dan tercinta, beserta keluarga yang selalu memberi dukungan, semangat dan do'a.
- Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
- Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
- Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Tugas Akhir Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
- Bapak Dr. Ir. H. Sukemi, M.T. selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
- Mbak Nurul Afifah, M.Kom. yang telah membantu membimbing dalam menyelesaikan Tugas Akhir.
- Mbak Renny Virgasari selaku Admin Jurusan Sistem Komputer yang telah banyak membantu administrasi dalam menyelesaikan Tugas Akhir.
- Abdi Bimantara, S.Kom. selaku bimbingan spiritual botnet yang telah membantu dalam menyelesaikan Tugas Akhir.
- Partner Botnet Nuzula Rahma Safitri yang selalu memberi semangat, dukungan serta mendengarkan keluh-kesah dalam menyelesaikan Tugas Akhir.

- RoomMate Tia Hermita dan Febi Rusmiati yang selalu memberi semangat, dukungan serta selalu menemani hari-hari penulis dalam menyelesaikan Tugas Akhir.
- Kookie dan Cia yang selalu menemani dan menghibur hari-hari ku dalam menyelesaikan tugas akhir ini.
- Teruntuk Selly Carolin, Leni Estiyani, Lisa Melinda, Aldi Predyansyah, Asri Safmi, Helti Yuniar, Ira Eriyani, Sinta Bella, Mitasari dan Squad SK17B yang selalu memberikan semangat dan dukungan dari awal perkuliahan sampai saat ini.
- Ahmad Afidin, Agung Setiawan, Amartya Bimantara, M Taufiq Qurahman, Aulia Melynda Putri dan Teman-teman seperjuangan Tim Grub Riset Comnets yang lainnya yang telah banyak membantu.
- Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya.

Penulis menyadari bahwa dalam penulisan Proposal Tugas Akhir ini masih terdapat banyak kesalahan dan masih jauh dari kata sempurna. Karena itu, penulis sangat memohon kritik dan saran yang bersifat membangun. Semoga Proposal Tugas Akhir ini dapat bermanfaat untuk semua yang membaca.

Indralaya, Juni 2021
Penulis

Komparasi Pada Klasifikasi Trafik Serangan *Malware Botnet* Dengan Metode *Support Vector Machine* (SVM)

Meutia Zamieyus (09011181722018)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : mzamieyus@gmail.com

Abstrak

Pada beberapa tahun terakhir penelitian mengenai *botnet* telah banyak dilakukan, *botnet* merupakan salah satu jenis *malware* yang menyerang dengan cara mengambil alih sistem komputer yang terhubung ke jaringan internet dengan mengendalikannya secara remote. Penelitian ini menggunakan dataset MedBIoT yang berasal dari *Tallinn University of Technology* terdapat tiga jenis *botnet* yaitu *bashlite*, *mirai* dan *torii*. Tujuan dari seleksi fitur *Correlation-based Feature Selection* (CFS) yaitu memfilter fitur sehingga dapat menemukan fitur yang terbaik untuk melakukan proses pengklasifikasi. Selain itu, Algoritma *Support Vector Machine* (SVM) terdiri dari tiga kernel yaitu *linear*, rbf dan *polynomial* yang digunakan untuk melakukan proses klasifikasi. Hasil dari penelitian ini menunjukkan bahwa algoritma *Support Vector Machine* (SVM) menggunakan seleksi fitur *Correlation-based Feature Selection* (CFS) dapat melakukan proses klasifikasi dengan baik pada serangan *malware botnet*, hasil klasifikasi menggunakan tiga kernel algoritma SVM menunjukkan hasil yang terbaik yaitu pada kernel *polynomial* mendapatkan nilai akurasi sebesar 99.96%, presisi 99.95%, recall 99.99% serta f-1 score 99.97%.

Kata Kunci : *Botnet Classification, MedBIoT, Correlation-based Feature Selection* (CFS), *Support Vector Machine* (SVM)

Comparison on Traffic Classification of Botnet Malware Attacks Using Support Vector Machine (SVM)

Meutia Zamieyus (09011181722018)

Departement of Computer Engineering, Faculty of Computer Science,
Sriwijaya University
Email : mzamieyus@gmail.com

Abstract

In recent years, research on botnets has been widely carried out, botnets are one type of malware that attacks by taking over systems connected to the internet network by controlling them remotely. This study uses the MedBIoT dataset originating from Tallinn University of Technology, there are three types of botnets, namely bashlite, mirai and torii. The purpose of the Correlation-based Feature Selection (CFS) feature selection is to filter features so that they can find the best features for the classification process. In addition, the Support Vector Machine (SVM) algorithm consists of three kernels, namely linear, RBF, and polynomial which are used to carry out the classification process. The results of this study indicate that the Support Vector Machine (SVM) algorithm using the Correlation-based Feature Selection (CFS) feature selection can perform the classification process well on botnet malware attacks, the classification results using three SVM algorithm kernels show the best results, namely the polynomial kernel get 99.96% accuracy, 99.95% precision, 99.99% recall and 99.97% f-1 score.

Keyword **:** *Botnet Classification, MedBIoT, Correlation-based Feature Selection* (CFS), *Support Vector Machine* (SVM)

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Malware atau *Malicious Software* adalah sebuah perangkat lunak yang dirancang khusus untuk mengganggu sistem operasi sehingga mendapatkan akses ke jaringan dan mengumpulkan informasi pribadi tanpa izin pengguna [1]. Berdasarkan tujuan dan penyebarannya *malware* dapat dikategorikan menjadi berbagai jenis seperti *virus*, *worm, trojan, spyware*, *ransomware*, *scareware*, *bot* dan *rootkit* [2]. Banyak serangan baru dikaitkan dengan penyebaran perangkat lunak yang berbahaya seperti, *ransomware* ataupun *bot malware*. Perangkat yang terinfeksi dengan *bot malware* dapat digunakan alat untuk melakukan serangan jarak jauh atau bahkan *cryptomining* [3]. *Botnet* merupakan salah satu jenis *malware* yang menyerang dengan cara mengambil alih sistem komputer yang terhubung ke jaringan internet dan mengendalikannya secara remote melalui malware (*malicious software*) yang disebut *bot*. Tujuan utama *botnet* adalah mendistribusi email spam, kombinasi serangan DDoS dan melakukan pencurian identitas. Saluran komunikasi antara *botnet* dan *botmaster* disebut sebagai *C*&*C* [4].

Pada penelitian [5] membahas tentang *traffic botnet* menggunakan beberapa algoritma *Machine Learning* yaitu *K-Nearest Neighbor*, *Random Forest*, ID3, *Adaboost*, *Multi Layer Perceptron*, *Naïve Bayes* dan QDA. Akan tetapi dari penelitian ini hanya terdapat hasil performa *precision*, *recall* dan data serangan yang digunakan masih sedikit.

Pada penelitian lain [6] membahas penerapan klasifikasi *botnet* pada infrastruktur IoT menggunakan beberapa algoritma *Machine Learning* yaitu *K-Nearest Neighbor*, *Decision Tree* dan *Random Forest*. Dengan menggunakan dua jenis klasifikasi yaitu *Binary* dan *Multiclass,* dari penelitian yang telah dilakukan maka didapat hasil akurasi pengklasifikasian *Binary* untuk setiap algoritma yaitu *Random Forest* 95,32%, *Decision Tree* 93,15% dan *K-Nearest Neighbor* 90,25%.

Sedangkan hasil akurasi dari pengklasifikasian *Multiclass* untuk setiap algoritma yaitu *Random Forest* 97,66%, *Decision Tree* 95,16% dan *K-Nearest Neighbor* 87,06%. Pada penelitian ini hasil performa akurasi cukup baik akan tetapi parameter yang digunakan untuk mempresentasikan klasifikasi masih sedikit.

Pada penelitian lainnya [7] membahas tentang deteksi serangan *botnet DDoS* menggunakan beberapa algoritma *Machine Learning* yaitu *Support Vector Machine, Artificial Neural Network, Decision Tree, Naïve Bayes*, dan *Unsupervised Machine Learning*, dengan menggunakan dua dataset yaitu UNBS-NB 15 dan KDD99. Hasil penelitian menggunakan dataset UNBS-NB 15 didapat akurasi untuk algoritma *Support Vector Machine* 84,32%, *Artificial Neural Network* 63,97%, *Decision Tree* 94,43%, *Naïve Bayes* 71,63% dan *Unsupervised Machine Learning* 94,78%, sedangkan dengan dataset KDD99 didapat akurasi untuk setiap algoritma yaitu *Support Vector Machine* 91,55%, *Artificial Neural Network* 97,44%, *Decision Tree* 93,3%, *Naïve Bayes* 96,74% dan *Unsupervised Machine Learning* 98,08%. Dari penelitian ini, menunjukkan performa algoritma *Support Vector Machine* memiliki nilai akurasi yang cukup baik pada kedua dataset namun masih bisa untuk ditingkatkan kembali, serta algoritma *Support Vector Machine* juga dapat menghindari *overfitting*.

Berdasarkan beberapa ulasan diatas, maka pada penelitian tugas akhir ini akan membahas komparasi pada klasifikasi trafik serangan *malware botnet* menggunakan pendekatan *Supervised Learning* yaitu *Support Vector Machine*.

1.2 Rumusan Masalah

Adapun rumusan masalah dari penelitian Tugas Akhir ini yaitu:

1. Bagaimana cara memilih fitur sehingga dapat meminimalisir waktu komputasi?
2. Bagaimana cara mengklasifikasi serangan *malware botnet*?
3. Bagaimana pengaruh macam-macam kernel pada metode *Support Vector Machine* terhadap nilai akurasi, presisi, recall dan f1-score?

1.3 Batasan Masalah

Adapun batasan masalah dari penelitian Tugas Akhir ini yaitu:

1. Hasil performa yang dilakukan adalah *Accuracy*, *Precision*, *Recall* dan *F1-Score*.
2. Hanya menerapkan metode *Support Vector Machine* untuk melakukan klasifikasi pada serangan *malware botnet*.
3. Hanya menggunakan tiga kernel pada metode *Support Vector Machine* yaitu kernel *linear, rbf* dan *polynomial*.
4. Tidak melakukan pencegahan pada serangan *malware botnet*.

1.4 Tujuan

Adapun tujuan dari penelitian Tugas Akhir ini yaitu:

1. Menerapkan seleksi fitur *Correlation-based Feature Selection* pada dataset yang digunakan.
2. Menerapkan metode *Support Vector Machine* untuk melakukan klasifikasi pada serangan *malware botnet*.
3. Mengukur dan menganalisa hasil dari akurasi, presisi, recall dan f1-score terhadap kinerja pengklasifikasi metode *Support Vector Machine*.

1.5 Manfaat

Adapun manfaat dari penelitian Tugas Akhir ini yaitu:

1. CFS (*Correlation-based Feature Selection*) dapat mempersingkat waktu komputasi.
2. Mampu mengklasifikasi serangan *malware botnet*.
3. Validasi dari berbagai macam kernel pada metode *Support Vector Machine* dapat meningkatkan hasil akurasi, presisi, recall dan f1-score.

1.6 Metodologi Penelitian

Pada penelitian Tugas Akhir ini akan melewati beberapa tahapan adalah sebagai berikut:

1. Tahapan Pertama (Studi Pustaka)

   Pada tahapan ini akan mencari informasi yang diperlukan dari beberapa sumber seperti jurnal ilmiah, buku, internet, serta artikel-artikel yang dapat digunakan untuk melakukan penelitian Tugas Akhir.

2. Tahapan Kedua (Perancangan Sistem)

   Pada tahapan ini akan merancang suatu sistem yang dapat dilakukan untuk mengklasifikasi serangan *malware botnet* menggunakan metode *Support Vector Machine* dengan bahasa pemrograman python.

3. Tahapan Ketiga (Pengujian dan Pengambilan Data)

   Pada tahapan ini melakukan pengambilan data dari website MedBIoT. Setelah itu dilakukan percobaan penelitian dengan batasan masalah yang ada di penelitian Tugas Akhir.

4. Tahapan Keempat (Hasil dan Analisa)

   Setelah mendapatkan data dari proses pengujian, maka langkah selanjutnya adalah melakukan analisis dan pengolahan data berdasarkan metode yang telah ditetapkan untuk mengetahui performa dari sistem yang telah dibuat.

5. Tahapan Kelima (Kesimpulan dan Saran)

   Pada tahapan ini akan ditarik kesimpulan berdasarkan rumusan masalah dari penelitian serta memberikan saran yang membangun untuk penelitian selanjutnya.

1.7 Sistematika Penulisan

Adapun sistematika penulisan digunakan untuk memperjelas isi setiap bab yang akan dibuat pada penelitian Tugas Akhir. Dibawah ini merupakan sistematika penulisan penelitian Tugas Akhir adalah sebagai berikut:

BAB I. PENDAHULUAN

Pada bab I ini terdiri dari latar belakang, tujuan penelitian, manfaat penelitian, rumusan masalah, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada bab II ini terdiri penjelasan teori-teori dasar tentang *Support Vector Machine*, *Malware Botnet*, Dataset yang digunakan, seleksi fitur yang digunakan, *Confusion Matrix* serta teori lain yang berhubungan dengan penelitian Tugas Akhir.

BAB III. METODOLOGI

Pada bab III ini terdiri dari proses penelitian dilakukan dan perancangan sistem klasifikasi serta penerapan metode penelitian Tugas Akhir.

BAB IV. HASIL DAN ANALISIS

Pada bab IV ini terdiri dari proses penelitian, serta analisa perbandingan dari hasil performa model kernel metode *Support Vector Machine*.

BAB V. KESIMPULAN DAN SARAN

Pada bab V ini akan ditarik beberapa kesimpulan dari hasil penjelasan di bab sebelumnya serta memberikan saran yang membangun untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] A. Bulazel, “A Survey On Automated Dynamic Malware Analysis Evasion and Counter-Evasion,” 2017.

[2] A. F. Agarap, “Towards Building an Intelligent Anti-Malware System: A Deep Learning Approach using Support Vector Machine (SVM) for Malware Classification,” no. 1, 2017, [Online]. Available: http://arxiv.org/abs/1801.00318.

[3] I. Ghafir, V. Prenosil, M. Hammoudeh, S. Jabbar, S. Khalid, and S. Jaf, “BotDet : A System for Real Time Botnet Command and Control Traffic Detection,” *IEEE Access*, vol. 6, pp. 38947–38958, 2018, doi: 10.1109/ACCESS.2018.2846740.

[4] M. Alauthman, N. Aslam, M. Al-kasassbeh, S. Khan, A. Al-Qerem, and K. K. Raymond Choo, “An efficient reinforcement learning-based Botnet detection approach,” *J. Netw. Comput. Appl.*, vol. 150, p. 102479, 2020, doi: 10.1016/j.jnca.2019.102479.

[5] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[6] A. Guerra-manzanares, “MedBIoT : Generation of an IoT Botnet Dataset in a Medium-sized IoT Network MedBIoT : Generation of an IoT Botnet Dataset in a Medium-sized IoT Network,” no. March, 2020, doi: 10.5220/0009187802070218.

[7] T. Anh, T. Hoang, V. Long, L. Hoang, S. Raghvendra, and K. Ishaani, “Performance evaluation of Botnet DDoS attack detection using machine learning,” *Evol. Intell.*, 2019, doi: 10.1007/s12065-019-00310-w.

[8] G. K. R. Anitha, “Structural analysis and detection of android botnets using machine learning techniques Structural analysis and detection of android botnets using,” *Int. J. Inf. Secur.*, vol. 17, no. 2, pp. 153–167, 2018, doi: 10.1007/s10207-017-0363-3.

[9] B. Abraham, A. Mandya, R. Bapat, F. Alali, D. E. Brown, and M. Veeraraghavan, “A Comparison of Machine Learning Approaches to Detect Botnet Traffic,” *Proc. Int. Jt. Conf. Neural Networks*, vol. 2018-July, pp. 1–8, 2018, doi: 10.1109/IJCNN.2018.8489096.

[10] L. Kong, G. Huang, and K. Wu, “Identification of Abnormal Network Traffic Using Support Vector Machine,” 2017, doi: 10.1109/PDCAT.2017.00054.

[11] H. Nguyen, “IoT Botnet Detection Approach Based on PSI graph and DGCNN classifier,” *2018 IEEE Int. Conf. Inf. Commun. Signal Process.*, no. Icsp, pp. 118–122, 2018.

[12] A. Azab, “Machine learning based Botnet Identification Traffic,” pp. 1789–1795, 2016, doi: 10.1109/TrustCom/BigDataSE/ISPA.2016.273.

[13] Y. Meidan *et al.*, “N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders,” *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, 2018, doi: 10.1109/MPRV.2018.03367731.

[14] H. T. Nguyen, Q. D. Ngo, and V. H. Le, “A novel graph-based approach for IoT botnet detection,” *Int. J. Inf. Secur.*, 2019, doi: 10.1007/s10207-019-00475-6.

[15] G. Vormayr, T. Zseby, and J. Fabini, “Botnet Communication Patterns,” vol. 19, no. 4, pp. 2768–2796, 2017.

[16] M. Monshizadeh, V. Khatri, and R. Kantola, “An adaptive detection and prevention architecture for unsafe traffic in SDN enabled mobile networks,” *Proc. IM 2017 - 2017 IFIP/IEEE Int. Symp. Integr. Netw. Serv. Manag.*, pp. 883–884, 2017, doi: 10.23919/INM.2017.7987395.

[17] W. Z. Khan, M. K. Khan, F. Bin Muhaya, and M. Y. Aalsalem, “A Comprehensive Study of Email Spam Botnet Detection,” no. c, 2015, doi: 10.1109/COMST.2015.2459015.

[18] K. Angrishi, “Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets,” pp. 1–17.

[19] A. H. Lashkari, G. D. Gil, M. S. I. Mamun, and A. A. Ghorbani, “Characterization of tor traffic using time based features,” *ICISSP 2017 - Proc. 3rd Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2017-Janua, no. Cic, pp. 253–262, 2017,

doi: 10.5220/0006105602530262.

[20] M. Mursalin, Y. Zhang, Y. Chen, and N. V. Chawla, “Automated epileptic seizure detection using improved correlation-based feature selection with random forest classifier,” *Neurocomputing*, vol. 241, no. February, pp. 204–214, 2017, doi: 10.1016/j.neucom.2017.02.053.

[21] Y. Pristyanto, S. Adi, and A. Sunyoto, “The effect of feature selection on classification algorithms in credit approval,” *2019 Int. Conf. Inf. Commun. Technol. ICOIACT 2019*, pp. 451–456, 2019, doi: 10.1109/ICOIACT46704.2019.8938523.

[22] A. S. Nugroho, “Pengantar Support Vector Machine ∗,” *J. Data Mining, Jakarta*, p. 3, 2007.

[23] S. Kilgallon, L. De La Rosa, and J. Cavazos, “Improving the effectiveness and efficiency of dynamic malware analysis with machine learning,” *Proc. - 2017 Resil. Week, RWS 2017*, pp. 30–36, 2017, doi: 10.1109/RWEEK.2017.8088644.

[24] G. Kirubavathi and R. Anitha, “Structural analysis and detection of android botnets using machine learning techniques,” *Int. J. Inf. Secur.*, vol. 17, no. 2, pp. 153–167, 2018, doi: 10.1007/s10207-017-0363-3.

[25] S. Su, Y. Sun, X. Gao, J. Qiu, and Z. Tian, “A correlation-change based feature selection method for IoT equipment anomaly detection,” *Appl. Sci.*, vol. 9, no. 3, 2019, doi: 10.3390/app9030437.

LAMPIRAN

Komparasi Pada Klasifikasi Trafik Serangan Malware Botnet Dengan Metode Support Vector Machine (SVM)

ORIGINALITY REPORT

9%	2%	1%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Sriwijaya University Student Paper	7%
2	repositori.usu.ac.id Internet Source	1%
3	digilib.unimed.ac.id Internet Source	1%
4	repository.its.ac.id Internet Source	1%

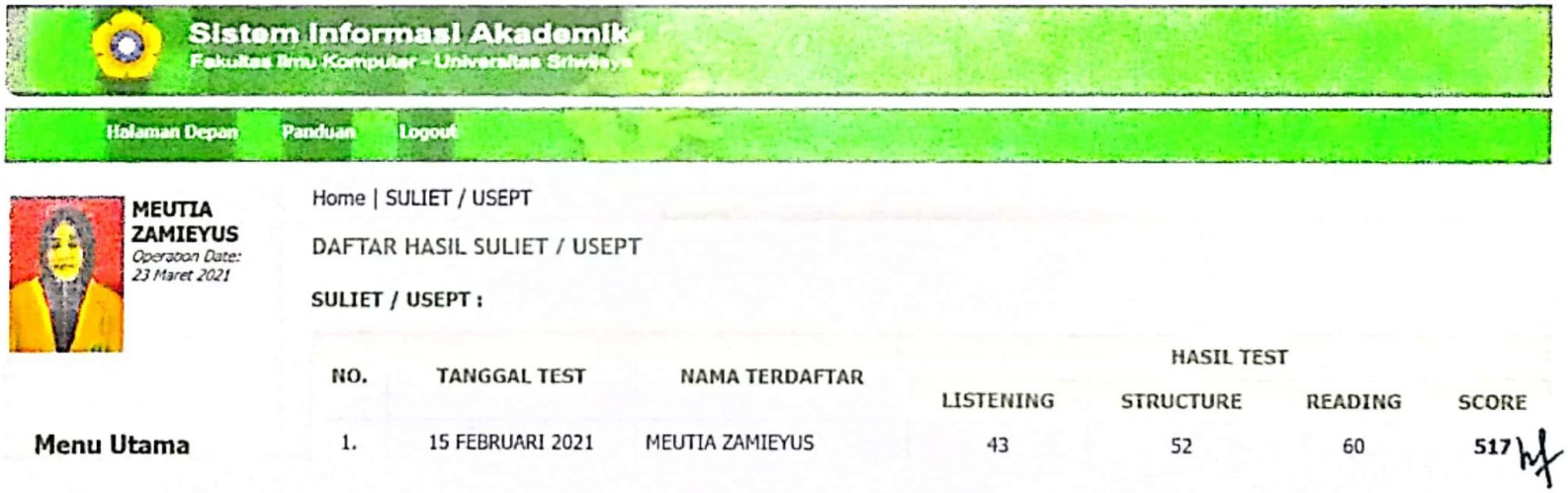
Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		

VERIFIKASI HASIL SULIET

NAMA : Meutia Zamieyus

NIM : 09011181722018

JURUSAN/PRODI : Sistem Komputer



NO.	TANGGAL TEST	NAMA TERDAFTAR	HASIL TEST			
			LISTENING	STRUCTURE	READING	SCORE
1.	15 FEBRUARI 2021	MEUTIA ZAMIEYUS	43	52	60	517

Mengetahui,

Kasubbag Akademik dan Kemahasiswaan

Samanigh Nainggolan, S.E.

NIP. 196309081984032002

Indralaya, 09 April 2021

Mahasiswa,

Meutia Zamieyus

NIM. 09011181722018

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER
Jalan Palembang – Prabumulih Km. 32 Indralaya Kabupaten Ogan Ilir Kode Pos 30662
Telepon (0711)7072729, 379249, 581700 Faksimili (0711) 379248, 581710
Pos-el : info@ilkom.unsri.ac.id

FORM PERBAIKAN UJIAN SKRIPSI (TUGAS AKHIR II)

Nama Mahasiswa	: Meutia Zamieyus
NIM	: 09011181722018.
Jurusan	: Sistem Komputer
Hari / Tanggal	: Kamis / 17 Juni 2021
Waktu	: 14:30 s.d 15:00 WIB
Judul Tugas Akhir	: Komparasi pada Klasifikasi Trafik Serangan Malware Botnet dengan Metode Support Vector Machine (SVM)
Pembimbing	: Deris Stiawan, M.T., Ph.D

Perbaikan/Saran :

Jangka Waktu Perbaikan :

Telah diperbaiki sesuai dengan saran dan koreksi tim penguji ujian komprehensif.

No.	Nama Penguji	Status Penguji	Tanda Tangan
1.	Ahmad Heryanto, M.T	Penguji	

Palembang, 17 Juni 2021
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP 196612032006041001

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER
Jalan Palembang – Prabumulih Km. 32 Indralaya Kabupaten Ogan Ilir Kode Pos 30662
Telepon (0711)7072729, 379249, 581700 Faksimili (0711) 379248, 581710
Pos-el : info@ilkom.unsri.ac.id

FORM PERBAIKAN UJIAN SKRIPSI (TUGAS AKHIR II)

Nama Mahasiswa	: Meutia Zamieyus
NIM	: 09011181722018.
Jurusan	: Sistem Komputer
Hari / Tanggal	: Kamis / 17 Juni 2021
Waktu	: 14:30 s.d 15:00 WIB
Judul Tugas Akhir	: Komparasi pada Klasifikasi Trafik Serangan Malware Botnet dengan Metode Support Vector Machine (SVM)
Pembimbing	: Deris Stiawan, M.T., Ph.D

Perbaikan/Saran :

Jangka Waktu Perbaikan :

Telah diperbaiki sesuai dengan saran dan koreksi tim penguji ujian komprehensif.

No.	Nama Penguji	Status Penguji	Tanda Tangan
1.	Deris Stiawan, M.T., Ph.D	Pendamping (Pembela)	

8/7/21
Palembang, ~~17 Juni~~ 2021
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP 196612032006041001