VISUALISASI SERANGAN *MALWARE SPYWARE* DENGAN MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE* (SVM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH:

ZARAH FITRIANI

09011381924093

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

VISUALISASI SERANGAN *MALWARE SPYWARE* DENGAN MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE* (SVM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh:

ZARAH FITRIANI

09011381924093

Palembang, 16 Juni 2023

Mengetahui,

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Kamis

Tanggal : 25 Mei 2023

Tim Penguji

1. Ketua : Ahmad Fali Oklilas, M.T
2. Sekretaris : Nurul Afifah, M.Kom
3. Pembimbing : Deris Stiawan, M.T., Ph.D
4. Penguji : Ahmad Heryanto, M.T

Mengetahui, 16/6/23

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini

Nama : Zarah Fitriani

NIM : 09011381924093

Judul : Visualisasi Serangan Malware *Spyware* Dengan Menggunakan Metode *Support Vector Machine* (SVM)

Hasil Pengecekan Plagiat/Turnitin: 8%

Menyatakan bahwa laporan tugas akhir ini adalah hasil karya saya sendiri dan tidak mengandung unsur penjiplakan atau plagiat. Saya sepenuhnya menyadari bahwa jika terbukti adanya penjiplakan atau plagiat dalam laporan tugas akhir ini, saya siap menerima sanksi akademik dari Universitas Sriwijaya. Pernyataan ini saya buat dengan kesadaran penuh dan tanpa adanya paksaan dari pihak manapun.

Palembang, Juni 2023

Yang menyatakan

Zarah Fitriani

NIM. 09011381924093

MOTTO DAN PERSEMBAHAN

"Dan barang siapa bertakwa kepada Allah, niscaya Allah menjadikan baginya kemudahan dalam urusannya"

Q.S At-Talaq:4

"The only way to do great work is to love what you do"

D.O – EXO

"Tidak ada rahasia untuk sukses. Semuanya adalah hasil dari persiapan, kerja keras dan belajar dari kegagalan"

Colin Powell

Skripsi ini saya persembahkan untuk:

Saya dengan tulus ingin mengungkapkan persembahan yang mendalam kepada orang tua tercinta saya. Tanpa kehadiran, dukungan, dan cinta tanpa syarat dari kalian, saya tidak akan pernah sampai pada tahap ini dalam menyelesaikan skripsi saya. Terima kasih atas semua doa, dorongan, dan pengorbanan yang kalian berikan untuk menjadikan saya pribadi yang lebih baik. Terima kasih juga karena kalian selalu menjadi sumber inspirasi dan motivasi terbesar bagi saya. Skripsi ini adalah bukti cinta dan dedikasi saya kepada kalian. Semoga persembahan ini dapat sedikit mewakili rasa terima kasih dan penghargaan saya kepada kedua orang tua tercinta yang selalu ada di sisi saya.

KATA PENGANTAR

Assalamu'alaikum Warrahmatulahi Wabarakatuh.

Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul "Visualisasi Serangan Malaware *Spyware* Dengan Menggunakan Metode *Support Vector Machine* (SVM)".

Dalam penelitian ini penulis menjelaskan mengenai visualsasi malware jenis *spyware Transponder* dengan menggunakan Metode *Support Vector Machine* (SVM) beserta hasil penelitian yang penulis lakukan. Penulis berharap tulisan ini dapat bermanfaat bagi orang banyak serta dapat menambah wawasan bagi pembaca.

Pada kesempatan ini, dengan segala kerendahan hati penulis mengucapkan rasa syukur kepada Allah SWT dan rasa terima kasih kepada semua pihak yang telah memberikan dukungan serta bimbingan dalam menyelesaikan Tugas Akhir ini, antara lain:

1. Allah SWT yang memberikan nikmat kemudahan, kesehatan dan kesempatan dalam melaksanakan Tugas Akhir ini.
2. Kedua orang tua tercinta, saudara dan keluarga besar yang selalu mendo'akan dan selalu memberi motivasi, dukungan baik moral, material dan spritual.
3. Bapak Jaidan Jauhari, S.Pd.,M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, M.T., Ph.D., IPU., ASEAN ENG. selaku Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya dalam membimbing, memberikan petunjuk, dan saran kepada penulis dalam penyusunan Tugas Akhir.

6. Bapak Ahmad Zarkasi M.T., selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer.
7. Mbak Sari Nuzulastri selaku Admin Jurusan Sistem Komputer yang telah membantu administrasi dalam menyelesaikan Tugas Akhir.
8. Mbak Nurul Afifah M.Kom yang selalu memberikan masukan dan saran kepada Tim Riset Malware *Spyware* (*Spyware-Transpoonder)*
9. Grup Riset COMNETS.
10. Dio Novaldo *support system* terbaik saya yang selalu mendukung dan menghibur saya serta selalu memberikan semangat dalam hal perkuliahan.
11. Amelia Pramudita dan sartika yang selalu berjuang bersama selama penyusunan laporan skripsi.
12. Almamater.

Penulis menyadari bahwa penulisan Tugas Akhir ini masih jauh dari kesempurnaan, oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun demi kesempurnaan Tugas Akhir ini dan semoga bermanfaat bagi kita semua baik dalam dunia Pendidikan maupun dalam lingkungan masyarakat.

Wassalamu'alaikum Warrahmatulahi Wabarakatuh.

Palembang, Juni 2023

Penulis

Zarah Fitriani

09011381924093

VISUALISASI SERANGAN MALWARE *SPYWARE* DENGAN MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE (*SVM)

ZARAH FITRIANI (09011381924093)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: zarahfitrianitkj1@gmail.com

ABSTRAK

Serangan malware *spyware* merupakan ancaman yang signifikan terhadap perangkat keras komputer dan privasi penguna. Untuk menganalisis dan mempermudah mengenali serangan tersebut dengan efektif, teknik visualisasi dapat memberikan wawasan yang berharga tentang pola dan karakteristiknya. Penelitian ini menggunakan algoritma *machine learning* yaitu *Support Vector Machine* (SVM). Dataset yang digunakan penelitian ini dari CIC MalMem 2022 yaitu data *benign* dan *spyware Transponder*. Seleksi fitur diterapkan pada penelitian ini untuk mengidentifikasi fitur-fitur yang paling relevan dalam membedakan antara data normal dan serangan. Hasil yang didapatkan menggunakan model SVM dengan 3 kernel SVM yaitu Linear, Polynomial dan *Radial Basis Function* (RBF). Berdasarkan validasi dari proses klasifikasi menggunakan kernel SVM mendapatkan hasil yang cukup tinggi, dimana dengan kernel Linear mendapatkan hasil akurasi yang paling unggul yaitu untuk 8 fitur akurasi 99.53%, 15 fitur akurasi 99.77% dan 24 fitur akurasi 99.96%.

Kata Kunci: *Spyware*, Visualisasi, *Support Vector Machine* (SVM), *Confusion Matrix*

VISUALIZATION OF MALWARE SPYWARE ATTACKS USING SUPPORT VECTOR MACHINE (SVM) METHOD

ZARAH FITRIANI (09011381924093)

Department of Computer Systems, Faculty of Computer Science,

University Sriwijaya

Email: zarahfitrianitkj1@gmail.com

ABSTRACT

Spyware malware attacks are a significant threat to computer hardware and user privacy. To analyze and make it easier to recognize such attacks effectively, visualization techniques can provide valuable insights into their patterns and characteristics. This research using a machine learning algorithm, Support Vector Machine (SVM). The dataset used in this study is from the CIC MalMem 2022 which is benign data and spyware Transponder. Feature selection was applied to this study to identify the features that were most relevant in distinguishing between normal data and attacks. The results obtained using the SVM model with 3 SVM kernels are Linear, Polynomial, and Radial Basis Function (RBF). Based on the validation of the classification process using the SVM kernel got quite high results, where the Linear kernel got the most superior accuracy results, for 8 features accuracy that is 99.53%, 15 features accuracy is 99.77% and 24 features accuracy is 99.96%.

***Keyword**: Spyware, Visualization, Support Vector Machine (SVM), Confusion Matrix*

DAFTAR ISI

LEMBAR PENGESAHAN i

HALAMAN PERSETUJUAN ii

HALAMAN PERNYATAAN..... iii

MOTTO DAN PERSEMBAHAN..... iv

KATA PENGANTAR..... v

ABSTRAK vii

ABSTRACT..... viii

DAFTAR ISI..... viii

DAFTAR GAMBAR..... xii

DAFTAR TABEL xiv

BAB I PENDAHULUAN..... 1

1.1 Latar Belakang 1

1.2 Rumusan Masalah 3

1.3 Tujuan..... 3

1.4 Manfaat..... 4

1.5 Batasan Masalah..... 4

1.6 Metodologi Penelitian 5

1.7 Sistematika Penulisan..... 5

BAB II TINJAUAN PUSTAKA..... 7

2.1 Penelitian Terdahulu..... 7

2.2 Malware..... 11

2.3 *Spyware* 12

2.2.1 *Spyware Transponder* 15

2.4 *Machine Learning* 16
2.5 *Support Vector Machine* (SVM) 16
2.6 *Kernel SVM* 18
2.7 Google Colaboratory 19
2.8 *Correlation Based Feature Selection* 19
2.9 *Confusion Matrix* 19
2.10 Dataset CIC-MalMem-2022 21
BAB III METODELOGI PENELITIAN 23
3.1 Pendahuluan 23
3.2 Kerangka Kerja Penelitian 23
3.3 Perancangan Sistem 24
3.3.1 Kebutuhan Perangkat Lunak 25
3.3.2 Kebutuhan Perangkat Keras 26
3.4 Persiapan Dataset 26
3.5 Seleksi Fitur 30
3.6 Data *Preprocessing* 30
3.7 *Support Vector Machine (SVM)* 31
3.8 Skenario Percobaan 31
3.9 Visualisasi 32
3.10 Validasi 33
BAB IV HASIL DAN ANALISA 34
4.1 Pendahuluan 34
4.2 Pengolahan Dataset 34
4.3 Analisa Hasil Visualisasi 36
4.3.1 Dataset *Benign* dan *Spyware-Transponder* 36

4.3.2 *Correlation Based Feature Selection* 37
4.3.3 Visualisasi *Benign* dan *Spyware-Transponder* 45
4.4 Hasil Validasi Kernel RBF 47
4.5 Hasil Validasi Kernel Linear 49
4.6 Hasil Validasi Kernel Polynomial 50
4.7 Analisa Hasil Validasi Perhitungan Manual 52
4.7.1 Kernel RBF 8 Fitur 52
4.7.2 Kernel RBF 15 Fitur 54
4.7.3 Kernel RBF 24 Fitur 55
4.7.4 Kernel Linear 8 Fitur 57
4.7.5 Kernel Linear 15 Fitur 58
4.7.6 Kernel Linear 24 Fitur 60
4.7.7 Kernel Polynomial 8 Fitur 61
4.7.8 Kernel Polynomial 15 Fitur 63
4.7.9 Kernel Polynomial 24 Fitur 64
4.8 Hasil Grafik Perbandingan antar Kernel SVM 66
BAB V KESIMPULAN DAN SARAN 70
5.1 Kesimpulan 70
5.2 Saran 71
DAFTAR PUSTAKA 72

DAFTAR GAMBAR

Gambar 2.1 Klasifikasi dua kelas “+1”, “-1” dan *margin hyperplane* 17

Gambar 3.1 Kerangka Kerja Penelitian 23

Gambar 3.2 Perancangan Sistem 24

Gambar 4.1 Dataset CIC-MalMem 2022 33

Gambar 4.2 Pemfilteran Dataset 34

Gambar 4.3 Visualisasi data *benign* dan data *spyware-Transponder* 35

Gambar 4.4 Visualisasi kolerasi antar fitur 36

Gambar 4.5 Visualisasi dari fitur – fitur dengan poin tertinggi dari >0.6 39

Gambar 4.6 Visualisasi dari fitur – fitur dengan poin tertinggi dari >0.5 41

Gambar 4.7 Visualisasi dari fitur – fitur dengan poin tertinggi dari >0.4 43

Gambar 4.8 Visualisasi *Parallel Coordinates* 8 fitur 44

Gambar 4.9 Visualisasi *Parallel Coordinates* 15 fitur 45

Gambar 4.10 Visualisasi *Parallel Coordinates* 24 fitur 45

Gambar 4.11 Confusion Matrix Kernel RBF 8 Fitur 51

Gambar 4.12 Confusion Matrix Kernel RBF 15 Fitur 53

Gambar 4.13 Confusion Matrix Kernel RBF 24 Fitur 54

Gambar 4.14 Confusion Matrix Kernel Linear 8 Fitur 56

Gambar 4.15 Confusion Matrix Kernel Linear 15 Fitur 57

Gambar 4.16 Confusion Matrix Kernel Linear 24 Fitur 59

Gambar 4.17 Confusion Matrix Kernel Polynomial 8 Fitur..... 60

Gambar 4.18 Confusion Matrix Kernel Polynomial 15 Fitur..... 62

Gambar 4.19 Confusion Matrix Kernel Polynomial 24 Fitur..... 63

Gambar 4.20 Hasil Grafik Perbandingan antar Kernel SVM 8 Fitur 65

Gambar 4.21 Hasil Grafik Perbandingan antar Kernel SVM 15 Fitur 68

Gambar 4.22 Hasil Grafik Perbandingan antar Kernel SVM 24 Fitur 67

DAFTAR TABEL

Tabel 2.1 Tabel Penelitian Terdahulu 7

Tabel 2.2 Jenis – Jenis *Spyware* 13

Tabel 2.3 *Confusion Matrix*..... 19

Tabel 2.4 Pengelompokan Keluarga Malware 21

Tabel 3.1 Spesifikasi Perangkat Lunak 24

Tabel 3.2 Spesifikasi Perangkat Keras 25

Tabel 3.3 Fitur dataset CIC-MalMem-2022 26

Tabel 3.4 *Class Name* and *Numeric Label* 30

Tabel 3.5 Skenario Percobaan 31

Tabel 4.1 Feature Selection Metode CBS 36

Tabel 4.2 8 Fitur dengan poin >0.6 38

Tabel 4.3 15 Fitur dengan poin >0.5 40

Tabel 4.4 24 Fitur dengan poin >0.4 42

Tabel 4.5 Hasil Kernel RBF 8 Fitur 46

Tabel 4.6 Hasil Kernel RBF 15 Fitur 47

Tabel 4.7 Hasil Kernel RBF 24 Fitur 47

Tabel 4.8 Hasil Kernel Linear 8 Fitur 48

Tabel 4.9 Hasil Kernel Linear 15 Fitur 48

Tabel 4.10 Hasil Kernel Linear 24 Fitur 49

Tabel 4.11 Hasil Kernel Polynomial 8 Fitur 49

Tabel 4.12 Hasil Kernel Polynomial 15 Fitur 50

Tabel 4.13 Hasil Kernel Polynomial 24 Fitur 50

Tabel 4.14 Validasi tertinggi antar kernel SVM 68

BAB I

PENDAHULUAN

1.1 Latar Belakang

Ancaman utama pada keamanan di internet adalah malware, yang dapat muncul sebagai kode berbahaya atau dalam berbagai bentuk. Malware merupakan perangkat lunak yang dirancang untuk menggangu operasi normal, mengumpulkan data pribadi tanpa persetujuan pengguna atau mengizinkan akses tidak sah ke sumber daya sistem. Para pencipta atau pembuat malware dapat memanfaatkan kerentanan dalam mekanisme keamanan jaringan dan sistem untuk menyerang target mereka[1]. Malware dengan tujuan merusak perangkat keras komputer dan penggunanya, baik secara aktif maupun pasif. Malware diklasifikasikan pada tingkat yang sangat tinggi berdasarkan prilakunya[2]. Berbagai jenis malware seperti *Virus*, *Worm, Adware*, *Spyware*, *Trojan Horse*, *Scareware* dan varian lainnya yang berbahaya yang digunakan untuk merusak sistem. Dengan aktivitas jahat yang selalu meningkat dari hari ke hari, kita perlu memperhatikan informasi dan keamanan data pribadi[3].

Spyware adalah ancaman serius bagi keamanan komputer saat ini. Internet, sebagian besar digunakan untuk login secara jarak jauh ke server yang menampung data dan aplikasi sensitive. *Sypware* merupakan kategori malware yang berbahaya yang mempengaruhi kerahasiaan dan privasi pengguna[4]. Pertama kali istilah "*spyware"* digunakan oleh *Microsoft* pada tanggal 16 oktober 1995. Pada tahun 2005 AOL melakukan penelitian yang mengungkapkan 61% komputer mengandung *spyware,* sementara 92% pengguna tidak menyadari keberadaanya di komputer pribadi mereka. Pada tahun 2013 diperkirakan ada 116 juta komputer yang terinfeksi malware. Tahun 2014 lab keamanan Google melaporkan bahwa serangan *spyware* telah meningkat secara signifikan. Alasan utama peningkatan ini adalah karena perangkat lunak ini memiliki kemampuan untuk berubah dan muncul dalam bentuk baru saat masih berfungsi[5].

Pada penelitian sebelumnya[6] membahas tentang pendeteksian malware *spyware* dengan menggunakan teknik mining. Algoritma *supervised learning* digunakan untuk mengklasifikasikan pola *spyware.* Penelitian ini menjelaskann tentang berbagai pola desain antisecurity yang dapat digunakan sebagai metrik untuk mendeteksi *spyware.*

Pada penelitian sebelumnya[7] menggunakan metode *Support Vector Machine* (SVM) untuk menglasifikasikan malware yang telah dikumpulkan dari jaringan langsung. Pada penelitian yang telah dilakukan menggunakan tiga teknik validasi yaitu Cross Validation, Leave-One-Out and Random Sampling. Hasilnya didapatkan akurasi klasifikasi adalah sekitar 94%, *sensitivity* dari 97% sampai 98% dan *specificity* dari 86% sampai 90%.

Pada penelitian sebelumnya[8] dilakukan klasifikasi biner dengan pendekatan big data untuk mendeteksi malware menggunakan dataset CIC-MalMem-2022 seimbang yang berisi data analisis memori. Penelitian dilakukan dengan menggunakan platform big data *Apache Spark* di Google Colab. Model klasifikasi dibuat menggunakan sembilan *machine learning* and *deep learning*. Hasil dari akurasi masing- masing algoritma tersebut untuk *Decision Tree* dengan akurasi 99.79%, *Random Forest* dengan akurasi 99.90%, Naïve Bayes dengan akurasi 98.41%, *Logistic Regression* dengan akurasi 99.97%, *Gradient Boosted Tree* dengan akurasi 99.94%, Linear SVC dengan akurasi 99.14%, MLP dengan akurasi 97.67%, DNN dengan akurasi 99.56% dan LSTM dengan akurasi 99.43%.

Pada penelitian sebelumnya[9] model deteksi malware yang dikaburkan yang mengekstraksi fitur dari dump memori menggunakan VolMemLyzer. Dataset MalMemAnalysis 2022 dibuat untuk menguji dan mengevaluasi kerangka kerja, dengan fokus pada simulasi malware yang disamarkan dengan mengeksekusi sampel malware dari tiga kategori utama, *Spyware, Ransomware,* dan *Trojan Horse.* Hasil dari penelitian ini algortima *Random Forest* akurasi 97%, *Naïve Bayes* akurasi 92%, KNN dengan akurasi 95%, *Decision Tree* akurasi 97% dan *Support Vector Machine* (SVM) akurasi 90%.

Support Vector Machine (SVM) adalah metode berbasis kernel yang sering digunakan untuk mengklasifikasikan biner, untuk menganalisis data berdimensi

tinggi, kompleks dan terperinci serta untuk menentukan pola. SVM memiliki kekuatan dan fleksibilitas yang besar dengan banyak keuntungan, termasuk kemampuan untuk beroperasi dalam ruang fitur berdimensi tinggi, kemampuan untuk menangani outlier dengan baik, kemampuan untuk memodelkan hubungan non-linier antara variabel, kemampuan yang baik dalam generalisasi serta penggunaan memori yang efisien. SVM memiliki generalisasi berkualitas tinggi untuk masalah klasifikasi biner[10].

Visualisasi merupakan teknik untuk mempresentasikan banyaknya serangan *spyware* yang ada pada dataset yang telah disediakan oleh *Canadian Institute For Cybersecurity* (CIC). Berdasarkan penjelasan sebelumnya sehingga penulis akan membahas mengenai visualisasi serangan malware *spyware* dengan menggunakan dataset yang sudah berformat .csv. Selanjutnya pada penelitian ini menggunakan algoritma *Support Vector Machine* (SVM) untuk mengklasifikasikan malware dan mengenali data tersebut ke bentuk gambar visual yang komplek. Dari hasil klasifikasi yang telah dilakukan dengan menggunakan algortima *Support Vector Machine* (SVM) akan divisualisasikan ke dalam bentuk diagram garis. Diagram garis tersebut akan digunakan untuk membantu mengidentifikasi dan menyimpulkan serangan yang terjadi agar mudah di pahami.

1.2 Rumusan Masalah

Perumusan masalah dari penelitian Tugas Akhir ini adalah Penelitian ini akan membahas bagaimana cara mengklasifikasikan data *benign* dan data *spyware Transponder* dengan metode *Support Vector Machine* serta bagaimana memvisualisasikan serangan *spyware Transponder* tersebut kedalam bentuk visual gambar yang menarik dan mudah dipahami.

1.3 Tujuan

Adapun tujuan dari penelitian Tugas Akhir ini adalah sebagai berikut:

1. Memvisualisasikan dan mengelompokan data *benign* dan data *spyware Transponder* dalam diagram *parallel coordinates*.

2. Menerapkan algoritma *Support Vector Machine* (SVM) untuk mengklasifikasikan data *benign* dan data *spyware Transponder.*
3. Visualisasi data *spyware Transponder* dapat memudahkan dalam mengenali serangan *spyware* yang ada.
4. Menggunakan metode *Correlation Based Feature Selection* untuk memilih fitur yang relavan agar mendapatkan hasil akhir yang baik dan akurat.

1.4 Manfaat

1. Dapat mempelajari penerapan algoritma *Support Vector Machine* (SVM) dalam pengklasifikasian malware.
2. Dapat melakukan proses klasifikasi dataset malware *spyware Transponder* dan *benign.*
3. Dapat mempersingkat waktu proses komputasi dengan fitur seleksi
4. Dapat memvisualiasikan dan menjelaskan data dalam bentuk diagram garis agar berupa informasi yang mudah dipahami.

1.5 Batasan Masalah

Adapun batasan masalah pada penelitian Tugas Akhir ini adalah sebagai berikut:

1. *Malware yang* digunakan adalah jenis *spyware Transponder.*
2. Menggunakan dataset dari *Canadian Institute for Cybersecurity* (CIC) yaitu CICMalMem2022.
3. Algoritma yang digunakan dalam visualisasi *spyware Transponder* yaitu algoritma *Support Vector Machine* (SVM) serta menggunakan *parallel coordinates* untuk tampilan visual data normal dan data serangan.
4. Tidak membahas mengenai pencegahan terhadap serangan yang ada pada *spyware Transponder.*

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian Tugas Akhir ini akan melewati beberapa tahapan sebagai berikut:

1. **Studi Pustaka/ Literatur**

   Tahap ini dilakukan setelah memastikan bahwa masalah yang akan diteliti relavan dan sesuai untuk dijadikan sebagai penelitian, dengan membaca literature yang sesuai dengan topik penelitian dan mencari dataset yang akan digunakan.

2. **Pengolahan Data**

   Pada tahap ini membahas proses bagaimana mengolah suatu data mentah menjadi siap olah, memvisualisasikan data, serta menerapkan metode pada sistem tugas akhir.

3. **Visualisasi**

   Pada tahap ini dilakukan proses visualisasi data *spyware Transponder* dan data *benign* dengan menggunakan algortima *Support Vector Machine* (SVM). Setelah proses visualisasi selesai, dilanjutkan pada proses validasi.

4. **Analisa**

   Setelah mendapatkan data dari tahap visualisasi, langkah selanjutnya adalah menganalisis hasil yang telah didapatkan sebelumnya untuk didapatkan hasil yang objektif.

5. **Kesimpulan dan Saran**

   Tahap terakhir adalah membuat kesimpulan dari permasalahan, studi pustaka, metodelogi, dan analisa hasil visualisasi. Selain itu beberapa saran yang dapat dijadikan penelitian selanjutnya.

1.7 Sistematika Penulisan

Adapun sistematika penulisan dalam penelitian Tugas Akhir ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Bab ini memberikan penjelasan mengenai dasar-dasar topik penelitian yang meliputi latar belakang, tujuan, manfaat, rumusan masalah, metodologi penelitian, dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini berisi landasan dasar-dasar teori yang berkaitan dengan inti pembahasan dari penelitian ini. Dasar teori ini mengenai tentang *malware* dll, serta metode *Support Vector Machine (SVM)* yang diterapkan.

BAB III. METODOLOGI PENELITIAN

Bab ini menguraikan proses penelitian secara sistematis. Penjelasan dalam subbab ini mencakup tahapan pengaturan sistem dan penerapan metode pada sistem dalam penelitian ini.

BAB IV. HASIL DAN ANALISIS

Bab ini berisi penjelasan mengenai hasil dari pengujian metode sistem, termasuk proses pengujian dan analisis visual dari data yang diperoleh.

BAB V. KESIMPULAN DAN SARAN

Bab ini menjelaskan tentang kesimpulan yang di dapat dari penelitian, serta menanggapi tujuan yang hendak dicapai seperti yang tertera pada BAB I, dan memberikan saran untuk penelitan selanjutnya.

DAFTAR PUSTAKA

[1] M. Wadkar, F. Di Troia, and M. Stamp, “Detecting malware evolution using support vector machines,” *Expert Syst. Appl.*, vol. 143, p. 113022, 2020, doi: 10.1016/j.eswa.2019.113022.

[2] V. C. D and A. K. S, “Impact of Malware in Modern Society,” *Int. J. Sci. Res. Eng. Dev.*, vol. 2, no. 3, pp. 593–600, 2019, [Online]. Available: www.ijsred.com

[3] A. Makandar and A. Patrot, “Malware *Class* recognition using image processing techniques,” *2017 Int. Conf. Data Manag. Anal. Innov. ICDMAI 2017*, pp. 76–80, 2017, doi: 10.1109/ICDMAI.2017.8073489.

[4] G. Shaw, “Spyware & Adware: The Risks facing Businesses,” *Netw. Secur.*, vol. 2003, no. 9, pp. 12–14, 2003, doi: 10.1016/S1353-4858(03)00908-5.

[5] H. M. Salih and M. S. Mohammed, “Spyware Injection in Android using Fake Application,” *Proc. 2020 Int. Conf. Comput. Sci. Softw. Eng. CSASE 2020*, pp. 100–105, 2020, doi: 10.1109/CSASE48920.2020.9142101.

[6] M. . NarasimaMallikarajunan.K., Preethi.S.R, Selvalakshmi.S, and Nithish.N, “DETECTION OF SPYWARE IN SOFTWARE,” no. Icoei, pp. 1138–1142, 2019.

[7] M. Kruczkowski and E. Niewiadomska-Szynkiewicz, “Support vector machine for malware analysis and *Class*ification,” *Proc. - 2014 IEEE/WIC/ACM Int. Jt. Conf. Web Intell. Intell. Agent Technol. - Work. WI-IAT 2014*, vol. 2, pp. 415–420, 2014, doi: 10.1109/WI-IAT.2014.127.

[8] M. Dener, G. Ok, and A. Orman, “applied sciences Malware Detection Using Memory Analysis Data in Big Data Environment,” 2022.

[9] T. Carrier, P. Victor, and A. Tekeoglu, “Detecting Obfuscated Malware using Memory Feature Engineering,” no. Icissp, pp. 978–989, 2022, doi: 10.5220/0010908200003120.

[10] L. Mohan, “Support Vector Machine Accuracy Improvement with *Class*ification,” pp. 1–5, 2020, doi: 10.1109/CICN.2020.85.

[11] S. Ni, Q. Qian, and R. Zhang, “Malware identification using visualization

images and deep learning," *Comput. Secur.*, vol. 77, pp. 871–885, 2018, doi: 10.1016/j.cose.2018.04.005.

[12] X. Liu, J. Zhang, Y. Lin, and H. Li, "ATMPA: Attacking machine learning-based malware visualization detection methods via adversarial examples," *Proc. Int. Symp. Qual. Serv. IWQoS 2019*, no. Ml, 2019, doi: 10.1145/3326285.3329073.

[13] I. Baptista, S. Shiaeles, and N. Kolokotronis, "A Novel Malware Detection System Based On Machine Learning and Binary Visualization," *2019 IEEE Int. Conf. Commun. Work. (ICC Work.*, pp. 1–6, 2019.

[14] D. Javaheri, M. Hosseinzadeh, and A. M. Rahmani, "Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines," *IEEE Access*, vol. 6, pp. 78321–78332, 2018, doi: 10.1109/ACCESS.2018.2884964.

[15] W. Kuo and C. Wang, "Study on Android Hybrid Malware Detection Based on Machine Learning," *2019 IEEE 4th Int. Conf. Comput. Commun. Syst.*, pp. 31–35, 2019.

[16] G. Tyagi, K. Ahmad, and M. N. Doja, "A novel framework for password securing system from key-logger spyware," *Proc. 2014 Int. Conf. Issues Challenges Intell. Comput. Tech. ICICT 2014*, pp. 70–74, 2014, doi: 10.1109/ICICICT.2014.6781255.

[17] S. Hinde, "Spyware: The spy in the computer," *Comput. Fraud Secur.*, vol. 2004, no. 12, pp. 15–16, 2004, doi: 10.1016/S1361-3723(05)70185-8.

[18] A. Gorlin, "The ghost in the machine," *Surrealism Archit.*, no. January, pp. 103–119, 2004, doi: 10.4324/9780203339541.

[19] T. Mjømen, "Assessing countermeasures against spyware," 2005.

[20] G. Mahajan, B. Saini, and S. Anand, "Algorithms and Tools," *2019 Second Int. Conf. Adv. Comput. Commun. Paradig.*, pp. 1–8, 2019.

[21] W. J. Melssen, L. M. C. Buydens, and B. Ust, "Visualisation and interpretation of Support Vector Regression models," vol. 595, pp. 299–309, 2007, doi: 10.1016/j.aca.2007.03.023.

[22] M. Kruczkowski, "Support Vector Machine for malware analysis and

*Class*ification," 2014, doi: 10.1109/WI-IAT.2014.127.

[23] P. Rai, "Kernel Methods and Nonlinear *Class*ification Piyush Rai Kernel Methods : Motivation Often we want to capture nonlinear patterns in the data," vol. 2011, 2011.

[24] C. Campbell and Y. Ying, *Learning with Support Vector Machines*.

[25] B. Alt, M. Can, and B. Diri, "Engineering Applications of Arti fi cial Intelligence A corpus-based semantic kernel for text *Class*i fi cation by using meaning values of terms," vol. 43, pp. 54–66, 2015, doi: 10.1016/j.engappai.2015.03.015.

[26] A. Zaiem and N. Charibaldi, "Komparasi Fungsi Kernel Metode Support Vector Machine untuk Analisis Sentimen Instagram dan Twitter (Studi Kasus : Komisi Pemberantasan Korupsi)," vol. 9, no. 2, pp. 33–42, 2021.

[27] T. Carneiro, R. V Medeiros, D. A. Nóbrega, T. Nepomuceno, G. Bian, and V. H. C. D. E. Albuquerque, "Performance Analysis of Google Colaboratory as a Tool for Accelerating Deep Learning Applications," pp. 1–9, 2018, doi: 10.1109/ACCESS.2018.2874767.

[28] N. Gopika, "Correlation Based Feature Selection Algorithm for Machine Learning," *2018 3rd Int. Conf. Commun. Electron. Syst.*, no. Icces, pp. 692–695, 2018.

[29] S. J. Omar, K. N. Fred, and M. Richard, "Hybrid model of Correlation based Filter Feature Selection and Machine Learning *Class*ifiers applied on Smart Meter Data set," *2019 IEEE/ACM Symp. Softw. Eng. Africa*, pp. 1–10, 2019, doi: 10.1109/SEiA.2019.00009.

[30] X. Deng, Q. Liu, Y. Deng, and S. Mahadevan, "An improved method to construct basic probability assignment based on the confusion matrix for *Class*ification problem," *Inf. Sci. (Ny).*, 2016, doi: 10.1016/j.ins.2016.01.033.

[31] S. Venkatraman, "*Class*ification of Malware Using Visualisation of Similarity Matrices," 2017, doi: 10.1109/CCC.2017.11.