**DETEKSIDAN KLASIFIKASI SERANGAN MALWARE PADASENSOR PENGUKUR KUALITAS AIR DI*MOBILE SENSOR NETWORK* (MSN) DENGAN METODE *NAIVE BAYES***



**OLEH :**

**NURUL AFIFAH, S.KOM**

**09042611822001**

**PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

 **UNIVERSITAS SRIWIJAYA**

**2018**

**DETEKSIDAN KLASIFIKASI SERANGAN MALWARE PADA SENSOR PENGUKUR KUALITAS AIR DI *MOBILE SENSOR NETWORK* (MSN) DENGAN METODE *NAIVE BAYES***

# **HALAMAN JUDUL**

**PROPOSAL TESIS**

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Magister



**OLEH :**

**NURUL AFIFAH, S.KOM**

**09042611822001**

**PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

 **UNIVERSITAS SRIWIJAYA**

**2018**

# **LEMBAR PENGESAHAN**

**DETEKSI DAN KLASIFIKASI SERANGAN MALWARE PADA SENSOR PENGUKUR KUALITAS AIR DI *MOBILE SENSOR NETWORK* (MSN) DENGAN METODE *NAIVE BAYES***

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Magister

**Oleh :**

**NURUL AFIFAH, S.KOM**

**09042611822001**

Palembang, Mei 2018

****Pembimbing 1

**Deris Stiawan, M.T,. Ph.D**

NIP197806172006041002

**DAFTAR ISI**

[**HALAMAN JUDUL** i](#_Toc507588184)

[**LEMBAR PENGESAHAN** ii](#_Toc507588185)

[**DAFTAR ISI** iii](#_Toc507588187)

[**DAFTAR GAMBAR** v](#_Toc507588188)

[**DAFTAR TABEL** v](#_Toc507588189)i

[**BAB I PENDAHULUAN** 1](#_Toc507588190)

[1.1 Latar Belakang 1](#_Toc507588191)

[1.2 Perumusan Masalah 2](#_Toc507588192)

[1.3 Batasan Masalah 2](#_Toc507588193)

[1.4 Tujuan dan Manfaat Penelitian 3](#_Toc507588194)

[1.6 Sistematika Penulisan 3](#_Toc507588196)

[**BAB II TINJAUAN PUSTAKA** 5](#_Toc507588197)

[2.1 Studi Literature 5](#_Toc507588198)

[2.2 Deteksi Serangan Malware 6](#_Toc507588199)

[2.3 Algoritma Naive Bayes 8](#_Toc507588200)

[**BAB III METODE PENELITIAN** 9](#_Toc507588201)

[3.1 Kerangka Kerja 9](#_Toc507588202)

[3.2 Alur Kerja Metodologi Penelitian 11](#_Toc507588203)

[3.3 Kebutuhan Sistem 12](#_Toc507588204)

[3.3.1 Kebutuhan Hardware 12](#_Toc507588203)

[3.3.2 Kebutuhan Software 12](#_Toc507588203)

[3.4 Metode Machine Learning 12](#_Toc507588205)

[3.4.1 Disassemble file dataset malware 13](#_Toc507588203)

[3.4.2 Feature Extraction 13](#_Toc507588203)

[3.4.3 Feature Selection 14](#_Toc507588203)

[3.4.4 Klasifikasi malware menggunakan algoritma Naive Bayes 14](#_Toc507588203)

[3.5 Pengambilan Data 15](#_Toc507588202)

[3.6 Rencana Pengujian Data 16](#_Toc507588203)

[3.7Jadwal Penelitian 16](#_Toc507588204)

[**DAFTAR PUSTAKA** 17](#_Toc507588201)

**DAFTAR GAMBAR**

**Gambar**[**2.1** Proses Studi Literatur 5](#_Toc507588202)

**Gambar**[**3.1** Kerangka Kerja 10](#_Toc507588202)

**Gambar**[**3.2**Alur kerja metodologi penelitian 11](#_Toc507588202)

**Gambar** [**3.3**Diagram Alur proses machine learning 13](#_Toc507588202)

**Gambar** [**3.4**Diagram Proses Klasifikasi Naive Bayes 15](#_Toc507588202)

**DAFTAR TABEL**

**Tabel**[**2.1**Klasifikasi Topik Penelitian Tentang Malware 6](#_Toc507588202)

**Tabel**[**3.1** Kebutuhan Hardware 12](#_Toc507588202)

**Tabel**[**3.2** Kebutuhan Software 12](#_Toc507588202)

**Tabel**[**3.3** Rencana Jadwal Penelitian 16](#_Toc507588202)

# **BAB I**

# **PENDAHULUAN**

 Pendahuluan bab ini menjelaskan tentang latar belakang penelitian yang berjudul: “Deteksi dan Klasifikasi Serangan Malware Pada Sensor Pengukur Kualitas Air di*Mobile Sensor Network* (MSN) dengan Metode *Naive Bayes*”. Dari latar belakang tersebut dirumuskan suatu permasalahan agar permasalahan tidak meluas maka diberikan batasan masalah. Setelah mengetahui masalah, selanjutnya yang dilakukan adalah mengetahui tujuan dan manfaat dari penelitian yang dilakukan serta metodologi yang akan digunakan dalam penelitian ini.

## **1.1 Latar Belakang**

 Serangan malware pada sensor dapat berdampak buruk bagi kinerja dan hasil pengukuran sensor tersebut. Pada umumnya malware dapat menyerang karena adanya transmisi secara public (C.Lupu et al.,2015). Serangan malware dapat menimbulkan kerugian pada perangkat (E.Mwangi et al.,2017). Untuk meminimalisir kerugian dan masalah pada perangkat telah banyak teknik yang dapat mendeteksi malware (A.Souri et al.,2018). Teknik deteksi malware dibagi menjadi beberapa proses yaitu: yang pertama disassemble file, yang kedua feature extraction, dan yang ketiga yaitu feature selection (Yuxin et al.,2017).

 Keunggulan dari teknik pendeteksian serangan malware sebagian besar ditentukan oleh metode yang digunakan (E.Mwangi et al.,2017). Metode yang sering digunakan dalam pendeteksian malware adalah metode-metode machine learning seperti metode SVM, Naive Bayes, Random Forest, Decision Tree dan lainnya (A.Souri et al.,2018; Y.Chuang et al.,2015). Dari beberapa penelitian yang pernah dilakukan, metode Naive Bayes lebih banyak memiliki keunggulan dibanding metode lainnya (Zhang H et al.,2016). Metode Naive Bayes biasanya digunakan dalam menyelesaikan klasifikasi masalah (Zhang H et al.,2016). Dalam beberapa tahun terakhir telah banyak dilakukan penelitian-penelitian dalam teknik deteksi serangan malware dengan menggunakan metode Naive Bayes, salah satunya adalah penelitian yang dilakukan oleh (Stiawan, Sandra, Alzahrani, Budiarto, 2017) yang melakukan penelitian tentang analisis komparasi metode K-means dan Naive Bayes untuk visualisasi brute force attack. Metode Naive Bayes menggunakan perhitungan probabilitas dan statistik yaitu teorema bayes yang merupakan teorema dalam statistika untuk menghitung peluang, Bayes optimal classifier menghitung peluang dari satu kelas dari masing-masing kelompok atribut yang ada dan menentukan kelas mana yang paling optimal (Zhang H et al.,2016).

 Saat ini ada banyak penelitian deteksi serangan malware, salah satunya pada wireless sensor network (WSN) (C.Lupu et al.,2015). Penelitian tentang malware banyak yang melakukan attack terhadap sistem operasi (OS) (Zhang C.,2017). Dari beberapa penelitian mengenai serangan malware tersebut, belum menunjukkan adanya hasil yang optimal untuk penelitian serangan malware pada sensor. Permasalahannya adalah masih saja ada malware yang mengganggu kinerja sensor sehingga menyebabkan kerugian pada perangkat. Dengan begitu, pada penelitian ini akan ditingkatkan sistem deteksi dengan meng-implementasikan teknik deteksi dan klasifikasi malware menggunakan metode Naive Bayes Classifier pada sensor pengukur kualitas air.

## **1.2 Perumusan Masalah**

Dari latar belakang diatas terdapat beberapa isu yang akan dibahas dalam penelitian ini :

1. Bagaimana proses deteksi *malware* yang menyerang sensor
2. Bagaimana proses ekstraksi dataset *malware* untuk menghasilkan *malicious code*
3. Bagaimana tingkat akurasi yang dihasilkan pada klasifikasi malware menggunakan metode *Naive Bayes*
4. Bagaimana kinerja sensor sebelum dan sesudah diserang *malware*

## **1.3 Batasan Masalah**

1. Data yang digunakan merupakan dataset dari *VX Heavens*
2. Proses deteksi *malware*menggunakan teknik N-grams
3. Metode yang digunakan dalam mengklasifikasi*malware* adalah *Naive Bayes*

## **1.4 Tujuan dan Manfaat Penelitian**

Secara umum tujuan dari penelitian ini adalah menghasilkan teknik yang dapat mendeteksi dan mengklasifikasi serangan *malware* yang masuk kedalam sensor pengukur kualitas air pada MSN yang diimplementasikan pada UAV dengan menggunakan metode *Naive Bayes*.

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Mendeteksi *malware* dengan menggunakan metode *N-grams*
2. Melakukan analisis *malware* yang telah diklasifikasi dengan algoritma *Naive Bayes* untuk memperoleh akurasi yang optimal
3. Mengukur kinerja sensor sebelum dan sesudah diserang *malware*

Manfaat yang dapat diambil dari penulisan proposal ini adalah menghasilkan sebuah teknik untuk mendeteksi *malware* yang menyerang sensor pengukur kualitas air di MSN yang diimplementasikan pada UAV agar sensor dapat bekerja dengan nilai akurasi yang baik sehingga dapat memberikan kemudahan dalam melakukan pengukuran kualitas air pada daerah terpencil yang minim air bersih.

## **1.5 Sistematika Penulisan**

 Agar memperoleh gambaran jelas mengenai penelitian ini, maka dibuatlah suatu sistematika penulisan yang berisi gambaran dalam tiap bab penelitian ini, yaitu:

1. **BAB I Pendahuluan**

Bab ini menjelaskan tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat serta sistematika penulisan

1. **BAB II Tinjauan Pustaka**

Bab ini menjelaskan mengenai literature review yang berhubungan dengan masalah dalam penelitian ini

1. **BAB III Metodologi Penelitian**

Bab ini menjelaskan tahapan atau metode secara rinci yang akan dilakukan dalam penelitian ini

1. **BAB I V Analisa dan Pembahasan**

Bab ini menjelaskan pembahasan dari pengujian serta analisa yang didapat dari data hasil pengukuran

1. **BAB V Kesimpulan**

Bab ini menjelaskan kesimpulan dari hasil yang diperoleh, serta merupakan jawaban yang diperoleh dari tujuan pada bab 1.

# **BAB II**

# **TINJAUAN PUSTAKA**

Pada penelitian ini studi yang diperlukan untuk mendeteksi malware adalah beberapa literature review yang membahas tentang metode-metode yang pernah dipakai dalam mendeteksi malware, serta perkembangan penelitian tentang malware dalam beberapa tahun terakhir.

**2.1 Studi Literatur**

 Berikut adalah proses studi literatur:

Mempelajari klasifikasi malware menggunakan metode Naive Bayes

Mempelajari tentang teknik deteksi malware di MSN

Mempelajari referensi tentang malware

Membuat perancangan pengklasifikasian malware

Membuat perancangan pendeteksian malware

Mencari referensi dataset malware

Membuat sketsa desain dan algoritma

Pemahaman kajian literatur

**Gambar 2.1** Proses Studi Literatur

Tahapan yang dilakukan dalam proses diatas yaitu mengkaji berbagai literatur yang berhubungan dengan penelitian yang dilakukan. Sebagai contoh mengambil literatur dari jurnal yang relevan dalam 3 tahun terakhir yang membahas mengenai serangan malware pada Mobile Sensor Network dengam menggunakan berbagai metode machine learning yang pernah dilakukan, agar dapat dijadikan landasan yang kuat sebagai pendukung dalam proses penelitian ini.

**2.2 Deteksi Serangan Malware**

Deteksi malware dengan menggunakan metode klasik sudah banyak dilakukan seperti metode statistik dan EWMA (C, Lupu et al, 2015). Tetapi sekarang teknik deteksi malware klasik tersebut sudah mulai digantikan dengan metode machine learning yang sangat membantu para peneliti dalam melakukan olah data pada penelitian mereka (E, Mwangi et al, 2017)

Beberapa macam teknik machine learning dalam pendeteksian malware bertujuan untuk menemukan adanya serangan malware yang menyerang suatu perangkat (Markus, R et al, 2017). Pada beberapa tahun terakhir penelitian mendeteksi malware terus dilakukan dengan mengoptimalisasi metode tambahan (hybrid). Seperti penelitian deteksi kode malicious dengan menambahkan pendekatan collaborative pada metode support vector machine (Col-SVM) (Zhang, C et al, 2017). Klasifikasi topikj penelitian yang telah dilakukan sebelumnya dapat dilihat pada tabel 2.1

**Tabel 2.1** Klasifikasi Topik berdasarkan penelitian tentang malware

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **SUBTOPIC** | **RESEARCH** | **DISCUSS** |
| 1 | Survey on Malware Detection Concept | 1. Markus, R et al (2017) | Analysis malware |
| 2. E, Mwangi et al (2017) | A survey of malware attack |
| 3. H, Chuang et al (2015) | Hybrid behavior |
| 2 | Machine learning method for malware detection and classification | 1. B, Pete et al (2017) | Self Organizing Feature Method for malware detection |
| 2. Zhang, D et al (2017) | Detection malware activities |
| 3. Sharmeen, S et al (2017) | Malware threats and detection |
| 4. Zhang, C et al (2017) | Col-SVM in malware detection |
| 5. Chen, M et al (2017) | Malware detection |
| 6. Yuxin et al (2017) | Behaviour graph |
| 7. J, Stiborek et al (2017) | Malware classification |
| 8. H, Deylami et al (2016) | Malware detection techniques |
| 9. S, Shrakaew et al (2015) | Malware detection using data mining with two feature set |
| 10. Katerina et al (2017) | Malware detection technique |
| 11. A, Shouri et al (2018) | Malware classification using data mining technique |
| 12. H, Steven et al (2016) | Behavioral analysis |
| 3. M, Masud et al (2010) | A hybrid model to detect malicious |
| 3 | Naive Bayes algorithm | 2. Stiawan, Deris et al (2017) | K-Means and Naive Bayes |
| 3. J, Stiborek et al (2017) | Probabilistic of dynamic malware |
| 4 | Malware attack in wireless sensor network | 1. D, Qin et al (2017) | Routing in WSN |
| 2. C, Lupu et al (2015) | Detection malicious node in WSN |

**2.3 Algoritma Naive Bayes**

Naive Bayes adalah algoritma dalam metode klasifikasi machine learning yang menerapkan teorema bayes, ini bisa diterapkan untuk klasifikasi multiclass dan biner (Zhang H et al.,2016). Naive Bayes mengevaluasi probabilitas masing-masing fitur secara independen, terlepas dari korelasi apa pun, dan membuat prediksi berdasarkan Teorema Bayes. Itulah sebabnya metode ini disebut naive. Untuk memahami algoritma Naive Bayes, konsep probabilitas kelas dan probabilitas bersyarat harus diperkenalkan terlebih dahulu.

a. Probabilitas kelas adalah probabilitas sebuah kelas dalam kumpulan data

$$P\left(C\right)= \frac{count (instances in C)}{count (instances in Ntotal)}$$

b. Probabilitas Bersyarat adalah probabilitas dari nilai fitur yang diberikan kelas.

$$P\left(V|C\right)= \frac{count (instances with V and C)}{count (instances with V)}$$

c. Probabilitas yang diberikan

$$P\left(A|B\right)= \frac{P\left(A\right)P(A)}{P(B)}$$

 Keuntungan menggunakan teorema bayes adalah mudah untuk dimengerti. Selain itu metode ini berfungsi dengan baik pada set data dengan fitur yang tidak relevan, karena probabilitas mereka berkontribusi pada output yang rendah. Oleh karena itu mereka tidak diperhitungkan ketika membuat prediksi. Selain itu, algoritma ini biasanya menghasilkan kinerja yang baik dalam hal sumber daya yang dikonsumsi, karena hanya perlu menghitung probabilitas fitur dan kelas, tidak perlu mencari koefisien seperti dalam algoritma lain (Zhang H et al.,2016). Berikut tahapan proses klasifikasi malware menggunakan Naive Bayes.

# **BAB III**

# **METODOLOGI PENELITIAN**

Penelitian ini mengenai deteksi dan klasifikasi malware yang menyerang sensor pengukur kualitas air pada Mobile Sensor Network (MSN) yang diimplementasikan pada UAV dengan menggunakan metode Naive Bayes. Sensor yang dipasang Mobile Sensor Network akan diletakkan pada dua UAV, sensor tersebut akan melakukan sensing yang akan dikirim ke base station. Karena MSN selalu melakukan pengiriman dan penerimaan data yang bersifat publik, maka malware bisa menyerang kapan saja dan membuat sistem yang ada di sensor menjadi terganggu. Untuk itu diperlukan sebuah langkah untuk mendeteksi malware tersebut. Berikut langkah-langkah lebih detail yang akan dilakukan dalam penelitian ini.

**3.1 Kerangka Kerja**

 Tahapan yang dilakukan dalam implementasi penelitian ini akan dibuat sebuah kerangka kerja sehingga penelitian akan sesuai dengan alur yang sudah direncanakan sebelumnya.

 Proses pertama adalah menemukan sebuah masalah yang akan dijadikan topik pada penelitian ini. Kemudian masalah tersebut akan dikaji lebih dalam dengan mencari berbagai literature yang berkaitan dengan masalah yang akan diangkat. Setelah itu akan didapat hipotesa yaitu pendeteksian serangan malware pada sensor pengukur kualitas air menggunakan metode Naive Bayes. Proses selanjutnya yaitu perancangan hardware dan software. Pada perancangan software terdapat dataset, kemudian data set tersebut akan di ekstrak untuk menghasilkan opcodes. Algoritma Naive Bayes akan dirancang kedalam program sehingga bisa dilakukan pengujian terhadap hardware. Setelah diuji akan masuk ke tahap validasi data dan analisis pengujian yang telah dilakukan, maka akan masuk ke tahap penarikan kesimpulan dari seluruh proses yang telah dilalui. Bagan kerangka kerja dapat dilihat pada gambar dibawah ini.

Feature Extraction & Selection

Mulai

Disassemble file dataset malware

Classification menerapkan metode Naive Bayes

Validasi data

Analisa dan Kesimpulan

Selesai

**Gambar 3.1** Kerangka kerja

**3.2Alur Kerja Metodologi Penelitian**

Proses perancangan hardware dan software yang akan dibuat dalam tahapan ini berupa diagram blok yang menggambarkan alur proses penelitian dapat dilihat pada gambar dibawah ini.



**Gambar 3.2** Alur kerja metodologi penelitian

 Pada gambar 3.2 diatas menjelaskan tentang diagram dari proses penelitian yang akan dilakukan, yaitu sebagai berikut:

1. Mengumpulkan dataset malware, dengan dataset tersebut akan di ekstrak sehingga menghasilkan opcodes
2. Opcodes akan menjadi input untuk proses kedua yakni untuk mengklasifikasikan malware dengan menggunakan metode yang diusulkan sesuai dengan kelas malware tersebut
3. Setelah didapat data malware, maka data tersebut akan menjadi input bagi proses ketiga yakni memasukkan data malware dan data file normal kedalam sensor sehingga akan didapat hasil yang menunjukkan perbedaan kinerja sensor sebelum diserang dan sesudah diserang malware.

**3.3Kebutuhan Sistem**

Perancangan sistem pada penelitian ini menjelaskan beberapa fitur dari perangkat hardware dan software yang digunakan untuk mendeteksi dan mengklasifikasi malware. Berikut adalah skema perancangan sistem yang akan diterapkan dalam penelitian ini.

**3.3.1 Kebutuhan Hardware**

Berikut adalah spesifikasi hardware yang dibutuhkan :

**Tabel 3.1** Kebutuhan hardware

|  |  |
| --- | --- |
| **No** | **Perangkat** |
| 1 | Windows 7/8 |
| 2 | Sensor pengukur kualitas air |
| 3 | WSN |
| 4 | UAV |

**3.3.2 Kebutuhan Software**

Berikut adalah spesifikasi hardware yang dibutuhkan :

**Tabel 3.2** Kebutuhan software

|  |  |  |
| --- | --- | --- |
| **No** | **Sistem** | **Tools** |
| 1 | Disassemble | IDA Pro |
| 2 | Classification | Matlab |

**3.4 Metode Machine Learning**

Metode machine learning mempermudah dalam mendeteksi malware. Proses metode machine learning dimulai dari proses pengambilan data, training data dan testing data. Berikut proses diagram yang dilakukan (A.Souri et al.,2018; Y.Chuang et al.,2015).

Data Intake

Data Transformation

Model Training

Model Testing

Model Deployment

Test Dataset

**Gambar 3.3** Diagram Alur proses machine learning

**3.4.1 Disassemble file dataset malware**

 Disassemble file merupakan proses mengubah kode mesin .exe ke bahasa assembly. Pada proses ini membutuhkan sebuah tools disassembler untuk mengubah dataset malware ke bahasa assembly (A.Souri et al.,2018; Y.Chuang et al.,2015).

**3.4.2 Feature Extraction**

Untuk klasifikasi yang akurat dan cepat, perlu dilakukannya proses fitur ekstraksi file kode mesin dari tampilan hexa dan tampilan bahasa assembly untuk mengexsploitasi informasi pelengkap yang dibawa oleh dua representasi malware ini. Informasi pelengkap yang biasanya terkait dengan malicious seperti obfuscation (informasi yang bersifat kebingungan) dan hasil penelitian akan menunjukkan bagaimana kombinasi informasi dari kedua tampilanuntuk membantu efektifitas dari keseluruhan sistem. Dalam sub-bagian berikut memberikan rincian tentang fitur-fitur yang akan digunakan dan alasan memilih fitur tersebut.

**3.4.3 Feature Selection**

Tahap kedua adalah tahap seleksi fitur atau Feature Selection. Dalam tahap ini fitur yang paling informatif yang dipilih dan satu yang terbaik diperiksa berdasarkan perhitungan akurasi classifier yang berhubungan dengan sejumlah fitur yang dipilih dengan menggunakan metode seleksi fitur yang berbeda. metode seleksi fitur yang digunakan dalam penelitian ini adalah:

1. Info Gain Attribute

Info Gain Attribute mengevaluasi fitur yang sesuai denganpengukuran gain informasi sehubungan dengan kelas.

2. Gain Ratio Attribute

Gain Ratio Attribute dirancang untuk mengatasi bias dalaminformasi yang diperoleh dengan mempertimbangkan bagaimana fitur yang membagi data.

3.Correlation-based Feature Selection (CFsSubset)

CFsSubset mengevaluasi prediksi setiap atribut dalam halredundansi dan hubungan di antara mereka. Ini memilih fitur yang memiliki korelasi yang besar dengan kelas.

**3.4.4 Klasifikasi malware menggunakan algoritma Naive Bayes**

 Naive Bayes adalah algoritma dalam metode klasifikasi machine learning yang menerapkan teorema bayes, ini bisa diterapkan untuk klasifikasi multiclass dan biner (Zhang H et al.,2016). Naive Bayes mengevaluasi probabilitas masing-masing fitur secara independen, terlepas dari korelasi apa pun, dan membuat prediksi berdasarkan Teorema Bayes.

Import Library

Load data

Normalization function, apply to data

Divide data into training set and test set

Create dataset for multiclass & Binary

Naive Bayes

Make prediction

Result

**Gambar 3.4** Diagram Proses Klasifikasi Naive Bayes

**3.5 Pengambilan Data**

Pengambilan data dilakukan pada saat proses ekstraksi dataset dan pendeteksian malware secara real-time, oleh karena itu data diperoleh pada saat training dataset dan pengujian. Data real-time tersebut dapat diubah ke dalam format tertentu. Untuk proses data ektraksi menggunakan diassembler file berupa .a (Assembly),dan hasil deteksi dituangkan kedalam format Txt dan juga Csv.

**3.6 Rencana Pengujian Data**

Data opcode dan register yang dihasilkan dari hasil fitur ekstraksi akan dilakukan pengujian ke dalam bentuk klasifikasi. Hasil klasifikasi dari algoritma Naive Bayes dipisahkan

## **3.7 Jadwal Penelitian**

**Tabel 3.3** Rencana Jadwal Penelitian

|  |  |  |
| --- | --- | --- |
| No | Kegiatan | Tahun 2018/2019 |
| Sep | Okt | Nop | Des | Jan | Feb | Mar | Apr | Mei | Jun |
| 1 | Literature review |  |  |  |  |  |  |  |  |  |  |
| 2 | Pengumpulan Data |  |  |  |  |  |  |  |  |  |  |
| 3 | Perancangan Hardware Software |  |  |  |  |  |  |  |  |  |  |
| 4 | Implementasi |  |  |  |  |  |  |  |  |  |  |
| 5 | Pengujian |  |  |  |  |  |  |  |  |  |  |
| 6 | Laporan Tesis & Jurnal |  |  |  |  |  |  |  |  |  |  |

# **DAFTAR PUSTAKA**

B, Pete., F,Richard., T, Frederick., & J, Kevin.(2017). Malware classification

using self organising feature maps and machine activity data. Elsevier,

399-410.

W, Markus., R, Alexander., N, Thur., & W, Aigner.(2017). A Knowledge-assisted

 visual malware analysis system: Design, validation, and reflection of

 KAMAS. Elsevier, 1-15.

Stiawan, Deris., Sandra, Sari., Alzahrani, Esam., Budiarto, Rahmat.(2017). Com

 parative analysis of K-Means method and Naive Bayes method for brute

 force attack visualization.IEEE(International Conference on anti cyber

 crimes.177-182.

H, Zhang., D, Yao., N, Ramakrishman., & Z, Zhang.(2016). Causality reasoning

 about network events for detecting stealthy malware activities. Elsevier

 180-198.

K, Zhang., C, Li., Y, Wang., X, Zhu., & H, Wang.(2017). Collaborative Support

 Vector Machine for malware detection. Elsevier, International Conference

 on Computational Science.1682-1691.

D, Qin., S, Yang., S, Jhia., Y, Zhang., J, Ma., & Q, Ding.(2017). Research on

 Trust Sensing Based Secure Routing Mechanism for Wireless Sensor

 Network. IEEE. 9599-9609.

S, Sharmeen., S, Huda., J, H, Abawajy., W, Ismail.,& M, Hassan.(2017). Malware

 Threats and Detection for Industrial Mobile-IoT Networks. IEEE. 1-9.

E, Mwangi., S, Masupe.,& M, Jeffrey.(2017). Internet of Things Malware : A Sur

 Vey. IJCSES.10-21.

P, I, Victorio., & E,C, Lupu.(2015). Detecting Malicious Data Injection in Event

 Detection Wireless Sensor Network. IEEE.1932-4537.

S, Chen., M, Xue., L, Fan., S, Hao., L, Xu., H, Zu & B, Li.(2017). Automated

 Poisoning Attacks and Defenses in Malware Detection System. Elsevier.

 1-44.

D, Yuxin., X, Xiaoling., C, Shen., & L, Ye.(2017). A Malware Detection Method

 Based on Family Behaviour Graph. Elsevier. 1-28.

J, Stiborek., T, Pevny., & M, Rehak.(2017). Probabilistic analysis of dynamic

 Malware traces. Elsevier. 221-239.

J, Stiborek., T, Pevny., & M, Rehak.(2017). Multiple Instance Learning for

 Malware Classification. Elsevier.1-32.

H, Deylami., R, M, Chandren., I, Ardekani., & A, Sarrafzadeh.(2016). Taxonomy

 Of Malware Detection Techniques: A Systematic Literature Review.

 IEEE.1-8.

S, Srakaew., P, Warot., & A, Suchitra.(2015). On the Comparison of Malware

 Detection Methods Using Data Mining with Two Feature Set. ISSN: 1738

 -9976 IJSIA.1-26.

C, Katerina.(2017). Machine Learning Methods for Malware Detection and

 Classification. University of Applied Sciences. 1-93.

A, Souri., R, Hosseini.(2018). A state of the art survey of Malware Detection

 Approaches using data mining techniques. Springerlink.1-22.

S, H, Steven., T, Larsen., & J, Padersen.(2016). An Approach for Detection

 And Family Classification of Malware based on Behavioral analysis. IEEE

 International Conference on Computing Networking and Communication.

 1-6.

M, Masud., K, Latifur., & T, Bhavani.2010. A Hybrid Model to Detect Malicious

 Executables. IEEE Proceedings.1-6.

H, Y, Chuang., & S,D, Wang.(2015). Machine Learning based hybrid behavior

 Models for malware analysis. IEEE.1-6.