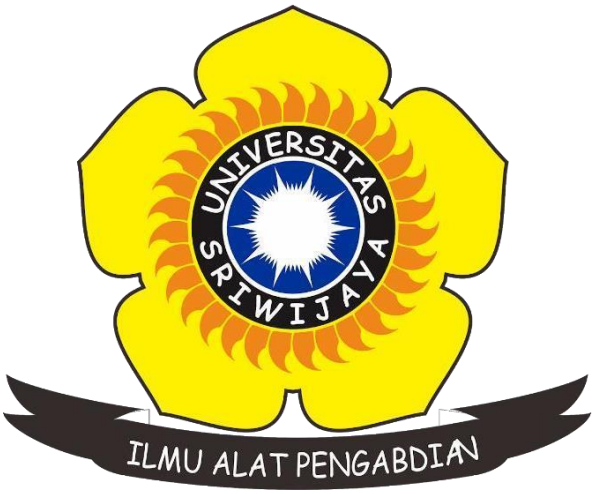
KLASIFIKASI MALWARE TROJAN HORSE DENGAN MENERAPKAN METODE GRU (GATED RECCURENT UNIT)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer (S1)



OLEH:

VANESA VALENTINA

09011382025098

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

KLASIFIKASI MALWARE *TROJAN HORSE* DENGAN MENERAPKAN METODE GRU (*GATED RECCURENT UNIT*)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer (S1)

Oleh

Vanesa Valentina
09011382025098

Palembang, Juni 2024

Pembimbing Tugas Akhir I	Pembimbing Tugas Akhir II
Prof. Deris Stiawan, M.T., Ph.D.	**Nurul Afifah, M.Kom**
NIP. 197806172006041002	**NIP. 199221102023212049**

Mengetahui, 10/7/24

Ketua Jurusan Sistem Komputer

UNIVERSITAS SRIWIJAYA FAKULTAS ILMU KOMPUTER JURUSAN SISTEM KOMPUTER

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Selasa

Tanggal : 4 Juni 2024

Tim Penguji

1. Ketua : Huda Ubaya, M. T.
2. Sekretaris : Kemahyanto Exaudi, M.T.
3. Penguji : Dr. Ahmad Zarkasi, M.T.
4. Pembimbing I : Prof. Deris Stiawan, M.T., Ph.D.
5. Pembimbing II : Nurul Afifah, M.Kom.

Mengetahui, 6/9/24

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Vanesa Valentina

NIM : 09011382025098

Judul : Klasifikasi malware Trojan Horse dengan metode *Gated Reccurent Unit* (GRU)

Hasil Pengeccekan 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. Peryataan ini saya buat dengan kesadaran penuh dan tanpa adanya paksaan dari pihak manapun.

Palembang, Juni 2024

Penulis,

Vanesa Valentina

NIM. 09011382025098

KATA PENGANTAR

Segala puji dan syukur atas kehadirat Tuhan, karena berkat Rahmat dan Karunia-Nya lah sehingga penulis dapat menyelesaikan Laporan Tugas Akhir dengan judul "**Klasifikasi Malware *Trojan Horse* Dengan Menerapkan Metode Gru (*Gated Reccurent Unit*)"**

Laporan ini merupakan salah satu syarat untuk memenuhi sebagian kurikulum dan syarat kelulusan Mata Kuliah Tugas Akhir pada Jurusan Sistem Komputer, Universitas Sriwijaya. Selesainya penulisan Laporan Tugas Akhir ini tidak terlepas dari peran serta semua pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikanucapan terima kasih yang sebesar-besarnya kepada:

1. Tuhan yang maha esa karena telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam melaksanakan Tugas Akhir.
2. Kedua Orang Tua, Keluarga dan Teman-teman yang selalu mendoakan serta memberikan motivasi dan semangat.
3. Bapak Prof. Dr. Erwin, S.SI, M.SI selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Jurusan Sistem Komputer.
5. Bapak Aditya Putra Perdana P, S.kom., M.T., Selaku Dosen Pembimbing Akademik.
6. Bapak Deris Stiawan, M.T., Ph.D., IPU., ASEAN-Eng., CPENT selaku Pembimbing I Tugas Akhir.
7. Ibu Nurul Afifah, M.Kom selaku Pembimbing II Tugas Akhir.
8. Mba Sari Anhar selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.
9. Dede Rizky Kurniawan yang selalu memberikan dukungan dan membantu selama penulisan laporan.

10. Risky Wahyuni dan Virginia Putri Lestari yang banyak membantu saya selama proses penulisan laporan.
11. Teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2020.
12. Kakak - kakak dan teman - teman di COMNET.

Penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan, oleh karenaitu penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar lebihbaik lagi dikemudian hari.

Akhir kata dengan segala keterbatasan, penulis berharap semoga laporan ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung atau pun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran dan penelitian.

Palembang, Juni 2024
Penulis,

Vanesa Valentina
NIM. 09011382025

KLASIFIKASI MALWARE TROJAN HORSE DENGAN METODE GATED RECURRENT UNIT (GRU)

VANESA VALENTINA (09011382025098)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer Universitas Sriwijaya

Email : vanesasimamora@gmail.com

ABSTRAK

Di era digital saat ini, teknologi merupakan bagian penting dalam kehidupan sehari- hari, yang juga meningkatkan risiko kejahatan siber. Trojan Horse adalah jenis malware yang menyamar sebagai program sah sehingga dapat diunduh ke komputer atau perangkat seluler. Dalam penelitian ini, penulis mengusulkan metode Gated Recurrent Unit (GRU) untuk mengidentifikasi malware dengan menggunakan dataset CIC-MalMem-2022. Hasil penelitian menunjukkan bahwa metode ini mencapai akurasi sebesar 98,39%.

Kata Kunci : Klasifikasi Biner, *Trojan Horse, Malware, GRU*

TROJAN HORSE MALWARE CLASSIFICATION USING THE GATED RECURRENT UNIT (GRU) METHOD

VANESA VALENTINA (09011382025098)

Computer Engineering Department, Computer Science Faculty Sriwijaya University

Email : vanesasimamora@gmail.com

ABSTRACT

In the current digital era, technology is an essential part of everyday life, which also increases the risk of cybercrime. A Trojan Horse is a type of malware that disguises itself as legitimate software to be downloaded onto a computer or mobile device. In this research, the authors propose a Gated Recurrent Unit (GRU) method to identify malware using the CIC-MalMem-2022 dataset. The research results show that this method achieves an accuracy of 98.39%.

Keywords : *Binary Classification, Trojan Horse, Malware, GRU*

DAFTAR ISI

LEMBAR PENGESAHAN.....ii

HALAMAN PERSETUJUAN..... iii

HALAMAN PERNYATAAN.....iv

KATA PENGANTAR.....v

ABSTRAK vii

ABSTRACT..... viii

DAFTAR ISI.....ix

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 Penelitian.....4

1.5 Manfaat Penelitian.....4

1.6 Metodelogi Penelitian.....4

1.7 Sistematika Penulisan.....5

BAB II TINJAUAN PUSTAKA.....7

2.1. Penelitian Terdahulu.....7

2.2. Malicious Software.....10

2.3. Malware Trojan Horse.....10

2.3.1. TrojanHorse Zeus 11
2.4. Random Oversampling 11
2.5. Gated Reccurent Unit 12
2.6. Confusion Matrix 13
2.6.1 Accuracy 14
2.6.2 Recall 15
2.6.3. Precision 15
2.6.4. F1-Score 15
BAB III METODELOGI PENELITIAN 16
3.1. Pendahuluan 16
3.2. Kerangka Kerja Penelitian 16
3.3. Perancangan Sistem 19
3.3.1. KebutuhanPerangkat Keras 20
3.3.2. KebutuhanPerangkat Lunak 20
3.4. Dataset 21
3.5. Data Understanding 27
3.6. Exploratory Data Analysis 27
3.7. Pre-processing 27
3.7.1 Feature Selection 27
3.7.2 Label Encoder 28
3.7.3 Normalisasi 30
3.8. Random Oversampling 30
3.9. Validasi hasil klasifikasi 30
3.10 Perbandingan Matrik 33
3.11 Analisis hasil klasifikasi 34

BAB IV HASIL DAN PEMBAHASAN.....35

4.1. Pendahuluan 35

4.2. Sample malware 35

4.3. Dataset.....37

4.4 Data Understanding 37

4.5 Exploratory Data Analysis 39

4.6 Pre-processing 39

4.6.1. Feature Selection 40

4.6.2. Label Encoder 40

4.6.3. Normalisasi.....41

4.6. Random Oversampling.....42

4.7. Validasi hasil klasifikasi.....43

4.8. Perbandingan Matrik 44

4.9. Analisis hasil klasifikasi 46

BAB V KESIMPULAN DAN SARAN 48

5.1. Kesimpulan.....48

5.2. Saran.....48

DAFTAR PUSTAKA 49

DAFTAR GAMBAR

Gambar 2.1 Representasi sel GRU 13

Gambar 3.1 Kerangka Kerja Penelitian 18

Gambar 3.2 Perancangan Sistem 19

Gambar 3.3 Flowchart label encoder 29

Gambar 3.4 Feature Selection 28

Gambar 3.5 Flowchart GRU 31

Gambar 3.6 Arsitektur model GRU 33

Gambar 4.1 Malware Trojan zeus 35

Gambar 4.2 Malware Behaviour 36

Gambar 4.3 Dataset telah difilter 37

Gambar 4.4 Jumlah data tiap kelas 37

Gambar 4.5 Data duplikat 38

Gambar 4.6 Data yang hilang 38

Gambar 4.7 Tipe data 38

Gambar 4.8 Histograf fitur dataset 39

Gambar 4.9 Fitur yang didrop…. 40

Gambar 4.10 Label Encoder 40

Gambar 4.11 Pelabelan pada data 40

Gambar 4.12 Normalisasi Robustscaler 41

Gambar 4.13 Data Imbalance 42

Gambar 4.14 Data Balance 42

Gambar 4.15 Confusion Matrix 43

Gambar 4.16 Hasil grafik training dan testing 47

Gambar 4.17 Grafik perbandingan akurasi… 47

DAFTAR TABEL

Tabel 2.1 Tabel Penelitian Terdahulu 8

Tabel 2.2 Tabel Confusion Matrix 14

Tabel 3.1 Spesifikasi Hardware 20

Tabel 3.2 Daftar Software 21

Tabel 3.3 Dataset CIC-MalMem2022 22

Tabel 3.4 Fitur dalam dataset 23

Tabel 3.5 Label dataset 29

Tabel 3.6 Hyperparameter 32

Tabel 3.7 Hyperparameter perbandingan Matrik 34

Tabel 4.1 Jumlah dataset setelah difilter 37

Tabel 4.2 Hasil klasifikasi 44

Tabel 4.3 Split 60:40 45

Tabel 4.4 Split 70:30 45

Tabel 4.5 Split 80:20 45

Tabel 4.6 Split 90:10 45

Tabel 4.7 Performa terbaik dari setiap split 46

BAB I
PENDAHULUAN

1.1 Latar Belakang

Malware (*Malicious Software*) adalah perangkat lunak jahat yang digunakan pengguna tidak bertanggung jawab untuk mendapatkan keuntungan pribadi dan merugikan sistem atau pengguna lain. Kemampuan dan jenis malware yang terus berkembang membuat malware menjadi sulit dideteksi [1]. Pada penelitian [2] menyebutkan salah satu pendekatan untuk deteksi malware yang popular adalah *anti- virus*, malware jenis baru terus bermunculan sehingga teknik deteksi harus terus diperbarui. Menurut penelitian [3] ada beberapa jenis malware seperti *trojan horse,botnet, spyware, virus, worm, adware* dan lain - lain.

Trojan Horse adalah jenis malware yang menyamar sebagai program atau aplikasi sah sehingga dapat diunduh ke komputer atau perangkat seluler [4]. Rekayasa sosial akan digunakan sebagai mekanisme untuk mengirimkan kode berbahaya yang tersembunyi di dalam perangkat lunak yang sah, dan eksekusinya oleh korban akan memungkinkan penyerang mengakses sistem pengguna dengan perangkat lunak mereka [5].

Memory Analysis adalah metode untuk memahami aktivitas pada sistem melalui cuplikan memori dan fitur yang diekstrak dari cuplikan memori. Analisis memori tidak langsung memerlukan cuplikan dan cuplikan ini penting untuk memastikan agar file memori tidak dalam pengaruh. File memori yang terpengaruh akan mengubah hasil analisis memori dan menghilangkan kemampuan analisis. [3]

Pada penelitian [6] GRU (*Gated Recureent Unit*) adalah model yang terinspirasi dari LSTM (*Long Short-Term Memory*). GRU dapat mengatasi masalah RNN (*Recurrent Neural Network*) hingga dapat menyelesaikan masalah ketergantungan jangka panjang pada metode LSTM sambil mengurangi adanya perhitungan pembaruan dari hidden state. Dalam mendeteksi malware, penelitian [3] menggunakan metode big data untuk melakukan klasifikasi biner. Penelitian ini menggunakan dataset CIC-MalMem-2022 yang berasal dari *Canadian Institute for Cybersecurity* pada tahun 2022. *Machine learning* dan *deep learning* digunakan untuk menganalisis memori dan mendeteksi malware. Hasil model menunjukkan bahwa setiap model melakukan pekerjaan yang sangat baik dalam klasifikasi

malware. Regresi Logistik adalah algoritma dengan kinerja terbaik dengan akurasi 99,98%.

Penelitian [7] menggunakan *Gated Reccurent Unit* (GRU) dan *Support Vector Machine* (SVM) untuk memproses dan mengekstraksi berbagai jenis pengetahuan dari teks yang tidak terstruktur. Jaringan GRU memiliki performa yang baik untuk tugas pembelajaran berurutan dan mengatasi masalah hilangnya gradien dalam RNN saat menangkap ketergantungan jangka panjang. Kumpulan data untuk pengujian berjumlah 1885 dokumen untuk pelatihan dan 940 dokumen untuk pengujian. Model GRU-SVM mencapai tingkat akurasi klasifikasi teks terbaik sebesar 94,75% yang menunjukan potensi penerapan GRU-SVM untuk masalah klasifikasi multi-kelas dengan jumlah kelas yang sedikit. Metode ini juga mencapai kinerja yang jauh lebih baik dalam *presicion, recall* dan *F-1 score*.

Dalam penelitian [8] , menggunakan metode *Gated Reccurent Unit* (GRU) untuk mengklasifikasikan aktivitas manusia karena memiliki kinerja tinggi dan akurasi yang lebih besar. Algoritma menggunakan dataset dari Wireless Sensor Data Mining (WSDM) yang dikumpulkan dari banyak individu dengan enam kelas aktivitas seperti berjalan, duduk, turun tangga, jogging, berdiri dan naik tangga. Eksperimen dilakukan untuk mengevaluasi kinerja GRU menggunakn Receiver Operating Charateristic (ROC) dan confusion matrix. Hasilnya adalah GRU memberikan kinerja tinggi dalam pengenalan aktivitas manusia. Algortima GRU akurasi sebesar 97,08%. Tingkat kerugian pengujian untuk GRU adalah 0,221, sedangkan presisi, sensitivitas, dan skor F1 untuk GRU adalah masing-masing 97,11%, 97,09%, dan 97,10%. Secara eksperimental, area di bawah kurva ROC (AUCS) adalah 100%.

Penelitian [9] bertujuan untuk mengembangkan pendekatan *deep learning* untuk kinerja yang lebih unggul dalam klasifikasi teks dengan pendekatan RNN lainnya. Pengujian ini mengusulkan struktur terpadu untuk menyelidiki efek *word embedding* dan GRU untuk klasifikasi teks pada dua dataset benchmark (Google snippets dan TREC). Nilai akurasi untuk dataset *Google snippsets* dan TREC sebesar 84% dan 95%. Berdasarkan hasil pengujian, model GRU efektif mempelajari penggunaan kata - kata dalam konteks teks saat pelatihan data.

Penelitian [10] menggunakan model hibrida GRU_CNN untuk mengklasifikasikan teks berita. *Convolutional Neural Network* (CNN) tidak dapat

menangkap hubungan semantik antara kata-kata, dan kinerja klasifikasi model CNN tunggal rendah. GRU dapat secara efektif mengekstrak informasi semantik dan hubungan struktur global dari teks. Hasil eksperimen menunjukkan bahwa model hibrida GRU_CNN memiliki kinerja klasifikasi yang kuat pada dataset Cnews, dengan akurasi 97.86%.

Berdasarkan latar belakang dan analisis penelitian yang telah disebutkan di atas, tugas akhir ini akan membahas cara klasifikasi malware *Trojan hors*e zeus. Judul penelitian ini adalah "Klasifikasi *Trojan Horse zeus* dengan menerapkan metode GRU". Penggunaan metode GRU akan bermanfaat untuk mengklasifikasikan serangan malware *trojan horse zeus*, memahami pola serangan dan kebiasaan malware.

1.2 Rumusan Masalah

Sesuai dengan latar belakang masalah yang ada, permasalahan yang akan dibahas pada penelitian ini adalah

1. Bagaimana cara memilih fitur ideal agar proses komputasi lebih cepat?
2. Bagaimana cara mengklasifikasikan data *Trojan horse zeus* dan data *benign*?
3. Bagaimana performa evaluasi model *Gated Reccurent Unit* dalam mengklasifikasi dari *Trojan horse*?

1.3 Batasan Masalah

Batasan masalah yang ada pada penulisan penelitian ini adalah sebagai berikut :

1. Metode yang digunakan dalam penelitian adalah *Gated Reccurent Unit* (GRU)
2. Menggunakan dataset dari *Canadian Institute for Cybersecurity* (CIC) yaitu CICMalMem2022 dengan jenis *Trojan horse zeus* dan *benign*.
3. Penelitian ini tidak membahas cara pencegahan terhadap malware *Trojan horse zeus*.

1.4 Tujuan Penelitian

Beberapa tujuan yang akan dicapai dalam penelitian ini yaitu :

1. Menerapkan teknik ROS untuk mendeteksi *Trojan horse zeus.*
2. Menerapkan metode *Gated Reccurent Unit* (GRU) untuk klasifikasi malware *Trojan horse* dan data *benign* pada dataset CIC-MalMem-2022.
3. Melakukan evaluasi dari performa model *Gated Recurrent Unit* untuk klasifikasi *malware Trojan horse*.

1.5 Manfaat Penelitian

Terdapat beberapa manfaat yang diharapkan dalam penelitian ini, yaitu :

1. Dapat mengklasifikasi dari *malware trojan horse* dengan model *Gated Reuccrent Unit* yang lebih optimal
2. Memberikan informasi mengenai teknik ROS untuk mendeteksi *malware Trojan horse.*
3. Memberikan manfaat dari hasil evaluasi performa model *Gated Recurrent Unit* untuk dijadikan refrensi.

1.6 Metodelogi Penelitian

Metodologi yang diterapkan dalam penulisan tugas akhir ini melalui beberapa tahapan sebagai berikut :

1. Studi Pustaka / Literatur

   Tahap ini diawali dengan mencari informasi dan masalah yang sesuai dan relevan untuk dijadikan bahan penelitian. Setalah itu mencari beberapa sumber untuk refrensi seperti jurnal ilmiah, buku, internet, dan lainnya yang mendukung proposal tugas akhir ini serta mencari dataset di website, pada penelitian ini, saya menggunakan dataset CIC – MalMem – 2022 UNB.
2. Perancangan Sistem

   Pada tahap ini, masalah proses seperti pembuatan metode atau teknik tertentu, serta perangkat lunak dan perangkat keras yang digunakan untuk konfigurasi sistem akan dibahas.

3. Pengujian

Pada tahap ini, pengujian dilakukan dengan menggunakan pendekatan yang digunakan dalam penelitian saat ini dan pendekatan yang digunakan dalam penelitian sebelumnya untuk memastikan bahwa hasilnya sesuai.

4. Analisa

Pada tahap ini, data yang diperoleh dari pengujian sebelumnya diolah dan dianalisis untuk mendapatkan data yang benar. Selanjutnya, hasil analisis dilakukan untuk mengidentifikasi kesalahan dalam perancangan sistem.

5. Kesimpulan dan Saran

Dalam langkah akhir ini, hasil dari semua langkah sebelumnya akan dirumuskan menjadi suatu kesimpulan. Selain itu, ada saran yang diperlukan untuk mengidentifikasi apa yang membuat hasil perancangan buruk dan sumbernya.

1.7 Sistematika Penulisan

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

BAB I PENDAHULUAN

Bab ini tentang topik penelitian yang meliputi latar belakang, tujuan, manfaat, rumusanmasalah, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini tentang teori penelitian yang berkaitan dengan malware *trojan horse zeus* dengan menerapkan metode GRU.

BAB III METODE PENELITIAN

Bab ini menjelaskan secara ilustratif, bagaimana langkah-langkah yang dilakukan padapenelitian. Penjelasannya meliputi tahapan perancangan

sistem dan penerapan metodedalam penelitian ini.

BAB IV HASIL DAN ANALISIS

Bab ini mengenai hasil percobaan yang dilakukan. Setalah mendapat hasil maka akandilakukan analisa, kemudian akan mendapat data yang akurat.

BAB V KESIMPULAN

Bab ini berisi kesimpulan yang didapat dari data penelitian yang dilakukan dan saranagar penelitian ini dapat dikembangkan lebih baik lagi.

DAFTAR PUSTAKA

[1] A. Kamboj, P. Kumar, A. K. Bairwa, and S. Joshi, "Detection of malware in downloaded files using various machine learning models," *Egypt. Informatics J.*, vol. 24, no. 1, pp. 81–94, 2023, doi: 10.1016/j.eij.2022.12.002.

[2] P. H. Barros, E. T. C. Chagas, L. B. Oliveira, F. Queiroz, and H. S. Ramos, "Malware-SMELL: A zero-shot learning strategy for detecting zero-day vulnerabilities.," *Comput. Secur.*, vol. 120, 2022, doi: 10.1016/j.cose.2022.102785.

[3] T. Carrier, P. Victor, A. Tekeoglu, and A. Lashkari, "Detecting Obfuscated Malware using Memory Feature Engineering," no. Icissp, pp. 177–188, 2022, doi: 10.5220/0010908200003120.

[4] M. F. Ab Razak, M. I. Jaya, Z. Ismail, and A. Firdaus, "Trojan Detection System Using Machine Learning Approach," *Indones. J. Inf. Syst.*, vol. 5, no. 1, pp. 38–47, 2022, doi: 10.24002/ijis.v5i1.5673.

[5] S. Wijayarathne, "Trojan Horse Malware - Case Study," *Sri Lanka Inst. Inf. Technol. (SLIIT), Malabe, Sri Lanka*, no. July, 2022.

[6] M. Lstm, G. Recurrent, U. Gru, F. Prediction, and C. Kim, "Water Level Prediction Model Applying a Long Short-Term," 2022.

[7] M. Zulqarnain, R. Ghazali, Y. M. M. Hassim, and M. Rehan, "Text classification based on gated recurrent unit combines with support vector machine," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 4, pp. 3734–3742, 2020, doi: 10.11591/ijece.v10i4.pp3734-3742.

[8] S. Mohsen, "Recognition of human activity using GRU deep learning algorithm," *Multimed. Tools Appl.*, vol. 82, no. 30, pp. 47733–47749, 2023, doi: 10.1007/s11042-023-15571-y.

[9] M. Zulqarnain, R. Ghazali, M. G. Ghouse, and M. F. Mushtaq, "Efficient processing of GRU based on word embedding for text classification," *Int. J. Informatics Vis.*, vol. 3, no. 4, pp. 377–383, 2019, doi: 10.30630/joiv.3.4.289.

[10] L. Deng *et al.*, "News Text Classification Method Based on the GRU_CNN Model," *Int. Trans. Electr. Energy Syst.*, vol. 2022, 2022, doi: 10.1155/2022/1197534.

[11] S. A. Roseline, S. Geetha, S. Kadry, and Y. Nam, "Intelligent Vision-Based

Malware Detection and Classification Using Deep Random Forest Paradigm," *IEEE Access*, vol. 8, pp. 206303–206324, 2020, doi: 10.1109/ACCESS.2020.3036491.

[12] A. Lichy, O. Bader, R. Dubin, A. Dvir, and C. Hajaj, "When a RF beats a CNN and GRU, together—A comparison of deep learning and classical machine learning approaches for encrypted malware traffic classification," *Comput. Secur.*, vol. 124, pp. 1–10, 2023, doi: 10.1016/j.cose.2022.103000.

[13] M. Gohari, S. Hashemi, and L. Abdi, "Android Malware Detection and Classification Based on Network Traffic Using Deep Learning," *2021 7th Int. Conf. Web Res. ICWR 2021*, pp. 71–77, 2021, doi: 10.1109/ICWR51868.2021.9443025.

[14] C. S. Yadav *et al.*, "Malware Analysis in IoT & Android Systems with Defensive Mechanism," *Electron.*, vol. 11, no. 15, pp. 1–20, 2022, doi: 10.3390/electronics11152354.

[15] M. R. Raza, "Cloud Sentiment Accuracy Comparison using," pp. 1–5, 2021, doi: 10.1109/ASYU52992.2021.9599044.Cloud.

[16] B. Harjeevan and S. Gill, "Malware : Types , Analysis and Classifications".

[17] H. Kanaker, N. A. Karim, S. A. B. Awwad, N. H. A. Ismail, J. Zraqou, and A. M. F. Al ali, "Trojan Horse Infection Detection in Cloud Based Environment Using Machine Learning," *Int. J. Interact. Mob. Technol.*, vol. 16, no. 24, pp. 81–106, 2022, doi: 10.3991/ijim.v16i24.35763.

[18] N. L. Y. Fui, A. Asmawi, and M. Hussin, "A dynamic malware detection in cloud platform," *Int. J. Differ. Equations*, vol. 15, no. 2, pp. 243–258, 2021, doi: 10.37622/IJDE/15.2.2020.243-258.

[19] K. P. Grammatikakis, I. Koufos, N. Kolokotronis, C. Vassilakis, and S. Shiaeles, "Understanding and mitigating banking trojans: From Zeus to emotet," *Proc. 2021 IEEE Int. Conf. Cyber Secur. Resilience, CSR 2021*, no. July, pp. 121–128, 2021, doi: 10.1109/CSR51186.2021.9527960.

[20] M. Hayaty, S. Muthmainah, and S. M. Ghufran, "Random and Synthetic Over-Sampling Approach to Resolve Data Imbalance in Classification," *Int.*

J. Artif. Intell. Res., vol. 4, no. 2, p. 86, 2021, doi: 10.29099/ijair.v4i2.152.

[21] S. ur Rehman *et al.*, "DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU)," *Futur. Gener. Comput. Syst.*, vol. 118, pp. 453–466, 2021, doi:10.1016/j.future.2021.01.022.