ANALISIS FORENSIK MOBILE-TROJAN METASPLOIT DENGAN *MACHINE LEARNING* (*DECISION TREE*)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
MUHAMMAD IKHLASUL AMAL
09011182025010

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

ANALISIS FORENSIK *MOBILE*-TROJAN METASPLOIT DENGAN *MACHINE LEARNING* (*DECISION TREE*)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh

MUAHMMAD IKHLASUL AMAL

09011182025010

Indralaya, 9 Juni 2024

Mengetauhi,

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

AUTHENTICATION PAGE

FORENSIC ANALYSIS OF MOBILE-TROJAN METASPLOIT WITH MACHINE LEARNING (DECISION TREE)

FINAL TASK

Submitted To Fulfill One Of He Requirement To
Obten A Bachelor's In Computer Science

By

MUAHMMAD IKHLASUL AMAL

09011182025010

Indralaya, 9 June 2024

Acknowledge,

Final Project Supervisor	Head Of Computer System Department
Prof. Deris Stiawan, M.T., Ph.D.	**Dr. Ir. H. Sukemi, M.T.**
NIP. 197806172006041002	NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Senin

Tanggal : 03 Juni 2024

Tim Penguji :

1. Ketua : Dr. Ahmad Zarkasi, M.T. _____

2. Sekretaris : Nurul Afifah, M.Kom. _____

3. Penguji : Huda Ubaya, M.T. _____

4. Pembimbing : Prof. Deris Stiawan, M.T., Ph.D. _____

Mengetahui, 9/7/24

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

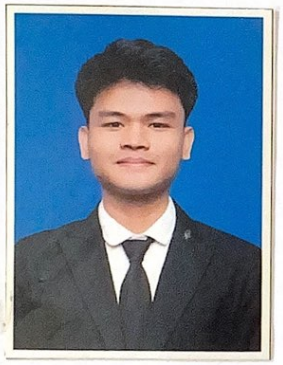
Yang bertanda tangan di bawah ini:

Nama : Muhammad Ikhlasul Aml
NIM : 09011182025010
Judul : Analisis Forensik Mobile-Trojan Metaspoit Dengan *Machine Learning* (*Decision Tree*)

Hasil pengecekan Software Itheticate/Turnitin : 7%

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

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan



Indralaya, Juni 2024

Muhammad Ikhlasul Amal

NIM. 09011182025010

KATA PENGANTAR

Asslaamualaikum Warahmatuallahi Wabarakatuh

Puji syukur Alhamdulillah kepada Allah SWT yang telah memberikan ridho dan berkah-Nya, sehingga atas izin-Nya penulis dapat menyelesaikan Laporan Tugas Akhir yang berjudul " Analisis Forensik Mobile-Trojan Metaspoit Dengan Machine Learning (Decision Tree)".

Dalam penyusunan Tugas Akhir ini, penulis telah banyak memperoleh bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, penulis mengucapkan rasa syukur dan ingin menyampaikan terimakasih sebesar-besarnya diberikan kepada :

1. Allah SWT yang telah memberikan saya rahmat dan karunia-Nya serta kesehatan untuk menyelesaikan laporan tugas akhir ini.
2. kepada orang tua, dan kakak yang saya cintai karena telah memberika doa dan motivasi kepada penulis.
3. Bapak Pof. 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 Universitas Sriwijaya.
5. Bapak Dr. Ahmad Zarkasi, M.T. selaku Dosen Pembimbing Akademik.
6. Bapak Prof. Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Skripsi yang telah membimbing serta memberikan ilmu dan motivasi terbaik.
7. Administrasi Jurusan Sistem Komputer yang telah membantu dan melancarkan proses administrasi terkait Tugas Akhir.
8. Kepada teman kelas SKB 2020 dan teman di lab comnets yang sudah memberikan banyak bantuan.
9. Dan seluruh pihak yang tidak dapat penulis sebutkan yang selalu memberikan semangat dan bantun yang bermanfaat

Penulis Menyadari bahwa laporan ini masih banyak kekurangan. Oleh karena itu penulis mengharapkan kritik dan saran dari semua pihak sebagai bahan evaluasi dari penulis agar laporan ini menjadi lebih baik dan bermanfaat bagi semua pihak

dan menjadi referensi bacaan dalam penelitian networking terkhusus pada serangan siber.

Penulis berharap semoga penulisan Proposal Tugas Akhir ini dapat menjadi tambahan wawasan dan ilmu pengetahuan bagi mahasiswa yang memerlukan khususnya mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung maupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran.

Wassalamualaikum Warahatullahi Wabarakatuh

Indralaya, ……..
Penulis,

Muhammad Ikhlasul Amal
NIM. 09011182025010

ANALISIS FORENSIK MOBILE-TROJAN METASPLOIT DENGAN *MACHINE LEARNING* (*DECISION TREE*)

MUHAMMAD IKHLASUL AMAL (09011182025010)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : mikhlasul27@gmail.com

ABSTRAK

Perkembangan teknologi mobile yang pesat telah membuka pintu keuntungan baru dalam hal konektivitas dan produktivitas. Namun, dampaknya terhadap keamanan menjadi semakin signifikan, terutama terkait dengan serangan malware pada perangkat mobile. Ancaman ini membawa risiko serius terhadap kerahasiaan dan integritas data pengguna. Pada penelitian ini malware yang akan menjadi objek penelitian ialah malware trojan, yaitu jenis malware yang menunjukkan dirinya sebagai aplikasi jinak atau tidak berbahaya, untuk menarik korban agar mengunduh dan menginstal malware. Trojan menyimpan informasi sistem di dalam dirinya sendiri, atau membuka komputer yang terinfeksi ke akses jarak jauh dan mengirimkan informasi ke komputer lain melalui internet. Oleh karena itu, penelitian ini bertujuan untuk menghadapi tantangan tersebut melalui pendekatan analisis forensik, dengan menggunakan metode machine learning, khususnya algoritma decision tree dalam melakukan deteksi dan visualisasi serta menerapkan prosedur proses investigasi forensik digital dari *National Institute of Standards and Technology* (NIST) sebagai alur penelitian dari tahap awal yaitu pengumpulan data (*Data Collection*) sampai tahap akhir yaitu pelaporan (*Reporting*). Penelitian yang telah dilakukan berhasil mempereloh hasil akurasi terbaik menggunakan metode decision tree dalam rasio validasi perbandingan data training 40% dan data testing 60% dengan performa akurasi sebesar 99.87%, nilai recall 97.03 %, nilai presisi 98.44%, dan nilai F1-Score 97.73% serta nilai spesifitas 98.37 %. dan mempereloh nilai visualisasi skor pengujian 100% dan skor validasi 99,91%

Kata kunci : *Malware, Trojan, Decision Tree, forensik, deteksi, visualisasi.*

Mengetauhi,

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

FORENSIC ANALYSIS OF MOBILE-TROJAN METASPLOIT WITH MACHINE LEARNING (DECISION TREE)

MUHAMMAD IKHLASUL AMAL (09011182025010)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : mikhlasul27@gmail.com

ABSTRACT

The rapid development of mobile technology has opened the door to new advantages in terms of connectivity and productivity. However, its impact on security is becoming increasingly significant, especially with regard to malware attacks on mobile devices. This threat brings serious risks to the confidentiality and integrity of user data. In this research, the malware that will be the object of research is trojan malware, which is a type of malware that presents itself as a benign or harmless application, to attract victims to download and install malware. Trojans store system information within themselves, or open infected computers to remote access and transmit information to other computers via the internet. Therefore, this research aims to face these challenges through a forensic analysis approach, using machine learning methods, especially the decision tree algorithm in performing detection and visualization and applying the digital forensic investigation process procedure from the National Institute of Standards and Technology (NIST) as a research flow from the initial stage, namely data collection to the final stage, namely reporting. The research that has been carried out has succeeded in obtaining the best accuracy results using the decision tree method in the validation ratio of 40% training data comparison and 60% testing data with accuracy performance of 99.87%, recall value 97.03%, precision value 98.44%, and F1-Score value 97.73% and specificity value 98.37%. and obtained a visualization score of 100% testing score and 99.91% validation score.

Keywords : *Malware, Trojan, Decision Tree, forensics, detection, visualization.*

Acknowledge,

Final Project Supervisor	Head Of Computer System Department
Prof. Deris Stiawan, M.T., Ph.D.	**Dr. Ir. H. Sukemi, M.T.**
NIP. 197806172006041002	NIP. 196612032006041001

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi *mobile* yang pesat telah membuka pintu keuntungan baru dalam hal konektivitas dan produktivitas. Namun, dampaknya terhadap keamanan menjadi semakin signifikan, terutama terkait dengan serangan *malware* pada perangkat *mobile*. Ancaman ini membawa risiko serius terhadap kerahasiaan dan integritas data pengguna. Oleh karena itu, penelitian ini bertujuan untuk menghadapi tantangan tersebut melalui pendekatan analisis forensik, dengan menggunakan metode *machine learning*, khususnya algoritma *decision tree*.

Malware (*Malicious Software*) adalah perangkat lunak apa pun dengan maksud niat jahat [1]. Bagaimana *malware* bekerja, yang mana mesin dan program yang terpengaruh, data akan dirusak dan dicuri. Ancaman ini bertujuan untuk mengakses data pribadi tanpa sepengetahuan korban dan mengambil serta mengendalikan perangkat [2], [3]. *Malware* juga dapat ditulis untuk mengganggu *normal functioning*, *bypass access controls*, mengumpulkan informasi sensitif, dan menampilkan iklan yang tidak diinginkan [1], [4].

Jenis malware yang menunjukkan dirinya sebagai aplikasi jinak atau tidak berbahaya, untuk menarik korban agar mengunduh dan menginstal malware, dikenal sebagai *malware* Trojan [1]. Trojan menyimpan informasi sistem di dalam dirinya sendiri, atau membuka komputer yang terinfeksi ke akses jarak jauh dan mengirimkan informasi ke komputer lain melalui internet [2]. Penyerang mendapatkan akses jarak jauh bertujuan untuk mencuri data, uang, menghapus dan memodifikasi file, membuat varian malware, serta mengawasi aktivitas pengguna sebagai layar monitor dan log mereka, dll [1].

Forensik digital (*Digital Forensics*) menjadi disiplin ilmu yang kompleks terutama dengan digitalisasi ini, terdapat banyak kejahatan digital terjadi oleh karena itu diperlukannya peneliti, praktisi, dan organisasi standardisasi untuk mengatasinya [5]. Forensik digital (*Digital Forensics*) adalah proses yang bertujuan untuk mengumpulkan bukti yang dapat digunakan untuk menentukan fakta-fakta di

sekitar suatu kejadian dengan sejumlah pertanyaan 5W+1H yang biasa ditanyakan dalam investigasi [6], [7].

Machine Learning adalah cabang dari artificial intelligence yang berfokus pada pengembangan komputer yang dapat belajar dari data. Teknologi ini biasanya digunakan di bidang penambangan dan analisis data, serta serta dalam prediksi perilaku di masa depan [6]. *Machine Learning* berperan dalam *cybersecurity* dan *digital forensics*. Penyelidik forensik digital menggunakan algoritme pembelajaran mesin untuk menganalisis sejumlah besar kumpulan data yang disimpan di berbagai lingkungan dan jaringan komputasi awan [8]. Kumpulan data ini kemudian dapat digunakan untuk memprediksi perilaku penggunanya. Selain itu, algoritme ini juga dapat melakukan pengenalan pola. Melalui penggunaan teknik *Machine Learning*, penyelidik menerapkan seperangkat aturan dan metode yang dapat digunakan untuk menemukan pola data yang menarik untuk mengidentifikasi potensi aktivitas kriminal [6].

Decision Tree adalah metode pembelajaran yang dapat digunakan untuk regresi dan klasifikasi tugas. Metode ini mudah diinterpretasikan dan dapat menghubungkan hasil dari tes dengan klasifikasi item data. Model *decision tree* mempertimbangkan berbagai logika keputusan dan memodelkannya ke dalam struktur seperti pohon [6] [9]. Decision tree memiliki peran yang signifikan dalam bidang digital forensik. Decision tree dapat digunakan dalam berbagai tahapan dalam proses forensik digital seperti Klasifikasi Bukti Digital, Analisis Log, Analisis Malware, Keputusan dalam Proses Investigasi, dan Pemulihan Data, dll.

Menurut *National Institute of Standards and Technology* (NIST) ada empat prosedur dan metodologi yang digunakan dalam Proses Investigasi Forensik Digital (*Digital Forensics Investigation Process*), untuk membantu organisasi memahami pentingnya penyelidikan mereka. Prosedur-prosedur tersebut dapat berupa dilakukan dengan cara yang berbeda tergantung pada kompleksitas penelitian [6]. Berikut tahapan proses investigasi forensik digital, pengumpulan data (*Data Collection*), Pemeriksaan (*Examination)*, Analisi (*Analysis)*, Pelaporan (*Reporting)* [5], [6], [7], [10]. NIST memiliki keunggulan dalam memilih dan menggunakan alat forensik. Setiap metodologi perlu diperbarui terus menerus mengikuti perkembangan digital teknologi [10].

Pada penelitian kali ini akan menggunakan metode *machine learning* (*decision tree)* sebagai metode yang digunakan untuk melakukan analisis forensik terhadap *mobile-Trojan Metasploit*. Dan menerapkan prosedur proses investigasi forensik digital dari *National Institute of Standards and Technology* (NIST) sebagai alur penelitian dari tahap awal yaitu pengumpulan data (*Data Collection*) sampai tahap akhir yaitu pelaporan (*Reporting).*

Pada penelitian ini [11] Algoritma Pohon Keputusan dalam Forensik Digital Chhabra dkk. mengusulkan kerangka kerja arsitektur yang menggabungkan kerangka kerja MapReduce, Sistem File Terdistribusi Hadoop, dan algoritme pohon keputusan algoritma pohon keputusan. Kerangka kerja ini terdiri dari empat langkah: menangkap lalu lintas jaringan, mengubahnya menjadi format yang dapat dibaca manusia, menyaring paket, menganalisis data untuk aktivitas berbahaya, dan terakhir, menyajikan analisis dan visualisasi ancaman. Sebuah pohon keputusan melabeli lalu lintas berbahaya dan tidak berbahaya, meningkatkan akurasi dan efisiensi waktu di setiap fase. Hasil penelitian mengungkapkan bahwa model tersebut dapat mendeteksi 99% dari semua lalu lintas berbahaya dan tidak berbahaya.

Pada penelitian ini [12] , pendekatan hybrid diusulkan oleh Usman et al. untuk mengatasi masalah terkait dengan sistem reputasi IP dengan menggabungkan kemampuan berbagai data teknik forensik seperti pembelajaran mesin, Analisis Malware Dinamis, dan Intelijen Ancaman Siber. Dengan menggunakan forensik data besar, ia dapat memprediksi kemungkinan kemungkinan serangan tertentu terjadi sebelum terjadi dan kemudian mengklasifikasikannya sesuai dengan karakteristik perilakunya. Sistem yang diusulkan dievaluasi terhadap berbagai sistem reputasi yang ada dengan menggunakan beberapa teknik ML seperti DT, SVM, dan NB. DT berkinerja baik dalam hal recall, F-measure, dan presisi skor. Performance comparison Table using $Dataset1$ DT mendapati skor, F-measure 78%, Precision 75%, Recall 80% dan pada Performance comparison Table using $Dataset2$ F-measure 99%, Precision 100%, Recall 98% serta pada Correctly Identified verses Incorrectly Identified Classes in $Dataset1$ Correct Prediction 93%, Incorrect Prediction 07% dan Correctly Identified verses Incorrectly Identified Classes in $Dataset2$ Prediction 93,5%, Incorrect Prediction 6,5%.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang ada, permasalahan yang akan dibahas pada penelitian ini, yaitu:

1. Bagaimana metode *Machine Learning* (*Decision Tree*) dalam melakukan analisis forensik dan efektivitas metode ini pada serangan mobile-trojan metasploit?
2. Bagaimana analisis forensik berupa deteksi terhadap serangan mobile-trojan metasploit?
3. Bagaimana analisis forensik berupa visualisasi terhadap serangan mobile-trojan metasploit?

1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini, yaitu:

1. Penelitian ini menggunakan dataset yang berasal dari lingkungan riset atau penelitian *Communication Network and Information Security Research Group* (COMNETS)
2. Penelitian ini hanya fokus pada penerapan metode *Machine Learning* (*Decision Tree*) khususnya dalam konteks analisis forensik terhadap serangan mobile-trojan metasploit.
3. Analisis forensik hanya berupa deteksi dan visualisasi terhadap serangan mobile-trojan metasploit.

1.4 Tujuan Penelitian

Berikut tujuan dilakukannya penelitian ini, yaitu:

1. Melakukan analisis forensik menggunakan metode *Machine Learning* (*Decision Tree*) sehingga mampu memberikan hasil pelaporan yang terperinci mencakup dokumentasi hasil, interpretasi kesimpulan dan rekomendasi tindak lanjut.
2. Melakukan evaluasi kinerja deteksi malware trojan dengan decision tree.
3. Melakukan evaluasi kinerja visualisasi malware trojan dengan decision tree.

1.5 Manfaat Penelitian

Beberapa manfaat yang bisa diperoleh dari hasil penelitian ini, yaitu:

1. Memberikan pemahaman pengembangan teknik analisis forensik, khususnya dalam konteks serangan mobile-trojan metasploit, dengan menerapkan metode *Machine Learning (Decision Tree*).
2. Mengembangkan sistem deteksi dan visualisasi serangan siber yang efektif dan dapat membantu melindungi jaringan komputer dari serangan yang merugikan.
3. Meningkatkan kesadaran bagi pembaca untuk melakukan pengamanan pada perangkat seluler agar terhindar dari serangan malware khususnya mobile-trojan.

1.6. Metodologi Penelitian

Metodologi penelitian yang diterapkan dalam penelitian ini meliputi beberapa tahapan sebagai berikut:

1.6.1 Machine Learning (Decision Tree)

Decision Tree digunakan dalam penelitian untuk mengeksekusi data yang telah dikumpulkan dengan metode ekstraksi data, data processing, identifikasi anomali dan feature selection selanjutnya digunakan untuk menganalisis hasil dari pengeksekusian data yang telah dilakukan tersebut.

1.6.2 Pengumpulan Data (*Data Collection*)

Tahap ini merupakan tahapan paling awal yaitu pengumpulan data, dengan tahapan sebagai beriku :

a. Identifikasi Sumber Data:

Menentukan sumber-sumber data forensik mobile yang relevan, termasuk log aplikasi, file sistem, log jaringan, dan data forensik lainnya yang berkaitan dengan serangan Trojan Metasploit.

b. Ekstraksi Data:

Mengekstraksi data dari sumber-sumber yang telah diidentifikasi. Yang melibatkan ekstraksi log jaringan, snapshot file sistem, dan informasi forensik dari perangkat mobile yang mungkin terinfeksi.

1.6.3 Pemeriksaan (*Examination*)

Tahap selanjutnya merupakan pemeriksaan yang mengekstraksi data yang telah dikumpulkan, dengan tahapan sebagai berikut :

a. Membuat Label:

Melakukan pelabelan dalam pengolahan data untuk mengklasifikasikan data apakah tergolong *benign* atau *malicious*.

b.Exploratory Data Analysis:

Exploratory Data Analysis adalah langkah penting dalam menyelidiki data dengan tujuan menemukan pola, mengidentifikasi anomali, menguji hipotesis, dan memverifikasi asumsi dengan menggunakan ringkasan statistik dan representasi grafis.

c. Data Preprocessing:

Membersihkan dan persiapkan data untuk analisis. Melibatkan penanganan nilai yang hilang, normalisasi, dan encoding jika diperlukan.

1.6.4 Analisis (*Analysis*)

Tahap ini merupakan tahapan menganalisis hasil dari tahap sebelumnya.

a. Pembangunan Model Decision Tree:

Menggunakan dataset yang telah dipersiapkan. Mengidentifikasi variabel target, misalnya, status terinfeksi atau tidak terinfeksi. Sesuaikan parameter Decision Tree seperti kedalaman dan kriteria pemilihan node.

b. Evaluasi Model:

Gunakan dataset evaluasi yang tidak terlibat dalam pelatihan untuk mengevaluasi kinerja model Decision Tree. Menggunakan metrik seperti akurasi, presisi, recall, dan F1-score untuk mengukur efektivitas model.

1.6.5 Pelaporan (*Reporting*)

Tahapan ini merupakan langkah akhir, hasil dari semua langkah yang dilakukan sebelumnya akan dirumuskan menjadi suatu kesimpulan serta saran dibutuhkan untuk mengetahui kekurangan pada hasil perancangan dan faktor penyebabnya.

a. Dokumentasi Hasil:

Mendokumentasikan hasil analisis forensik mobile dengan Decision Tree. Sertakan deskripsi model, aturan keputusan, dan hasil evaluasi kinerja secara rinci.

b. Interpretasi Kesimpulan:

Hasil dari analisis di tulis ke dalam kesimpulan dan mejelaskan temuan-temuan kunci dan signifikansi hasil analisis.

1.7 Sistematika Penulisan

Sistematika dalam penulisan skripsi ini sebagai berikut :

BAB I PENDAHULUAN

Bab pertama berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan yang dipakai.

BAB II TINJAUAN PUSTAKA

Bab kedua akan menjelaskan mengenai penelitian terkait, dasar-dasar teori dan istilah-istilah penting yang menjadi landasan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ketiga berisi tentang tahapan atau alur penelitian yang dilakukan. Dimulai dari studi literatur, perancangan topologi dan tahapan pembuatan dataset, pengumpulan data, pemeriksaan, analisis, dan pelaporan.

BAB IV HASIL DAN ANALISIS

Bab keempat akan menjelaskan hasil dari pengujian serta analisis terhadap hasil yang diperoleh.

BAB V KESIMPULAN DAN SARAN

Bab kelima atau terakhir berisi kesimpulan dan saran dari penulis atas hasil dan analisa dari penelitian yang telah dilakukan.

DAFTAR PUSTAKA

[1] A. Qamar, A. Karim, and V. Chang, "Mobile malware attacks: Review, taxonomy & future directions," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 887–909, 2019, doi: 10.1016/j.future.2019.03.007.

[2] A. C. Cinar and T. B. Kara, "The current state and future of mobile security in the light of the recent mobile security threat reports," *Multimed. Tools Appl.*, vol. 82, no. 13, pp. 20269–20281, 2023, doi: 10.1007/s11042-023-14400-6.

[3] M. ElKashlan, H. Aslan, M. Said Elsayed, A. D. Jurcut, and M. A. Azer, "Intrusion Detection for Electric Vehicle Charging Systems (EVCS)," *Algorithms*, vol. 16, no. 2, Feb. 2023, doi: 10.3390/a16020075.

[4] M. N. Alenezi, H. Alabdulrazzaq, A. A. Alshaher, and M. M. Alkharang, "Evolution of Malware Threats and Techniques: A Review," *Int. J. Commun. Networks Inf. Secur.*, vol. 12, no. 3, pp. 326–337, 2020, doi: 10.17762/ijcnis.v12i3.4723.

[5] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A review of mobile forensic investigation process models," *IEEE Access*, vol. 8, pp. 173359–173375, 2020, doi: 10.1109/ACCESS.2020.3014615.

[6] Y. A. B. B, H. Shaker, and B. Kumar, *Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022)*. Atlantis Press International BV, 2023. doi: 10.2991/978-94-6463-110-4.

[7] R. Wilson and H. Chi, "A Framework for validating aimed mobile digital forensics evidences," *Proc. ACMSE 2018 Conf.*, vol. 2018-Janua, 2018, doi: 10.1145/3190645.3190695.

[8] E. Nowroozi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A survey of machine learning techniques in adversarial image forensics," *Comput. Secur.*, vol. 100, p. 102092, 2021, doi: 10.1016/j.cose.2020.102092.

[9] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Comput. Sci.*, vol. 2, no. 3, pp. 1–21, 2021, doi: 10.1007/s42979-021-00592-x.

[10] R. Umar, I. Riadi, and G. M. Zamroni, “Mobile forensic tools evaluation for digital crime investigation,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, pp. 949–955, 2018, doi: 10.18517/ijaseit.8.3.3591.

[11] G. S. Chhabra, V. Singh, and M. Singh, “Hadoop-based analytic framework for cyber forensics,” *Int. J. Commun. Syst.*, vol. 31, no. 15, pp. 1–17, 2018, doi: 10.1002/dac.3772.

[12] N. Usman *et al.*, “Intelligent Dynamic Malware Detection using Machine Learning in IP Reputation for Forensics Data Analytics,” *Futur. Gener. Comput. Syst.*, vol. 118, no. May, pp. 124–141, 2021, doi: 10.1016/j.future.2021.01.004.

[13] R. M. A. Mohammad and M. Alqahtani, “A comparison of machine learning techniques for file system forensics analysis,” *J. Inf. Secur. Appl.*, vol. 46, no. September 2016, pp. 53–61, 2019, doi: 10.1016/j.jisa.2019.02.009.

[14] I. K. Thajeel, K. Samsudin, S. J. Hashim, and F. Hashim, “Machine and Deep Learning-based XSS Detection Approaches: A Systematic Literature Review,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 7, p. 101628, 2023, doi: 10.1016/j.jksuci.2023.101628.

[15] A. S. Review, “Android Mobile Malware Detection Using Machine Learning :,” pp. 1–34, 2021.

[16] L. E. Richter, A. Carlos, and D. M. Beber, *Multi-Pattern Matching Based Dynamic Malware Detection in Smart Phones*.

[17] R. Surendran, T. Thomas, and S. Emmanuel, “A TAN based hybrid model for android malware detection,” *J. Inf. Secur. Appl.*, vol. 54, no. May, 2020, doi: 10.1016/j.jisa.2020.102483.

[18] V. Sihag, M. Vardhan, and P. Singh, “A survey of android application and malware hardening,” *Comput. Sci. Rev.*, vol. 39, no. May, 2021, doi: 10.1016/j.cosrev.2021.100365.

[19] Y. Salah, I. Hamed, S. Nabil, A. Abdulkader, and M.-S. M. Mostafa, “Mobile Malware Detection: A Survey,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 17, no. 1, 2019, [Online]. Available: https://sites.google.com/site/ijcsis/

[20] A. Lekssays, B. Falah, and S. Abufardeh, “A novel approach for android malware detection and classification using convolutional neural networks,”

ICSOFT 2020 - Proc. 15th Int. Conf. Softw. Technol., no. September, pp. 606–614, 2020, doi: 10.5220/0009822906060614.

[21] K. Barapatre and P. Parkhi, "Android Spy Agent-Remote Access Trojan," *Int. Res. J. Eng. Technol.*, no. May, pp. 4548–4552, 2020, [Online]. Available: www.irjet.net

[22] VICTOR CHEBYSHEV, "Mobile malware evolution 2019," *SECURELIST by Kaspersky*, 2019. https://securelist.com/mobile-malware-evolution-2019/96280/ (accessed Dec. 13, 2023).

[23] P. Ahlawat, S. Dhar, S. Wagh, and A. Koppad, "Remote Access Tool Using Metasploit," pp. 425–427, 2017.

[24] "Reverse connection," *wikipedia*, 2023. https://en.wikipedia.org/wiki/Reverse_connection (accessed Dec. 13, 2023).

[25] T. H. Sandhu, "Machine Learning and Natural Language Processing – a Review," *Int. J. Adv. Res. Comput. Sci.*, vol. 9, no. 2, pp. 582–584, 2018, doi: 10.26483/ijarcs.v9i2.5799.

[26] M. Alloghani, D. Al-Jumeily, J. Mustafina, A. Hussain, and A. J. Aljaaf, *A Systematic Review on Supervised and Unsupervised Machine Learning Algorithms for Data Science*. 2020. doi: 10.1007/978-3-030-22475-2_1.

[27] B. Charbuty and A. Abdulazeez, "Classification Based on Decision Tree Algorithm for Machine Learning," *J. Appl. Sci. Technol. Trends*, vol. 2, no. 01, pp. 20–28, 2021, doi: 10.38094/jastt20165.

[28] A. Waluyo, H. Jatnika, M. R. S. Permatasari, T. Tuslaela, I. Purnamasari, and A. P. Windarto, "Data Mining Optimization uses C4.5 Classification and Particle Swarm Optimization (PSO) in the location selection of Student Boardinghouses," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 874, no. 1, 2020, doi: 10.1088/1757-899X/874/1/012024.

[29] J. Mrva, S. Neupauer, L. Hudec, J. Sevcech, and P. Kapec, "Decision support in medical data using 3D decision tree visualisation," *2019 7th E-Health Bioeng. Conf. EHB 2019*, no. November, 2019, doi: 10.1109/EHB47216.2019.8969926.

[30] H. H. Patel and P. Prajapati, "Study and Analysis of Decision Tree Based Classification Algorithms," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 10, pp. 74–

78, 2018, doi: 10.26438/ijcse/v6i10.7478.

[31] J. Bulow and M. Scherman, “Insider Threat detection using Isolation Forest,” pp. 1–67, 2018, [Online]. Available: http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8952203&fileOId=8952292