DETEKSI SERANGAN *DDOS DOS* DAN *MITM* PADA JARINGAN *SMARTHOME* DENGAN MENGGUNAKAN METODE *DECISION TREE*

SKRIPSI

Oleh:

EDO PRATAMA

09011182126007

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

LEMBAR PENGESAHAN

DETEKSI SERANGAN DDOS DOS DAN MITM PADA JARINGAN SMARTHOME DENGAN MENGGUNAKAN METODE DECISION TREE

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh
Gelar Sarjana Komputer

Program Studi Sistem
Komputer Jenjang S1

Oleh:

EDO PRATAMA

09011182126007

Palembang, 6 Januari 2025

Pembimbing I	Pembimbing II
Prof. Ir. Deris Stiawan, M.T., Ph.D.	**Nurul Afifah, M.Kom.**
NIP. 197806172006041002	NIP. 199211102023212049

Mengetahui,
Ketua Jurusan Sistem Komputer

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

AUTHENTICATION PAGE

DETECTION OF DDOS DOS AND MITM ATTACKS ON SMARTHOME NETWORKS USING DECISION TREE METHOD

THESIS

Submitted in Partial Fulfillment of Requirements for the
Degree of Bachelor of Computer Science

Dept. Of Computer System
Bachelor's Degree

By:

EDO PRATAMA

09011182126007

Palembang, 16 January 2025

Supervisor

Prof. Ir. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Co - Supervisor

Nurul Afifah, M.Kom.
NIP. 199211102023212049

Acknowledge,
Head of Computer Systems Department

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

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 09 Januari 2025

Tim Penguji :

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

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Edo Pratama

NIM : 09011182126007

Judul : Deteksi Serangan *DDoS DoS MITM* Pada Jaringan *Smarthome* Dengan Menggunakan Metode *Decision Tree*

Hasil Pengecekan Software *iThenticate/Turnitin* : 7%

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

Demikian, pernyataan ini saaya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Palembang, 7 Januari 2025

g menyatakan

Edo Pratama

NIM. 09011182126007

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh. Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan segala nikmat dan karunia-Nya sehingga penulis dapat menyelesaikan Skripsi dengan judul "**Deteksi Serangan *DDoS DoS MITM* Pada Jaringan *Smarthome* Dengan Menggunakan Metode *Decision Tree***". Shalawat beriringkan salam senantiasa tercurahkan kepada Nabi Muhammad Shallallahu 'Alaihi Wasallam yang telah membawa kedamaian dan rahmat untuk semesta alam serta menjadi suri tauladan bagi umatnya.

Skripsi ini merupakan salah satu syarat untuk memenuhi sebagian kurikulum dan syarat kelulusan Mata Kuliah Skripsi pada Jurusan Sistem Komputer, Universitas Sriwijaya. Dalam penyusunan Skripsi ini, penulis telah banyak memperoleh bantuan, bimbingan dan saran baik moril maupun materil dari berbagai pihak. Oleh karena itu, ucapan terima kasih sebesar-besarnya diberikan kepada:

1. Allah SWT yang selalu memberikan rahmat dan karunia-Nya kepada penulis.
2. Ibu Dalilam, Bapak Zoherman, dan Adik penulis tercinta serta seluruh keluarga besar yang telah banyak memberikan do'a, nasihat, serta motivasi kepada penulis selama ini.
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 Universitas Sriwijaya.
5. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D., IPU., ASEAN-Eng. selaku Dosen Pembimbing I Tugas Akhir dan juga Dosen Pembimbing Akademik.
6. Ibu Nurul Afifah, M.Kom. selaku Dosen Pembimbing II Tugas Akhir.
7. Bapak Angga selaku admin Jurusan Sistem Komputer.
8. Ibu Devi Putri Pranata selaku teman dekat.

9. Kakak - Kakak tingkat SK Unggulan dan SK Reguler yang termasuk tim riset COMNETS.
10. Teman teman seperjuangan Jurusan Sistem Komputer Angkatan 2021 terkhusus kelas A.
11. Seluruh pihak yang membantu dalam menyelesaikan laporan ini yang tidak bisa disebutkan satu persatu.
12. Almamater

Penulis menyadari bahwa masih terdapat kekurangan dalam penulisan Skripsi ini, baik dari materi maupun teknik penyajiannya, mengingat kurangnya pengetahuan dan pengalaman penulis. Untuk itu, penulis mengharapkan adanya kritik dan saran yang membangun agar dapat memperbaiki kekurangan-kekurangan tersebut kedepannya nanti.

Penulis berharap semoga penulisan Skripsi 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.

Palembang, 7 Januari 2025
Penulis,

Edo Pratama
NIM.09011182126007

DETEKSI SERANGAN DDOS DOS DAN MITM PADA JARINGAN SMARTHOME DENGAN MENGGUNAKAN METODE DECISION TREE

Edo Pratama (09011182126007)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

Email: 09011182126007@student.unsri.ac.id

ABSTRAK

Smart Home merupakan salah satu teknologi otomatisasi yang digunakan untuk memfasilitasi aktivitas rumah dengan bantuan *Internet of Things* (IoT). Teknologi IoT memunkinkan benda - benda di sekitar kita terhubung dengan Internet seperti sensor, kamera, dan perangkat pintar lainnya. Dengan berkembangnya teknologi IoT memungkinkan menjadi salah satu target serangan *cyber* seperti *Distributed Denial of Service* (DDoS), *Denial of Service* (DoS), dan *Man in the Middle* (MITM). Dalam penelitian ini penulis melakukan sebuah simulasi serangan nyata menggunakan serangan DDoS, DoS, dan MiTM terhadap perangkat *Smart Home* yang lemah akan keamanannya sebagai pengujian. Pembuktian menggunakan Tools *Information Security* menjadi salah satu titik keberhasilan dari pengujian ini dengan menggunakan tools seperti *CapLoader, Network Miner, Dynamite Lab, dan IDS snort*, selain itu penggunaan *T – shark* juga berperan sebagai solusi untuk melakukan *ekstraksi* data dari .pcap – csv yang bakalan digunakan untuk diuji coba dengan algoritma *Machine Learning* dengan memanfaatkan model *Decision Tree.* Hasil penelitian menunjukkan bahwa metode *Decision Tree* dengan kriteria gini mencapai performa dengan nilai f1_score terbaik pada model *Decison Tree* kriteria gini dengan nilai MITM 98.68%, Benign 99.97%, DDoS 99.99%,dan DoS 99.96%.

Kata Kunci: Smarthome, DDoS, DoS, MiTM, Snort, T-Shark, Caploader, Network Miner, DynamiteLab, Decision Tree.

DETECTION OF DDOS DOS AND MITM ATTACKS ON SMARTHOME NETWORKS USING DECISION TREE METHOD

Edo Pratama (09011182126007)

Department of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email: 09011182126007@student.unsri.ac.id

ABSTRACT

Smart Home is a form of automation technology designed to facilitate household activities with the help of the Internet of Things (IoT). IoT technology enables objects around us, such as sensors, cameras, and smart devices, to connect to the Internet. However, the advancement of IoT technology also makes it a target for cyberattacks such as Distributed Denial of Service (DDoS), Denial of Service (DoS), and Man-in-the-Middle (MITM) attacks. In this study, the authors conducted a real-world simulation of attacks, including DDoS, DoS, and MITM, on vulnerable Smart Home devices as a form of security testing. The use of information security tools played a crucial role in the success of this testing, employing tools such as CapLoader, Network Miner, Dynamite Lab, and IDS Snort. Additionally, T-Shark was utilized to extract data from .pcap files into .csv format for testing with Machine Learning algorithms, specifically using the Decision Tree model. The results of the study demonstrated that the Decision Tree method with the Gini criterion achieved excellent performance, with the highest F1-scores recorded for the following categories: MITM at 98.68%, Benign at 99.97%, DDoS at 99.99%, and DoS at 99.96%.

Keyword: Smarthome, DDoS, DoS, MiTM, Snort, T-Shark, Caploader, Network Miner, DynamiteLab, Decision Tree.

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Smarthome merupakan salah satu teknologi otomatisasi yang digunakan untuk memfasilitasi aktivitas di rumah, dan sangat memungkinkan untuk mengoperasikan dan memantau rumah dengan bantuan *Internet of Things* (*IoT*) [1]. *IoT* adalah konsep di mana objek-objek fisik atau perangkat elektronik yang berbeda dapat terhubung satu sama lain melalui jaringan internet, berbagi data dan informasi secara otomatis tanpa perlu campur tangan manusia. Ini membuka pintu bagi pengumpulan data yang lebih luas dan integrasi yang lebih baik antara dunia fisik dan dunia digital [2].

Teknologi *IoT* memungkinkan benda-benda di sekitar kita terhubung dengan Internet, seperti sensor, kamera, dan perangkat pintar lainnya [3]. Dengan barkembangnya teknologi IoT dari waktu ke waktu, Jaringan IoT menjadi salah satu target serangan *cyber*, yang sebagian besar disebabkan oleh sifat IoT yang terbatas [4].

Ada berbagai macam–macam jenis pelanggaran, serangan seperti *Distributed Denial-of-Service* (*DDoS*) yaitu sebuah serangan yang dapat membanjiri target dengan memanfaatkan *bootnet* melalui jaringan komputer yang terdiri dari banyak perangkat yang telah terinfeksi oleh *malware* tanpa sepengetahuan pemiliknya serangan pelanggaran *DDoS* ini dapat mengakibatkan bencana bagi penggunaan IoT [4], [5], *Denial of Service* (*DoS*) merupakan upaya untuk membuat mesin atau sumber daya jaringan tidak tersedia dengan membanjiri pengguna yang dituju dengan cara sementara atau tidak terbatas dengan mengganggu layanan melalui sumber yang sama [6], *Man in the Middle* (*MITM*) merujuk pada jenis serangan keamanan komputer di mana seorang penyerang memposisikan dirinya di antara dua entitas yang berkomunikasi, seperti antara pengguna dan server, tanpa diketahui oleh keduanya [7] .

Decion Tree merupakan salah satu algoritma *machine learning* yang paling efektif saat mendeteksi serangan *multiclass* pada jaringan *IoT smarthome* [8]. Algoritma *Decision Tree* merupakan algoritma pembelajaran yang dapat konsisten

dan mudah beradaptasi untuk masalah *klasifikasi* dan *regresi*, dengan potensi penerapan di berbagai bidang [9]. *Decision Tree* membutuhkan kombinasi pengetahuan yang cukup mendalam mengenai *Machine Learning*. Teknik ini juga biasanya digunakan untuk mendeteksi serangan pada suatu perangkat *IoT*, mengungguli model canggih yang ada dan mencapai tingkat akurasi dan *F1_score* yang tinggi [10].

Pada penelitian penulis melakukan *attack* pada perangkat untuk mengambil dataset dengan kondisi perangkat yaitu *normal, mix,* dan *attack*. Dataset merupakan kumpulan serangan *DDoS, DoS, MITM*, dan data *Benign* [11]. Dataset menunjukkan bahwa Perangkat yang terkena infeksi serangan *DDoS, DoS,* dan *MITM* akan merubah pola lalu lintas yang tidak biasa dan tidak wajar pada *wireshark* [12]. *Wireshark* adalah perangkat lunak analisis jaringan yang dapat merekam dan menganalisis paket data yang melewati antarmuka jaringan. Saat terjadi serangan *DDoS,* akan terjadi lonjakan besar dalam jumlah paket yang dikirim ke perangkat yang *smarthome* [13]. Pola lalu lintas ini akan menunjukkan karakteristik yang khas dari serangan *DDoS,* seperti banyaknya paket yang dikirim secara bersamaan dari berbagai alamat IP yang berbeda (dengan *botnet* sebagai contoh), atau jenis serangan *DDoS* tertentu seperti *SYN flood* atau *UDP flood* [14].

Penelitian [15] melakukan analisis serangan pada jaringan yang terhubung pada *attacker* yang diskenariokan menggunakan jaringan pribadi. Dampak dari aktivitas itu mengakibatkan perangkat perangkat *smarthome* menjadi terhenti dan lambat, semua ini terjadi karena serangan *DDoS* dan *DoS* yang menargetkan jaringan IoT *smarthome*, sedangkan serangan *MITM* berfungsi untuk melihat apa saja yang sedang terjadi pada jaringan *smarthome* tersebut [16].

Penelitian [17] menggunakan *dataset .pcap* yang diambil menggunakan *wireshark dan* diolah menjadi *.csv*, hasil *Attack* pada jaringan pribadi lalu dilakukan *ekstraksi* data untuk melihat data secara keseluruhan menggunakan tools *T-Shark* lalu dilakukan pengelolahan data menggunakan algoritma *Decision Tree*.

Penelitian menggunakan dataset yang telah dibuat dari hasil *mapping* Jaringan pribadi yang terhubung keperangkat *IoT smarthome*. Hasil kerja *Decision Tree* menunjukkan bahwa kinerja algoritma *Decision Tree* lebih unggul dari performa Algoritma *Machine Learning* lainnya untuk penelitian ini. Sebagian besar

metode ini digunakan oleh data besar seperti data *DDoS* dan *DoS*. Hasil kinerja menunjukkan bahwa tingkat penyebaran *DDoS* bernilai 61,1%, *DoS* bernilai 13,2%, *MITM* 25,2%, dan *Benign* bernilai 0,5%.

Penelitian [18] menggunakan sampel *smarthome COMNETS* dataset yang di analisis dengan metode *Decision Tree*. Hasil analisis menunjukkan bahwa serangan dengan tipe *Misc Attack* atau *Maliciuos Attack* dengan jenis *DDoS*, *Misc Attack* atau *Maliciuos Attack* dengan jenis *DoS*, dan *ARP spoofing* dengan jenis *MITM*, serangan ini (DDoS dan DoS) adalah serangan yang dilakukan dengan cara membanjiri target (Jaringan IoT *smarthome*) sehingga system atau jaringan tersebut tidak dapat berfungsi seperti jaringan normal bisasanya, dan Serangan (*MITM*) berfungsi sebagai mata mata kejadian apa saja yang dilakukan didalam jaringan *IoT smarthome*.

Penelitian ini [19] mendeteksi adanya *anomali* pada jaringan *IoT* termasuk juga jenis serangan *Distributed Denial-of-Service* dan *Denial-of-Service* menggunakan dataset LATAM-DoS-IoT, LATAM-DDoS-IoT, LATAM-Bot-DoS-IoT, LATAM-Bot-DDoS-IoT mendapatkan nilai F1-Score untuk model Decision tree dengan dataset LATAM-DoS-IoT senilai 99,99%, 98,90% untuk LATAM-DDoS-IoT, 99,98% untuk LATAM-Bot- DoS-IoT, dan 98,86% untuk nilai LATAM-Bot-DDoS-IoT. Nilai yang didapatkan dengan menggunakan metode *Decision tree* sangat tinggi, Metode deteksi anomali dalam sistem *smarthome* IoT memerlukan algoritma yang efektif dan efisien untuk mengidentifikasi perilaku tidak biasa atau mencurigakan yang dapat mengindikasikan adanya gangguan atau ancaman keamanan. Beberapa metode yang telah diuji, seperti *Adaboost*, *Artificial Neural Network* (ANN), *Random Forest*, *Long Short-Term Memory* (LSTM), dan Decision Tree, menunjukkan hasil yang menjanjikan dalam mendeteksi anomali. [20].

Pada penelitian ini akan dilakukan deteksi jaringan menggunakan metode *Decision Tree* dan *divalidasi* dengan menggunakan beberapa tools seperti *CapLoader*, *Network Miner*, *lab.dynamite* dan *IDS snort* dengan sample dataset *pcap* hasil mapping yang dirujuk pada penulis [21], [22]. Oleh karena itu, penelitian ini akan diberi judul "*Deteksi Serangan DDoS DoS dan MITM Pada Jaringan Smarthome Dengan Menggunakan Metode Decision Tree*" dengan harapan metode

Decison Tree mampu menyelesaikan persoalan pelabelan aktivitas serangan serta persoalan fitur pada penelitian sebelumnya.

1.2 Rumusan Masalah

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

1. Bagaimana cara mendeteksi serangan *DDoS, DoS,* dan *MITM* ?
2. Bagaimana cara melakukan ekstraksi data pada dataset *DDoS, DoS,* dan *MITM* ?
3. Bagaimana cara mengukur performa metrik dan hasil deteksi menggunakan algoritma *Decision Tree* ?

1.3 Batasan Masalah

Berikut batasan masalah pada penelitian ini, yaitu:

1. Penelitian ini tidak akan membahas lebih jauh tentang bagaimana aksi pencegahan dan penanganan dari Serangan *DDoS, DoS, dan MITM.*
2. Penelitian ini hanya mendeteksi Serangan *DDoS, DoS, MITM.*

1.4 Tujuan

1. Mampu mendekteksi serangan *DDoS, DoS,* dan *MITM* menggunakan beberapa tools dibidang Information Security.
2. Mampu melakukan ekstraksi data pada dataset *DDoS, DoS,* dan *MITM* menggunakan T-Shark.
3. Mampu menghasilkan model terbaik pada aloritma *Decision Tree* dalam mendeteksi serangan *DDoS, DoS,* dan *MITM*.

1.5 Manfaat

1. Menampilkan keberadaan Serangan *DDoS, DoS, MITM* pada jaringan *smarthome* dengan akurat.
2. Menampilkan hasil analisa serangan *DDoS, DoS, MITM* dan aktivitas dari Jaringan *smarthome*.
3. Menampilkan Performa terbaik dari algoritma *Machine Learning*.

1.6 Metodologi Penelitian

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

1. Studi Pustaka / Literatur

   Tahap ini diawali dengan mencari informasi dan masalah yang sesuai dan relevan untuk diangkat sebagai penelitian. Kemudian mencari beberapa referensi seperti artikel, publikasi ilmiah, buku dan sumber lain yang relevan dan berkaitan langsung dengan topik Skripsi ini.

2. Perancangan Sistem

   Tahap ini membahas masalah proses bagaimana cara membangun metode atau pendekatan tertentu, perangkat lunak maupun perangkat keras yang digunakan untuk konfigurasi sistem.

3. Pengujian

   Pada tahap ini dilakukan pengujian berdasarkan metode yang digunakan dalam penelitian dan metode-metode yang digunakan oleh penelitian sebelumnya, sehingga didapatkan hasil yang sesuai.

4. Analisa

   Tahap ini dilakukan pengolahan data dan analisa data yang didapatkan dari hasil pengujian yang dilakukan sebelumnya untuk mendapatkan data yang aktual. Kemudian hasil akan dianalisis dengan tujuan untuk mengetahui kekurangan pada hasil perancangan sistem tersebut.

5. Kesimpulan dan Saran

   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.

1.7 Sistematika Penulisan

Adapun sistematika dalam penulisan Skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini merupakan penjelasan berisi mengenai Latar belakang, Rumusan Masalah, Batasan Masalah, Tujuan, Manfaat, Metodologi penelitian dan Sistematika penulisan yang digunakan dalam Skripsi ini.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi mengenai bacaan *literature* yang menjadi referensi serta penjelasan pendukung dari penelitian Deteksi serangan *DDoS*, *DoS*, dan *MITM*.

BAB III METODOLOGI PENELITIAN

Pada bab ini membahas proses penelitian, kerangka penelitian, serta menjelaskan metodologi penelitian.

BAB IV HASIL DAN ANALISA

Pada bab ini menjelaskan hasil dari penelitian dan mendeteksi serangan DDoS, DoS, dan MITM dengan menerapkan metode *Decison Tree* pada jaringan *smarthome*.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan dari penelitian yang dilakukan serta saran untuk penelitian selanjutnya dimasa mendatang.

DAFTAR PUSTAKA

[1] M. Syahdi Nasution, Muhammad Amin, and Wirda Fitriani, "Smart Sistem Iot Pemberi Pakan Ikan Dengan Menggunakan Metode Time Schedulling Berbasis Mikrokontroller," *J. Zetroem*, vol. 5, no. 2, pp. 161–164, 2023, doi: 10.36526/ztr.v5i2.3082.

[2] N. Hardi, R. Afuw Rouf Subyan, and A. Arbasyah, "Alat Berbasis IOT Smarthome Monitoring dan Kontrol via Telegram Menggunakan Nodemcu," *Insantek*, vol. 4, no. 1, pp. 7–11, 2023, doi: 10.31294/instk.v4i1.2018.

[3] R. Muzawi, Y. Efendi, and N. Sahrun, "Prototype Pengendalian Lampu Jarak Jauh Dengan Jaringan Internet Berbasis Internet of Things(IoT) Menggunakan Rasberry Pi 3," *J. Inf.*, vol. 3, no. 1, pp. 46–50, 2018, doi: 10.25139/ojsinf.v3i1.642.

[4] N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3559–3570, 2020, doi: 10.1109/JIOT.2020.2973176.

[5] P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-to-peer botnet," *1st Work. Hot Top. Underst. Botnets, HotBots 2007*, vol. 7, no. 2, pp. 113–127, 2007.

[6] S. Grabovsky, P. Cika, V. Zeman, V. Clupek, M. Svehlak, and J. Klimes, "Denial of Service Attack Generator in Apache JMeter," *Int. Congr. Ultra Mod. Telecommun. Control Syst. Work.*, vol. 2018-Novem, pp. 1–4, 2018, doi: 10.1109/ICUMT.2018.8631212.

[7] A. Mallik, A. Ahsan, M. M. Z. Shahadat, and J. C. Tsou, "Man-in-the-middle-attack: Understanding in simple words," *Int. J. Data Netw. Sci.*, vol. 3, no. 2, pp. 77–92, 2019, doi: 10.5267/j.ijdns.2019.1.001.

[8] E. Scornet, G. Biau, and J. P. Vert, "Consistency of random forests," *Ann. Stat.*, vol. 43, no. 4, pp. 1716–1741, 2015, doi: 10.1214/15-AOS1321.

[9] E. Scornet, "Random forests and kernel methods," *IEEE Trans. Inf. Theory*, vol. 62, no. 3, pp. 1485–1500, 2016, doi: 10.1109/TIT.2016.2514489.

[10] Z. Jin, J. Shang, Q. Zhu, C. Ling, W. Xie, and B. Qiang, "RFRSF: Employee Turnover Prediction Based on Random Forests and Survival Analysis," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes*

Bioinformatics), vol. 12343 LNCS, pp. 503–515, 2020, doi: 10.1007/978-3-030-62008-0_35.

[11] S. Manickam *et al.*, "Labelled Dataset on Distributed Denial-of-Service (DDoS) Attacks Based on Internet Control Message Protocol Version 6 (ICMPv6)," *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/8060333.

[12] M. Salman, Di. Husna, and N. Viani, "Static Analysis Method on Portable Executable Files for REMNUX based Malware Identification," in *2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST)*, Oct. 2019, pp. 1–6. doi: 10.1109/ICAwST.2019.8923331.

[13] T. V. Phan, S. Sultana, T. G. Nguyen, and T. Bauschert, "Q - TRANSFER: A Novel Framework for Efficient Deep Transfer Learning in Networking," *2020 Int. Conf. Artif. Intell. Inf. Commun. ICAIIC 2020*, pp. 146–151, 2020, doi: 10.1109/ICAIIC48513.2020.9065240.

[14] P. R C and R. R R Robinson, "A Comparative Study of Defense Mechanisms against SYN Flooding Attack," *Int. J. Comput. Appl.*, vol. 98, no. 18, pp. 16–21, 2014.

[15] Sutarti and Khairunnisa, "Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan Ddos (Distributed Denial of Service) Berbasis Honeypot," *J. PROSISKO*, vol. 4, no. 2, p. 8, 2017.

[16] R. Abdillah, A. A. Trinoto, and I. Himawan, "Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional. STATIC ANALYSIS USING MOBILE SECURITY FRAMEWORK FOR SMART HOME APPLIANCES," *J. Inf. Syst. Applied, Manag. Account. Res.*, vol. 7, no. 3, pp. 760–765, 2023, doi: 10.52362/jisamar.v7i3.1161.

[17] K. Zhang, K. Yang, S. Li, D. Jing, and H. B. Chen, "ANN-Based outlier detection for wireless sensor networks in smart buildings," *IEEE Access*, vol. 7, pp. 95987–95997, 2019, doi: 10.1109/ACCESS.2019.2929550.

[18] S. Megira, A. R. Pangesti, and F. W. Wibowo, "Malware Analysis and Detection Using Reverse Engineering Technique," *J. Phys. Conf. Ser.*, vol. 1140, no. 1, p. 012042, Dec. 2018, doi: 10.1088/1742-6596/1140/1/012042.

[19] J. G. Almaraz-Rivera, J. A. Perez-Diaz, J. A. Cantoral-Ceballos, J. F. Botero,

and L. A. Trejo, “Toward the Protection of IoT Networks: Introducing the LATAM-DDoS-IoT Dataset,” *IEEE Access*, vol. 10, no. October, pp. 106909–106920, 2022, doi: 10.1109/ACCESS.2022.3211513.

[20] N. Sarwar, I. S. Bajwa, M. Z. Hussain, M. Ibrahim, and K. Saleem, “IoT Network Anomaly Detection in Smart Homes Using Machine Learning,” *IEEE Access*, vol. 11, no. September, pp. 119462–119480, 2023, doi: 10.1109/ACCESS.2023.3325929.

[21] S. Raheja, G. Munjal, J. Jangra, and R. Garg, “Rule-Based Approach for Botnet Behavior Analysis,” *Intell. Data Anal. Terror Threat Predict. Archit. Methodol. Tech. Appl.*, pp. 181–208, 2021, doi: 10.1002/9781119711629.ch8.

[22] S. Chakrabarti, “Study of Snort-Based IDS,” no. Icwet, pp. 43–47, 2010.

[23] U. H. Garba, A. N. Toosi, M. F. Pasha, and S. Khan, “SDN-based detection and mitigation of DDoS attacks on smart homes,” *Comput. Commun.*, vol. 221, no. April, pp. 29–41, 2024, doi: 10.1016/j.comcom.2024.04.001.

[24] A. Wijayanto, I. Riadi, and Y. Prayudi, “TAARA Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 7, no. 2, pp. 208–217, 2023, doi: 10.29207/resti.v7i2.4589.

[25] E. Anthi, L. Williams, A. Javed, and P. Burnap, “Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks,” *Comput. Secur.*, vol. 108, p. 102352, 2021, doi: 10.1016/j.cose.2021.102352.

[26] K. Faqih and A. N. Afandi, “Smart Home Fog Computing Architecture Based on Internet of Things (IoT),” pp. 260–263.

[27] T. Purnama, Y. Muhyidin, and D. Singasatia, “Implementasi Intrusion Detection System (Ids) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi,” *J. Teknol. Inf. Dan Komun.*, vol. 14, no. 2, pp. 358–369, 2023, doi: 10.51903/jtikp.v14i2.726.

[28] R. Kurniawan and F. Prakoso, “Implementasi Metode IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System) untuk Meningkatkan Keamanan Jaringan,” *Sentinel*, vol. 3, no. 1, pp. 231–242,

2020, doi: 10.56622/sentineljournal.v3i1.20.

[29] A. R. Jakhale, “Design of anomaly packet detection framework by data mining algorithm for network flow,” *ICCIDS 2017 - Int. Conf. Comput. Intell. Data Sci. Proc.*, vol. 2018-Janua, pp. 1–6, 2017, doi: 10.1109/ICCIDS.2017.8272665.

[30] L. Alghamdi, M. Akter, J. Kropczynski, P. J. Wisniewski, and H. Lipford, “Co-designing Community-based Sharing of Smarthome Devices for the Purpose of Co-monitoring In-home Emergencies,” *Conf. Hum. Factors Comput. Syst. - Proc.*, 2023, doi: 10.1145/3544548.3581239.

[31] J. Singh, D. Watkinson, T. Farnham, and D. Puccinelli, *Detecting and Controlling Smart Lights with LiTalk*, vol. 1, no. 1. Association for Computing Machinery, 2022. doi: 10.1145/3556558.3558581.

[32] S. Fleck and W. Straßer, “Smart camera based monitoring system and its application to assisted living,” *Proc. IEEE*, vol. 96, no. 10, pp. 1698–1714, 2008, doi: 10.1109/JPROC.2008.928765.

[33] C. Keles, A. Karabiber, M. Akcin, A. Kaygusuz, B. B. Alagoz, and O. Gul, “A smart building power management concept: Smart socket applications with DC distribution,” *Int. J. Electr. Power Energy Syst.*, vol. 64, pp. 679–688, 2015, doi: 10.1016/j.ijepes.2014.07.075.

[34] C. Martinez, L. Eras, and F. Dominguez, “The Smart Doorbell: A proof-of-concept Implementation of a Bluetooth Mesh Network,” *2018 IEEE 3rd Ecuador Tech. Chapters Meet. ETCM 2018*, 2018, doi: 10.1109/ETCM.2018.8580325.

[35] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, “Cyber-attack modeling analysis techniques: An overview,” *Proc. - 2016 4th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2016*, pp. 69–76, 2016, doi: 10.1109/W-FiCloud.2016.29.

[36] A. Ahmad Hania, “Mengenal Artificial Intelligence, Machine Learning, & Deep Learning,” *J. Teknol. Indones.*, vol. 1, no. June, pp. 1–6, 2017, [Online]. Available: https://amt-it.com/mengenal-perbedaan-artificial-inteligence-machine-learning-deep-learning/

[37] Y. Y. Song and Y. Lu, “Decision tree methods: applications for classification

and prediction," *Shanghai Arch. Psychiatry*, vol. 27, no. 2, pp. 130–135, 2015, doi: 10.11919/j.issn.1002-0829.215044.

[38] P. Goloboff, "Improvements to resampling measures of group support," *Cladistics*, vol. 19, no. 4, pp. 324–332, 2003, doi: 10.1016/s0748-3007(03)00060-4.

[39] T. Wongvorachan, S. He, and O. Bulut, "A Comparison of Undersampling, Oversampling, and SMOTE Methods for Dealing with Imbalanced Classification in Educational Data Mining," *Inf.*, vol. 14, no. 1, 2023, doi: 10.3390/info14010054.

[40] A. Irfani, N. Iman, F. Dwi Sumadi, and Z. Sari, "Low Rate DDOS Attack Detection Using KNN On SD-IOT," *Repositor*, vol. 5, no. 1, pp. 603–608, 2023.

[41] L. Wu, Z. Qiu, Z. Zheng, H. Zhu, and E. Chen, "Exploring Large Language Model for Graph Data Understanding in Online Job Recommendations," *Proc. AAAI Conf. Artif. Intell.*, vol. 38, no. 8, pp. 9178–9186, 2024, doi: 10.1609/aaai.v38i8.28769.

[42] M. L. Sylvia and S. Murphy, *Exploratory Data Analysis*, vol. 44, no. 2013. 2023. doi: 10.1891/9780826163240.0014.

[43] A. Ainurrohmah and D. T. Wiyanti, "Analisis Performa Algoritma Decision Tree, Naive Bayes, K-Nearest Neighbor untuk Klasifikasi Zona Daerah Risiko Covid-19 di Indonesia," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 1, pp. 115–122, 2023, doi: 10.25126/jtiik.20231015935.