DETEKSI *MAN IN THE MIDDLE* (MITM) *ATTAC*K PADA *SMARTHOME* DENGAN MENGGUNAKAN *DECISION TREE*

SKRIPSI

OLEH:

BAYU AKBAR PEBRIAN

09011382025109

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI *MAN IN THE MIDDLE* (MITM) *ATTACK* PADA *SMARTHOME* MENGGUNAKAN METODE *DECISION TREE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh:

BAYU AKBAR PEBRIAN
09011382025109

Palembang, Juni 2024

Pembimbing I Tugas Akhir	Pembimbing II Tugas Akhir
Prof. Deris Stiawan, M.T., Ph.D.	**Kemahyanto Exaudi, M.T**
NIP.197806172006041002	NIP. 198405252023211018

Mengetahui, 9/7/24
Ketua Jurusan Sistem Komputer

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

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 04 Juni 2024

Tim Penguji :

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

Mengetahui, 9/7/24

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

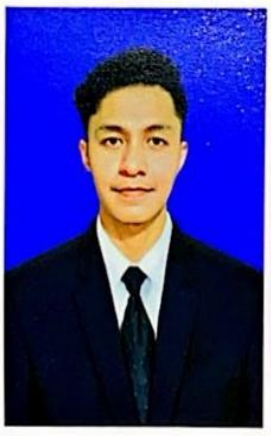
Yang bertanda tangan dibawah ini :

Nama	:	Bayu Akbar Pebrian
NIM	:	09011382025109
Judul	:	Deteksi Man In The Middle (MitM) Attack Pada Smarthome Menggunakan Metode Decision Tree

Hasil Pengecekan Software *iThenticate/Turnitin* : 13%

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, Juni 2024

Yang menyatakan

Bayu Akbar Pebrian

NIM. 09011382025109

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas kehadirat Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini yang berjudul *"*Deteksi *Man In The Middle* (MITM) *Attack* Pada *Smarthome* Menggunakan Metode *Decision Tree".*

Tujuan dari penulisan Tugas Akhir ini adalah untuk melengkapi salah satu syarat memperoleh gelar sarjana komputer di jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian serta observasi dari berbagai sumber literatur yang mendukung dalam penulisan Tugas Akhir ini.

Atas selesainya Tugas Akhir ini, penulis mengucapkan rasa syukur kepada Tuhan Yang Maha Esa, dan juga terima kasih kepada yang terhormat:

1. Kedua Orang Tua dan Keluarga tercinta yang selalu mendoakan serta memberikan dukungan dan semangat yang besar selama penyelesaian Tugas Akhir ini.
2. Bapak Prof. Dr. Erwin, S.Si., M.Si., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Firdaus, M. Kom., selaku Dosen Pembimbing Akademik.
5. Bapak Prof. Deris Stiawan, M.T., Ph.D., selaku Dosen Pembimbing I Tugas Akhir.
6. Bapak Kemahyanto Exaudi, S.kom, M.T., selaku Dosen Pembimbing II Tugas Akhir
7. Ibu Nurul Afifa, M.Kom., selaku dosen yang membantu dalam pengerjaan Tugas Akhir
8. Mba Sari selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.
9. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya yang tidak bisa saya sebutkan satu persatu.

10. Seluruh teman-teman seperjuangan Angkatan 2020 Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
11. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu yang telah memberikan doa dan bantuan dalam penyelesaian Tugas Akhir ini.
12. Almamater Universitas Sriwijaya.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Tugas Akhir ini. Oleh karena itu, segala saran dan kritik sangatla penting bagi penulis. Akhir kata, semoga Tugas Akhir ini dapat bermanfaat dan berguna bagi Akademik.

Palembang, Juni 2024
Penulis,

Bayu Akbar Pebrian
NIM. 09011382025109

DETEKSI MAN IN THE MIDDLE (MITM) ATTACK PADA SMARTHOME MENGGUNAKAN METODE DECISION TREE

Bayu Akbar Pebrian (09011382025109)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: 09011382025109@student.unsri.ac.id

ABSTRAK

Man In The Middle jenis serangan di mana penyerang secara diam-diam menyusup dan memantau, memodifikasi komunikasi antara dua pihak tanpa sepengetahuan mereka. dan dapat mengubah alamat *mac* dari perangkat yang diserang. Pada penelitian ini menggunakan dataset dari COMNETS *Smarthome* yang terdiri dua jenis kelas yaitu, *benign* dan mitm untuk mendeteksi serangan *man in the middle attack arp poisoning* dengan menggunakan metode *Decision Tree*. Pada metode *Decision Tree* menggunakan dua jenis kriteria yaitu, *gini* dan *entropy*. Hasil dari penelitian ini membuktian bahwa metode *Decision Tree* menggunakan kriteria gini mampu dalam mendeteksi serangan *man in the middle attack* dengan mencapai performa terbaik dengan tingkat *accuracy* sebesar 99.22%, *precision* sebesar 99.64%, *recall* sebesar 99.50%, dan *f1-score* sebesar 99.57%

Kata Kunci : *Man In The Middle Attack, Decision Tree, ARP Poisoning*

DETEKSI MAN IN THE MIDDLE (MITM) ATTACK PADA SMARTHOME MENGGUNAKAN METODE DECISION TREE

Bayu Akbar Pebrian (09011382025109)
Department of Computer Systems, Faculty of Computer Science
Sriwijaya University
Email: 09011382025109@student.unsri.ac.id

ABSTRACT

Man In The Middle type of attack in which the attacker secretly infiltrates and monitors, modifies the communication between two parties without their knowledge. and can change the mac address of the attacked device. In this study using a dataset from COMNETS Smarthome which consists of two types of classes, namely, benign and mitm to detect man in the middle attacks arp poisoning using the Decision Tree method. The Decision Tree method uses two types of criteria, namely, gini and entropy. The results of this study prove that the Decision Tree method using the gini criterion is able to detect man in the middle attacks by achieving the best performance with an accuracy rate of 99.22%, precision of 99.64%, recall of 99.50%, and f1-score of 99.57%.

Keywords : *Man In The Middle Attack, Decision Tree, ARP Poisoning*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam penelitian [1] tentang *smarthome* mengacu pada ruang hunian yang dilengkapi dengan berbagai perangkat dan sistem yang terhubung ke internet yang dapat dipantau, dikontrol, dan diotomatisasi dari jarak jauh. Perangkat dan sistem ini, seperti termostat, pencahayaan, kamera keamanan, dan peralatan, dirancang untuk meningkatkan kemudahan, kenyamanan, efisiensi energi, dan keamanan bagi pemilik rumah. Dalam konteks literatur yang ditinjau, *smarthome* juga dikaitkan dengan potensi ancaman keamanan siber, yang mengarah pada kebutuhan akan sistem deteksi anomali yang efektif untuk melindungi perangkat yang saling terhubung dan data yang mereka hasilkan.

Penelitian [2] dampak *Man In The Middle Attack* (MitM) terhadap kerahasiaan, integritas, ketersediaan, dan privasi sistem IoT, teknik yang dilakukan untuk melakukan serangan diantaranya, *Sniffing*, *Packet Injection*, *Session Hijacking*, SSL *Striping*. Dengan menekankan pengaruh langsung pada ketiga aspek *Confidentiality*, *Integrity*, *Availability* (CIA). Berdasarkan penelitian [3] teknik yang digunakan untuk mengimplementasikan serangan MitM. Seperti, *spoofing* DNS, ARP *poisoning*. Serangan MiTM ini dilakukan dengan mengeksploitasi kelemahan protokol ARP untuk memonitor dan memanipulasi komunikasi antara IoT dan titik akses. ARP *spoofing* sebagai metode yang digunakan dalam MitM, yang selaras dengan konsep mengeksploitasi kelemahan protokol ARP untuk memonitor dan memanipulasi komunikasi. Penelitian ini [4] ARP poisoning pada smarthome adalah serangan di mana node jahat di jaringan mengirimkan pesan ARP palsu untuk memperoleh kontrol atas komunikasi antara perangkat di rumah pintar. Serangan ini dapat membahayakan keamanan sistem rumah pintar dan mengakibatkan akses yang tidak sah ke perangkat-perangkat yang terhubung dalam jaringan tersebut. Untuk mencegah serangan ARP dalam Internet of Things, metode pencegahan dapat dilakukan dengan menggunakan mesin Linux sebagai gateway untuk memantau dan menyaring paket ARP jahat.

Metode ini melibatkan langkah-langkah seperti mengaktifkan IP forwarding, mengikat alamat IP ke alamat MAC, mendeteksi penyerang menggunakan Wireshark.

Penelitian [5] menggunakan *machine learning* untuk mendeteksi MitM pada IoT menggunakan dataset MNIST dan CIFAR10. Hasil model DNN mendapatkan akurasi sebesar 95%. Keakuratan model diperoleh melalui hasil evaluasi serangan MitM pada berbagai pengaturan. Pengaturan *double-black-box*, pengaturan *black-box-classifier*, pengaturan *black-box-encoder*, pengaturan *black-box*.

Penelitian ini [6] mendeteksi *anomaly* pada jaringan termasuk juga *Man In The Middle Attack* dengan menggunakan metode *Random Forest*. Pada penelitian ini menggunakan dataset dari IoTID20. Temuan menunjukkan bahwa Model *Random Forest* mendapatkan akurasi terbaik untuk mengidentifikasi serangan MitM pada IoT. Pada penelitian [7] melakukan deteksi serangan pada IoT, termasuk serangan Man in the Middle (MitM), dengan menggunakan model machine learning, untuk melakukan studi perbandingan. Kedua model tersebut dilatih dan diuji menggunakan dataset ML-Edge-IIoTset dan DNN-Edge-IIoTset.

Penelitian ini [8] mendeteksi berbagai jenis serangan pada IoT yang salah satunya MitM, lalu menggunakan dua model, *Naïve Bayes* dan *Decision tree* untuk melakukan studi perbandingan. Kedua model dilatih dan diuji menggunakan dataset ML-Edge-IIoTset dan DNN-Edge-IIoTset. Hasil penilitan bahwa Decision Tree memiliki performa yang lebih baik.

Penelitian ini [9] menggunakan tiga model *machine learning*. *Linear Regression* (LR), *Multi-variate Linear Regression* (MLR), dan *Gaussian Process Regression* (GPR) untuk mendeteksi *Man In The Middle Attack*. Keakuratan model bervariasi berdasarkan persentasi pembelajaran. *Gaussian Process Regression* 89 % sedangkan *Linear Regression* dan *Multi-variate Linear Regression* menghasilkan akurasi 68 % dan 70 %. Proses untuk mendapatkan akurasi dan mengevaluasi model melibatkan analisis ukuran kinerja seperti, *accuracy, precision, sensitivity, specificity, false discovery rate* (FDR), *false negative rate* (FNR), *false omission rate* (FOR), dan *false positive rat*e (FPR).

Dalam penelitian ini [10] menggunakan model decision tree dengan pengambilan dataset yang terdiri dari 436 paket data, yang dimana 109 paket untuk empat jenis serangan yang diuji termasuk *Man In The Middle Attack.* Pemilihan model didasarkan kemampuan untuk mengatasi fitur yang *high dimensional* dengan kinerja yang memuaskan.

Dalam penelitian ini [11] menggunakan delapan model machine learning. *Logistic regression* (LR), *naïve bayes* (NB), *support vector machine* (SVM), *decision tree* (DT), *random forest* (RF), *k-Nearest Neighbor* (KNN), *Adaboost*, dan *XGBoost*. Untuk mengeveluasi dataset ToN-IoT. Dibagi menjadi dua set, satu untuk pelatihan dengan 70% dari dataset dan yang lainnya untuk mengevaluasi kinerja algoritme ML yang dipilih. Hasil penelitian menunjukkan bahwa XGBoost mengungguli semua pendekatan ML lainnya dalam tugas klasifikasi biner dan klasifikasi multi-kelas.

Penelitian ini [12] mengusulkan model machine learning untuk mengenali pola serangan salah satunya adalah *Decision Tree*. Berdasarkan pembahasan di atas maka dari itu penulis akan melakukan penelitian dengan judul **Deteksi *Man In The Middle* (MitM) *Attack* Pada *Smarthome* Menggunakan Metode *Decision tree***

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dibahas sebelumnya maka tugas akhir ini mendapatkan beberapa permasalahan yang akan dibahas pada penelitian ini meliputi:

1. Bagaimana proses ekstraksi dataset *Man In The Middle Attack*
2. Bagaimana teknik *random oversampling* diterapkan pada kumpulan data yang tidak seimbang?
3. Bagaimana cara model *decision tree* digunakan untuk mendeteksi *Man In The Middle Attack*?

1.3 Batasan masalah

Batasan masalah dalam penulisan penelitian tugas akhir ini adalah sebagai berikut:

1. Dataset yang digunakan adalah dataset COMNETS *SMARTHOME*.
2. Melakukan deteksi serangan *Man In The Middle Attack* dengan menggunakan algoritma *decicion tree*.
3. Serangan *Man In The Middle Attackt* yang dibahas adalah *Arp Poisoning*.
4. Tidak ada pembahasan mengenai pencegahan serangan *Man In The Middle Attack* pada penelitian ini.

1.4 Tujuan

Berdasarkan latar belakang dan rumusan masalah yang telah dibahas sebelumnya, adapun terdapat beberapa yang ingin dicapai dalam penulisan Tugas Akhir ini, yaitu:

1. Melakukan ekstraksi dataset yang berbentuk .pcap menjadi .csv menggunakan *T-shark* pada kalilinux.
2. Menerapkan teknik *random oversampling* pada data yang tidak seimbang untuk proses deteksi serangan *Man In The Middle Attack*.
3. Melakukan evaluasi performa algoritma *decision tree* dalam mendeteksi serangan *Man In The Middle Attack*.

1.5 Manfaat

Adapun manfaat dari penelitian tugas akhir ini antara lain adalah:

1. Memahami proses ekstraksi dataset menggunakan *T-shark* pada kalilinux.
2. Memberikan solusi terhadap ketidakseimbangan data, memastikan deteksi yang akurat dan handal terhadap serangan *Man In The Middle Attackt*.
3. Mengevaluasi seberapa baik model *decision tree* dalam mendeteksi.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian Tugas Akhir ini akan melalui beberapa tahapan, yaitu:

1. Tahap Pertama Studi Pustaka/Studi Literatur

   Tahap ini dilakukan setelah masalah yang didapatkan telah sesuai untuk dijadikan sebagai penelitian, membaca artikel, jurnal atau makalah yang berhubungan dengan tugas akhir.

2. Tahap Kedua Perancangan Sistem

   Tahap kedua ini akan membahas masalah proses bagaimana sistem tersebut di rancang dan di bangun untuk deteksi *Man In The Middle Attack* menggunakan algoritma *Decicion Tree*.

3. Tahap Pengujian

   Pada tahap ini dilakukan pengujian berdasarkan metode yang digunakan dalam penelitian dan metode-metode yang digunakan oleh penelitian sebelumnya, sehingga didapatan 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

   Tahapan ini merupakan langkah akhir, hasil dari semua langkah yang dilakukan sebelumnya akan dirumuskan menjadi suatu kesimpulan.

1.7 Sistematika Penulisan

Agar dapat mempermudah proses penyusunan dan memperjelas isi dari setiap bab maka akan dibuat sistematika dalam penulisan yaitu sebagai berikut:

BAB I PENDAHULUAN

Berisi penjelasan secara singkat dan sistematis mengenai topik-topik dalam penelitian yang meliputi latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan metodologi penelitian dan terakhir sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan mengenai beberapa literature review yang berhubungan dengan masalah deteksi *Man In The Middle Attack* dengan menggunakan algoritma *Decision Tree* yang mengacu pada penelitian sebelumnya.

BAB III METODOLOGI PENELITIAN

Pada bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan mengenai bab ini meliputi tahapan-tahapan yang akan dilakukan serta mempersiapkan data *Man In The Middle Attack* dan *normal*, penerapan algoritma *Decision Tree* serta model yang akan digunakan sehingga tujuan dari penulis tercapai.

BAB IV HASIL DAN ANALISA

Pada bab ini menjelaskan hasil yang telah diperoleh pada tahap sebelumnya, serta analisa data yang didapat dari hasil pengujian.

BAB V KESIMPULAN

Bab ini berisikan kesimpulan tentang hasil pengujian yang telah dilakukan, serta merupakan jawaban yang diperoleh dari tujuan yang ingin dicapai, dan berisikan saran-saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] J. I. I. Araya and H. Rifà-Pous, "Anomaly-based cyberattacks detection for smart homes: A systematic literature review," *Internet of Things*, vol. 22, no. January, p. 100792, Jul. 2023, doi: 10.1016/j.iot.2023.100792.

[2] H. Fereidouni, O. Fadeitcheva, and M. Zalai, "IoT and Man-in-the-Middle Attacks," 2023, [Online]. Available: http://arxiv.org/abs/2308.02479

[3] M. Kalita, S. Dutta, and A. Yesmin, "A Survey on Man in the Middle Attack : Classification , Defense Mechanisms and Challenges," vol. 2, no. 7, pp. 62–66, 2016.

[4] W. Gao *et al.*, "ARP Poisoning Prevention in Internet of Things," *Proc. - 9th Int. Conf. Inf. Technol. Med. Educ. ITME 2018*, pp. 733–736, 2018, doi: 10.1109/ITME.2018.00166.

[5] D. Wang, C. Li, S. Wen, S. Nepal, and Y. Xiang, "Man-in-the-Middle Attacks Against Machine Learning Classifiers Via Malicious Generative Models," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 5, pp. 2074–2087, Sep. 2021, doi: 10.1109/TDSC.2020.3021008.

[6] P. Maniriho, E. Niyigaba, Z. Bizimana, V. Twiringiyimana, L. J. Mahoro, and T. Ahmad, "Anomaly-based Intrusion Detection Approach for IoT Networks Using Machine Learning," *CENIM 2020 - Proceeding Int. Conf. Comput. Eng. Network, Intell. Multimed. 2020*, no. Cenim, pp. 303–308, 2020, doi: 10.1109/CENIM51130.2020.9297958.

[7] D. Stiawan, "Anomaly Detection and Monitoring in Internet of Things Communication," 2016.

[8] O. Bin Samin, N. A. A. Algeelani, A. Bathich, G. M. Adil, A. Qadus, and A. Amin, "Malicious Agricultural IoT Traffic Detection and Classification: A Comparative Study of ML Classifiers," *J. Adv. Inf. Technol.*, vol. 14, no. 4, pp. 811–820, 2023, doi: 10.12720/jait.14.4.811-820.

[9] N. Sivasankari and S. Kamalakkannan, "Detection and prevention of man-in-the-middle attack in iot network using regression modeling," *Adv. Eng. Softw.*, vol. 169, no. May, p. 103126, 2022, doi: 10.1016/j.advengsoft.2022.103126.

[10] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9042–9053, 2019, doi: 10.1109/JIOT.2019.2926365.

[11] A. A. Alsulami, Q. Abu Al-Haija, and A. Tayeb, "Anomaly-based Intrusion Detection System for IoT Networks With Improved Data Engineering," no. October, 2022, doi: 10.20944/preprints202210.0431.v1.

[12] T. Li, Z. Hong, and L. Yu, “Machine Learning-based Intrusion Detection for IoT Devices in Smart Home,” in *2020 IEEE 16th International Conference on Control & Automation (ICCA)*, Oct. 2020, vol. 2020-Octob, pp. 277–282. doi: 10.1109/ICCA51439.2020.9264406.

[13] A. R. Gad, M. Haggag, A. A. Nashat, and T. M. Barakat, “A Distributed Intrusion Detection System using Machine Learning for IoT based on ToN-IoT Dataset,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 6, pp. 548–563, 2022, doi: 10.14569/IJACSA.2022.0130667.

[14] Y. Zhai, N. Ma, B. An, and D. Ruan, “An effective over-sampling method for imbalanced data sets classification,” *Chinese J. Electron.*, vol. 20, no. 3, pp. 489–494, 2011.

[15] J. Su, S. He, and Y. Wu, “Features selection and prediction for IoT attacks,” *High-Confidence Comput.*, vol. 2, no. 2, p. 100047, 2022, doi: 10.1016/j.hcc.2021.100047.

[16] M. Nour, H. Sindi, and K. Polat, “Biomedical Datasets,” *Hindawi Math. Probl. Eng.*, vol. 2020, p. 17, 2020, [Online]. Available: https://doi.org/10.1155/2020/2836236