DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA *SMART HOME* MENGGUNAKAN METODE ALGORITMA *K-NEAREST NEIGHBOR*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

HANIF AZFA SADIFATIASMI

09011382025135

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA *SMART HOME* MENGGUNAKAN METODE ALGORITMA *K-NEAREST NEIGHBOR*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Program Studi Sistem Komputer

Jenjang S1

Oleh :

HANIF AZFA SADIFATIASMI

09011382025135

Palembang, 8 November 2024

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

Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

AUTHENTICATION PAGE

DETECTION OF MAN IN THE MIDDLE (MITM) ATTACKS ON SMARTHOMES USING THE K-NEAREST NEIGHBOR METHOD

SKRIPSI

Submitted To Complete One Of The Requirements For Obtaining A Bachelor's Degree in Computer Science

By:

HANIF AZFA SADIFATIASMI

Palembang, November 2024

Final Project Advisor I	Final Project Advisor II
Prof. Deris Stiawan, M.T., Ph.D.	**Kemahyanto Exaudi, M.T**
NIP.197806172006041002	**NIP. 198405252023211018**

Acknowledge,

Head Of Computer Science Departement

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

NIP. 196612032006041001

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jumat

Tanggal : 13 September 2024

Tim Penguji :

1. Ketua : Aditya Putra Perdana Prasetyo, S.Kom., M.T.
2. Penguji : Huda Ubaya, S.T., M.T.
3. Pembimbing I : Prof. Deris Stiawan, M.T., Ph.D.
4. Pembimbing II : Kemahyanto Exaudi, S.Kom., M.T.

Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Hanif Azfa Sadifatiasmi
NIM : 09011382025135
Judul : Deteksi Serangan *Man In The Middle* (MITM) Pada *Smart Home* Menggunakan Metode Algoritma *K-Nearest Neighbor*

Hasil Pengecekan Software *iThenticate/Turnitin* : 11%

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 saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Palembang, 14 November 2024

Yang menyatakan

Hanif Azfa Sadifatiasmi

NIM. 09011382025135

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa, penulis telah diberikan kesehatan, kekuatan, serta kesanggupan sehingga penulis mampu menyelesaikan Proposal Tugas Akhir ini yang berjudul "Deteksi Serangan *Man In The Middle* (MITM) Pada *Smart Home* Menggunakan Metode Algoritma *K-Nearest Neighbor* ".

Penyusunan Tugas Akhir ini merupakan salah satu kewajiban yang harus dipenuhi untuk meraih gelar sarjana komputer di Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya. Dalam penyusunannya, penulis mengacu pada berbagai sumber literatur dan hasil penelitian yang relevan.

Bersyukur ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini. Penulis juga ingin menyampaikan terima kasih kepada yang terhormat :

1. Atas karunia Allah SWT berupa kesehatan, berkah, dan kesempatan, penulis panjatkan rasa syukur yang mendalam atas selesainya Tugas Akhir ini..
2. Orang Tua penulis, Bapak dan Ibu, yang selalu memberikan motivasi, doa,serta dukungannya untuk penulis dan menguatkan dalam menyelesaikan Proposal Tugas Akhir.
3. Bapak Prof. Dr. Erwin, S.SI,M.SI., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Rahmat Fadli Isnanto, S.SI., M.SC. selaku Dosen Pembimbing akademik.
6. Bapak Prof. Deris Stiawan, M.T., Ph.D., selaku Dosen Pembimbing I Tugas Akhir.

7. Bapak Kemahyanto Exaudi, S.Kom., M.T selaku Dosen Pembimbing II Tugas Akhir.
8. Ibu Nurul Afifah, M.Kom., selaku dosen yang membantu dalam pengerjaan Tugas Akhir.
9. Mbak Sari selaku Admin Program Studi Sistem Komputer yang telah membantu administrasi dalam menyelesaikan Tugas Akhir.
10. Semua relasi penulis, rekan seangkatan penulis angkatan 2020 yang menjadi teman seperjuangan pada Sistem Komputer, Universitas Sriwijaya.
11. Bapak/Ibu dosen Jurusan Sistem Komputer yang telah senantiasa membagi ilmu dan pengalamannya kepada saya, penulis ucapkan terima kasih yang sebesar-besarnya.
12. Mutiara Farhanah Azzahra yang selalu menemani penulisan Skripsi saya dan selalu menjadi support system selama proses mengerjakan skripsi.

Kesempurnaan hanya milik Allah dan Rasulnya , Kesalahan dan Kekhilafan pasti selalu ada menghampiri setiap manusia terutama diri saya pribadi. Maka dari itu jikalau dalam penulisan Proposal Tugas akhir ini ini masih terdapat banyak kekurangan dan kesalahan ,penulis meminta kritik dan saran yang membangun dengan harapan agar dapat perbaiki di masa yang akan datang ,dan semoga tulisan ini dapat bermanfaat bagi semuanya.

Palembang, 19 November 2024
Penulis,

Hanif Azfa Sadifatiasmi
NIM. 09011382025135

DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA *SMART HOME* MENGGUNAKAN METODE ALGORITMA *K-NEAREST NEIGHBOR*

Hanif Azfa Sadifatiasmi (09011382025135)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: hanifazfas@gmail.com

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 *K-Nearest Neighbor*.. Hasil dari penelitian ini membuktian bahwa metode *K-Nearest Neighbor* mampu dalam mendeteksi serangan *man in the middle attack* dengan mencapai performa terbaik dengan tingkat *accuracy* sebesar 98.95%, *precision* sebesar 98.86%, *recall* sebesar 98.96%, dan *f1-score* sebesar 98.91%

Kata Kunci : *ARP Poisoning, K-Nearest Neighbor, Man In The Middle Attack*

DETECTION OF MAN-IN-THE-MIDDLE (MITM) ATTACKS ON SMART HOMES USING THE K-NEAREST NEIGHBOR ALGORITHM

Hanif Azfa Sadifatiasmi (09011382025135)
Department of Computer Systems, Faculty of Computer Science
Sriwijaya University
Email: hanifazfas@gmail.com

ABSTRACT

A Man-in-the-Middle (MITM) attack is a type of cyberattack where an attacker secretly intercepts and monitors, and possibly modifies, communication between two parties without their knowledge. This type of attack can also alter the MAC address of the compromised device. In this research, a dataset from COMNETS Smarthome consisting of two classes, benign and MITM, was used to detect ARP poisoning attacks using the K-Nearest Neighbor algorithm. The results of this research demonstrate that the K-Nearest Neighbor method is capable of detecting Man-in-the-Middle attacks with a high level of accuracy, achieving a precision of 98.86%, recall of 98.96%, and F1-score of 98.91%.

Keywords : *ARP Poisoning, K-Nearest Neighbor, Man In The Middle Attack*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Serangan MITM adalah serangan dimana penyerang diam-diam mentransfer dan mungkin mengubah korespondensi antara dua pihak yang mempercayainya berkomunikasi secara langsung satu sama lain. Serangan MITM adalah istilah umum karena ketika pelakunya memposisikan dirinya dalam diskusi antara klien dan aplikasi; baik untuk mendengarkan secara sembunyi-sembunyi atau meniru salah satu pihak, sehingga tampak seolah-olah pertukaran informasi biasa sedang berlangsung. [1] [2]

Penyadapan dinamis merupakan modus operandi dalam serangan MITM yang berbahaya. Penyerang berperan sebagai perantara dalam komunikasi antara dua korban, memanipulasi pesan yang dipertukarkan untuk menipu mereka agar percaya bahwa mereka sedang berkomunikasi secara langsung dan aman. Berbeda dengan serangan MITM pasif yang hanya memantau komunikasi, penyadapan dinamis aktif memodifikasi dan menyuntikkan pesan baru. Penyerang harus mampu mencegat semua pesan penting antara dua korban dan menggantinya dengan pesan yang dibuatnya sendiri. [3]

Serangan MITM bagaikan peretas yang menyamar di tengah komunikasi digital, mengintai dan memanipulasi data yang dipertukarkan. Serangan ini menjadi momok bagi keamanan komputer, karena menargetkan data yang mengalir antara dua pihak, membahayakan kerahasiaan dan integritasnya. [4] . MITM bagaikan pemain ketiga dalam permainan bola basket yang menyelinap di antara dua pemain yang ingin mengoper bola. Peretas MITM mencuri bola, yaitu data yang dipertukarkan, tanpa sepengetahuan atau persetujuan pengirim dan penerima. Serangan MITM dikenal dengan berbagai nama, seperti *Session hijacking*, TCP *hijacking*, dan TCP *session hijacking*. Para profesional keamanan komputer selalu siaga terhadap ancaman MITM, karena serangan ini dapat membahayakan berbagai aspek, seperti data keuangan, informasi pribadi, dan bahkan kontrol sistem kritis.. [4]

Dalam penelitian [5] tentang *smart home* 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, *smart home* 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 terdahulu [7] dalam bidang deteksi intrusi pada *Internet of Things* (IoT) telah menunjukkan potensi besar dalam penggunaan machine learning untuk meningkatkan akurasi dan efisiensi deteksi. Dalam penelitian ini, penulis menggunakan algoritma machine learning untuk membangun sistem deteksi intrusi terdistribusi pada IoT. Sistem ini menggunakan dataset ToN-IoT untuk melatih model machine learning salah satunya memakai *K-Nearest Neighbor* dan mencapai tingkat akurasi yang tinggi dalam mendeteksi serangan siber.

Penelitian terdahulu [10] serangan MITM dianalisis secara langsung dengan teknik ARP *poisoning*. Metode forensik statik digunakan untuk mendeteksi aktivitas ilegal pada jaringan Wi-Fi. Penelitian ini berfokus pada analisis traffic jaringan dan proses pencarian bukti serangan MITM dengan teknik ARP *Poisoning*. Hasilnya, penelitian ini berhasil menganalisis dan menemukan bukti serta informasi pelaku. Penelitian ini menunjukkan bahwa deteksi serangan MITM masih dilakukan secara manual dengan mengamati data traffic saat serangan terjadi. Oleh karena itu, penelitian ini menggunakan metode klasifikasi K-NN untuk mendeteksi serangan MITM dan mempermudah analisis bagi pengguna yang diserang..

Berdasarkan beberapa ulasan penelitian diatas, penulis akan melakukan deteksi *MITM* menggunakan dataset berbentuk *pcap*. yang terlebih dahulu diekstraksi sehingga menjadi *.csv* dan menggunakan machine learning sebagai bahan analisa yang dapat digunakan sebagai referensi. Dengan demikian, penulis mengusulkan penelitian dengan judul **Deteksi Serangan *Man In The Middle***

(MITM) Pada *Smart Home* Menggunakan Metode Algoritma *K-Nearest Neighbor.*

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, berikut rumusan masalah yang akan dikaji dalam penelitian ini antara lain sebagai berikut:

1. Teknik apa yang tepat untuk diterapkan pada kumpulan data yang tidak seimbang dalam penelitian ini?
2. Bagaimana cara menerapkan model *K-Nearest Neighbor* untuk mendeteksi MITM *Attack* pada jaringan Smart Home?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini antara lain:

1. Dataset yang digunakan adalah Dataset COMNETS SMARTHOME.
2. Serangan MITM menggunakan algoritma *K-Nearest Neighbor*.
3. Serangan MITM *Attack* yang dibahas adalah *ARP Spoofing*
4. Tidak membahas mengenai pencegahan serangan MITM pada penelitian ini.

1.4 Tujuan

Adapun tujuan dari penulisan tugas akhir ini adalah sebagai berikut:

1. Menerapkan algoritma K-Nearest Neighbor untuk deteksi trafik serangan MITM pada jaringan *Smart Home.*
2. Menghitung akurasi deteksi serangan MITM pada jaringan *Smart Home.*

1.5 Manfaat

Adapun manfaat yang ingin dicapai dari penelitian ini yaitu:

1. Memberikan solusi terhadap ketidakseimbangan data, memastikan deteksi yang akurat dan handal terhadap serangan *Man In The Middle Attack.*
2. Mengevaluasi seberapa baik model *K-Nearest Neighbor* dalam mendeteksi serangan MITM.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini akan melewati beberapa tahapan sebagai berikut:

1. Tahap Pertama (Studi Pustaka/literature)

   Tahap pertama dalam metodologi penelitian ini adalah studi pustaka, di mana fondasi penelitian dibangun dengan kokoh. Pada tahap ini, informasi yang relevan dengan topik penelitian dikumpulkan dari berbagai sumber, seperti jurnal ilmiah, buku, artikel online, dan sumber terpercaya lainnya..
2. Tahap Kedua (Perancangan Sistem)

   Penerapan metode penelitian menjadi fokus utama pada tahap ini. Metode penelitian diimplementasikan melalui pembangunan sistem, persiapan infrastruktur hardware dan software, serta konfigurasi dan pemrograman yang diperlukan..
3. Tahap Ketiga (Pengujian)

   Dalam tahap ini, memvalidasi metodologi penelitian dan memverifikasi penelitian sebelumnya dengan cara memastikan keakuratan metodologi, memvalidasi hasil penelitian sebelumnya, dan menganalisis data uji.
4. Tahap Keempat (Analisa)

   Tahap ini berfokus pada analisis data hasil pengujian dengan menerapkan pendekatan tertentu untuk menghasilkan kesimpulan yang objektif dengan cara menganalisis data, menerapkan pendekatan, dan menarik kesimpulan.
5. Tahap Kelima (Kesimpulan dan Saran)

   Pada tahap ini akan dilakukan kesimpulan berdasarkan permasalahan, studi pustaka, metodologi penelitian, dan analisa hasil pengujian. Serta saran untuk penulis selanjutnya jika ingin dijadikan referensi.

1.7 Sistematika Penulisan

Adapun sistematika penulisan dalam Tugas Akhir ini adalah sebagai berikut

BAB I PENDAHULUAN

Pada Bab I merupakan gerbang awal yang akan menjelaskan inti dari penelitian ini dengan memaparkan latar belakang, rumusan masalah, tujuan

penelitian, manfaat penelitian, batasan masalah, metodologi penelitian, sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada Bab II bagaikan lautan ilmu pengetahuan tentang deteksi serangan MITM

BAB III METODOLOGI PENELITIAN

Pada Bab III akan membahas secara detail mengenai proses penelitian, kerangka penelitian, dan metodologi penelitian.

BAB IV HASIL DAN ANALISA

Pada Bab IV menjelaskan hasil dari penelitian dan analisis Deteksi Serangan MITM Pada *Smart Home* Menggunakan Metode Algoritma *K-Nearest Neighbor.*

BAB V KESIMPULAN DAN SARAN

Pada Bab V berisi tentang kesimpulan dari penelitian yang dilakukan serta saran untuk penelitian selanjutnya dimasa mendatang.

DAFTAR PUSTAKA

[1] U. Meyer and S. Wetzel, "A Man-in-the-Middle Attack on UMTS," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, 2004, pp. 90–97. doi: 10.1145/1023646.1023662.

[2] L. B. Kish, "Protection against the man-in-the-middle-attack for the kirchhoff-loop-johnson(-like)-noise cipher and expansion by voltage-based security," *Fluct. Noise Lett.*, vol. 6, no. 1, pp. 1–7, 2006, doi: 10.1142/S0219477506003148.

[3] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-middle attack to the HTTPS protocol," *IEEE Secur. Priv.*, vol. 7, no. 1, pp. 78–81, 2009, doi: 10.1109/MSP.2009.12.

[4] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016, doi: 10.1109/COMST.2016.2548426.

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

[6] S. A. M. Al-Juboori, F. Hazzaa, Z. S. Jabbar, S. Salih, and H. M. Gheni, "Man-in-the-middle and denial of service attacks detection using machine learning algorithms," *Bull. Electr. Eng. Informatics*, vol. 12, no. 1, pp. 418–426, 2023, doi: 10.11591/eei.v12i1.4555.

[7] 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.

[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] K. Ameta and S. S. Sarangdevot, "Machine Learning-Based Intrusion Detection for IOT Devices," *Lect. Notes Networks Syst.*, vol. 693 LNNS, pp.

1001–1007, 2023, doi: 10.1007/978-981-99-3243-6_81.

[10] G. Kamajaya, I. Riadi, and Y. Prayudi, “Analisa Investigasi Static Forensics Serangan Man in the Middle Berbasis Arp Poisoning,” *JIKO (Jurnal Inform. dan Komputer)*, vol. 3, no. 1, pp. 6–12, 2020, doi: 10.33387/jiko.v3i1.1692.

[11] Á. Michelena *et al.*, “A novel intelligent approach for man-in-the-middle attacks detection over internet of things environments based on message queuing telemetry transport,” *Expert Syst.*, vol. 41, no. 2, pp. 1–15, 2024, doi: 10.1111/exsy.13263.

[12] B. Bhushan, “Man-In-The-Middle Attack in Wireless and Computer Networking- A review,” 2017.

[13] M. S. Shelke, P. R. Deshmukh, and P. V. K. Shandilya, “A Review on Imbalanced Data Handling Using Undersampling and Oversampling Technique,” *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 4, pp. 444–449, 2017, doi: 10.23883/ijrter.2017.3168.0uwxm.

[14] R. Qaddoura, A. M. Al-Zoubi, I. Almomani, and H. Faris, “A multi-stage classification approach for iot intrusion detection based on clustering with oversampling,” *Appl. Sci.*, vol. 11, no. 7, 2021, doi: 10.3390/app11073022.

[15] T. Denœux, O. Kanjanatarakul, and S. Sriboonchitta, “A new evidential K-nearest neighbor rule based on contextual discounting with partially supervised learning,” *Int. J. Approx. Reason.*, vol. 113, pp. 287–302, 2019, doi: 10.1016/j.ijar.2019.07.009.

[16] J. Gou, H. Ma, W. Ou, S. Zeng, Y. Rao, and H. Yang, “A generalized mean distance-based k-nearest neighbor classifier,” *Expert Syst. Appl.*, vol. 115, pp. 356–372, 2019, doi: 10.1016/j.eswa.2018.08.021.

[17] R. Vinayakumar, M. Alazab, S. Srinivasan, Q. V. Pham, S. K. Padannayil, and K. Simran, “A Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities,” *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4436–4456, 2020, doi: 10.1109/TIA.2020.2971952.

[18] R. Kohavi and F. Provost, “Applications of Machine Learning and the Knowledge,” *Res. Mach. Learn.*, vol. 30, pp. 349–354, 1998.

[19] M. K. Uçar, M. Nour, H. Sindi, and K. Polat, “The Effect of Training and

Testing Process on Machine Learning in Biomedical Datasets," *Math. Probl. Eng.*, vol. 2020, 2020, doi: 10.1155/2020/2836236.