DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA *SMART HOME* MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE* (SVM)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu

Syarat Memperoleh Gelar Sarjana

Komputer

Oleh :

Danny Andreas

09011382025151

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA *SMART HOME* MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE* (SVM)

SKRIPSI

Program Studi Sistem Komputer

Jenjang S1

Oleh :

Danny Andreas

09011382025151

Palembang, 17 November 2024

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

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 19661203200604100

AUTHENTICATION PAGE

DETECTING MAN IN THE MIDDLE (MITM) ATTACKS ON SMART HOME USING THE SUPPORT VECTOR MACHINE (SVM) METHOD

THESIS

Dept. of computer System

Bachelor's Degree

By:

DANNY ANDREAS

09011382025151

Palembang, 12 November 2024

Supervisor	Co-Supervisor
Prof Deris Stiawan, M.T., Ph.D.	Kemalryanto Exaudi, S.Kom, M.T.
NIP.197806172006041002	NIP. 198405252023211018

Acknowledge,
Head Of Computer System Dapartement

Dr. Ir. Sukemi, M.T.
NIP. 19661203200604100

LEMBAR PERSETUJUAN

Telah di uji dan lulus pada :

Hari : Jumat

Tanggal : 18 Oktober 2024

Tim Penguji :

1. **Ketua : Aditya Putra Perdana P, M.T.**
2. **Pembimbing I : Prof. Deris Stiawan, M.T., Ph.D**
3. **Pembimbing II : Kemahyanto Exaudi, S,Kom, M.T.**
4. **Penguji : Ahmad Heryanto, M.T.**

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Danny Andreas

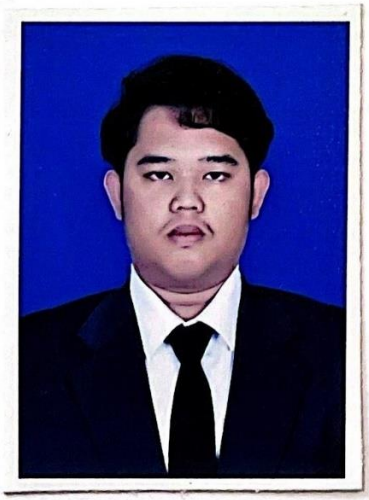
NIM : 09011382025151

Judul : Deteksi Serangan *Man In The Middle* (MITM) Pada *Smart home* Menggunakan Metode *Support Vector Machine* (SVM)

Hasil Pengecekan Software *Thenticate/Turnitin: 7%*

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

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



ang , November 2024

Danny Andreas

NIM. 09011382025151

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas kehadirat Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya sehingga penulis dapat menyelesaikan Skripsi ini yang berjudul *"***Deteksi Serangan *Man In The Middle* (MITM) *pada Smart home* menggunakan Metode *Support Vector Machine***"**.

Tujuan dari penulisan Skripsi 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 Skripsi ini.

Atas Selesainya Skripsi ini, penulis mengucapkan rasa Syukur kepada Tuhan Yang Maha Esa, dan juga terima kasih kepada yang terhormat :

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat dan kesehatan dan kesempatan kepada penulis dalam Menyusun Skripsi ini.
2. Kedua Orang Tua dan Keluarga tercinta yang selalu mendoakan serta memberikan dukungan dan semangat yang besar selama penyelesaian Skripsi 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 Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Sutarno, S.T., M.T., selaku Dosen Pembimbing Akademik.
6. Bapak Prof. Deris Stiawan, M.T., Ph.D., selaku Dosen Pembimbing I Skripsi
7. Bapak Kemahyanto Exaudi, S.kom, M.T., selaku Dosen Pembimbing II Skripsi.
8. Ibu Nurul Afifa, M.Kom., selaku dosen yang membantu dalam pengerjaan Skripsi.
9. Mba Sari selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.
10. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya yang tidak bisa saya sebutkan satu persatu.

11. Seluruh teman-teman seperjuangan Angkatan 2020 Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
12. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu yang telah memberikan doa dan bantuan dalam penyelesaian Skripsi ini.
13. Putri Nurhaliza Candra yang selalu menemani penulisan Skripsi saya dan selalu menjadi *support system* selama progress mengerjakan Skripsi.
14. Almamater Universitas Sriwijaya.

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 Skripsi 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, November 2024

Penulis,

Danny Andreas

09011382025151

DETEKSI SERANGAN *MAN IN THE MIDDLE* (MITM) PADA *SMART HOME* MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE* (SVM)

Danny Andreas (09011382025151)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer Universitas Sriwijaya
Email: dannyandreas06@gmail.com

ABSTRAK

Serangan MITM memungkinkan pihak ketiga menyusup di antara perangkat yang berkomunikasi untuk mencuri atau memodifikasi data tanpa terdeteksi, sehingga meningkatkan risiko keamanan pada jaringan *smart home*. Penelitian ini bertujuan mendeteksi serangan *Man in the Middle* (MITM) pada jaringan *smart home* menggunakan algoritma *Support Vector Machine* (SVM). Dataset yang digunakan adalah COMNETS SMART HOME, yang berisi data serangan MITM berbasis teknik ARP Poisoning, diekstraksi dari format .pcap menjadi .csv menggunakan T-Shark. Teknik *random oversampling* diterapkan untuk mengatasi ketidakseimbangan kelas dalam dataset guna meningkatkan akurasi deteksi. Model SVM diuji dengan kernel linear, polynomial, dan *Radial Basis Function* (RBF), dengan rasio data pelatihan dan pengujian dari 50:50 hingga 90:10. Perbandingan terbaik diperoleh pada rasio 80:20 dengan kernel linear, mencapai akurasi 98,45%, presisi 98,03%, *recall* 99,36%, dan skor F1 sebesar 98,69%. Hasil menunjukkan bahwa SVM dengan kernel linear efektif dalam mendeteksi serangan MITM pada jaringan *smart home*.

Kata Kunci : ARP Poisoning, Man in the Middle (MITM), Smart home, Support Vector Machine (SVM), Random Oversampling.

DETECTING MAN IN THE MIDDLE (MITM) *ATTACKS ON SMART HOME USING THE SUPPORT VECTOR MACHINE* (SVM) *METHOD*

Danny Andreas (09011382025151)
Dept. of Computer System, Faculty of Computer Science, Universitas Sriwijaya
Email: dannyandreas06@gmail.com

ABSTRACT

MITM attacks allow third parties to infiltrate between communicating devices to steal or modify data without being detected, increasing the security risk of smart home networks. This study aims to detect Man in the Middle (MITM) attacks on smart home networks using the Support Vector Machine (SVM) algorithm. The dataset used is COMNETS SMART HOME, which contains MITM attack data based on the ARP Poisoning technique, extracted from .pcap format to .csv using T-Shark. Random oversampling technique is applied to overcome class imbalance in the dataset to improve detection accuracy. The SVM model was tested with linear, polynomial, and Radial Basis Function (RBF) kernels, with a training and testing data ratio of 50:50 to 90:10. The best comparison was obtained at a ratio of 80:20 with a linear kernel, achieving an accuracy of 98.45%, a precision of 98.03%, a recall of 99.36%, and an F1 score of 98.69%. The results show that SVM with a linear kernel is effective in detecting MITM attacks on smart home networks.

Keyword : ARP Poisoning, Man in the Middle (MITM), Smart home, Support Vector Machine (SVM), Random Oversampling.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan komputer adalah salah satu bidang teknologi komputer yang telah menarik banyak minat dari banyak profesional keamanan dan orang "awam". Bidang ini diperlukan oleh teknik-teknik yang telah dikenal sebelumnya dan baru dikembangkan yang memberikan penyerang sarana untuk melancarkan serangan yang canggih, memberi mereka akses ke sumber daya di jaringan dan membahayakan jaringan tersebut dalam prosesnya salah satu teknik yang terkenal adalah serangan.

infrastruktur penting yang digunakan untuk berkomunikasi dan bertukar informasi. Namun, keamanan jaringan komputer masih menjadi perhatian utama, terutama dalam menghadapi serangan *Man-in-The-Middle* (MITM). Serangan MITM melibatkan pihak ketiga yang mencuri, memodifikasi, atau memantau komunikasi antara dua entitas yang seharusnya berinteraksi secara langsung. Serangan MITM memanfaatkan celah dalam lapisan komunikasi jaringan, seperti protokol TCP/IP, untuk menyusup ke dalam jaringan dan mencuri informasi sensitif. Dalam serangan ini, penyerang menciptakan lingkungan palsu di antara dua entitas yang berkomunikasi dan mengambil alih *information*. Dampak serangan ini dapat sangat merugikan, termasuk kebocoran infomasi pribadi, pencurian identitas, atau edukasi manipulasi. [1].

Dalam penelitian ini [2] algoritma yang diusulkan dapat mendeteksi serangan MITM di sisi lain, algoritme juga dapat menemukan lokasi penyerang pada saat yang sama, yang tidak dipertimbangkan dalam penelitian sebelumnya. [3] Deteksi serangan MITM sangat sulit karena pola eksekusinya yang cerdas. Untuk mempertahankan jaringan, keamanan siber para ahli perlu meningkatkan teknologi yang ada untuk mendeteksi serangan MITM.

Penelitian terdahulu [4] membahas tentang *smart home* mengacu pada tempat hunian yang dilengkapi dengan berbagai perangkat dan sistem yang saling terhubung melalui internet. Perangkat ini dapat di pantau, dikontrol, serta

diotomatisasi dari jarak jauh menggunakan aplikasi atau *platfrom* tertent. Contoh perangkat tersebut meliputi kamera keamanan (CCTV), sistem pencahayaan yang dapat diatur sesuai keinginan pengguna, serta peralatan seperti kulkas dan mesin cuci yang terintegrasi dengan jaringan.

Penelitian terdahulu [5] membahas tentang *Internet od Things* (IoT) dan kerentanan yang dihadapinya dengan focus, khusus pada serangan MITM. Peneliti menjelaskan bagaimana IoT telah mengubah ruang *industry* dan pribadi dengan memungkinkan perangkat yang terhubung seperti sensor dan actuator untuk berkomunikasi dan berbagai data. Namun, konektivitas ini disertai dengan resiko keamanan serangan MITM yang memungkinkan penyerang untuk mencegat dan memanipulasi komunikasi antara perangkat IoT.

Penelitian terdahulu [6] membahas terkait serangan MITM yang menggunakan teknik *ARP Poisoning* pada jaringan Wifi public. Serangan MITM terjadi Ketika penyerang memanipulasi cache ARP untuk mengalihkan komunikasi antara dua host, sehingga memungkinkan penyerang menyadap, memodifikasi atau menghentikan lalu lintas data tanpa terdeteksi. Teknik *ARP Poisoning* memanfaatkan kelemahan protokol ARP untuk menyusup ke dalam komunikasi antar perangkat. Dengan menggunakan perangkat lunak seperti *Wireshark,* penelitian ini berhasil menagkap lalu lintas jaringan dan mengidentifikasi bukti digital berupa paket data yang direkam, seperti alamat IP dan MAC yang di duplikasi. Bukti tersebut kemudian digunakan untuk mengidentifikasi pelaku serangan dengan memastikan ketepatan informasi yang di temukan.

Penelitian terdahulu [7] menggunakan lima model machine learning. *Shallow Neural Network* (SNN), *Decision Trees* (DT), *Bagging Trees* (BT) *Support Vector Machine, dan k-Nearst Neighbor* (KNN). Dengan menggunakan dataset IoTID20 dan teknik rekayasa fitur yang eksensif, model ini berhasil mencapai akurasi hingga 100% dalam mendeteksi anomaly. Sistem ini sangat penting dalam meningkatkan keamanan jaringan IoT yang rentan terhadap berbagai serangan siber.

Berdasarkan uraian diatas, penulis melakukan deteksi MITM dengan menggunakan dataset yang di lakukan ekstraksi dari *.pcap* menjadi bentuk *.csv* dan menggunakan *machine learning* sebagai bahan analisa yang dapat digunakan sebagai referensi, sehingga penulis akan melakukan penelitian dengan judul "***Deteksi Serangan Man in The Middle (MITM) pada smart home menggunakan metode Support Vector Machine (SVM)***"

1.2 Rumusan masalah

Berdasarkan penulisan latar belakang masalah yang ada. permasalahan yang akan dibahas pada penelitian ini meliputi:

1. Bagaimana proses ekstraksi dataset *COMNETS SMART HOME*?
2. Bagaimana teknik *random oversampling* diterapkan pada kumpulan data yang tidak seimbang?
3. Bagaimana cara menerapkan model *support vector machine* digunakan untuk mendeteksi serangan pada MITM?

1.3 Batasan masalah

Batasan masalah dalam penulisan penelitian Skripsi ini adalah sebagai berikut:

1. Dataset yang digunakan hanya dataset *COMNETS SMART HOME*.
2. Melakukan deteksi serangan MITM dengan menggunakan algoritma *Support Vector Machine*.
3. Serangan MITM yang dibahas adalah *Arp Poisoning*.
4. Tidak membahas mengenai pencegahan serangan MITM pada penelitian ini.

1.4 Tujuan

Adapun tujuan yang ingin dicapai dalam penulisan Skripsi ini adalah sebagai berikut:

1. Melakukan ekstraksi dataset yang berbentuk *.pcap* menjadi *.csv* menggunakan Tshark pada sistem operasi *kalilinux*.

2. Menerapkan teknik *random oversampling* pada data yang *inbalance* untuk proses deteksi serangan *Man-in-The-Middle*.

3. Melakukan evaluasi performa algoritma *support vector machine* dengan *polynomial kernel, linear kernel,* dan *RBF kernel* dalam mendeteksi serangan MITM.

1.5 Manfaat

Adapun manfaat dari penelitian Skripsi ini antara lain adalah:

1. Memahami proses ekstrasi dataset menggunakan *T-Shark* pada *kalilinu.*
2. Memberikan Solusi terhadap keseimbangan data, melalui teknik oversamling untuk memastikan akurasi dan kehandalan yang lebih baik dalam deteksi serangan MITM.
3. Membantu dalam memahami efektivitas model SVM untuk mendeteksi serangan MITM dengan menggunakan beberapa jenis kernel, yaitu Polynomial, linear dan RBF.

1.6 Metodologi Penelitian

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

1. Metode Studi Pustaka dan Literatur

   Pada metode ini penulis melakukan pencarian dan pengumpulan referensi berupa literatur yang terdapat pada buku, jurnal dan internet yang berkaitan dengan penelitian yang sedang akan dilakukan.

2. Metode Perancangan Sistem

   Metode ini mengenai bagaimana membangun dan menerapkan metode pada sistem Skripsi, apa saja yang digunakan pada penelitian seperti software apa saja yang digunakan, alat yang digunakan, terakhir bagaimana proses konfigurasi dan penerapan metode pada Skripsi.

3. Metode Pengujian

Metode Pengujian ini dilakukan terhadap dataset yang telah didapat dengan menggunakan machine learning untuk mendapatkan hasil akurasi yang diinginkan.

4. Metode Analisis

   Pada metode ini dari hasil pengujian dari penelitian yang dilakukan. Kemudian akan dilakukan analisis terhadap kelebihan dan kekurangannya, sehingga diharapkan dapat menghasilkan kesimpulan dan saran yang dapat digunakan sebagai referensi yang baik untuk penelitian selanjutnya.

5. Metode Kesimpulan dan Saran

   Pada tahapan terakhir ini penulis membuat kesimpulan dari seluruh kegiatan penelitian dari studi pustaka sampai analisis hasil penelitian, serta memberikan saran untuk penelitian selanjutnya.

1.7 Sistematika Penulisan

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

BAB I PENDAHULUAN

Pada bab ini merupakan penjelasan berisi mengenai Latar belakang, Tujuan, Manfaat, Rumusan Masalah, Batasan Masalah, 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 *Man-in-The-Middle*.

BAB III METODOLOGI PENELITIAN

Pada bab ini menjelaskan secara sistematis, bagaimana proses

penelitian dilakukan. Penjelasan mengenai bab ini meliputi tahapan-tahapan yang akan dilakuka serta mempersiapkan data MITM dan Benign, penerapan *support vector machine* serta model yang akan digunakan sehingga tujuan dari penulis tercapai.

BAB IV HASIL DAN ANALISA

Pada bab ini menjelaskan hasil dari penelitian dan analisis Deteksi Serangan *Man-in-The-Middle* (MITM) Pada *Smart home* Menggunakan Metode *Support Vector Machine* (SVM).

BAB V KESIMPULAN DAN SARAN

Bab ini berisikan Kesimpulan tentang hasil pengujian yang telah dilakukan, serta merupakan jawaban yang di peroleh dari tujuan yang ingin di capai, dan berisikan saran-saran untuk penelitian selannjutnya

DAFTAR PUSTAKA

[1] D. Firmansyah, "Penerapan Teknologi Blockchain Untuk Mengatasi Serangan Man in the Middle," *J. JOCOTIS-Journal Sci. Inform. Robot. E-ISSN xxxx-xxxx*, vol. 1, no. 1, pp. 73–80, 2023.

[2] Y. Yang, X. Wei, R. Xu, L. Peng, L. Zhang, and L. Ge, "Man-in-the-Middle Attack Detection and Localization Based on Cross-Layer Location Consistency," *IEEE Access*, vol. 8, pp. 103860–103874, 2020, doi: 10.1109/ACCESS.2020.2999455.

[3] A. O. Egwali and S. O. Alile, "Man-In-The-Middle Attack Detection Based on Bayesian Belief Network," *Int. J. Acad. Inf. Syst. Res.*, vol. 4, no. 4, pp. 44–53, 2020.

[4] 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.

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

[6] 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.

[7] 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.

[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] M. Thankappan, H. Rifa-Pous, and C. Garrigues, "A Signature-Based Wireless Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks," *IEEE Access*, vol. 12, no. February, pp. 23096–23121, 2024, doi: 10.1109/ACCESS.2024.3362803.

[10] 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.

[11] 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.

[12] 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.

[13] S. M. Morsy and D. Nashat, “D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing,” *IEEE Access*, vol. 10, pp. 49142–49153, 2022, doi: 10.1109/ACCESS.2022.3172329.

[14] D. Bruschi, A. Di Pasquale, S. Ghilardi, A. Lanzi, and E. Pagani, “A Formal Verification of ArpON - A Tool for Avoiding Man-in-the-Middle Attacks in Ethernet Networks,” *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 6, pp. 4082–4098, 2022, doi: 10.1109/TDSC.2021.3118448.

[15] 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.

[16] 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.

[17] R. Mohammed, J. Rawashdeh, and M. Abdullah, “Machine Learning with Oversampling and Undersampling Techniques: Overview Study and Experimental Results,” *2020 11th Int. Conf. Inf. Commun. Syst. ICICS 2020*, pp. 243–248, 2020, doi: 10.1109/ICICS49469.2020.239556.

[18] I. Muhammad and Z. Yan, “Supervised Machine Learning Approaches: a Survey,” *ICTACT J. Soft Comput.*, vol. 05, no. 03, pp. 946–952, 2015, doi: 10.21917/ijsc.2015.0133.

[19] Y. Jiahao, X. Jiang, S. Wang, K. Jiang, and X. Yu, “SVM-BILSTM: A fault detection method for the gas station IoT system based on deep learning,” *IEEE Access*, vol. 8, pp. 203712–203723, 2020, doi: 10.1109/ACCESS.2020.3034939.

[20] V. Kadam, S. Kumar, A. Bongale, S. Wazarkar, P. Kamat, and S. Patil, “Enhancing surface fault detection using machine learning for 3d printed products,” *Appl. Syst. Innov.*, vol. 4, no. 2, 2021, doi: 10.3390/asi4020034.

[21] M. Nour, H. Sindi, and K. Polat, “Biomedical Datasets,” *Hindawi Math. Probl. Eng.*, vol. 2020, p. 17, 2020.