Deteksi Serangan *Man in the middle* (MITM) Attack Pada Smart home Dengan Mengunakan Metode *Deep Neural Networks*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu

Syarat Memperoleh Gelar Sarjana

Komputer

Oleh :

Alfi Aushaf Fernanda

09011382025106

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN\

Deteksi Serangan *Man in the middle* (MITM) *Attack* Pada Smart home Dengan Mengunakan Metode *Deep Neural Networks*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Program Studi Sistem Komputer
Jenjang S1

Oleh:

Alfi Aushaf Fernanda
09011382025106

Palembang, 5 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. 196612032006041001

AUTHENTICATION PAGE

Deteksi Serangan *Man in the middle* (MITM) *Attack*
Pada Smart home Dengan Mengunakan Metode
Deep Neural Networks

THESIS

Dept. Of Computer System
Bachelor's Degree

By:

Alfi Aushaf Fernanda
09011382025106

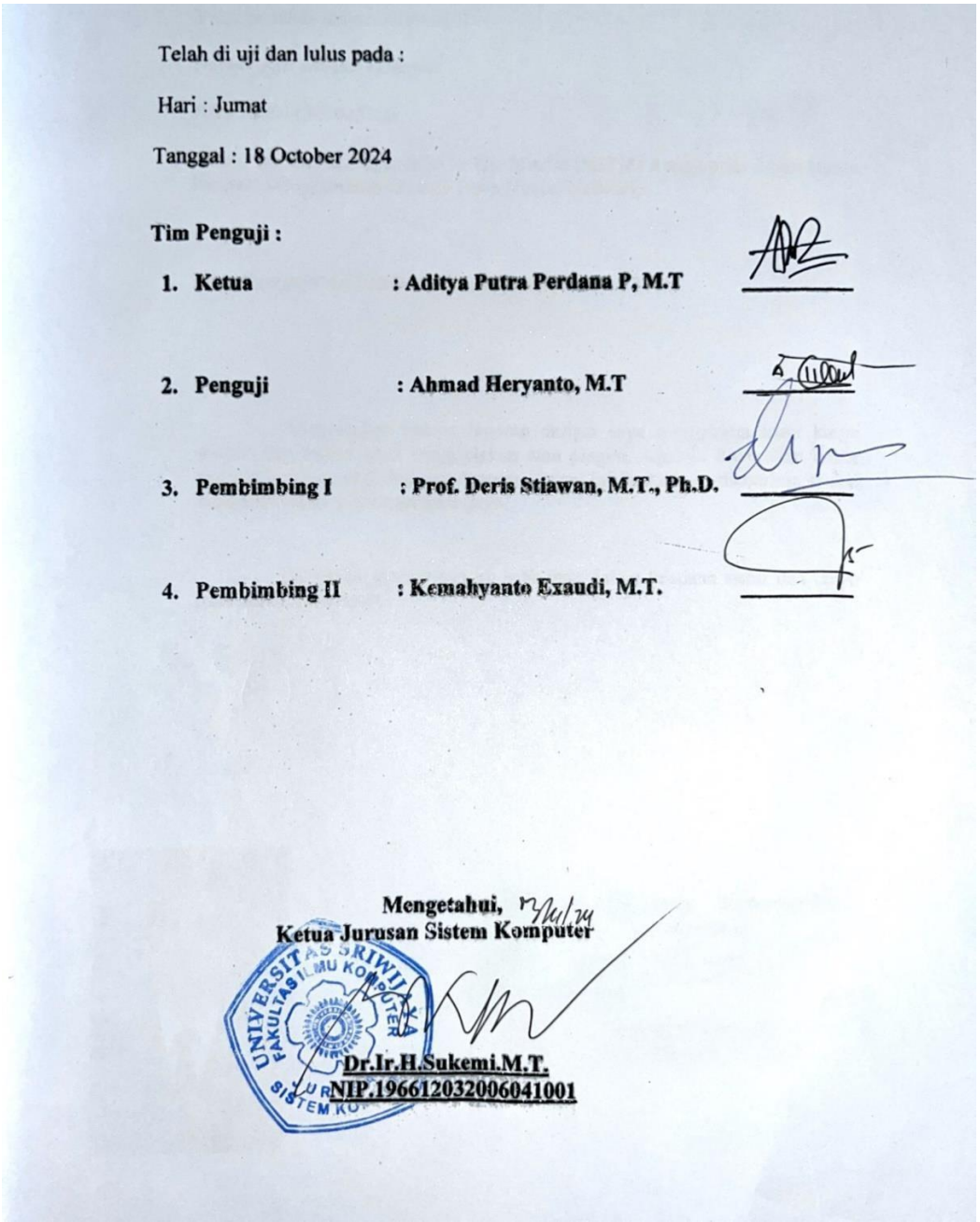
Palembang, 12 November 2024

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

Acknowledge, I
Head Of Computer System Departement

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

LEMBAR PERSETUJUAN



Telah di uji dan lulus pada :

Hari : Jumat

Tanggal : 18 October 2024

Tim Penguji :

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

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Alfi Aushaf Fernanda

NIM : 09011382025106

Judul : Deteksi Serangan Man in The Middle (MITM) Attack pada Smart Home Dengan Menggunakan Metode Deep Neural Networks

Hasil Pengecekan Software *iThenticate/Turnitin* : 15%

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

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

bang, September 2024
menyatakan

Alfi Aushaf Fernanda
NIM. 09011382025106

KATA PENGANTAR

Segala puji dan syukur penulis ucapkan kepada Allah SWT , karena berkat rahmat dan karunia-Nyalah penulis dapat menyelesaikan Proposal Skripsi ini dengan judul "Deteksi Serangan *Man in the middle* (MITM) *Attack* Pada *Smart home* Dengan Mengunakan Metode *Deep Neural Networks*". Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad SAW beserta keluarga, Sahabat dan para pengikutnya yang insyaallah istiqomah hingga akhir zaman.

Pada kesempatan ini, penulis juga mengucapkan terima kasih kepada seluruh pihak yang telah membantu, membimbing, dan terus mendukung penulis dalam menyelesaikan Skripsi ini diantaranya :

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam menyusul Skripsi ini.
2. Kedua orang tua penulis yang selalu memberikan doa tebaik serta dukungan secara moril dan materil.
3. Bapak Prof 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 Muhammad Ali Buchari, M.T. selaku Sekretaris Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Ahmad Heryanto, S.KOM, M.T. selaku Dosen Pembimbing Akademik.
7. Bapak Deris Stiawan, M.T., Ph.D., IPU., ASEAN Eng selaku Pembimbing 1 Skripsi.
8. Bapak Kemahyanto Exaudi, S.Kom, M.T. selaku Pembimbing 2 Skripsi.
9. Mbak Nurul afifah selaku dosen yang membimbing dalam koding Skripsi.
10. Mbak Sari selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal administrasi selama perkuliahan.
11. Bapak, Ibu dosen jurusan Sistem Komputer yang telah memberikan ilmunya serta pengalamannya kepada saya.

12. Seluruh sahabat dan teman penulis yang selalu memberi dukungan yang tidak bisa penulis sebutkan satu persatu.
13. Teman-teman sekelas SK20 Bukit Universitas Sriwijaya , Terimakasih untuk setiap kebersamaan dan bantuannya selama mengerjakan Skripsi dan perkuliahan.
14. Kakak-kakak tingkat yang satu riset dengan terimakasih telah membantu saya menyelesaikan Skripsi ini.
15. Adik-adik saya Alya Aisyah Maharani dan Alda Safira Mahadewi, yang selalu memberikan dukungan dan support selama proses mengerjakan skripsi.
16. Yang tersayang, yang selalu menemani penulisan Skripsi Saya dan selalu menjadi support system selama proses mengerjakan Skripsi.
17. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan semangat serta do'anya dalam penyelesaian 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 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,

Alfi Aushaf Fernanda
09011382025106

Abstrak

Deteksi Serangan *Man in the middle* (MITM) *Attack* Pada Smart home Dengan Mengunakan Metode *Deep Neural Networks*

Oleh

Alfi Aushaf Fernanda (09011382025106)

Serangan MITM merupakan ancaman serius yang memungkinkan penyusup mencegat dan mengubah komunikasi antar perangkat dalam jaringan Internet of Things (IoT). Penelitian ini mengusulkan metode deteksi serangan Man-in-the-Middle (MITM) pada sistem *smart home* menggunakan algoritma *Deep Neural Network* (DNN). Dataset COMNETS SMART HOME digunakan dalam penelitian ini dengan jenis serangan ARP Poisoning. Data diolah menggunakan metode *oversampling* untuk menyeimbangkan kelas data dan diimplementasikan melalui DNN untuk mendeteksi anomali. Hasil menunjukkan bahwa metode ini berhasil mencapai akurasi hingga 98% pada pengujian dengan rasio data pelatihan dan pengujian sebesar 90:10. Penerapan algoritma DNN menunjukkan performa tinggi dalam mendeteksi serangan MITM, menjadikannya alternatif yang efektif untuk meningkatkan keamanan jaringan pada sistem *smart home*.

Kata Kunci: Arp Poisoning, Deep Neural Network (DNN), Internet of Things (Iot), Man-in-the-middle (MITM), Smart home.

Abstrak

Deteksi Serangan *Man in the middle* (MITM) *Attack* Pada Smart home Dengan Mengunakan Metode *Deep Neural Networks*

By

Alfi Aushaf Fernanda (09011382025106)

MITM attacks pose a serious threat by enabling intruders to intercept and alter communications between devices in an Internet of Things (IoT) network. This research proposes a method for detecting Man-in-the-Middle (MITM) attacks in smart home systems using a Deep Neural Network (DNN) algorithm. The study uses the COMNETS SMART HOME dataset with ARP Poisoning attacks. Data were processed with an oversampling technique to balance classes, then implemented through DNN to detect anomalies. The results show that this method achieved up to 98% accuracy in testing with a 90:10 training-to-testing data ratio. The application of the DNN algorithm demonstrated high performance in detecting MITM attacks, making it an effective alternative for enhancing network security in smart home systems.

Keywords: Arp Poisoning, Deep Neural Network (DNN), Internet of Things (Iot), Man-in-the-middle (MITM), Smart home.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam penelitian [1] Internet memainkan peran penting dalah kehidupan kita. Secara konvensional internet digunakan untuk melakukan rutinitas sehari-hari, mulai dari komunikasi pribadi dan membeli barang secara online. *Internet of Things* (IoT) didefinisikan sebagai jaringan objek fisik yang terdiri dari sensor dan koneksi yang memungkinkan perangkat tersebut terhubung dan bertukar data melalui internet.

Oleh karena itu, terdapat ancaman dan serangan yang diketahui seperti *Distributed Denial of Service attack* (DDos) dan *Man-in-the-middle* (MitM) yang biasanya dapat membahayakan system berbasis IoT. DDoS adalah ancaman keamanan yang terutama mempengaruhi ketersediaan layanan. Mitm dapat menyembunyikan semua aspek keamanan dan privasi system. Serangan MitM biasanya lebih kompleks dan sulit diidentifikasi dibandingkan serangan lainnya. MitM biasanya mencakup berbagai macam serangan. Di Tengah komunikasi, pelaku dapat menguasai saluran komunikasi dan menyelaraskan kembali tautan koneksi asli untuk mengirimkan data komersial di antara mereka.

Pada penelitian [2] membahas kinerja deteksi anomali dari enam belas *machine learning* dan *deep neural network* (DNN) pada lima dataset. Saya menganalisis dan membandingkan kinerja masing-masing enam belas metode. Dan tidak memungkinkan mengamati manfaat kinerja yang jelas dan konsisten untuk metode berbasis DNN Ketika Kumpulan data berisi anomaly konteksual.

Pada penelitian [3] membahas DNN yang dimana telah meningkat karena banyak laporan keberhasilan dalam berbagai tugas dan kemampuannya yang telah terbukti dalam melakukan inferensi Tingkat tinggi. Korelasi data yang kompleks dengan potensi data dalam jumlah besar dan dimensi besar. Deteksi anomaly multivariat tidak terkucali pada tren yang mengarah pada ledakan Teknik berbasis DNN yang menunjukkan kemajuan metodologis dan

peningkatan kinerja. Penggunaan arsitektur DNN meningkat karena kebutuhan untuk mengeksplorasi pola data yang berpotensi kompleks yang mendasari evolusi data temporal multivariat.

Tren Smarthome ini telah menyebabkan komunitas pengembangan model yang lebih kompleks untuk meningkatkan kinerja metode berbasis DNN, tanpa adanya bukti teoretis dan empiris bahwa metode berbasis ini lebih baik dari pada metode berbasis DNN. Model berbasis DNN lebih rumit untuk dilatih, memerlukan estimasi jumlah parameter yang ekstensif, dan memerlukan ukuran sampel pelatihan serta sumber daya komputasi yang besar. Selain itu, seiring dengan dikembangkannya model yang lebih besar, kompleksitasnya terus meningkat. Oleh karena itu, pertanyaannya tetap apakah kompleksitas yang ditimbulkan oleh metode berbasis DNN adalah akibat dari peningkatan kinerja, atau kemajuan yang dilaporkan dalam beberapa tahun terakhir hanyalah ilusi. Dan penggunaan metode tradisional sebaiknya lebih diutamakan.

Berdasarkan penjelasan diatas Pertumbuhan Tren Smarthome telah mendorong pengembangan model kompleks berbasis DNN. Namun, belum ada bukti yang membenarkan keunggulan metode ini. Model berbasis DNN sulit dilatih, memerlukan estimasi parameter yang besar, dan kompleksitasnya terus meningkat. Metode tradisional sebaiknya lebih diutamakan.

1.2 Tujuan

Berdasarkan perumusan masalah yang telah ditentukan, maka dibentuk juga tujuan yang ingin dicapai dari penelitian ini, yaitu antara lain:

1. Mengetahui Teknik *Man in the middle* menyerang perangkat Smart home.
2. Menyeimbangkan dataset dengan menggunakan *random oversampling*.
3. Mendeteksi anomali pada Smart home menggunakan metode DNN

1.3 Manfaat

Adapun manfaat yang ingin dicapai dari penelitian ini yaitu:

1. Dapat memberikan bahan uji untuk mengembangkan dan mengevaluasi guna meningkatkan keamanan terhadap ancaman baru yang terus berkembang.

2. Dapat mengatasi ketidak seimbangan dengan *random oversampling* pada dataset smart home.

3. Dapat mengetahui seberapa baik metode *Deep Neural Network* dalam mengklasifikasi dataset.

1.4 Rumusan Masalah

Berdasarkan konteks tersebut, rumusan masalah dalam penelitian ini dapat diidentifikasi sebagai berikut:

1. Menyiapkan dataset untuk diproses dalam deteksi anomali.
2. Deteksi anomali dalam data Smart home menggunakan metode DNN.
3. Mengatasi ketidak seimbangan data (*imbalance data*) untuk mencapai kinerja optimal.

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini antara lain:

1. Fokus pada dataset yang digunakan berupa dataset *Smart home* .
2. Tidak menggunakan matriks lainnya dan hanya menggunakan algoritma DNN (*deep neural network*) untuk deteksi yang terdiri akurasi, presisi, perolehan, dan skor F1.

1.6 Metodologi Penelitian

1. Metode Studi Pustaka dan Literatur

   Pada metode ini, penulis mencari dan mengumpulkan referensi dari berbagai sumber seperti buku, jurnal, dan internet yang relevan dengan penelitian yang akan dilakukan..

2. Metode Perancangan Sistem

Metode ini mengenai bagaimana membangun dan menerapkan metode pada sistem Skripsi, Apa yang digunakan dalam penelitian, seperti perangkat lunak, peralatan, dan proses konfigurasi serta penerapan metode pada Skripsi.

3. Metode Pengujian

Metode pengujian ini dilakukan pada kumpulan data yang diperoleh menggunakan pembelajaran mesin dan memberikan hasil dengan akurasi yang diinginkan.

4. Metode Analisis

Pada metode ini didasarkan pada hasil pengujian penelitian yang dilakukan. Analisis kelebihan dan kekurangan kemudian dilakukan untuk menarik kesimpulan dan saran yang dapat menjadi bahan penelitian selanjutnya.

5. Metode Kesimpulan dan Saran

Pada tahap akhir ini, penulis menarik kesimpulan dari seluruh kegiatan penelitian, mulai dari tinjauan pustaka hingga analisis hasil penelitian, dan memberikan rekomendasi untuk penelitian selanjutnya.

1.7 Sistematika Penulisan

Adapun sistematika dalam penulisan Skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang, tujuan, manfaat, rumusan masalah, batasan masalah, metode penelitian, dan uraian sistematik 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 *mitm* pada *Smarthome Comnets*.

BAB III METODOLOGI PENELITIAN

Pada bab ini menguraikan proses penelitian dan kerangka penelitian serta menjelaskan metodologi penelitian.

BAB IV HASIL DAN ANALISA

Pada bab ini menjelaskan hasil investigasi dan analisis dari analisis Deteksi Serangan *Man In The Middle* Menggunakan Metode *Deep Neural Network* (DNN).

BAB V KESIMPULAN DAN SARAN

Pada bab ini menyajikan kesimpulan dari penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya di masa yang akan datang.

DAFTAR PUSTAKA

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

[2] 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.

[3] K. Benton and T. Bross, "Timing Analysis of SSL/TLS Man in the Middle Attacks," pp. 1–9, 2013, [Online]. Available: http://arxiv.org/abs/1308.3559

[4] 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.

[5] Wang et al, "Man-in-the-Middle Attacks against Machine Learning Classifiers Via Malicious Generative Models," vol 3, 2021.

[6] Maniriho et al, "Anomaly-based Intrusion Detection Approach for IoT Networks Using Machine Learning," vol 2, no. 2, 2020.

[7] 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.

[8] Sivasankari and Kamalakkannan, "Detection and prevention of man-in-the-middle attack in iot network using regression modeling," 2022.

[9] S. Tang, S. Yuan, and Y. Zhu, "Data Preprocessing Techniques in Convolutional Neural Network Based on Fault Diagnosis Towards Rotating Machinery," pp. 149487–149496, 2020, doi: 10.1109/ACCESS.2020.3012182.

[10] 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.

[11] 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.

[12] K. Sahoo, A. K. Samal, J. Pramanik, and S. K. Pani, “Exploratory Data Analysis using Python,” vol. 3075, no. 12, pp. 4727–4735, 2019, doi: 10.35940/ijitee.L3591.1081219.

[13] 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.

[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] F. Kotob, “What Is Sustainability?,” no. November 2011, 2015.