SISTEM DETEKSI *MAN IN THE MIDDLE* (MITM) ATTACK PADA JARINGAN *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) MENGGUNAKAN *ARTIFICIAL NEURAL NETWORK*

TUGAS AKHIR

Oleh :

Yogi Yaspranika
09011181621121

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2020

SISTEM DETEKSI *MAN IN THE MIDDLE* (MITM) ATTACK PADA JARINGAN *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) MENGGUNAKAN *ARTIFICIAL NEURAL NETWORK*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

Yogi Yaspranika
09011181621121

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

LEMBAR PENGESAHAN

SISTEM DETEKSI *MAN IN THE MIDDLE* (MITM) ATTACK PADA JARINGAN *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) MENGGUNAKAN *ARTIFICIAL NEURAL NETWORK*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

YOGI YASPRANIKA
09011181621121

Indralaya, Agustus 2020

Pembimbing I,

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

Pembimbing II,

Ahmad Heryanto, S.Kom., M.T.
NIP. 198701222015041002

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah Diuji dan lulus pada :

Hari : Kamis

Tanggal : 06 Agustus 2020

Tim Penguji :

1. **Ketua** : **Rahmat Fadli Isnanto, M.Sc** (.....)
2. **Anggota I** : **Ahmad Zarkasi, S.T, M.T** (.....)
3. **Anggota II** : **Aditya Putra Perdana P, M.T** (.....)

Mengetahui,
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama **:Yogi Yaspranika**

Nim **:09011181621121**

Program Studi **:Sistem Komputer**

Judul Skripsi **:Sistem Deteksi *Man In The Middle* (MITM) *Attack* Pada Jaringan *Supervisory Control And Data Acquisition* Menggunakan *Artificial Neural Network***

Hasil Pengecekan *Software iThenticate/Turnitin* : 6%

Menyatakan bahwa laporan Tugas Akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / *plagiat.* Apabila ditemukan unsur penjiplakan / *plagiat* dalam laporan Tugas Akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, Agustus 2020

METERAI TEMPEL

6000

Yogi Yaspranika
09011181621121

HALAMAN PERSEMBAHAN

Motto :

Hai orang-orang beriman apabila dikatan kepadamu: “berlapang – lapanglah dalam mejelis”, maka lapangkanlah niscaya Allah akan memberi kelapangan untukmu. Dan apabila dikatakan: “Berdirilah kamu”, maka berdirilah, niscaya Allah akan meninggikan orang – orang yang beriman diantaramu dan orang – orang yang diberi ilmu pengetahuan beberapa derajat. Dan Allah Maha Mengetahui apa yang kamu kerjakan.
(QS. Al-Mujadilah: 11)

Sesungguhnya sesudah kesulitan itu ada kemudahan. Maka apabila kamu telah selesai dari suatu urusan, kerjakanlah dengan sungguh – sungguh urusan yang lain, dan hanya kepada Tuhanmulah hendaknya kamu berharap (QS. Ash – Sharh: 6 - 8)

Dengan Mengucapkan syukur Alhamdulillah atas rahmat dari Allah SWT., aku persembahkan karya kecil ini untuk :

- Ibunda dan Ayahanda tercinta
- Seluruh Keluarga Besarku
- Kawan - kawan seperjuangan di jurusan Sistem Komputer
- Almamaterku

KATA PENGANTAR

Pujidan syukur kepada Allah SWT, atas limpahan rahmat dan karunia-Nya yang telah memberikan penulis kesehatan dan kesempatan sebaik-baiknya, sehingga penulis dapat merampungkan Proposal Tugas Akhir in dengan judul "Sistem Deteksi *Man In The Middle* (MITM) Attack pada jaringan *Supervisory Control And Data Acquisition* (SCADA) dengan Menggunakan Metode *Artificial Neural Network*"**.**

Penulisan Proposal Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Proposal Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Ayahanda Mat Diyas dan ibunda yang kusayangi Yetnilidar serta keluarga penulis tercinta, yang telah mencurahkan segenap cinta dan kasih saying serta perhatian moril maupun materil kepada penulis selama melaksanakan dan mengikuti perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya, semoga Allah SWT selalu melindungi, melimpahkan rahmat, kesehatan, karunia dan keberkahan di dunia maupun di akhirat atas budi baik yang telah diberikan kepada penulis.
2. Bapak Jaidan Jauhari, S.Pd., M.T., 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 Ahmad Zarkasi, S.T., M.T. selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

6. Bapak Ahmad Heryanto, S.Kom,. M.T. selaku Dosen Pembimbing II Tugas Akhir di jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Kak Tri Wanda Septian., S. Kom., M.T yang telah membantu dalam penyelesaian Tugas Akhir.
8. Mbak Winda Kurnia Sari selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
9. Teman – teman perjuangan di grub Riset Comnets Nasbih, Deri, Maulidin, Hary, Farhan, Octa, Guntur, Aulia, Meyyen, Fitri, Wedeh, Aisah, Monica, Komar, Septiano dan Ichwanul
10. Seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
11. Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya.

Akhir kata penulis menyadari bahwa dalam penulisan Proposal Tugas Akhir ini masih jauh dari kesempurnaan. Oleh karena itu, penulis memohon saran dan kritik yang sifatnya membangun demi kesempurnaan Proposal Tugas Akhir ini dan semoga bermanfaat bagi kita semua baik dalam dunia Pendidikan maupun dalam lingkungan masyarakat. Aamiin.

Indralaya, Agustus 2020
Penulis

Yogi Yaspranika
Nim. 09011181621121

Sistem Deteksi *Man In The Middle* (MITM) *Attack* Pada Jaringan *Supervisory Control And Data Acquisition* (SCADA) Menggunakan *Artificial Neural Network*

Yogi Yaspranika (09011181621121)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

E-mail : yogiyaspranika@gmail.com

Abstrak

Intrusion Detection Systems adalah salah satu teknik untuk deteksi serangan yang terjadi di jaringan. *Supervisory Control And Data Acquisition* adalah sistem kontrol industri yang digunakan untuk infrastruktur kritis, salah satu protokol yang digunakan dalam komunikasi Scada adalah IEC 60870-5-104, protokol ini memiliki kerentanan pada kemanan *application layer* dan *data link layer*. Serangan *Man in the Middle* adalah serangan yang dilakukan *attacker* untuk mengambil alih saluran komunikasi tanpa disadari korban. *Artificial Neural Network* dapat digunakan untuk mendeteksi paket serangan dan paket normal. Hasil deteksi dievaluasi dengan *confusion matrix* untuk menentukan akurasi deteksi serangan MITM. Dari hasil penelitian ini diperoleh akurasi yang sangat baik mencapai 99.93% kemudian dengan FPR 0.14% untuk kesalahan deteksi.

Kata Kunci : *Instrusion Detection System, Supervisory Control And Data Acquisition, IEC 60870-5-104, Man In The Middle.*

Indralaya, Agustus 2020

Pembimbing I,

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

Pembimbing II,

Ahmad Heryanto, S.Kom., M.T.
NIP. 198701222015041002

Mengetahui,
Ketua Jurusan Sistem Komputer

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

Man In The Middle (MITM) Attack detection system on Supervisory Control And Data Acquisition (SCADA) network using Artificial Neural Network

Yogi Yaspranika (09011181621121)

Dept. of Computer Engineering, Faculty of Computer Science, Sriwijaya University
Email : yogiyaspranika@gmail.com

Abstract

Intrusion Detection Systems is a technique to attack detection which happens in network. Supervisory Control and Data Acquisition is industrial control systems used for critical infrastructure, a protocol to used in Scada communication is IEC 60870-5-104, this protocol has vulnerabilities security in the application layer and data link layer. Man in the Middle attack is an attack is done by attacker to take over communication channels unnoticed victims. Artificial Neural Networks can be used to detect attack packages and normal packages. The results of detection is evaluated with the Confusion Matrix to recognize how much the accuracy of MITM attack detection. From this research obtained 99.93% very good accuracy with FPR 0.14% for error detection.

Keywoard : *Instrusion Detection System, Supervisory Control And Data Acquisition, IEC 60870-5-104, Man In The Middle.*

Indralaya, Agustus 2020

Pembimbing I,

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

Pembimbing II,

Ahmad Heryanto, S.Kom., M.T.
NIP. 198701222015041002

Mengetahui,
Ketua Jurusan Sistem Komputer

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

DAFTAR ISI

Halaman

BAB III

TINJAUN PUSTAKA

BAB IV

HASIL DAN ANALISIS

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR RUMUS

Halaman

BAB I
PENDAHULUAN

1.1. Latar Belakang

Supervisory Control And Data Acquisition (SCADA) adalah *Industry Control System* (ICS) automatis yang digunakan untuk memonitoring dan mengendalikan proses industri seperti distribusi minyak dan gas, distribusi air dan jaringan tenaga listrik yang tersebar jauh secara geografis dimana akuisisi data terpusat sangat penting dalam pengoperasian sistem. Secara historis sistem Scada dirancang dengan jaringan *private network,* namun karena perangkat Scada tersebar jauh secara geografis, komunikasi Scada dituntut terhubung ke jaringan internet [1]. Ini memaparkan jaringan Scada ke dunia maya dan membuat Scada rentan terhadap serangan *cyber*.

Disisi lain,serangan *Man In The Middle* mempunyai risiko yang sangat tinggi pada jaringan Scada [2]. Serangan M*an In The Middle* adalah jenis serangan dimana penyerang diam-diam mengambil alih saluran komunikasi antara dua perangkat atau lebih, penyerang dapat melakukan interupsi, modifikasi atau mengganti trafik komunikasi perangkat korban [3].

Salah satu protokol komunikasi Scada adalah IEC 60870-5-104 digunakan untuk mengirim pesan telekontrol dasar antar perangkat berdasarkan standar TCP/IP, yang memungkinkan transmisi data secara simultan antara beberapa perangkat dan layanan [4]. Protokol IEC 60870-5-104 memiliki kerentanan pada keamanan a*pplication layer* dan d*ata link layer*. Kerentanan pada *application layer* menyebabkan protokol ini dapat diserangan dengan *spoofing* dan serangan *non-repudiation.* Sedangkan kerentanan pada *data link layer* menyebabkan protokol ini dapat di serangan menggunakan *snipping, modification data* dan *replay attack* [5].

Penggunaan *Intrusion Detection System* (IDS) pada jaringan Scada adalah konsep yang relatif baru. Beberapa penelitian menggunakan pendekatan IDS telah

dilakukan pada sistem Scada, seperti *signature-based* dan *anomaly-based* [6,7,8,9]. Proyek Digital Bond Quickdraw [6] merilis IDS berbasis signature untuk DNP3, Bacnet, Modbus dan S7 menggunakan *snort.*

Pada penelitian [7] membahas penerapan *rule-based* IDS untuk jaringan Scada protokol IEC 60870-5-104 menggunakan analisis protokol dan metode *Deep Packet Inspection.* Hasil penelitian ini menunjukkan *rule-based* IDS efektif dalam mengidentifikasi semua paket serangan tanpa ada *false alert* untuk serangan yang terdapat pada database sistem, tetapi tidak bisa mendeteksi serangan yang tidak terdapat pada database sistem.

Pada penelitian lain [8] membahas tentang sistem deteksi anomali berbasis *model-based* untuk serangan pada gardu daya listrik berdasarkan protokol IEC 60870-5-104, menggunakan tiga model serangan yaitu, *Arp Spoofing, DoS* dan C*ommand Injection.* Model deteksi dirancang dengan beberapa algoritma *Supervised Learning* seperti *Naive Bayes, Nearest Neighbor, Decision Tree* dan *Rule Learners,* dari hasil pengujian didapat bahwa algoritma *Rule Learners* memiliki akurasi terbaik yaitu 91,69%. Sedangkan pada penelitian lainnya [9] menunjukkan hasil deteksi anomali dengan algoritma *Artificial Neural Network* mempunyai akurasi yang lebih baik yaitu 99,64%.

Berdasarkan beberapa ulasan diatas, maka penelitian ini mengusulkan *Intrusion Detection Systems* berbasis *anomaly* untuk deteksi serangan *Man In The Middle* pada jaringan *Supervisory Control And Data Acquisition* protokol IEC 60870-5-104 dengan menggunakan pendekatan *Supervised Learning* yaitu *Artificial Neural Network.*

1.2. Tujuan

Adapun tujuan dari penelitian Tugas Akhir ini adalah sebagai berikut :

1. Membedakan antara paket normal dan paket serangan pada jaringan *Supervisory Control And Data Acquisition* sehingga dapat mendeteksi serangan *Man In The Middle*

2. Menerapkan algoritma *Artificial Neural Network* untuk deteksi trafik serangan *Man In The Middle* pada jaringan *Supervisory Control And Data Acquisition*
3. Menghitung akurasi deteksi serangan *Man In The Middle* pada jaringan *Supervisory Control And Data Acquisition* dengan algoritma *Artificial Neural Network.*

1.3. Manfaat

Berikut adalah manfaat yang ingin didapat dari penelitian Tugas Akhir :

1. Dapat membedakan paket serangan dan paket normal pada jaringan *Supervisory Control And Data Acquisition*
2. Dapat mendeteksi serangan *Man in The Middle* pada jaringan *Supervisory Control And Data Acquisition*
3. Dapat mengetahui tingkat akurasi metode *Artificial Neural Network* dalam deteksi serangan *Man in The Middle* pada jaringan *Supervisory Control And Data Acquisition*.

1.4. Rumusan Masalah

Berikut adalah perumusan masalah untuk penelitian Tugas Akhir :

1. Bagaimana mengekstrak dataset pcap, kemudian mencari pola serangan *Man In The Middle?*
2. Bagaimana metode *Artificial Neural Network* dapat mengenali serangan *Man in The Middle* pada jaringan *Supervisory Control And Data Acquisition* menggunakan paket normal*?*

1.5. Batasan Masalah

Berikut merupakan batas permasalahan untuk penelitian Tugas Akhir ini:

1. Penelitian dilakukan pada jaringan *Supervisory Control And Data Acquisition* protokol IEC 60870-5-104
2. Mengklasifikasi serangan *Man In The Middle* pada jaringan *Supervisory Control And Data Acquisition* menggunakan *Artificial Neural Network*
3. Serangan yang dideteksi hanya serangan *Man in The Middle*

4. Menggunakan *dataset* yang ter*capture traffic* normal dan serangan *Man in The Middle*
5. pengujian secara *offline*
6. tidak membahas cara pencegahan serangan *Man in The Middle.*

1.6. Metodologi Penelitian

Berikut merupakan metodologi penelitian tugas akhir yang akan melewati beberapa tahapan sebagai berikut :

1. Tahapan Pertama(Studi pustaka)

   Pada tahapan ini penulis mengkaji dan memahami referensi dari media pembelajaran dengan membaca buku, naskah ilmiah, serta artikel yang terkait langsung dengan penelitian ini.
2. Tahapan Kedua (Perancangan Sistem)

   Pada tahapan ini penulis merancang dan membuat sistem deteksi serangan *Man in The Middle* menggunakan algoritma *Artificial Neural Network* dan menentukan perangkat-perangkat yang diperlukan pada penelitian ini, baik perangkat keras maupun perangkat lunak.
3. Tahapan Ketiga(Pengujian)

   Pada tahap berikut ini penulis melakukan percobaan penelitian sesuai dengan batasan masalah pada penelitian ini.
4. Tahapan Keempat (Hasil dan Analisis)

   Pada tahapan ini penulis melakukan analisis terhadap hasil pengujian tersebut untuk mengetahui apa kelebihan dan kekurangan rancangan sistem serta faktor yang mempengaruhi.
5. Tahapan Kelima (Kesimpulan dan Saran)

   Pada tahap ini penulis menarik kesimpulan penelitian berdasarkan rumusan masalah penelitian, studi pustaka penelitian, metodologi dan analisis hasil penelitian, serta memberikan saran untuk tahapan penelitian selanjutnya.

1.7. Sistematika Penulisan

Berikut merupakan sistematika penulisan yang digunakan dalam Penelitian Tugas Akhir :

BAB I. PENDAHULUAN

Bab ini terdiri dari penjelasan landasan topik Penelitian Tugas Akhir seperti latar belakang,tujuan, manfaat,rumusan masalah, metodologi penelitian, dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini terdiri dari penjelasan dasar teori penelitian yaitu *Supervisory Control and Data Acquisition, Intrusion Detection System, Man in The Middle Attack, Artificial Neural Network,* serta teori lain yang mempunyai berhubungan dengan penelitian.

BAB III. METODOLOGI PENELITIAN

Bab ini terdiri dari penjelasam proses penelitian Tugas Akhir, tahap perancangan sistem penelitian dan cara penerapan metode secara terarah.

BAB IV. PENGUJIAN DAN ANALISIS

Bab ini terdiri dari penjelasan hasil pengujian sistem pada penelitian Tugas Akhir serta menunjukkan analisis hasil dari data yang didapatkan.

BAB V. KESIMPULAN DAN SARAN

Bab ini terdiri dari penjelasan kesimpulan yang di dapat dari penelitian Tugas Akhir, dan menjawab tujuan yang ingin didapatkan seperti yang tertera pada Bab Pendahuluan, dan memberikan saran untuk dilakukan pada penelitian selanjutnya.

DAFTAR PUSTAKA

[1] M. Teixeira, T. Salman, M. Zolanvari, and R. Jain, "SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach," *Futur. Internet*, vol. 10, Aug. 2018.

[2] P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, and E. Panaousis, "Attacking IEC-60870-5-104 SCADA Systems," *1st IEEE Serv. Work. Cyber Secur. Resil.Internet Things*, pp. 41–46, 2019.

[3] 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.

[4] Q. Saif Qassim *et al.*, "Simulating command injection attacks on IEC 60870-5-104 protocol in SCADA system," *Int. J. Eng. Technol.*, vol. 7, pp. 153–159, 2018.

[5] D. S. Pidikiti, R. Kalluri, R. K. S. Kumar, and B. S. Bindhumadhava, "SCADA communication protocols: vulnerabilities, attacks and possible mitigations," *CSI Trans. ICT*, vol. 1, no. 2, pp. 135–141, 2013.

[6] "Project Quickdraw ICS." [Online] . Available :https://github.com/digitalbond/Quickdraw-Snort. [Accessed: 25-Feb-2020]

[7] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, and H. F. Wang, "Rule-based Intrusion Detection System for SCADA networks," *IET Renew.Power Gener.Conf.*, vol. 2013, 2013.

[8] E. Hodo, S. Grebeniuk, H. Ruotsalainen, and P. Tavolato, "Anomaly detection for simulated IEC-60870-5-104 traffic," *ARES '17*, pp. 1–7, 2017.

[9] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial

Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, 2019.

[10] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput.Secur.*, vol. 56, pp. 1–27, Feb. 2016.

[11] M. Petr, *Description and analysis of IEC 104 Protocol Petr Matoušek*. Faculty of Information Technology BUT, 2017.

[12] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, "Intrusion Detection System for IEC 60870-5-104 based SCADA networks," *IEEE Power Energy Soc. Gen. Meet.*, pp. 1–5, 2013.

[13] S. Rachel and Subhashkar, "An Overview of the Man-In-The-Middle Attack," *Natl. Conf. Contemp. Res. Innov. Comput.Sci.*, pp. 1–6, 2017.

[14] O. Eigner, P. Kreimel, and P. Tavolato, "Detection of man-in-the-middle attacks on industrial control networks," in *International Conference on Software Security and Assurance (ICSSA)*, 2016, pp. 64–69.

[15] B. Bhushan and G. Sahoo, "Man-In-The-Middle Attack in Wireless and Computer Networking- A review," *3rd Int. Conf. Adv. Comput. Autom.*, pp. 1–6, 2017.

[16] J. Jabez and B. Muthukumar, "Intrusion detection system (ids): Anomaly detection using outlier detection approach," *Procedia Comput. Sci.*, vol. 48, pp. 338–346, 2015.

[17] J. Peng, K. R. Choo, and H. Ashman, "User profiling in intrusion detection: A review," *J. Netw. Computer.Appl.*,vol. 72, pp. 14–27, 2016.

[18] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," *IEEE Commun.Surv.Tutorials*, vol. 00, no. 0, pp. 2671–2701, 2018.

[19] N. Kaja, A. Shaout, and D. Ma, “An intelligent intrusion detection system,” *Appl. Intell.*, vol. 49, no. 9, pp. 3235–3247, 2019.

[20] A. Shaik, R.Dr.K.Nageswara, and Dr.J.A.Chandulal, “Intrusion Detection System Methodologies Based on Data Analysis” *International Journal of Computer Application*, vol. 5, no. 2, pp. 10–20, 2010.

[21] J. Hussain, S. Lalmuanawma, and L. Chhakchhuak, “A two-stage hybrid classification technique for network intrusion detection system,” *Int. J. Comput. Intell.Systems.*, vol. 9, no. 5, pp. 863–875, 2016.

[22] G. S. Georgiou, P. Christodoulides, and S. A. Kalogirou, “Implementing artificial neural networks in energy building applications - A review,” *IEEE Int. Energy Conf. ENERGYCON 2018*, pp. 1–6, 2018.

[23] A. Stetco *et al.*, “Machine learning methods for wind turbine condition monitoring: A review,” *Renew. Energy*, vol. 133, pp. 620–635, 2018.

[24] H. Ramchoun, M. Amine, J. Idrissi, Y. Ghanou, and M. Ettaouil, “Multilayer Perceptron: Architecture Optimization and Training,” *Int. J. Interact. Multimed.Artif.Intell.*, vol. 4, pp. 26–30, 2016.

[25] L. Haghnegahdar and Y. Wang, “A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection,” *Neural Comput.Appl.*, pp. 1–15, 2019.

[26] W. Xie, G. Liang, Z. Dong, B. Tan, and B. Zhang, “An Improved Oversampling Algorithm Based on the Samples’ Selection Strategy for Classifying Imbalanced Data,” *Math. Probl.Eng.*, vol. 2019, pp. 1–13, 2019.

[27] P. Maynard, K. Mclaughlin, and S. Sezer, “An Open Framework for Deploying Experimental SCADA Testbed Networks,” *Ind. Control Syst. Cyber Secur. Res.*, pp. 89–98, Aug. 2018.

[28] G. K. Armah, G. Luo, and K. Qin, “A Deep Analysis of the Precision Formula for Imbalanced Class Distribution,” *Int. J. Mach. Learn. Comput.*,vol. 4, no. 5, pp. 417–422, 2014.