Vol. 1 No. 2 2024 **E-ISSN : 3031-9692**
Institut Teknologi dan Bisnis STIKOM Bali, 22-04-2024

Klasifikasi Deteksi Anomali Menggunakan Metode Machine Learning

Gede Satria Wibawa Prabuningrat[1)], Dandy Pramana Hostiadi[2)], Ni Luh Putri Srinadi[3)]
Program Studi Magister Sistem Informasi
Institut Teknologi dan Bisnis STIKOM Bali
Denpasar, Indonesia
e-mail: *222012020@stikom-bali.ac.id[1)], dandy@stikom-bali.ac.id[2)] , putri@stikom-bali.ac.id[3)]*

Abstrak

Pada masa sekarang ini, perkembangan era digitalisasi telah mengalami perkembangan yang sangat signifikan, selain itu juga peningkatan penggunaan media layanan internet yang cenderung mengalami kenaikan namun diimbangi dengan kenaikan tingkat potensi kejahatan. Salah satu upaya yang dapat dilakukan untuk mengurangi potensi kejahatan ini adalah pembentukan sistem keamanan pada jaringan internet yang dapat mendeteksi anomali. Deteksi anomali memiliki tujuan untuk menemukan perilaku menyimpang yang tidak seharusnya pada suatu pola dalam penggunaan jaringan internet. Pada penelitian ini akan dilakukan deteksi anomali menggunakan pendekatan metode machine learning decission tree dengan melakukan optimasi feature selection untuk mencari performa terbaik. Studi kasus pendeteksian anomali yang digunakan pada penelitian ini adalah dataset public UNSW NB-15. Hasil yang didapatkan pada penelitian ini menunjukan bahwa pada dataset tersebut, berhasil mendeteksi aktifitas anomali dalam jaringan dengan evaluasi pada nilai AUC:0.992, CA:0.999, F1-Score:0.999, Precission:0.999, Recall:0.999 dan MCC:0.984. Teknik analisis ini dapat membantu administrator jaringan dalam mengantisipasi indikasi adanya aktifitas anomali yang mengarah pada aktifitas serangan di dalam jaringan.

Kata kunci: *Network Traffic, Anomaly Detection, Machine Learning.*

1. Pendahuluan

Seiring dengan perkembangan teknologi internet dan komputer saat ini hampir semua orang menggunakan teknologi komputer dan internet. Berkat kemajuan tersebut banyak kebutuhan serta pekerjaan dengan mudah dapat dikerjakan[1] dan secara tidak langsung hal ini telah menjadi fondasi esensial yang sangat berpengaruh bagi kelangsungan berbagai sektor kehidupan manusia. Adapun aspek yang cenderung memiliki ketergantungan terhadap infrastruktur teknologi internet dan komputer adalah aspek bisnis, pendidikan dan komunikasi[2]. Hal ini mengakibatkan, keamanan siber dan perlindungan terhadap berbagai serangan telah menjadi pertanyaan yang mendesak pada saat ini. Alasan utama dibalik hal tersebut adalah pertumbuhan dan ketergantungan terhadap penggunaan internet dan jaringan komputer sehingga potensi kejahatan oleh orang yang tidak bertanggung jawab dapat memanfaatkan momentum ini untuk melakukan sebuah penyerangan sehingga dapat menjadi keuntungan bagi orang yang tidak bertanggung jawab tersebut. Serangan siber dapat menyebabkan kerusakan yang signifikan parah dan dapat menimbulkan kerugian finansial yang signifikan dalam jaringan skala besar[3].

Seperti yang diketahui, siber sekuriti adalah sebuah kumpulan teknologi, teknik, proses dan kebijakan yang bekerja bersama dan di desain untuk melindungi komputer, jaringan, *software program* dan data dari serangan[4] dan akses, perubahan dan perusakan yang tidak sah[5]. Oleh karena itu, mengingat hal ini menjadi sangat krusial maka diperlukan cara yang akan berperan penting dalam keamanan saat ini untuk mendeteksi berbagai serangan siber atau anomali dalam sebuah jaringan serta pengembangan sistem deteksi intrusi yang efektif dan efisien[6]. Teknik-teknik kecerdasan buatan (AI), terutama dalam bentuk *machine learning* dapat dimanfaatkan untuk merancang sistem deteksi intrusi yang cerdas berbasis data. Pada awal penelitian tentang deteksi anomali banyak didasari dengan penggunaan metode *signature based*. Namun hal ini memiliki kendala yang patut diperhitungkan yaitu harus selalu dilakukan perbaharui terkini pada basis data jika *signature* baru muncul[7]. Metode ini berhasil dalam mendeteksi serangan yang sudah teridentifikasi sebelumnya, namun tidak efektif dalam menghadapi serangan yang belum diketahui. Sementara itu, deteksi anomali mengandalkan mekanisme heuristic untuk mengenali aktivitas berbahaya yang belum teridentifikasi sebelumnya[8]. Maka, diperlukan lebih banyak penelitian untuk mengembangkan teknik deteksi anomali lalu lintas jaringan yang menggunakan klasifikasi *machine learning* yang lebih mutakhir agar dapat menemukan jenis anomali yang baru.

Pada penelitian sebelumnya terdapat beberapa penelitian sebelumnya yang berhubungan dengan klasifikasi deteksi anomali pada jaringan lalu lintas komputer. Penelitian yang dilakukan oleh Qian Ma *et al*[9], yang berjudul *A novel model for anomaly detection in network traffic based on kernel support vector machine*. Penulis mengusulkan sebuah model dengan menggunakan metode *Kernel Support Vector Machine*(SVM) untuk mendeteksi anomali dalam lalu lintas jaringan. Penelitian ini menggunakan 3 dataset dan menghasilkan lebih dari 99% akurasi pada semua dataset dengan menggunakan metode yang diusulkan.

Penelitian yang dipersembahkan oleh Mahmoud Said Elsayed *et al*[10] adalah dengan melakukan pendekatan *Long Short Term Memory* (LSTM) *autoencoder* dan *One-class Support Vector Machine*(OC-SVM) untuk mendeteksi serangan anomali pada *unbalanced* dataset dengan melakukan pelatihan model hanya menggunakan kelas normal pada dataset. Penelitian ini menggunakan InSDN Dataset sebagai data uji yang berisi beragam skenario serangan dan kelas serangan seperti *DoS, DDoS, Web attacks, Password-Guessing, Bot-net, Exploitation* dan *Probe attacks.* Penelitian ini mampu menghasilkan komparasi akurasi terbaik sebesar 90.5% dengan menggunakan metode LSTM-Autoencoder-OC-SVM.

Penelitian berjudul *Network Anomaly Detection inside Consumer Networks-A Hybrid Approach* yang disampaikan oleh Darsh Patel *et al*(11) mempersembahkan pendekatan hibrida untuk mendeteksi anomali dengan hanya menggunakan informasi jaringan dasar seperti *Packet Size, Source, Destination Port, Time, Transmission Control Protocol* (TCP) *Flags.* Penulis melakukan *feature extraction* terhadap informasi jaringan dasar tersebut yang didapat melalui *capture traffic* menggunakan aplikasi *wireshark*. Penelitian ini memberikan bukti hasil terbaik dengan melakukan komparasi metode *Isolation Forest* dan *One-Class Support Vector Machine* (OCSVM) dan terbukti dengan menggunakan pendekatan hibrida ini mampu memberikan akurasi terbaik sebesar 91.55% dengan perbandingan 83.757% dan 87.909% tapi juga mampu memberikan hasil deteksi *false-positive rate* yang rendah dibandingankan dengan OCSVM dan *Isolation Forest* (8.442% dibandingkan dengan 11.333% dan 16.618%).

Penelitian yang dilakukan oleh Zavrak, S., dan Iskefiyeli[12] dengan judul *Anomaly-Based Intrusion Detection From Network Flow Features using Variational Autoencoder* yang berfokus terhadap pendeteksian *anomalous network traffic* berdasarkan *flow-based* data dengan menggunakan metode *deep learning*. Penulis disini melakukan perbandingan metode terbaik antara metode *Autoencoder, Variational Autoencoder* dan *One-Class Support Vector Machine* terhadap hasil *ROC curves* dan *AUC.* Berdasarkan hasil penelitian tersebut, rate deteksi dari *VAE* lebih baik dari pada *AE* dan *OCSVM*.

Penulis Nagaraja, A., *et al*[13] mempersembahkan penelitian mengenai komparasi hasil dengan melakukan transformasi fitur terhadap dataset KDD dan NSL-KDD untuk mendeteksi *anomalous traffic.* Transformasi fitur ini dilakukan dengan cara *clustering* atribut dari dataset dan kemudian mencari *similarity* pada setiap fitur. Hal ini digunakan untuk mendapatkan pengurangan dimensi input pada dataset. Penulis juga melakukan klasifikasi metode dengan menerapkan hasil transformasi dataset terhadap metode *Naive Bayes, BayesNet, SMO, J48 Decision Tree* dan *KNN.* Hasil analisis penelitian ini membuktikan bahwa metode pendekatan ini memberikan hasil yang lebih baik dan dapat meningkatkan performa parameter *accuracy, precision* dan *recall.*

Penelitian yang berjudul *Network Anomaly Detection Using Deep Learning Techniques* yang dilakukan oleh Hooshmand, M., dan Hosahalli, D.,[14] mempersembahkan metode pendekatan *Convolutional Neural Network* (CNN) terhadap dataset UNSW-NB15 dengan cara melakukan pembagian data traffic menjadi *transmission control procotol* (TCP), *user diagram protocol* (UDP) dan OTHER *protocol*. Penulis disini melakukan seleksi fitur dengan menggunakan teknik *Chisquare* dan melakukan *over-sampling* untuk mengatasi masalah *imbalance*. Metode ini mampu menghasilkan rata-rata *f-score* 0.85, 0.97, 0.86 dan 0.78 pada masing-masing katagori seperti TCP, UDP, OTHER dan ALL.

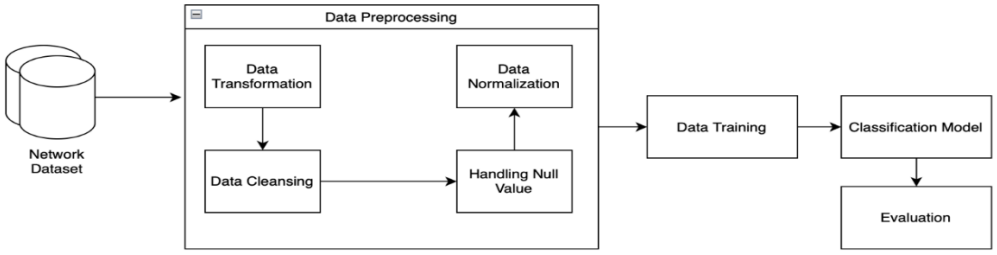
Penelitian yang dipersembahkan oleh Ying-Feng Hsu dan Morito Matsuoka[15], yang berjudul *A Deep Reinforcement Learning Approach for Anomaly Network Intrusion Detection System* yang berfokus terhadap sistem deteksi intrusi jaringan anomali dengan melakukan *deep reinforcement learning-based* (DRL). Penulis disini mampu mempersembahkan sistem yang dapat memperbaharui diri sendiri terhadap tingkah laku atau pola trafik jaringan yang baru. Studi kasus pada penelitian ini menggunakan NSL-KDD dan UNSW-NB15 dan data trafik riil kampus yang didapatkan berdasarkan *time sequence* selama 14 hari. Selain itu juga, penulis melakukan klasifikasi menggunakan 3 metode berbeda seperti *Random Forest* (RF), *Support Vector Machine* (SVM) dan *Multiplayer Perception* (MLP). Dapat disimpulkan hasil penelitian ini bahwa metode yang diusung oleh penulis yaitu DRL mampu memberikan hasil akurasi tertinggi, performa yang lebih baik dari sisi kecepatan proses dan keefektifitasan dalam memperbaharui model.

Pada penelitian ini nantinya akan melakukan klasifikasi deteksi anomali pada dataset UNSW-NB15 dengan menggunakan metode Decision Tree dan akan dilakukan komparasi terhadap dataset yang akan dilakukan *preprocessing* berupa normalisasi data untuk menghilangkan data yang noise dan

transformasi data dengan data yang hanya dilakukan transformasi data untuk mendapatkan performa terbaik.

2. Metode Penelitian

Pada penelitian yang diusulkan ini dengan melakukan perkenalan model untuk mendapatkan hasil lebih baik dalam hal akurasi dengan menggunakan klasifikasi individu yaitu tree. Arsitektur model sistem akan dijelaskan pada bagian ini dan juga akan disampaikan teknik pre-processing data dan algoritma klasifikasi. Secara umum, arsitektur model sistem yang diusulkan ditampilkan pada Gambar 1.



Gambar 1. Arsitektur Model

2.1 Arsitektur Model

Langkah awal pada bagian ini adalah membagi lalu lintas jaringan dataset menjadi du akelas, yaitu attacker dan normal dengan mengimplementasikan klasifikasi machine learning tree sebagai model deteksi serangan anomali. Hal ini terdiri dari beberapa tahapan : *data transformation, data cleansing, handling null value* dan *data normalization*.

2.2 *Data Transformation*

Pada bagian ini menjelaskan proses transformasi data yang dilakukan dengan cara melakukan perubahan fitur data *categorical* menjadi *numeric*. Fitur yang diubah pada bagian ini seperti *srcip, dstip, state, is_sm_ips_ports, proto* dan *service*. Dikarenakan *srcip* dan *dstip* merupakan *categorical features* pada internet protocol versi 4 yang dimana mempunyai 32-bit angka. IPv4 ini direpresentasikan memiliki empat bilangan desimal dari 0 ke 255 dan dibagi dengan beberapa periode. Pada kasus penelitian ini, untuk menkonversi IPv4 menjadi format 32-bit *binary* menggunakan model dari Python *ipaddress*. Dan fitur *state, is_sm_ips_ports, proto* dan *service* akan dilakukan konversi menggunakan *one hot encoding* menggunakan aplikasi Orange Data Mining. Hasil dari konversi IPv4 menjadi *numeric* dapat ditampilkan pada Tabel 1.

Tabel 1. Tranformasi IPv4 menjadi numerik

srcip	***unpack()***	***dstip***	***unpack()***
59.166.0.0	1000734720	149.171.126.9	2511044105
59.166.0.6	1000734726	149.171.126.7	2511044103
59.166.0.5	1000734725	149.171.126.5	2511044101
59.166.0.3	1000734723	149.171.126.0	2511044096
10.40.182.3	170440195	10.40.182.3	170440195
.....	.....	.....	.....
10.40.170.2	170437122	10.40.170.2	170437122

2.3 *Data Cleansing*

Data trafik lalu lintas jaringan memiliki beberapa fitur yang tanpa nilai dan hal ini nantinya akan dapat memberi dampak terhadap performa klasifikasi. Oleh karena itu, *data cleansing* ini dibutuhkan untuk menghilangkan fitur yang tidak dibutuhkan pada proses klasifikasi ini. Seperti contoh pada kasus ini, ada satu fitur yang dihilangkan yaitu *attack_cat* karena tidak diperlukan pada proses klasifikasi.

2.4 *Handling Null Value*

Tidak semua fitur yang memiliki nilai *null* atau *NaN* dapat dihilangkan pada proses *data cleansing*. Pada dataset ini memiliki nilai *missing value* atau *null* sebesar 3,5% data. Ada beberapa fitur yang memiliki

nilai *null* atau *NaN* yang tinggi tidak dihilangkan namun pada proses ini *record* data yang miliki nilai *null* akan dihapus sehingga karena proses ini terjadi maka jumlah *record* dataset yang awalnya berjumlah 2.540.044 *record* mengalami penurunan menjadi 1.087.202 *record*.

2.5 *Data Normalization*

Setelah melalui beberapa tahapan sebelumnya, semua data sudah mengalami perubahan dan menjadi *numeric*. Dikarenakan adanya perbedaan rentang data pada setiap fitur maka diperlukan proses standarisasi dengan menggunakan *data normalization to interval* (0,1). Seperti contoh, *srcip* dan *dstip* yang memiliki rentang data berbeda dengan fitur data yang lainnya. Perbandingan nilai pada setiap fitur dapat dilihat pada Tabel 2.

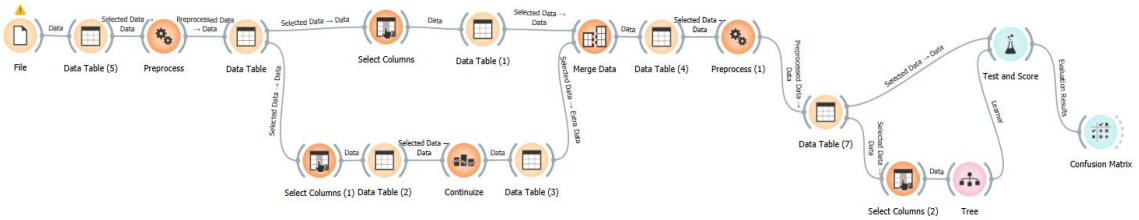
Data *numeric* yang telah dihasilkan dalam tahapan *pre-processing* data dan kemudian dibentuk sebagai nilai standar yang akan digunakan sebagai input dalam proses indentifikasi menggunakan konsep *machine learning tree*. Output dari proses ini adalah sejumlah lalu lintas jaringan yang diidentifikasi sebagai kelas *attacker* atau normal.

Tabel 2. Data sebelum proses normalisasi

srcip	*sport*	*dstip*	*dsport*	*dur*	....	*ct_dst_src_ltm*
1000734720	33661	2511044105	1024	0.036133	....	2
1000734726	1464	2511044103	53	0.001119	....	1
1000734725	3593	2511044101	53	0.001209	....	1
1000734723	49664	2511044096	53	0.001169	....	1
170440195	32119	170440195	111	0.078339	....	2
1000734725	2142	2511044102	53	0.001134	....	1
1000734727	0	2511044100	0	0.0	....	2
.....	.....	.....	.....	.....	....	.....
170437122	12660	170437122	53	0.001167	....	2

3. Hasil dan Pembahasan

Bagian ini menyajikan hasil dan pembahasan dari penelitian yang menggunakan data UNSW-NB15 sebagai studi kasus. Pada penelitian ini mengimplementasikan dan mengevaluasi metode yang diusulkan dengan menggunakan *software* Orange Data Mining pada laptop M2 Apple Chipset dengan 16GB RAM. Seperti pada Gambar 1 yang berisi tentang proses klasifikasi pada *software* Orange Data Mining.



Gambar 2. Proses klasifikasi pada *software* Orange Data Mining.

UNSW-NB15 memiliki fitur sejumlah 2.540.044 data dan terbagi kedalam empat file *CSV* dengan 48 fitur dan 1 kelas label yang menunjukkan nilai *attacker* atau normal. Kelas label ini memiliki 10 kelas yang terdiri dari 1 kelas normal dan 9 kelas tipe serangan : *Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode* dan *Worms.* Seperti yang ditunjukan pada Tabel 3.

Tabel 3. Spesifikasi Dataset UNSW-NB15

Dataset	Jumlah Data	Jumlah Fitur
UNSW-NB15	2.540.044	49

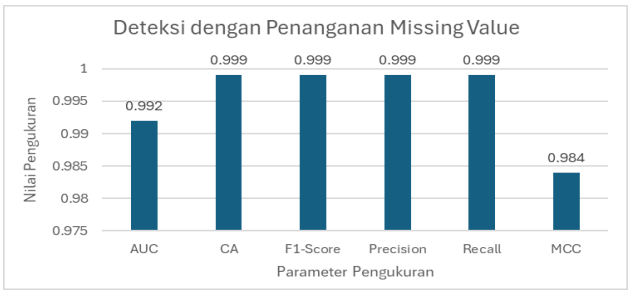
Proses awal pengolahan data adalah data transformasi, yaitu perubahan data kategorikal menjadi numerik. Proses data transformasi menggunakan teknik *one-hot-encode.* Hasil perubahan menambah

jumlah fitur dari 49 fitur menjadi 209 fitur. Fitur yang dirubah antara lain adalah *state, service, is_sm_ips_ports* dan *proto*. Kemudian dilakukan proses data *cleansing*, melakukan penanganan data kosong dan menghilangkan satu fitur yaitu *attack_cat*. Fitur *attack_cat* dihapus karena dalam penelitian ini bertujuan untuk mendeteksi adanya eksistensi serangan dan bukan mendeteksi jenis serangan yang ada. Hasil data cleansing adalah mereduksi data traffik sebesar

Tabel 4. Hasil Proses Data Cleansing

Jumlah Data Awal	Setelah Proses Data Cleansing	Persentase Reduksi Data
2.540.044	1.087.202	57%

Kemudian dilakukan proses data normalisasi, yaitu membentuk skala data menjadi rentang nilai 0-1. Setelah itu, data di bagi menjadi dua yaitu data latih yang digunakan dalam pelatihan model dan data uji yang digunakan untuk menguji model klasifikasi. Dalam penelitian ini digunakan komposisi data yaitu 70% untuk pelatihan dan 30% untuk pengujian. Hasil pemodelan menunjukkan bahwa model Decission tree memiliki rata performa diatas 98%. Hasil performa model ditunjukkan pada Gambar 3.



Gambar 3. Hasil Deteksi dengan metode Decission Tree

Sebagai perbandingan, kita melakukan komparasi hasil terhadap dataset yang telah dilakukan *pre-processing* dan penghapusan *missing value* pada fitur data dengan data yang tidak mengalami proses *missing value* terhadap metode klasifikasi *tree.* Disini kita menggunakan semua fitur kecuali *attack_cat*, dimana hasil akurasi keseluruhan dan kinerja klasifikasi dinyatakan dalam hal *AUC, CA, F1-score, Precision, Recall* dan *MCC*. Perbandingan menunjukkan bahwa usulan dengan teknik penanganan *missing value* memiliki nilai yang lebih baik dari parameter *AUC, CA, F1-score, Precision, Recall* dan *MCC*. *Hasil* komparasi dapat dilihat pada Tabel 5.

Tabel 5. Hasil komparasi pada UNSW-NB15 Dataset

Model	**AUC**	**CA**	**F1-Score**	**Precision**	**Recall**	**MCC**
Deceision Tree Non Handling Null	0.991	0.996	0.996	0.996	0.996	0.981
Usulan Decision Tree + Remove Null	0.992	0.999	0.999	0.999	0.999	0.984

4. Kesimpulan

Pada penelitian ini, kita mengusulkan metode klasifikasi *tree* pada dataset UNSW-NB15 dengan melakukan *pre-processing* data dari proses persiapan data latih, *data transformation, data cleansing, handling missing value* dan *data normalization* dalam mendeteksi anomali pada lalu lintas jaringan. Dan terbukti pada penelitian ini bahwa proses *pre-processing* data ini dapat mempengaruhi hasil perfoma dari sebuah metode klasifikasi.

Penelitian selanjutnya memfokuskan pada jumlah perbandingan komparasi dengan metode klasifikasi lainnya dan selain itu juga, mungkin dapat ditambahkan fitur ekstraksi atau fitur engineering untuk melihat dan membuktikan bahwa dengan melakukan *pre-processing* data lebih banyak dapat mempengaruhi performa dari metode klasifikasi machine learning. Dan juga dapat ditambahkan dataset network sebagai pembanding.

Daftar Pustaka

[1] Fadhlurrohman, M., Muliawati, A., & Hananto, B. (2021). Analisis Kinerja Intrusion Detection System pada Deteksi Anomali dengan Metode Decision Tree Terhadap Serangan Siber Analysis of Intrusion Detection System Performance on Anomaly Detection with Decision Tree Method Against Cyber Attacks. Ilmu Komputer Agri-Informatika, 8(2), 90–94. http://journal.ipb.ac.id/index.

[2] Grace Martha Geertruida Bororing. (2024). PENGEMBANGAN ALGORITMA MACHINE LEARNING UNTUK MENDETEKSI ANOMALI DALAM JARINGAN KOMPUTER. Review Pendidikan Dan Pengajaran, 7(1), 1361–1368.

[3] Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. Communications in Computer and Information Science, 1235 CCIS, 121–131. https://doi.org/10.1007/978-981-15-6648-6_10

[4] Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. In Information (Switzerland) (Vol. 10, Issue 4). MDPI AG. https://doi.org/10.3390/info10040122

[5] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access, 6, 35365–35381. https://doi.org/10.1109/ACCESS.2018.2836950

[6] Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). IntruDTree: A machine learning based cyber security intrusion detection model. Symmetry, 12(5). https://doi.org/10.3390/SYM12050754

[7] Institute of Electrical and Electronics Engineers., & International Federation for Information Processing. (2018). IEEE/IFIP Network Operations and Management Symposium : Cognitive Management in a Cyber World : NOMS Taiwan : 23-27 April 2018, Taipei, Taiwan.

[8] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access, 7, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

[9] Ma, Q., Sun, C., Cui, B., & Jin, X. (2021). A novel model for anomaly detection in network traffic based on kernel support vector machine. Computers and Security, 104. https://doi.org/10.1016/j.cose.2021.102215

[10] Said Elsayed, M., Le-Khac, N. A., Dev, S., & Jurcut, A. D. (2020). Network Anomaly Detection Using LSTM Based Autoencoder. Q2SWinet 2020 - Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, 37–45. https://doi.org/10.1145/3416013.3426457

[11] Patel, D., Srinivasan, K., Chang, C. Y., Gupta, T., & Kataria, A. (2020). Network anomaly detection inside consumer networks—a hybrid approach. Electronics (Switzerland), 9(6), 1–12. https://doi.org/10.3390/electronics9060923

[12] Zavrak, S., & Iskefiyeli, M. (2020). Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder. IEEE Access, 8, 108346–108358. https://doi.org/10.1109/ACCESS.2020.3001350

[13] Nagaraja, A., Boregowda, U., Khatatneh, K., Vangipuram, R., Nuvvusetty, R., & Sravan Kiran, V. (2020). Similarity Based Feature Transformation for Network Anomaly Detection. IEEE Access, 8, 39184–39196. https://doi.org/10.1109/ACCESS.2020.2975716

[14] Hooshmand, M. K., & Hosahalli, D. (2022). Network anomaly detection using deep learning techniques. CAAI Transactions on Intelligence Technology, 7(2), 228–243. https://doi.org/10.1049/cit2.12078

[15] Hsu, Y. F., & Matsuoka, M. (2020, November 9). A Deep Reinforcement Learning Approach for Anomaly Network Intrusion Detection System. Proceedings - 2020 IEEE 9th International Conference on Cloud Networking, CloudNet 2020. https://doi.org/10.1109/CloudNet51028.2020.9335796