ANALISIS DATA *TIME SERIES* UNTUK *FORECASTING* DATA *CYBER ATTACK* PADA HONEYPOT MENGGUNAKAN METODE *SUPPORT VECTOR REGRESSION* (SVR)

OLEH:

CUH MEIZI SASFINI
09011381924120

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

TAHUN 2023

ANALISIS DATA *TIME SERIES* UNTUK *FORECASTING* DATA *CYBER ATTACK* PADA HONEYPOT MENGGUNAKAN METODE *SUPPORT VECTOR REGRESSION* (SVR)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH:

CUH MEIZI SASFINI
09011381924120

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

TAHUN 2023

LEMBAR PENGESAHAN

ANALISIS DATA *TIME SERIES* UNTUK *FORECASTING* DATA *CYBER ATTACK* PADA HONEYPOT MENGGUNAKAN METODE *SUPPORT VECTOR REGRESSION* (SVR)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

CUH MEIZI SASFINI
09011381924120

Indralaya, 16 Oktober 2023

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. Sukemi, M.T.	**Ahmad Heryanto, S.Kom, M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Senin
Tanggal : 2 Oktober 2023

Tim Penguji:

1. Ketua : **Ahmad Fali Oklilas, M.T.**

2. Sekretaris : **Nurul Afifah, M.Kom.**

3. Penguji 1 : **Dr. Ahmad Zarkasi, M.T.**

4. Pembimbing : **Ahmad Heryanto, S.Kom, M.T.**

Mengetahui, 19/10/23
Ketua Jurusan Sistem Komputer

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

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	: Cuh Meizi Sasfini
NIM	: 09011381924120
Judul	: Analisis Data *Time Series* Untuk *Forecasting* Data *Cyber Attack* Pada Honeypot Menggunakan Metode *Support Vector Regression* (SVR)

Hasil Pengecekan Software Ithenticate/Turnitin: 8%

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 saksi akademik dari universitas Sriwijaya.

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

Inderalaya, 11 Oktober 2023

Cuh Meizi Sasfini
NIM. 09011381924120

KATA PENGANTAR

Segala puji dan syukur atas kehadirat Allah Yang Maha Esa, untuk semua berkat, kasih sayang, serta karunia-Nya penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini yang berjudul "Analisis Data *Time Series* Untuk *Forecasting* Data *Cyber Attack* Pada Honeypot Menggunakan Metode *Support Vector Regression* (SVR)"

Dalam kesempatan ini penulis mengucapkan rasa syukur kepada Allah Yang Maha Esa, yang telah memberikan karunianya dan perlindungannya selama dalam awal penulisan sampai selesainya penulisan Proposal Tugas Akhir ini dengan lancar. Dan tak lupa pula saya ucapkan terima kasih kepada pihak yang telah memberikan bantuan serta motivasi dalam penyelesaian penulisan Proposal Tugas Akhir ini

1. Kedua Orang Tua tercinta yang selalu memberikan dukungan, doa serta motivasi yang tak terhingga.
2. Bapak Prof. Dr. Ir. Erwin, M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. H. Sukemi. M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
4. Bapak Prof. Dr. Ir. Bambang Tutuko, M.T. selaku Dosen Pembimbing Akademik.
5. Bapak Ahmad Heryanto, S.Kom, M.T. selaku Dosen Pembimbing Tugas Akhir telah berkenan untuk meluangkan diri untuk membimbing, memberi saran serta motivasi yang terbaik untuk penulis bisa menyelesaikan Tugas Akhir ini.
6. Mbak Renny Virgasari admin Jurusan Sistem Komputer yang telah membantu mengurus berkas
7. Soniawati selaku rekan Tugas Akhir dan rekan segala bidang sekaligus teman terdekat yang banyak memberikan banyak bantuan kepada penulis.

8. Teman-teman Sistem Komputer Angkatan 2019.
9. Semua pihak yang telah membantu sebelum dan selama penulisan Proposal Tugas Akhir yang tidak dapat saya sebutkan satu persatu.

Dalam pembuatan dan penyusunan proposal Tugas Akhir ini penulis sadar bahwa proposal ini masih jauh dari sempurna, oleh karena itu penulis penulis sangat menerima kritik, saran, dan koreksi terhadap isi dari proposal ini yang bersifat membangun agar proposal ini dapat lebih baik lagi. Semoga dengan proposal ini akan menjadi tambahan ilmu pengetahuan dan pengembangan wawasan kita dan bermanfaat bagi semuanya.

Indralaya, Oktober 2023

Penulis

Cuh Meizi Sasfini
NIM. 09011381924120

ANALYSIS OF TIME SERIES DATA FOR FORECASTING CYBER ATTACK DATA ON HONEYPOTS USING THE SUPPORT VECTOR REGRESSION (SVR) METHOD

Cuh Meizi Sasfini (09011381924120)
Department of Computer Systems, Faculty of Computer Science,
Sriwijaya University
email: cuhmeizi685@gmail.com

ABSTRACT

Cyber Attack is a crime that attacks computer systems that can shut down or damage information technology services. Every act of attack will have an impact on gaining access to services, manipulating and various dangerous actions. There are various reasons why cyber attacks can occur, one of which is that there is still very little information about the predictability of cyber security. This study aims to determine and obtain the results of forecasting time series data and IP Address on honeypot using the Support Vector Regressio method and determine the Support Vector Regression (SVR) method that can produce the best forecasting in forecasting IP data and cyber attack time data on honeypot data. In this study using the Support Vector Regression (SVR) method with three kernels namely Linear, Polynomial, and Radial Basis Function (RBF). The kernel that gives the best results is based on the smallest MAE, RMSE, and MAPE values. The results of this study obtained, the assessment of the best time data forecasting results obtained using the RBF kernel function with cross validation which obtained the smallest error with MAE = 5.6904%, RMSE = 6.5858%, and MAPE = 4.7047% before data scaling, and with MAE = 0.8212%, RMSE = 0.9493%, and MAPE = 1.3199% after data scaling. While the IP data forecasting model obtained using the Polynomial kernel function MAPE = 5.2212% before data scaling and MAPE = 1.0% after data scaling.

Keywords: *Cyber Attack, Support Vector Regression, Kernel.*

ANALISIS DATA *TIME SERIES* UNTUK *FORECASTING* DATA *CYBER ATTACK* PADA HONEYPOT MENGGUNAKAN METODE *SUPPORT VECTOR REGRESSION* (SVR)

Cuh Meizi Sasfini(09011381924120)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
email: cuhmeizi685@gmail.com

ABSTRAK

Cyber Attack adalah suatu tindak kejahatan yang menyerang sistem komputer yang dapat mematikan atau merusak layanan teknologi informasi. Setiap tindakan serangan akan berdampak terhadap memperoleh akses layanan, memanipulasi dan berbagai tindakan yang berbahaya. Ada berbagai alasan masalah mengapa *cyber attack* itu bisa terjadi, salah satunya informasi mengenai prediktibilitas keamanan dunia maya masih sangat sedikit. Penelitian ini bertujuan untuk mengetahui dan mendapatkan hasil peramalan data *time series* dan *IP Address* pada honeypot menggunakan metode Support Vector Regressio serta mengetahui metode *Support Vector Regression* (SVR) yang dapat menghasilkan peramalan terbaik dalam melakukan peramalan data IP dan data waktu serangan siber pada data honeypot. Pada penelitian ini menggunakan metode *Support Vector Regression* (SVR) dengan tiga kernel yaitu *Linear, Polynomial, dan Radial Basis Function* (RBF). Kernel yang memberikan hasil terbaik berdasarkan nilai MAE, RMSE, dan MAPE terkecil. Hasil dari penelitian ini didapatkan, penilaian hasil peramalan data waktu terbaik diperoleh dengan menggunakan fungsi kernel RBF dengan *cross validasi* yang memperoleh error yang paling kecil dengan nilai MAE = 5.6904%, RMSE = 6.5858%, dan MAPE = 4.7047% sebelum penskalaan data, dan dengan nilai MAE = 0.8212%, RMSE = 0.9493%, dan MAPE = 1.3199% setelah penskalaan data. Sedangkan model peramalan data IP diperoleh dengan menggunakan fungsi kernel *Polynomial* MAPE = 5.2212% sebelum penskalaan data dan MAPE = 1.0% setelah penskalaan data.

Kata Kunci: Cyber Attack, Support Vector Regression, Kernel

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

BAB I. PENDAHULUAN

1.1 Latar Belakang

Cyber Attack adalah suatu tindak kejahatan yang menyerang sistem computer yang dapat mematikan atau merusak layanan teknologi informasi. Setiap tindakan serangan akan berdampak terhadap memperoleh akses layanan, memanipulasi dan berbagai tindakan yang berbahaya[1][2].

Ada banyak masalah keamanan yang ditimbulkan, seperti pembajakan jarak jauh, peniruan identitas, penolakan serangan layanan, tebakan kata sandi, dan man-in-the-middle[3]. Cyber attack ini dapat membahayakan keamanan jaringan-jaringan internet yang digunakan sehingga hal ini dapat membuat kerugian bagi suatu organisasi atau juga merugikan orang-orang, baik itu secara fisik, ekonomi, social, dan bahkan politik[4].

Efek dari cyber attack ini dapat mengganggu, menyangkal, dan bahkan melumpuhkan pengoperasian infrastruktur penting termasuk jaringan komunikasi, jaringan listrik, rumah sakit, serta sistem pertahan dan militer[4]. Oleh karena itu setiap pelanggaran fungsinya oleh cyber attack secara otomatis mempengaruhi keselamatan dunia maya[5]. Walaupun dengan berbagai cara yang sudah dilakukan untuk menanggulangi dan mengurangi serangan-serangan tersebut seperti DDoS, Brute Force, Malware, Social Engineering, Man in The Middle (MITM), dan Phishing. Namun masih ada yang belum tahu darimana dan bagaimana serangan-serangan tersebut datang[6].

Ada berbagai alasan masalah mengapa cyber attack itu bisa terjadi, salah satunya Informasi mengenai prediktibilitas keamanan dunia maya masih sangat sedikit, padahal prediksi tersebut dapat memberikan informasi yang cukup penting mengenai pertahanan jaringan dunia maya[5].

Beberapa upaya yang sudah dilakukan dari pemerintah, akademisi, dan industri untuk mengantisipasi hal ini, salah satunya dengan membuat sistem untuk meramalkan kapan cyber attacks tersebut datang[2]. Jika cyber attack diprediksi

dalam waktu yang wajar sebelum terjadi, tindakan defensive untuk mencegah efek destruksifnya dapat direncanakan[5]. Ada berbagai metode yang dapat digunakan dalam melakukan peramalan salah satunya yang paling umum digunakan ialah time series forecasting, dimana metode ini berfokus pada analisis data yang sekuensial terhadap waktu, lalu memprediksi data-data yang akan datang berdasarkan data sebelumnya, data time series ialah sekumpulan data yang didapatkan dari pengamatan suatu kejadian yang terjadi berdasarkan indeks waktu dengan selang waktu yang tetap[2][5].

Pada peneliti[4], melakukan forecasting pada data serangan siber menggunakan Model ARIMA dan Bayesian State Space Model. Hasil yang di dapat menggunakan metode ARIMA Model dapat memprediksi serangan per minggu lebih akurat dibanding dengan prediksi per-bulan, kedua menggunakan metode Bayesian State Space, sistem ini dapat memprediksi serangan pada Cyber Event satu minggu lebih cepat berdasarkan jumlah serangan Cyber dari minggu sebelumnya. Peneliti[7], metode DC-Algoritma yang diusulkan dapat memberikan tingkat akurasi forecasting yang lebih tinggi dari pada metode lain, dengan kompleksitas waktu yang relatif lebih rendah. Peneliti[8] Intrusion Detection Honeypot (IDH) deangan Social Leopard Algorithm (SoLA) hasil percobaan menegaskan bahwa IDH yang diusulkan secara signifikan meningkatkan waktu deteksi ransomware, kecepatan, dan akurasi dibandingkan dengan model deteksi ransomware canggih yang ada.

Pada penelitian[9], penggunaan metode SVR mampu mendeteksi hubungan linier dan nonlinear di dalam ruang fitur dengan algoritma pembelajaran yang mudah dan efisien. Implementasi menggunakan Netbeans 8.2 metode SVR memberikan hasil akurasi sebesar 94,654%. Penelitian[10], model regresi cukup sederhana dan mudah digunakan, Ini keuntungan paling signifikan dari pendekatan yang diusulkan. Memperoleh hasil akurasi sebesar 96,69% berhasil dicapai sesuai dengan metrik akurasi. Penelitian[11], Pendekatan yang diusulkan dievaluasi berdasarkan MAPE, MAE, MSE, R2, NMSE, waktu komputasi, dan metrik PRED. SVRT memberikan kinerja prediksi terbaik dibandingkan dengan metode GA dan BIC. Nilai error MAE yang dihasilkan oleh SVRT lebih kecil (hingga 0,064%) dibandingkan dengan metode GA dan BIC (hingga 0,44% dan 0,31%).

SVR menggunakan fungsi kernel untuk memetakan kumpulan sampel ke ruang fitur. SVR memiliki banyak keunggulan dalam menyelesaikan sampel kecil, pengenalan pola dimensi nonlinier dan tinggi, dan telah banyak diterapkan pada masalah praktis, termasuk prediksi kecepatan lalu lintas, prediksi konduktivitas, rediksi spasial kerentanan longsor, dan peramalan[6].

Konsep metode SVR didasarkan pada meminimalkan risiko kesalahan dengan memperkirakan fungsional dengan meminimalkan nilai kesalahan. Data yang digunakan adalah data numerik yang telah dinormalisasi.

Berdasarkan hasil dari penelitian terdahulu, maka pada penelitian ini, penulis akan mencoba melakukan pengolahan data time series dan juga data source IP yang terjadi di honeypot, forecasting diharapkan untuk dapat mengetahui secara akurat kapan dan apa serangan tersebut datang selanjutnya, dan juga evaluasi proses model dilakukan untuk mengetahui kinerja dari metode yang digunakan, beberapa cara evaluasi untuk mendapatkan validasi hasil yang dapat digunakan diantaranya adalah Mean Absolute Error (MAE), Root Mean Square Error (RMSE) dan Mean Absolute Percentage Error (MAPE). Oleh karena itu peneliti memilih untuk mengangkat judul "Analisis Data Time Series Untuk Forecasting Data Cyber Attack Pada Honeypot Menggunakan Metode *Support Vector Regression (SVR)*" yang diharapkan nantinya dapat memberikan solusi atau jawaban terhadap permasalahan yang diidentifikasi sebelumnya.

1.2 Perumusan Masalah

Perumusan masalah dalam tugas akhir ini yaitu:

1. Bagaimana mengetahui dan mendapatkan nilai perubahan data pada data time series dan IP Address di waktu yang akan datang pada data honeypot?
2. Bagaimana hasil evaluasi validasi peramalan dengan metode Support Vector Regression pada data time series dan IP Address?

1.3 Batasan Masalah

Batasan masalah dalam tugas akhir ini yaitu:

1. Metode yang digunakan untuk forecasting adalah Support Vector Regression.

2. Dataset yang digunakan Dataset-lab.informatika.umm.
3. Fitur yang digunakan pada dataset adalah timestamp dan source_ip

1.4 Tujuan

Tujuan dari penulisan tugas akhir ini yaitu:

1. Untuk mengetahui dan mendapatkan hasil peramalan data time series dan IP Address pada honeypot menggunakan metode Support Vector Regressio.
2. Untuk mengetahui metode Support Vector Regression yang dapat menghasilkan peramalan terbaik dalam melakukan peramalan data IP dan data waktu serangan siber pada data honeypot.

1.5 Manfaat

Manfaat dari penulisan tugas akhir ini yaitu:

1. Memberikan alternatif metode peramalan data time series dan data IP Address dengan menggunakan metode Support Vector Regression dalam berbagai bidang ilmu pengetahuan.
2. Menambah wawasan mengenai metode peramalan Support Vector Regression dengan tiga fungsi kernel (linear, polynomial, dan rbf) pada data time series di data honeypot.

1.6 Metode Penelitian

Pada tugas akhir ini menggunakan metodelogi sebagai berikut:

1. Metode Studi Pustaka dan Literatue

   Pada metode ini mencari dan mengumpulkan referensi yang berupa literatur yang terdapat pada jurnal, buku, dan internet sebanyak mungkin mengenai serangan siber, time series forecasting, data honeypot, dan support vector regression.
2. Metode Konsultasi

   Pada metode ini melakukan konsultasi kepada pihak-pihak yang memiliki pengetahuan serta wawasan yang baik dalam mengatasi permasalahan yang ditemui pada penulisan tugas akhir.
3. Metode Pembuatan Model

Pada metode ini membuat suatu perancangan pemodelan dengan menggunakan simulasi baik berupa software maupun hardware yang bisa digunakan dengan baik agar bisa memperlancar proses pembuatan model.

4. Metode Pengujian

   Pada metode ini dilakukan pengujian terhadap simulasi dan hasil yang dilihat dari pengujian dapat berupa seberapa efektif metode yang digunakan serta melihat apakah metode tersebut dapat menghasilkan akurasi yang baik atau tidak.

5. Metode Analisa, Kesimpulan dan Saran

   Pada metode ini hasil dari pengujian terhadap metode support vector regression dituangkan dalam analisa dari hasil penelitian yang dilakukan untuk memperoleh berbagai petunjuk yang dapat menghasilkan kesimpulan serta saran yang diharapkan dapat digunakan sebagai referensi untuk peneliti selanjutnya.

1.7 Sistematika Penulisan

Adapun sistematika penulisan dalam penelitian ini ialah:

BAB I PENDAHULUAN

Bab ini berisi latar belakang penelitian, rumusan masalah penelitian, batasan masalah penelitian, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi dasar teori yang menunjang penulisan mengenai peramalan serangan cyber yang dituangkan dalam penelitian terkait, ringkasan hasil kajian literatur, landasan teori dan dataset yang digunakan dalam penelitian ini

BAB III METODOLOGI PENELITIAN

Bab ini berisi kerangka kerja atau tahapan dan metode yang akan dilakukan dalam penelitian ini.

BAB IV HASIL DAN ANALISA

Bab ini berisi analisa dan pembahasan dari hasil penelitian yang dilakukan untuk memperoleh berbagai petunjuk yang dapat menghasilkan kesimpulan dari penelitian itu sendiri.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang didapat dari hasil penelitian, serta memberikan saran atau future work yang akan dilakukan terhadap penelitian yang dilakukan.

DAFTAR PUSTAKA

[1] C. Chen, K. Zhang, M. Ni, and Y. Wang, "Cyber-attack-tolerant Frequency Control of Power Systems," J. Mod. Power Syst. Clean Energy, vol. 9, pp. 307–315, March. 2021.

[2] A. Yeboah-ofori, S. Islam, S. I. N. W. E. E. Lee, Z. I. A. U. S. H. Shamszaman, S. Member, and K. Muhammad, "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security,"IEEE Access, vol. 9, pp. 94318-94337, July. 2021.

[3] Y. K. Saheed and M. O. Arowolo, "Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms," IEEE Access, vol. 9, pp. 161546–161554, December. 2021.

[4] J. Z. Bakdash et al., "Malware in the future? Forecasting of analyst detection of cyber events," J. Cybersecurity, vol. 4, no. 1, July. 2018.

[5] M. Buinevich and A. Vladyko, "Forecasting issues of wireless communication networks' cyber resilience for an intelligent transportation system: An overview of cyber attacks," Inf., vol. 10, no. 1, January. 2019.

[6] A. Okutan, S. J. Yang, and K. McConky, "Forecasting Cyber Attacks with Imbalanced Data Sets and Different Time Granularities," Researchgate, vol.1, March. 2018.

[7] P. Goyal et al., "Discovering Signals from Web Sources to Predict Cyber Attacks," IEEE System, vol. 1, no. 1, August, 2018.

[8] Y. Liu et al., "Cloudy with a chance of breach: Forecasting cyber security incidents," Proc. 24th USENIX Secur. Symp., vol. 3, pp. 1009–1024,August. 2015.

[9] E. M. Priliani, A. T. Putra, and M. A. Muslim, "Forecasting Inflation Rate Using Support Vector Regression (SVR) Based Weight Attribute Particle Swarm Optimization (WAPSO)," Sci. J. Informatics, vol. 5, no. 2, pp. 118–127, Nov. 2018.

[10] D. O. Sahin, S. Akleylek, and E. Kilic, "LinRegDroid: Detection of Android Malware Using Multiple Linear Regression Models-Based Classifiers," IEEE Access, vol. 10, pp. 14246–14259, February. 2022.

[11] A. Al-badwi and C. Ruan, "Predicting Multi-Attribute Host Resource Utilization Using Support Vector Regression Technique," IEEE Access, vol. 8, pp. 66048–66067, April. 2020.

[12] E. Nunes et al., “Darknet and deepnet mining for proactive cybersecurity threat intelligence,” IEEE Int. Conf. Intell. Secur. Informatics Cybersecurity Big Data, ISI 2016, vol.1, pp. 7–12, July. 2016.

[13] R. Harang and A. Kott, “Burstiness of Intrusion Detection Process: Empirical Evidence and a Modeling Approach,” IEEE Trans. Inf. Forensics Secur., vol. 12, no. 10, pp. 2348–2359, Nov. 2017.

[14] N. R. Sabar, X. Yi, and A. Song, “A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security,” IEEE Access, vol. 6, pp. 10421–10431, March. 2018.

[15] M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, “Survey of attack projection, prediction, and forecasting in cyber security,” IEEE Commun. Surv. Tutorials, vol. 21, no. 1, pp. 640–660, 2019.

[16] Z. Wu, S. Pan, G. Long, J. Jiang, X. Chang, and C. Zhang, “Connecting the Dots: Multivariate Time Series Forecasting with Graph Neural Networks,” Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., pp. 753–763, May. 2020.

[17] J. Zhao, H. Mo, and Y. Deng, “An Efficient Network Method for Time Series Forecasting Based on the DC Algorithm and Visibility Relation,” IEEE Access, vol. 8, pp. 7598–7608,January. 2020.

[18] C. Meng, X. S. Jiang, X. M. Wei, and T. Wei, “A Time Convolutional Network Based Outlier Detection for Multidimensional Time Series in Cyber-Physical-Social Systems,” IEEE Access, vol. 8, pp. 74933–74942, May. 2020.

[19] S. Sibi Chakkaravarthy, D. Sangeetha, M. V. Cruz, V. Vaidehi, and B. Raman, “Design of intrusion detection honeypot using social leopard algorithm to detect IoT ransomware attacks,” IEEE Access, vol. 8, pp. 169944–169956, September. 2020.

[20] S. Lu and S. Huang, “Segmentation of Multivariate Industrial Time Series Data Based on Dynamic Latent Variable Predictability,” IEEE Access, vol. 8, pp. 112092–112103, June. 2020.

[21] F. Liu, Y. Lu, and M. Cai, “A hybrid method with adaptive sub-series clustering and attention-based stacked residual LSTMs for multivariate time series forecasting,” IEEE Access, vol. 8, pp. 62423–62438, April. 2020.

[22] C. Li, X. Wang, Z. Cheng, and Y. Bai, “Forecasting bus passenger flows by using a clustering-based support vector regression approach,” IEEE Access, vol. 8, pp. 19717–19725, January. 2020.

[23] H. Hou et al., “Hierarchical Long Short-Term Memory Network for Cyberattack Detection,” IEEE Access, vol. 8, pp. 90907–90913, May. 2020.

[24] B. Cai, G. Huang, N. Samadiani, G. Li, and C. H. Chi, “Efficient Time Series Clustering by Minimizing Dynamic Time Warping Utilization,” IEEE Access, vol. 9, pp. 46589–46599, March. 2021.

[25] N. Bhusal, M. Gautam, and M. Benidris, “Detection of Cyber Attacks on Voltage Regulation in Distribution Systems Using Machine Learning,” IEEE Access, vol. 9, pp. 40402–40416, March. 2021.

[26] J. Duan and H. Kashima, “Learning to rank for multi-step ahead time-series forecasting,” IEEE Access, vol. 9, pp. 49372–49386, April. 2021.

[27] T. Chadza, “Learning to Learn Sequential Network Attacks Using Hidden Markov Models,” vol. 8, July. IEEE Access, vol. 8, pp. 134480-134497, July. 2020.

[28] F. Martinez, M. P. Frias, M. D. Perez-Godoy, and A. J. Rivera, “Time Series Forecasting by Generalized Regression Neural Networks Trained With Multiple Series,” IEEE Access, vol. 10, pp. 3275–3283, January. 2022.

[29] F. Kayim and A. Yilmaz, “Time Series Forecasting With Volatility Activation Function,” IEEE Access, vol. 10, no. September, pp. 104000–104010, October. 2022.

[30] C. Puri, G. Kooijman, B. Vanrumste, S. Member, and S. Luca, “Forecasting Time Series in Healthcare With Gaussian Processes and Dynamic Time Warping Based Subset Selection,” IEEE J. Biomed. Heal. Informatics, vol. 26, no. 12, pp. 6126–6137, December. 2022.

[31] “Smart Mode: DDoS Attack Detection using Machine Learning,” ResearchGate, vol. 7, pp. 185-188, June. 2020.

[32] H. Beitollahi, “Application Layer DDoS Attack Detection Using Cuckoo Search Algorithm-Trained Radial Basis Function,” IEEE Access, 63844-63854, vol. 10, pp. June. 2022.

[33] Ö. Aslan, “A New Malware Classification Framework Based on Deep Learning Algorithms,” IEEE Access, vol. 9, pp. 87936–87951, June. 2021.

[34] M. Nadeem, A. L. I. Arshad, S. Riaz, S. S. Band, S. Member, and A. Mosavi, “Intercept the Cloud Network From Brute Force and DDoS Attacks via Intrusion Detection and Prevention System,” IEEE Access, vol. 9, pp. 152300–152309, November. 2021.

[35] F. Abri, “Markov Decision Process for Modeling Social Engineering Attacks and Finding Optimal Attack Strategies,” IEEE Access, vol. 10, pp. 109949–109968, October. 2022.

[36] Y. Yang, S. Member, X. Wei, and R. Xu, “Man-in-the-Middle Attack Detection and Localization Based on Cross-Layer Location Consistency,” IEEE Access, vol. 8, pp. 103860-103874, June. 2020.

[37] J. Lee, Y. Lee, D. Lee, H. Kwon, and D. Shin, “Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups,” IEEE Access, vol. 9, pp. 80866-80872, June. 2021.

[38] N. Eliot, D. Kendall, and M. Brockway, “A Flexible Laboratory Environment Supporting Honeypot Deployment for Teaching Real-World Cybersecurity Skills,” IEEE Access, vol. 6, pp. 34884–34895, July. 2018.

[39] L. Shi, Y. Li, T. Liu, J. I. A. Liu, B. Shan, and H. Chen, “Dynamic Distributed Honeypot Based on Blockchain,” IEEE Access, vol. 7, pp. 72234–72246, June. 2019.

[40] B. Li, Y. Xiao, Y. Shi, Q. Kong, Y. Wu, and H. Bao, “Anti-Honeypot Enabled Optimal Attack Strategy for Industrial Cyber-Physical Systems,” IEEE Open J. Comput. Soc., vol. 1, pp. 250–261, November. 2020.

[41] T. Huamin, D. Qiuqun, and X. Shanzhu, “Reconstruction of time series with missing value using 2D representation-based denoising autoencoder,” J. Syst. Eng. Electron., vol. 31, pp. 1087–1096, December. 2020.

[42] D. I. Purnama and S. Setianingsih, “Support vector regression (SVR) model for forecasting number of passengers on domestic flights at Sultan Hasanudin airport Makassar,” J. Mat. Stat. dan Komputasi, vol. 16, pp. 391-403, May. 2020.

[43] K. Ghanem, F. J. Aparicio-Navarro, K. G. Kyriakopoulos, S. Lambotharan, and J. A. Chambers, “Support Vector Machine for Network Intrusion and Cyber-Attack Detection,” Sens. Signal Process. Def. Conf. SSPD 2017, vol. 1, pp. 1–5, January. 2017.

[44] D. Lei, H. Zhang, H. Liu, Z. Li, and Y. Wu, “Maximal Uncorrelated Multinomial Logistic Regression,” IEEE Access, vol. 7, pp. 89924–89935, July. 2019.

[45] X. Xie, K. Luo, and G. Wang, “A NewL Multi-Kernel Learning Support Vector Regression Ensemble Algorithm With AdaBoost,” IEEE Access, vol. 10, pp. 20375–20384, February. 2022.

[46] P. Schneider and F. Xhafa, “Anomaly detection,” Anom. Detect. Complex Event Process. over IoT Data Streams, vol. 3, pp. 49–66, January. 2022.

[47] M. Singh, R. K. Dubey, and S. Kumar, “Vehicle telematics: An Internet of Things and Big Data approach,” Artif. Intell. Mach. Learn. EDGE Comput., vol. 15, pp. 235–254, April. 2022.

[48] P. Aji, K. Wakamori, and H. Mineno, “Short-term solar power forecasting using svr on hybrid pv power plant in indonesia,” *Adv. Intell. Syst. Comput.*, vol. 10 , pp. 235–246, October. 2020.

[49] Saif, Syaifuddin (2020), “Honeypot Data”, *Mendeley Data*, V1, doi: 10.17632/6fc7my86t4.1.

[50] Izhari. Fahmi, “Analisis Algoritma Dbscan Dalam Menentukan Parameter Epsilon Pada Clustering Data Numerik,” *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)*, vol. 1, pp. 156-158, February. 2020.