Jurnal Pengabdian pada Masyarakat

literasi

e-ISSN 2775-3301

Diseminasi Teknik Klasifikasi *Naïve Bayes* pada *Instrusion Detection System* di Perusahaan Artajasa

Muhammad Kamil Suryadewiansyah[1], Dolly Virgian Shaka Yudha Sakti[2], Teja Endra Eng Tju[3,*]
[1,2,3]Universitas Budi Luhur, Fakultas Teknologi Informasi;
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260, DKI Jakarta, Indonesia
[*]Email: teja.endraengtju@budiluhur.ac.id

Kilas Artikel

Volume 2 Nomor 2
Agustus 2022
DOI:xxx/ejpm.v%i%.xxxx

Article History
Submission: 09-07-2022
Revised: 09-07-2022
Accepted: 13-07-2022
Published: 01-08-2022

Kata Kunci:
ATM, Confusion Matrix, False Negative, False Positive, IDS.

Keywords:
ATM, Confusion Matrix, False Negative, False Positive, IDS.

Korespondensi:
Teja Endra Eng Tju
teja.endraengtju@budiluhur.ac.id

Abstrak

Artajasa sebagai penyedia layanan transaksi *online real time* menghadapi tantangan untuk memantau lalu-lintas transaksi dan melakukan identifikasi transaksi yang diperbolehkan ataupun tidak. Kegiatan pengabdian masyarakat ini bertujuan membuat aplikasi berbasis *web* untuk membantu menganalisa *alert* dari sistem deteksi yang sebelumnya dilakukan secara manual. Pelaksanaan kegiatan terdiri dari wawancara dan observasi, pengumpulan dan pengolahan data, analisa dan perancangan aplikasi, pengujian dan implementasi aplikasi. Dengan algoritma *Naïve Bayes*, hasil prediksi dari data histori diperoleh akurasi 0,88 dan hasil *User Acceptance Test* menunjukkan bahwa semua fungsi telah dicoba dan berjalan dengan baik. Dengan adanya aplikasi yang dibuat maka pekerjaan tim keamanan Artajasa menjadi efektif dan efisian karena tidak perlu lagi memeriksa setiap data *alert*, namun cukup fokus pada hasil perbedaan antara hasil prediksi dan *alert*.

Abstract

Artajasa as a real-time online transaction service provider faces the challenge of monitoring transaction traffic and identifying transactions that are allowed or not. This community service activity aims to create a web-based application to help analyze alerts from the detection system that was previously carried out manually. The implementation of activities consists of interviews and observations, data collection and processing, application analysis and design, application testing and implementation. With the Naïve Bayes algorithm, the prediction results from the historical data obtained an accuracy of 0.88 and the results of the User Acceptance Test showed that all functions had been tried and worked well. With the application made, the work of artajasa's security team becomes effective and efficient because there is no need to check every alert data anymore, but simply focus on the results of the difference between the results of predictions and alerts.

1. PENDAHULUAN

Artajasa (PT. Artajasa Pembayaran Elektronis) adalah perusahaan perintis transaksi elektonik di Indonesia sebagai penyedia jaringan infrastruktur untuk perbankan (Artini, Wati, and Afrizal 2020). Saat ini Artajasa memberikan layanan transfer dana antar bank secara *online real time* melalui mesin ATM (Anjungan Tunai Mandiri/Automatic Teller Machine (Indrayani et al. 2019)) dan menjamin keamanan, integritas, dan pemantauan yang tinggi untuk semua level dan jenis transaksi. Dalam pemantauan transaksi, Artajasa telah menggunakan IDS (*Intrusion Detection System* (Khraisat et al. 2019)) yang disediakan oleh vendor. Namun demikian

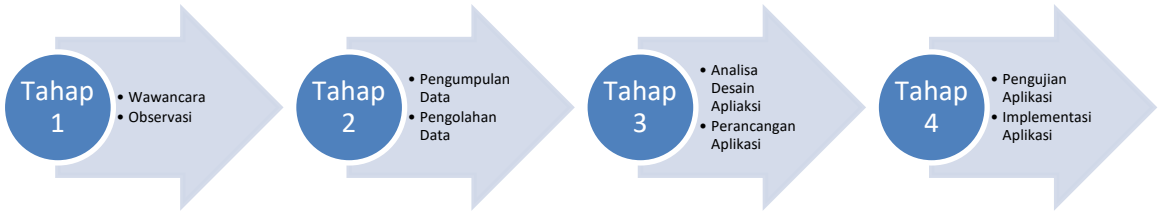
log (catatan transaksi) dari IDS perlu dianalisa yang saat ini dilakukan secara manual oleh tim keamanan Artajasa sehingga cukup menguras sumber daya. Analisa tersebut sangat diperlukan untuk meningkatkan akurasi IDS agar lebih efektif.

Berdasarkan paparan di atas, Artajasa dipilih sebagai mitra dalam kegiatan pengabdian kepada masyarakat yang bertujuan membuat aplikasi untuk menganalisa *log* dari IDS dengan teknik klasifikasi menggunakan algoritma Naïve Bayes (Webb 2016) sebagai diseminasi hasil penilitian. Dari hasil implementasi tersebut diharapkan meningkatkan efisiensi sumber daya tim keamanan Artajasa dalam upayanya untuk meningkatkan efektifitas IDS yang digunakan.

2. METODE

Kegiatan pengabdian kepada masyarakat ini terdiri dari empat tahap, seperti ditunjukkan pada Gambar 1. Pada tahap pertama dilaksanakan wawancara dengan bahasa Indonesia kepada tim keamanan jaringan Artajasa untuk mengetahui cara kerja saat ini dalam hal pengolahan data dari IDS, selanjutnya dilakukan observasi langsung dengan melihat dan mempelajari jaringan, interkoneksi, dan perangkat yang digunakan. Tahap kedua adalah pengumpulan data dalam media penyimpanan berbentuk *log file* kemudian data diolah ke dalam bentuk *spreedsheet* sehingga mudah dipelajari, dipilih, dan dipilah sesuai kebutuhan. Tahap ketiga, setelah dilakukan penelitian pada *dataset* dan pengukuran hasil prediksi pada data uji (*substantive test* (Bailey and Jensen 1977)), kemudian dibuat analisa desain sesuai kebutuhan pengguna dan perancangan aplikasi berbasis *web*. Tahap terakhir, pengujian aplikasi dengan UAT (*User Acceptance Test* (Priyatna et al. 2020)) *checklist* serta dilanjutkan implementasi setelah hasilnya sudah memenuhi tujuan.

Dalam setiap tahapan di atas pelaksanaan kegiatan dilengkapi seperangkat komputer dengan *hardware* (Processor Intel Core i7-7700HQ, Memory 8 GB DDR4-2400 RAM, SSD 128 GB NVME M.2 + HDD 1 TB 5,400RPM) dan *software* (OS Windows 10 Home, XAMPP Contol Panel V3.3.0, PHP 7.4.28, Sublime Text 3, PHPmyAdmin) yang memadai. Sedangkan komputer untuk implementasi disediakan oleh pihak Artajasa berupa *server* dengan spesifikasi yang lebih baik.



Gambar 1. Tahapan Kegiatan Pengabdian kepada Masyarakat.

3. HASIL & PEMBAHASAN

Berdasarkan hasil wawancara dan observasi, dilakukan pengumpulan data yang sesuai dengan kebutuhan untuk dilakukan penelitian dengan algoritma *Naïve Bayes* (Webb 2016). Dari hasil pengolahan awal (*data preprocessing* (Bhaya 2017)) data diperoleh dataset dengan 575 data yang secara acak dibagi menjadi data latih sebanyak 515 dan dan uji sebanyak 60. Fitur-fitur yang terdapat pada dataset sekaligus probabilitas dari setiap variabel sebagai bagian dari penerapan algoritma *naïve bayes* disajikan pada Tabel 1.

e-ISSN 2775-3301
DOI: xxxxx/ejpm.vxix.xxxx

Tabel 1. Fitur-fitur dan Hasil Perhitungan Probabilitas setiap Variabel pada Data Latih.

Fitur	Variabel	Jumlah Kejadian		Probabilitas	
		Yes	***No***	***Yes***	***No***
Alert (A) (sebagai Kelas/*Prior*)	*Yes* (Y)	264	-	P(Y)=0,512621	-
	No (N)	-	251	-	P(N)=0,487379
Level Asset (L)	Critical (LC)	147	118	P(LC|Y)=0,556818	P(LC|N)=0,470120
	Medium (LM)	117	133	P(LM|Y)=0,443182	P(LM|N)=0,529880
IP *Destination* (D)	x.y.2.250 (D1)	65	55	P(D1|Y)=0,246212	P(D1|N)=0,219124
	x.y.2.253 (D2)	82	63	P(D2|Y)=0,310606	P(D2|N)=0,250996
	x.z.46.130 (D3)	58	60	P(D3|Y)=0,219697	P(D3|N)=0,239044
	x.z.57.65 (D4)	59	73	P(D4|Y)=0,223485	P(D4|N)=0,290837
IP *Category* (C)	Internal (CI)	57	208	P(CI|Y)=0,215909	P(CI|N)=0,828685
	Eksternal (CE)	89	25	P(CE|Y)=0,337121	P(CE|N)=0,099602
	Others (CO)	118	18	P(CO|Y)=0,446970	P(CO|N)=0,071713
Event (E)	4624 (E1)	30	49	P(E1|Y)=0,113636	P(E1|N)=0,195219
	4625 (E2)	33	15	P(E2|Y)=0,125000	P(E2|N)=0,059761
	4634 (E3)	12	42	P(E3|Y)=0,045455	P(E3|N)=0,167331
	4662 (E4)	50	115	P(E4|Y)=0,189394	P(E4|N)=0,458167
	4782 (E5)	17	11	P(E5|Y)=0,064394	P(E5|N)=0,043825
	XSS (E6)	122	19	P(E6|Y)=0,462121	P(E6|N)=0,075697

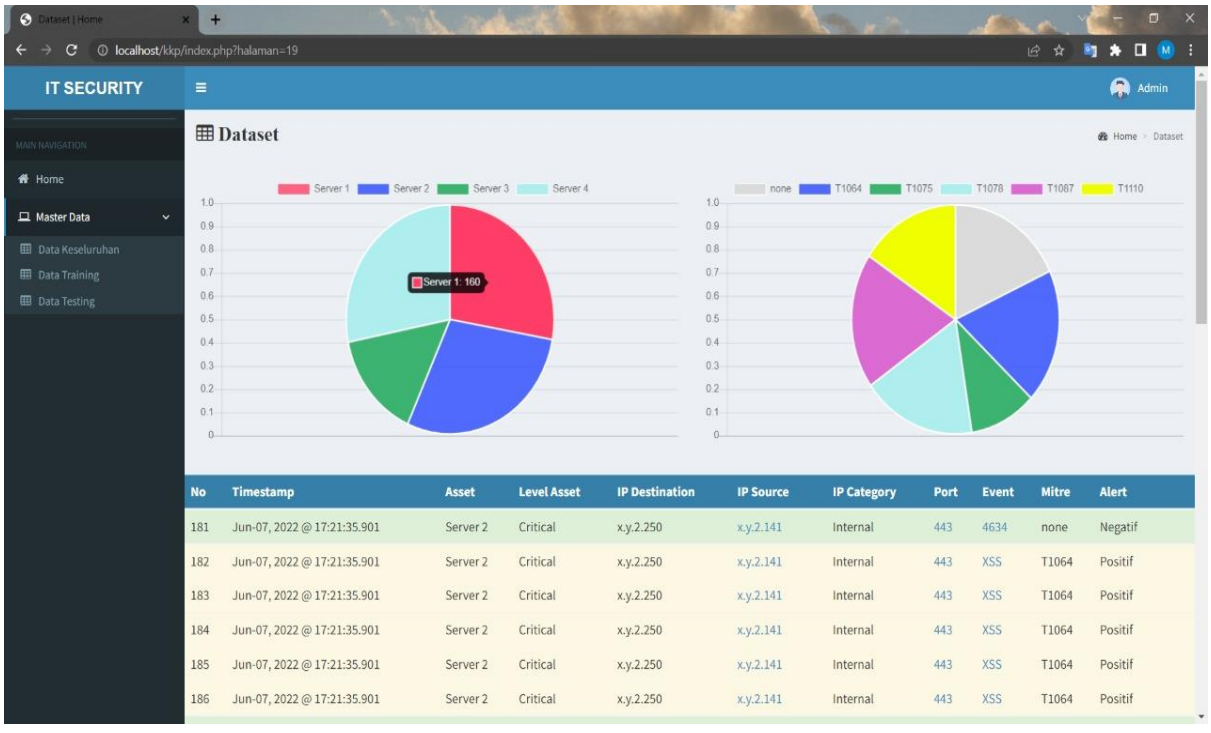
Hasil perhitungan probabilitas di Tabel 1 digunakan sebagai acuan untuk perhitungan *Naïve Bayes Classification* (Zhang 2016) pada setiap data uji sehingga untuk setiap variabel yang ada dihitung dengan nilai probabilitas *Yes* dan *No*. Perbandingan hasil perhitungan nilai *Yes* dan *No* diambil yang lebih besar sebagai hasil prediksi. Selanjutnya hasil prediksi dibandingan dengan kelas atau prior yaitu variabel *Alert* (A) dari IDS. Jika hasil prediksi dan *alert* sama-sama *Yes* maka disebut *True Positive* (TP). Jika hasil prediksi dan *alert* sama-sama *No* maka disebut *True Negative* (TN). Jika hasil prediksi *Yes* dan *alert No* maka disebut *False Positive* (FP). Jika hasil prediksi *No* dan *alert Yes* maka disebut *False Negative* (FN). Secara komprehensif hasil pengukuran pada data uji disajikan dalam bentuk *Confusion Matrix* (Caelen 2017) yang disajikan pada Tabel 2.

Tabel 2. *Confusion Matrix* dari Data Uji.

		Prediksi		
		***Yes* (Positif)**	***No* (Negatif)**	
Alert	***Yes* (Positif)**	TP = 25	FN = 3	$Recall = \frac{TP}{(TP+FN)} = 0{,}89$
	***No* (Negatif)**	FP = 5	TN = 27	
		$Presisi = \frac{TP}{(TP+FP)} = 0{,}83$		$Akurasi = \frac{(TP+TN)}{(TP+TN+FP+FN)} = 0{,}88$

Kelas bernilai *Yes* berarti *alert* dari IDS yang menunjukkan bahwa transaksi tersebut tidak diijinkan dan diblokir, sebaliknya bernilai *No* berarti transaksi normal dan diijinkan oleh Artajasa. Dalam hal hasil prediksi yang berbeda yaitu FP dan FN merupakan hasil yang harus diminimalkan karena keduanya kritikal bagi Artajasa. Jika faktualnya transaksi tersebut *Yes* maka jangan sampai diijinkan terjadi, dan jika faktualnya transaksi tersebut *No* maka jangan sampai diblokir sehingga nasabah bank tidak bisa bertransaki. Untuk memastikan fakta yang tepat maka dilakukan analisa lebih dalam pada data *alert* tersebut dan hasil kesimpulannya dipakai untuk menyesuaikan konfigurasi IDS.

Untuk membantu mendeteki FP dan FN dengan lebih efisien maka dibuatlah aplikasi berbasis *web* sebagai alat bantu kerja untuk tim keamanan Artajasa dengan *user interface* ditunjukkan pada Gambar 2. Sebelum implementasi, aplikasi tersebut telah diuji dengan UAT yang hasilnya ditunjukkan pada Tabel 2, tampak bahwa semua fungsi yang diuji di dalam *checklist* telah berjalan dengan baik dan memenuhi kriteria harapan dari pengguna (tim keamanan Artajasa).



Gambar 2. *User Interface* Aplikasi IDS *Analysis*.

e-ISSN 2775-3301
DOI: xxxxx/ejpm.vxix.xxxx

Tabel 3. Hasil Pengujian Aplikasi dengan UAT.

No.	Fungsi	Pengujian	Harapan	Hasil
1.	*Login*	Melakukan proses *login* dengan *user* yang sudah terdaftar	Sistem dapat diakses jika *user* berhasil melakukan proses *login*	Sesuai
		Melakukan proses *login* dengan melakukan *input username* dan *password* yang salah	Sistem dapat menampilkan *alert* '*username* dan *password* salah' dan kembali ke halaman *login*	Sesuai
2.	*Import Data Training*	Melakukan proses *input* data training.xlsx ke dalam *database* melalui aplikasi	Sistem dapat melakukan *input* data *training* ke dalam *database*	Sesuai
3.	*Training Data*	Melakukan proses *training data* dengan program pada aplikasi	Sistem dapat memproses data *training*	Sesuai
4.	*Import Data Testing*	Melakukan proses input data testing.xlsx ke dalam database melalui aplikasi	Sistem dapat melakukan input data training ke dalam database	Sesuai
5.	*Testing Data*	Melakukan proses *testing data* berdasarkan hasil *training* dengan program aplikasi	Sistem dapat melakukan *testing data* dan rekomendasi baru	Sesuai
6.	*Update*	Melakukan proses *update* data hasil *testing*	Sistem dapat melakukan *update data* hasil *testing*	Sesuai
7.	*Export*	Melakukan proses *export* hasil data *testing* maupun hasil data *testing* yang sudah di *update*	Sistem dapat melakukan *export* hasil data *testing* maupun hasil data *testing* yang sudah di *update*	Sesuai

4. KESIMPULAN

Dengan teknik klasifikasi *Naïve Bayes*, pekerjaan tim keamanan Artajasa dalam hal menganalisa data *alert* dari IDS menjadi lebih efektif dan efisien. Lebih efektif karena yang sebelumnya harus memeriksa setiap data *alert* satu persatu menjadi sangat berkurang dengan cukup memeriksa hasil klasifikasi yang menghasilnya FP dan FN. Dengan demikian akan menjadi efisen karena bisa menghemat banyak waktu dan tenaga.

Untuk penggunaan aplikasi yang sudah dibuat, sebaiknya tim keamanan Artajasa senantiasa melakukan pemutakhiran data histori agar meningkatkan hasi akurasi dan mengurangi hasil FP dan FN.

DAFTAR PUSTAKA

Artini, Deden, Theresia Wati, and Sarika Afrizal. 2020. "Analysis of Knowledge Management Readiness in PT Artajasa Pembayaran Elektronis." Pp. 226–30 in *2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*. IEEE.

Bailey, Andrew D., and Daniel L. Jensen. 1977. "A Note on the Interface between Compliance and Substantive Tests." *Journal of Accounting Research* 15(2):293. doi: 10.2307/2490354.

Bhaya, Wesam S. 2017. "Review of Data Preprocessing Techniques in Data Mining." *Journal of Engineering and Applied Sciences* 12(16):4102–7.

Caelen, Olivier. 2017. "A Bayesian Interpretation of the Confusion Matrix." *Annals of Mathematics and Artificial Intelligence* 81(3–4):429–50. doi: 10.1007/s10472-017-9564-8.

Indrayani, Chablullah Wibisono, Sanni Aritra, and Iskandar Muda. 2019. "Customer Satisfaction as Intervening Between Use Automatic Teller Machine (ATM), Internet Banking and Quality of Loyalty (Case in Indonesia)." *International Journal of Financial Research* 10(6):54. doi: 10.5430/ijfr.v10n6p54.

Khraisat, Ansam, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. 2019. "Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges." *Cybersecurity* 2(1):20. doi: 10.1186/s42400-019-0038-7.

Priyatna, Bayu, April Lia Hananto, Muhammad Nova, Program Studi Sistem Informasi, and Universitas Buana Perjuangan Karawang. 2020. "Application of UAT (User Acceptance Test) Evaluation Model in Minggon E-Meeting Software Development." *SYSTEMATICS* 2(3):110–17.

Webb, Geoffrey I. 2016. "Naïve Bayes." Pp. 1–2 in *Encyclopedia of Machine Learning and Data Mining*. Boston, MA: Springer US.

Zhang, Zhongheng. 2016. "Naïve Bayes Classification in R." *Annals of Translational Medicine* 4(12):241–241. doi: 10.21037/atm.2016.03.38.