Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.2023107123
Vol. 10, No. 6, Desember 2023, hlm. 1223-1232 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

ANALISIS PERILAKU ENTITAS UNTUK PENDETEKSIAN SERANGAN INTERNAL MENGGUNAKAN KOMBINASI MODEL PREDIKSI MEMORI DAN METODE PCA

Rahmat Budiarto[1], Yanif Dwi Kuntjoro[*2]

[1]Albaha University, Saudi Arabia, [2]Universitas Pertahanan, Citeureup
Email: [1]rahmat@bu.edu.sa, [2]yanif.kuntjoro@idu.ac.id
[*]Penulis Korespondensi

(Naskah masuk: 07 Maret 2023, diterima untuk diterbitkan: 27 November 2023)

Abstrak

Tingkat ketahanan siber di Indonesia terhitung rendah dibanding dengan negara lain di dunia, terbukti dengan masih banyaknya kejahatan siber yang terjadi, seperti pencurian data dan identitas, penipuan dan peretasan situs-situs institusi pemerintah maupun swasta yang melibatkan peran internal secara penuh maupun sebagian. Menangkis serangan dari luar jaringan institusi/organisasi relatif lebih mudah dilakukan dibandingkan dengan menangkis serangan kejahatan siber dari dalam jaringan. Serangan dari luar dapat dicegah menggunakan firewall, anti virus dan perangkat lunak khusus untuk pendeteksi penyusupan/malware. Penelitian ini bertujuan untuk membangun suatu model analisis perilaku entitas berazaskan Model Prediksi Memori (MPM) yang dikombinasikan dengan metode seleksi fitur *principal component analysis* (PCA) yang diimplementasikan untuk mendeteksi serangan/anomali siber yang melibatkan internal. Model prediksi memori yang terdiri dari 6 lapisan hirarki, mengenali masukan dari lapisan hirarki rendah ke lapisan hirarki tinggi kemudian dilakukan proses pencocokan dan menciptakan serangkaian ekspektasi dari lapisan hirarki tinggi ke rendah.. Setiap tingkat hierarki mengingat urutan pola masukan temporal yang sering diamati dan menghasilkan label atau 'nama' untuk urutan ini. Algoritma PCA diterapkan untuk mengurangi jumlah fitur trafik sehingga mempercepat proses deteksi, Data untuk percobaan diambil dari jaringan nyata dengan 150 pengguna dan data serangan flooding dari dataset MACCDC. Hasil eksperimen dalam suatu jaringan testbed menunjukkan hasil akurasi pendeteksian mencapai 94.01%, presisi 95.64%, Sensitivitas 99.28% dan F1-Score 96.08%. Model yang diusulkan (PCA-MPM) menunjukkan kemampuan menjalankan pembelajaran secara *on-the-fly* yang sangat diperlukan untuk mengenali perubahan fitur pada pola serangan yang sifatnya berevolusi dari waktu ke waktu. Pada gilirannya model ini dapat mendukung sistem pertahanan siber holistik yang sedang dikembangkan. Sistem yang sedang dikembangkan diharapkan dapat memenuhi kebutuhan dalam negeri akan teknologi siber untuk mengurangi ketergantungan dari negara lain karena dikembangkan secara lokal.

Kata kunci: *ketahanan siber, serangan internal, analisis perilaku entitas, pemilihan fitur, PCA, model memori*

ENTITY BEHAVIOR ANALYSIS FOR DETECTION OF INSIDER ATTACKS USING A COMBINATION OF MEMORY PREDICTION MODEL AND PCA METHOD

Abstract

Compared to other countries in the world, the level of cyber resilience in Indonesia is low as evidenced by the number of cybercrimes that occur, such as data and identity theft, fraud, and hacking of websites of government and private institutions that involve full or partial insider roles. Fending off attacks from outside the institutional or organizational network is relatively easier than fending off cybercrime attacks from within the network. External attacks can be prevented using firewalls, anti-virus software, and special software for intruder and malware detection. This study intention is to build a model for analyzing entity behavior using a memory prediction model and uses the principal component analysis (PCA) as a feature selection method and implement it to detect cyber-attacks and anomalies involving insiders. The memory-prediction model recognizes bottom-up inputs that matched in hierarchy and evokes a series of top-down expectations. Each hierarchy level remembers frequently observed temporal sequences of input patterns and generates labels or 'names' for these sequences. To accelerate the detection process, the PCA algorithm is deployed to reduce the number of significant features of the traffic. Data for the experiment was taken from a real network with 150 users accessing the network. The experimental results in a testbed network show that the detection accuracy reaches 94.01%, the precision is 95.64%, the sensitivity is 99.28%, and the F1-score is 96.08%. The proposed model (PCA-MPM) is also capable of performing on-the-fly learning where this capability is needed to recognize feature changes in attacks that

evolve over time. In turn, this model can support a holistic cyber defense system that is being developed. The system being developed is expected to meet the domestic need for cyber technology and reduce dependence on other countries as it is developed locally.

Keywords: *cyber resilience, insider attack, entity behavior analysis, feature selection, PCA, memory model*

1. PENDAHULUAN

Sebagai salah satu isu strategis ketahanan nasional Indonesia, keamanan dan ketahanan siber perlu mendapatkan perhatian serius dari pemerintah. Langkah strategis perlu diambil untuk meningkatkan kualitas keamanan dan ketahanan siber Indonesia, diantaranya meningkatkan kemandirian teknologi siber nasional. Tingkat ketahanan siber di Indonesia terhitung rendah dibanding dengan negara lain di dunia, terbukti dengan masih banyaknya kejahatan siber yang terjadi, seperti pencurian data dan identitas, penipuan dan peretasan situs-situs institusi pemerintah maupun swasta yang melibatkan peran internal secara penuh maupun sebagian. Menangkis serangan dari luar jaringan institusi/organisasi relatif lebih mudah dilakukan dibandingkan dengan menangkis serangan kejahatan siber dari dalam jaringan. Serangan dari luar dapat dicegah menggunakan *firewall*, anti-virus dan perangkat lunak khusus untuk pendeteksi penyusup/malware.

Mendeteksi suatu serangan yang melibatkan orang dalam (*insider*) lebih sukar karena sistem pertahanan yang digunakan mungkin mengira serangan tersebut adalah kegiatan normal dari satu entitas di dalam sistem/jaringan. Oleh karena itu, diperkenalkan metode analisiS perilaku pengguna (*User Behavior Analysis*--UBA). Definisi UBA berasal dari pelacakan, pengumpulan, dan kemudian menilai data pengguna dan tindakan mereka di dalam *platform* menggunakan sistem pemantauan. Alih-alih menebak, UBA membantu menemukan akar penyebab perubahan perilaku umum seperti keterlibatan pengguna, tingkat konversi, dan retensi. Ini juga dapat membantu menjawab pertanyaan tentang apa yang ingin dicapai pengguna saat menggunakan aplikasi. UBA banyak digunakan dalam industri keamanan siber, di mana UBA dapat mendeteksi ancaman atau upaya peretasan. Salah satu fungsi utama UBA adalah penentuan garis dasar aktivitas normal yang spesifik bagi penggunanya. Melalui teknologi big data dan algoritma pembelajaran mesin, perilaku pengguna dapat diidentifikasi dan dinilai hampir secara *real-time*.

Sistem pencegah/pendeteksi serangan sudah banyak tersedia di pasar, selain mahal, sistem tersebut masih mempunyai beberapa kelemahan, seperti: tingkat akurasi pendeteksian yang rendah, terlalu banyak menghasilkan *false alarm*, dan ketidak mampuan melaksanakan pembelajaran secara real-time untuk varian baru serangan. Kemampuan sistem untuk melaksanakan pembelajaran secara real-time diperlukan untuk mengatasi serangan/virus/malware yang berevolusi dengan cepat. Cara tradisional untuk mendeteksi serangan/anomali dalam satu jaringan *enterprise* yang menggunakan rule-based/knowledge-based, sudah tidak lagi mencukupi untuk memberi tingkat akurasi yang memadai, karena jenis serangan telah berkembang menjadi lebih canggih dan berevolusi dengan cukup cepat. Oleh karena itu diperlukan sistem pendeteksi dengan kemampuan kecerdasan yang lebih tinggi dan mampu melakukan pembelajaran secara *real-time (on-the-fly learning*).

Merujuk latar belakang di atas, penelitian ini mencoba membangun sistem cerdas pendeteksi serangan yang melibatkan orang dalam menggunakan analisis perilaku entitas/penggunan. Alih-alih mengikuti cara tradisional dalam mendeteksi serangan/anomali yang menggunakan sistem berbasis aturan (rule-based) ataupun sistem berbasis pengetahuan (knowledge-based), penelitian ini lebih memilih menggunakan analisis perilaku entitas dengan memanfaatkan pemodelan memori manusia (Eichenbaum, 2010) untuk memprediksi perilaku entitas berdasarkan data trafik entitas tersebut. Dalam hal ini, sistem pertama-tama dilatih untuk membangun profil entitas di dalam jaringan, kemudian meneliti batas-batas kenormalan perilaku tersebut. Eksperimen dilakukan di dalam persekitaran '*testbed*' dengan beberapa entitas dan sistem akan memprediksi apakah entititas tertentu melakukan kegiatan *illegal*, yang kemudian diakhiri dengan pengambilan keputusan untuk menentukan apakah entitias tersebut normal atau serangan/anomali. Tujuan utama penelitian ini adalah untuk membantu pemerintah dalam meningkatkan kemandirian teknologi siber nasional dan sekaligus bermanfaat untuk mengurangi kebergantungan teknologi informasi dan komunikasi (TIK), khususnya teknologi siber dari negara lain.

Penelitian tentang UBA, telah banyak dilaksanakan, diantaranya Zhang et al. (2019) menggunakan lingkungan sosial seluler dari pengguna dan menyelidiki pengguna yang berkorelasi dengan kebiasaan jangka panjang dan pengaruh jangka pendek terbesar untuk pengguna target masing-masing, menggunakan teori optimasi. Sampel perilaku pengguna tersebut diintegrasikan ke dalam *database* sampel pengguna target untuk membangun mekanisme sampel untuk meningkatkan akurasi prediksi perilaku pengguna secara signikan. Kemudian, dua model optimasi berdasarkan tingkat kesamaan dan tingkat interaksi masing-masing dirumuskan untuk memilih pengguna berkorelasi optimal yang sesuai untuk menganalisis dua faktor utama perilaku pengguna

target; Selanjutnya, strategi pembaruan adaptif berdasarkan teori fuzzy diusulkan untuk menggambarkan pentingnya dua faktor secara real time dan kuantitatif. Kemudian, teori Apriori diperkenalkan untuk memprediksi perilaku layanan pengguna berikutnya secara akurat; khususnya, mekanisme pembaruan database sampel Apriori dibangun untuk mengintegrasikan sampel pengguna berkorelasi optimal secara efektif. Akhirnya, hasil simulasi ekstensif menunjukkan bahwa algoritma yang diusulkan mengungguli beberapa algoritma terkait dalam hal akurasi, prediksi dan efisiensi operasi. Penelitan terkait analisis perilaku entitas dalam bidang keamanan siber dapat dilihat di artikel pada referensi: Stiawan (2010), Sun et al. (2019), Perichappan (2018), dan Deng at al. (2019).

Sementara itu, Sharipuddin et al. (2020, 2021) membangun suatu sistem pendeteksi penyusupan (*Intrusion Detection System* – IDS) dan berhasil memperbaiki akurasi dan presisi pendeteksian dengan menggunakan *Principal Components Analysis* (PCA) sebagai ekstraksi fitur. Eksperimen pada dataset hasil ekstraksi fitur dari suatu jaringan *testbed Internet of Things* (IoT) telah dilaksanakan untuk menginvestigasi pengaruh dari proses ekstraksi terhadap pendeteksian serangan dan hasilnya menunjukkan akurasi pendeteksian sempurna, yaitu 100%.

Sebuah kerangka kerja baru untuk mengungkapkan fungsi neokorteks otak manusia diusulkan oleh Hawkins et al. (2019) dan Eichenbaum (2010). Kerangka kerja prediksi memori telah diterapkan di berbagai bidang, termasuk identifikasi objek (Cinalli et al., 2020), (Santhakumar and Kasaei, 2022), kedokteran (Chakravarty et al., 2020), pembelajaran online (Yan dan Au, 2019), jaringan waktu nyata (Cui, et al. 2016).

Teknik kecerdasan buatan (AI) telah pula digunakan untuk mendeteksi serangan/anomali, diantaranya: Shaukat et al. (2020, 2020, 2021) menggunakan teknik pembelajaran mesin dan Stiawan et al. (2022) menggunakan model *Long Short Term Memori* (LSTM) yang dilengkapi dengan metode pemilihan fitur, PCA. Sementara itu, penelitian menyangkut pendeteksian serangan/anomali secara *online/real-time* telah banyak pula dilakukan, seperti penelitian yang dilakukan oleh Li et al. (2019); Losing, Hamm et al. (2018); Mohammed & Bouchachia (2020) dan Pasha et al. (2018)

Budiarto, et al., (2022) mengusulkan suatu model memori dengan menerapkan kerangka prediksi memori, dinamakan "*simplified single cell assembled sequential hierarchical memory* (s.SCASHM)". Kemudian model ini digunakan sebagai alat untuk memprediksi perilaku entitas dan mendeteksi serangan yang melibatkan orang dalam maupun anomaly. Hasil experimen menunjukkan bahwa model memori yang diusulkan berhasil memprediksi perilaku trafik entitas dengan tingkat akurasi bervariasi dari 72% hingga 83% dan mampu melakukan pembelajaran *on-the-fly*, ketika datang pola baru serangan. Penelitian dalam makalah ini mengadopsi model yang telah diusulkan oleh Budiarto (2022) dan mengkombinasikannya dengan metode PCA sebagai pemilihan fitur.

Makalah ini disusun sebagai berikut. Bagian 1 membahas pengenalan, disusul dengan Bagian 2 yang membahas tentang metode yang digunakan dalam penelitian ini dan dilanjutkan dengan Bagian 3 yang berisi tentang hasil penelitian dan pembahasan. Sebagai penutup, Bagian 4 menyimpulkan keseluruhan penelitian.

2. METODE PENELITIAN

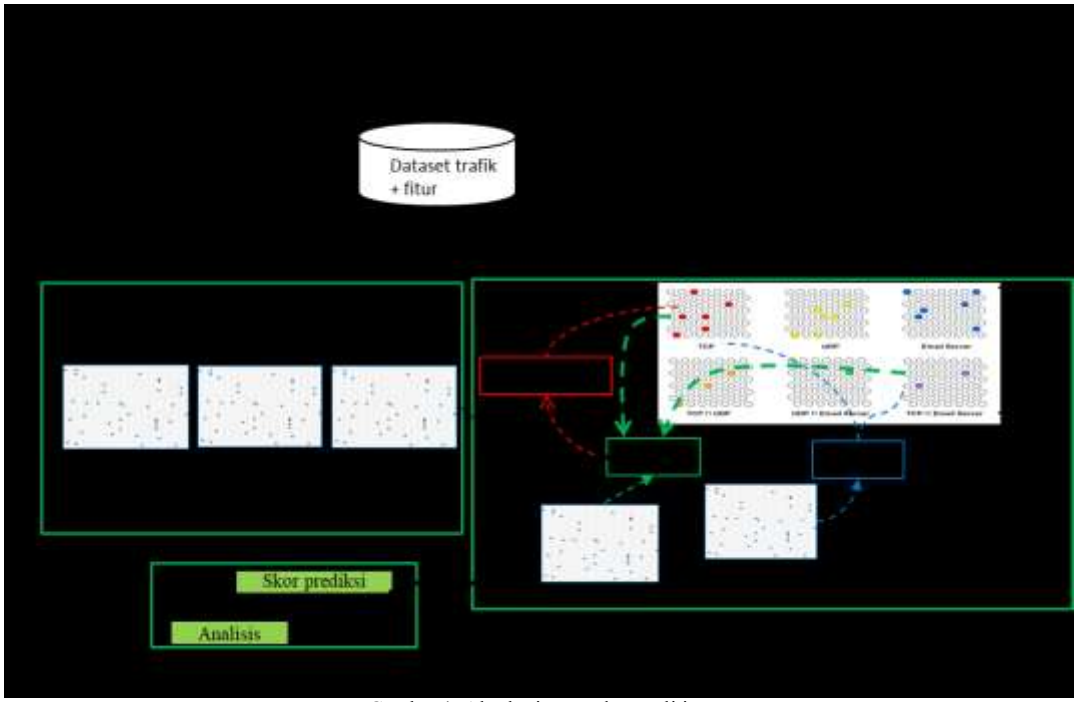
Metode yang digunakan dalam penelitian ini terdiri dari dua tahapan. Tahapan 1 adalah pembangunan dataset untuk eksperimen. Tahapan 2 adalah pembangunan enjin untuk memprediksi trafik perilaku pengguna berbasis model prediksi memori. Gambar 1 menunjukkan alur kerja metode penelitian yang diusulkan dan dijelaskan dengan rinci pada bagian berikut.

2.1. Ekstraksi Fiture Menggunakan PCA

Dengan memaksimumkan nilai varians, analisis komponen utama (PCA) melakukan transformasi linier data asal kepada sistem koordinat baru. PCA biasa digunakan untuk mereduksi dimensi suatu data dengan tetap mempertahankan karakteristik data tersebut. Atribut trafik yang digunakan, diantaranya: *source+destination IP address, port numbers, payload length*, dll, Algoritma PCA yang digunakan untuk melakukan ekstraksi fitur trafik ditunjukkan oleh Algoritma 1.

Algoritma 1
Input: Data trafik
Output: FITUR (Kumpulan Fitur Terpilih)

```
Import modul decomposition dari sklearn
data ← unggah_dataset
def main()
    Y ← baca(data)
    pca =decomposition.PCA(n_components=9)
        pca.fit(Y)
    Y = pca.transform(Y)
   FITUR←Y
end
```



Gambar 1. Alur kerja metode penelitian

```
0: Start
1: Proses masukan 'xt'
2:          Unggah variabel prediksi 'p'
3:          While 'xt' tidak dalam bentuk sederhana
4:                    Pecahkan 'x' menjadi bagian yang lebih kecil
5:                    Simpan ke dalam set Y
6:          End While
7:          Bandingkan 'p' dengan setiap elemen pada Y
8:          If 'p' matching
9:                    Set 'p' ke dalam set berikutnya
10:                   If sebarisan masukan lengkap matched
11:                             Return detail informasi lengkap
12:                   End If
13:         End If
14:         Set n ← 0
15:         While Y tidak kosong
16:                   Masukan elemen-elemen Y ke dalam Ln
                      dari Model Memori sesuai dengan nilai 't'
17:                   If  terjadi matched
18:                      If sebarisan masukan lengkap matched
19:                         Return detail informasi lengkap
20:                      End If
21:                   Else
22:                      If  n+ 1 < 6
23                        Pindahkan Y ke dalam  Ln+1 dari Model Memori
24:                      Set n menjadi n+1
25:                      Else
26:                         Buat super-set baru untuk Y
27:                      End If
28:                   End If
29:         End While
30: End
```

Gambar 2. *Pseudocode* model memori

2.2. Proses Prediksi

Proses prediksi trafik serangan/anomali dijalankan dengan mengimplementasi model memori dari hasil penelitian oleh Budiarto, at al. (2022). Secara *real-time* model memori ini diimplementasikan sebagai perkakas untuk menganalisis perilaku entitas berdasarkan data trafiknya. Data trafik yang diperoleh dari fase ekstraksi data, diubah ke dalam bentuk rentetan paket jaringan individu, dengan merepresentasikan setiap *byte* data trafik tersebut ke dalam bentuk atomik berupa vektor terdiri dari rentetan 2048 bit sebagai *Sparse Distribute Representation* (SDR– bentuk dasar untuk

diinputkan ke dalam modul model memori). Vektor bit ini diinputkan ke dalam modul model prediksi memori untuk dianalisis. Output dari modul model memori selanjutnya digunakan untuk proses prediksi galat dan kebarangkalian bahwa *event* tersebut termasuk kategori serangan/anomali. *Pseudocode* dari modul model memori ditunjukkan oleh Gambar 2.

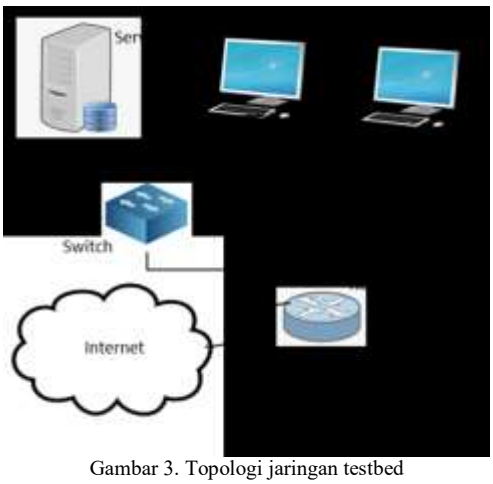
2.3. Topologi Jaringan *Testbed*

Data untuk eksperimen diambil dari jaringan di gedung Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Albaha, Saudi Arabia, selama 2 pekan (1 – 14 Desembar 2022). Tercatat ada lebih dari 150 pengguna mengakses jaringan selama periode tersebut. Karena tidak memungkinkan untuk menginjeksi trafik serangan/anomali ke dalam jaringan produksi, maka data yang sudah didapatkan tersebut dijalankan kembali secara simulasi di dalam lingkungan jaringan *testbed* yang terdiri dari 3 komputer yang terhubung ke sebuah *switch.* Sebuah server dikonfigurasi untuk menjalankan 4 server virtual. Komputer PC-2 digunakan untuk menghasilkan paket trafik melalui modul pembangkit paket untuk menyuntikkan trafik ke dalam jaringan. Trafik serangan diambil dari dataset MACCDC (MACCDC, 2021). Jenis serangan yang dipilih adalah *flooding attacks*. Trafik beberapa user disimulasi dgn memasukkan trafik serangan yang diambil dari MACCDC, sehingga beberapa trafik user mengandung fitur-fitur serangan. Setelah itu, trafik-trafik ini coba dikenali dengan metode yang diusulkan. Modul pendeteksi diinstal pada PC-1, yang terhubung ke *mirrored port* pada *switch* sehingga pendeteksi mampu melihat semua trafik di dalam segmen jaringan yang sedang dimonitor. Spesifikasi dari PC-1 dan PC-2 adalah sebagai berikut: CPU Intel Core i7, 8 GB RAM dan hardisk berukuran 500 GB. Untuk sever, digunakan komputer dengan spesifikasi CPU Intel Core i7, 16 GB RAM dan hardisk berukuran 1 TB. Semua komputer menjalankan sistem operasi Windows 10. Modul untuk model prediksi memori diimplementasikan dalam bahasa pemrograman Java, sedangkan modul prediksi menggunakan *deep learning* (DL) diimplementasikan dalam bahasa pemrograman Python dan pustaka Scikit-Learn. Gambar 3 mengilustrasikan jaringan testbed yang digunakan dalam eksperimen.

2.4. Skenario Eksperimen

Setelah jaringan *testbed* disiapkan, simulasi data trafik yang telah diperoleh selama 2 pekan observasi dijalankan dengan skenario berikut.

- Rancangan dan rencana simulasi data trafik (Bila anomali terjadi? dan anomali apa yang terjadi?).



Gambar 3. Topologi jaringan testbed

- Tetapkan 12 *user/node* (empat node server dan 8 user paling aktif, berdasarkan jumlah trafik).
- Buat paket trafik yang diperlukan secara manual, termasuk paket anomali/serangan.
- Memulai menyuntikkan data trafik ke jaringan dan pada saat yang sama mencatat trafik melalui *mirroring port*.
- secara manual beri label anomali yang disimulasikan serta trafik aplikasi tertentu (label ini digunakan selama eksperimen untuk memverifikasi hasil).
- Simpan trafik yang didapatkan ke dalam file dalam format *.pcap* sebagai kumpulan data untuk eksperimen analisis perilaku entitas/pengguna.

Eksperimen dilakukan dengan memberi umpan data trafik mentah untuk pembelajaran dan deteksi berkelanjutan. Dalam eksperimen pembelajaran mendalam (*deep learning*), 7 hari pertama trafik digunakan sebagai data pelatihan, dan 7 hari terakhir digunakan sebagai data pengujian. Nilai Rata-rata diambil sebagai hasil akhir.

2.5. Evaluasi Kinerja

Dalam mengevaluasi hasil experimen, penulis menggunakan beberapa metrik untuk mengukur kinerja sistem yang diusulkan. Metrik kinerja tersebut termasuk: Akurasi, Presisi, Sensitivitas, F1-score, dan Spesifisitas menggunakan formula dalam (1) – (5) (Gu et al., 2020).

$$Akurasi = \frac{TP+TN}{TP+FP+FN+TN} \quad (1)$$

$$Presisi = \frac{TP}{TP+FP} \quad (2)$$

$$Sensitifitas = \frac{TP}{TP+FN} \quad (3)$$

$$Spesifisitas = \frac{TN}{TN+FP} \quad (4)$$

Tabel 1. Data yang ditangkap dari jaringan

Kelas	*Flows*		Protokol/Aplikasi
	Jumlah trafik	(%)	
WEB	7029000	78.91	Menjelajah HTTP, HTTPS
HTTP-STR	153000	1.71	HTTP *Streaming*
EDONKEY	562500	5.75	eDonkey, eMule *obfuscated*
BITTORRENT	51300	0.57	Bittorent
CHAT	438300	1.87	MSN, IRC, Yahoo Msn, HTTP Chat, Jabber
EMAIL	533700	4.56	SMTP, HTTP Mail, , POP3, POP3s, IMAP, IMAPs
FTP	5400	0.05	FTP-data, FTP control
STREAMING	25200	0.28	Ms. Media Server, Real Player, iTunes, Quick Time
GAMES	4500	0.05	NFS3, HTTP Games, Blizzard Battlenet, Quake II/III, Counter Strike
UNKNOWN	197100	2.19	NBS, Ms-ds, Epmap, Serangan

$$F1\ Score = \frac{2*(Sensitifitas*Presisi)}{Sensitifitas+Presisi} \quad (5)$$

Dimana,

TP= *True Positive*, yaitu data positif yang terdeteksi benar.

TN= *True Negative*, yaitu data negatif yang terdeteksi benar.

FP= *False Positive*, yaitu data negatif namun terdeteksi sebagai data positif.

FN= *False Negative*, yaitu data positif namun terdeteksi sebagai data negatif.

TP, TN, FP, FN disebut sebagai komponen *Confusion Matrix* dan nilai-nilainya didapat dari pengamatan selama melaksanakan eksperimen.

3. HASIL DAN PEMBAHASAN

Bab ini memaparkan hasil eksperimen berikut dengan pembahasannya.

3.1. Hasil Ekstraksi Fitur

Tabel 1 menunjukkan data trafik yang berhasil dicatat selama eksperimen, kemudian data trafik ini diekstrak menggunakan metode PCA yang hasilnya ditunjukkan pada Tabel 2.

Tabel 2. Hasil ekstraksi fitur

Kelas	Jumlah fitur optimum
WEB	9
HTTP-STR	9
EDONKEY	12
BITTORRENT	7
CHAT	11
EMAIL	11
FTP	8
STREAMING	15
GAMES	14
UNKNOWN	13

3.2. *Top User Profiling*

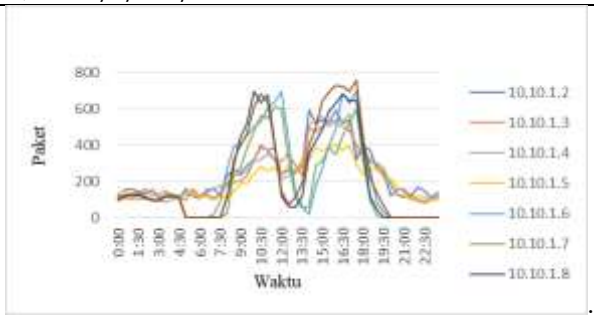
Pada eksperimen ini, kedelapan *top user* dibuat *profile*nya. Hasil *profiling* yang ditampilkan pada Gambar 4 diambil dari data rata-rata jumlah paket selama 14 hari pengamatan.

3.3. Perbandingan dengan Model *LSTM-PCA*

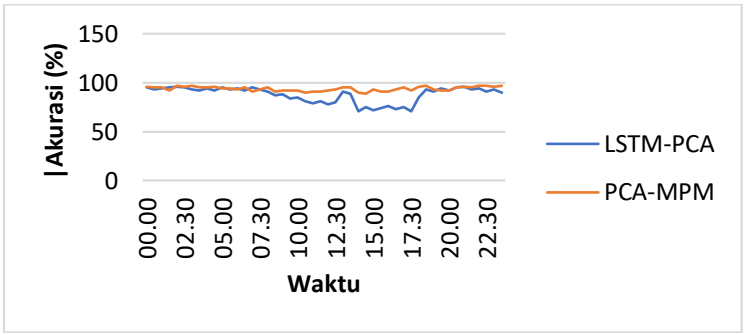
Eksperimen ini bertujuan untuk melihat perbandingan akurasi dalam memprediksi aliran trafik antara model prediksi memori dengan model LSTM-PCA. Model ini diadopsi dari penelitian yang telah dilakukan oleh Stiawan et al. (2022). Hasil eksperimen yang ditampilkan pada Gambar 5, menunjukkan bahwa model prediksi memori mampu mempertahankan konsistensi rata-rata akurasi selama masa fluktuasi dari pukul 9 pagi sampai pukul 5 petang perhari, sementara model LSTM-PCA gagal untuk mempertahankan akurasi prediksi karena model ini tidak mempunyai kemampuan untuk melakukan pembelajaran *on-the-fly* dan mungkin karena sampel yang digunakan untuk *training* tidak cukup banyak.

Tabel 3 menunjukkan hasil perhitungan pengukuran kinerja dari pendektesian anomali yang terjadi di beberapa aplikasi pilihan berdasarkan pengamatan *Confusion Matrix*. Secara umum kombinasi metode pemilihan fitur PCA dan model prediksi memori menghasilkan akurasi lebih baik dari model LSTM-PCA. Akurasi yang diperoleh mencapai 94.01% untuk pendeteksian kelas *UNKNOWN*.

Proses pembentukan model memori untuk trafik normal dan anomali pada Gambar 1 dalam eksperimen diamati melalui statistik aktivitas pengaktifan sel dalam memori. Tabel 4 menunjukkan hasil pengamatan statistik pengaktifan sel memori yang terjadi.



Gambar 4. Hasil *profiling* 8 user teraktif (rata-rata perhari)



Gambar 5. Perbandingan akurasi LSTM-PCA vs. PCA-MPM

Tabel 3. Hasil pengukuran metrik kinerja pendeteksian untuk beberapa aplikasi (LSTM-PCA vs. PCA-MPM)

Aplikasi	Akurasi (%)		Presisi (%)		Sensitivitas (%)		F1-score (%)		Spesifisitas	
	PCA-MPM	LSTM	PCA-MPM	LSTM	PCA-MPM	LSTM	PCA-MPM	LSTM	PCA-MPM	LSTM
WEB	90.15	79.54	88.55	76.96	98.65	96.32	91.80	84.00	57.93	46.18
CHAT	90.18	72.99	90.33	75.88	98.59	92.43	93.13	82.87	30.00	20.07
EMAIL	92.78	74.10	**95.64**	75.25	98.77	93.02	95.87	82.11	56.67	28.60
STREAMING	93.66	80.05	95.11	82.01	99.01	95.99	**96.08**	86.56	55.67	28.56
GAMES	93.22	81.52	94.88	82.17	99.14	96.23	95.65	87.32	59.27	38.90
UNKNOWN	**94.01**	91.76	93.75	79.98	**99.28**	96.78	95.45	86.77	**60.39**	40.79

Table 4. Statistik pengaktifan sel memori selama eksperimen.

	Nomor Eksperimen				
	1	2	3	4	5
Sel aktif	86%	51%	80%	85%	49%
Sel non-aktif	12%	37%	14%	9%	41%
Sel mati	2%	12%	6%	7%	10%

Waktu yang diperlukan untuk proses pemprofilan (*profiling*) dan pendeteksian anomali juga diukur dalam eksperimen, seperti ditunjukkan oleh Tabel 5.

Tabel 5. Waktu pemrosesan pendeteksian dan *profiling* (dalam detik)

	Node ID							
	10.10.1.1	10.10.1.2	10.10.1.3	10.10.1.4	10.10.1.5	10.10.1.6	10.10.1.7	10.10.1.8
	Det. Prof.	Det. Prof.	Det. Prof.	Det. Prof.	Det. Prof.	Det. Prof.	Det. Prof.	Det. Prof.
LSTM-PCA	0.04 0.14	0.05 0.14	0.05 0.15	0.06 0.16	0.07 0.16	0.09 0.10	0.16 0.17	0.12 0.19
PCA-MPM	0.02 0.11	0.02 0.12	0.02 0.12	0.02 0.14	0.02 0.28	0.04 0.45	0.07 0.52	0.06 0.50

*Det.: Deteksi, Prof.: *Profiling*

3.4 Pembahasan

Kinerja model yang diusulkan, PCA-MPM lebih konsisten dibandingkan model LSTM-PCA seperti ditunjukkan oleh Gambar 5. Hal ini disebabkan model PCA-MPM menggunakan streaming data dan tidak memerlukan training, sementara model LSTM-PCA menggunakan data statis, memerlukan training dan bersifat invarian waktu. Model LSTM-PCA memerlukan dataset yang cukup besar untuk keperluan training sehingga pembelajarannya memakan waktu dan ketidak-mampuan beradaptasi dengan perubahan data yang menyebabkan penurunan nilai akurasi. Di sisi lain, PCA-MPM unggul dalam pendeteksian anomali untuk streaming data. Kinerja akurasi model PCA-MPM terburuk yang sempat diamati adalah 72%. Model PCA-MPM mencapai konvergensi pembelajaran lebih cepat dibanding model LSTM-PCA karena tidak perlu memperbarui sel-sel memori yang sedang aktif, selama perubahan signifikan dari streaming data tidak terjadi. Seperti dapat disimak pada Tabel 4, sel

memori dibentuk ketika informasi baru didapat dari streaming data.

Model PCA-MPM yang diusulkan tidak dirancang untuk pembelajaran yang memiliki ketergantungan jangka panjang dari rangkaian memori orde tinggi, karena akan memerlukan waktu pemrosesan yang lama, seperti yang diperlukan oleh model memori temporal berhirarki (*hierarchical temporal memory*) (Hawkins & Blakeslee, 2015). Sementara itu pengukuran waktu yang diperlukan oleh model PCA-MPM untuk pendektesian trafik anomali dan *profiling* suatu entiti menunjukkan hasil yang menjanjikan, seperti yang ditunjukkan oleh Tabel 5. Menimbang waktu pemprosesan dan kompleksitas model, model PCA-MPM berpotensi untuk diadopsi sebagai cara untuk menganalisis perilaku entitas untuk mencegah serangan internal secara *real-time*.

4. KESIMPULAN

Dalam makalah ini, penulis telah memperkenalkan penggunaan kombinasi PCA sebagai alat untuk pemilihan fitur dan model prediksi memori (PCA-MPM) untuk mendeteksi trafik anomali/serangan siber yang melibatkan orang dalam. Hasil eksperimen menunjukkan model PCA-MPM mampu memperagakan pendeteksian serangan/anomali yang melibatkan orang dalam dengan tingkat akurasi mencapai 94.01% untuk pendeteksian kelas trafik *unknown*. Secara umum PCA-MPM mencapai akurasi 90.15% hingga 94.01%. Disamping itu, PCA-MPM juga mampu memberikan akurasi yang lebih baik daripada model LSTM-PCA, karena mampu melaksanakan pembelajaran *on-the-fly*, sehingga sistem dapat mengenali pola baru dari serangan/anomali. Oleh karena itu, PCA-MPM dapat diimplementasikan sebagai sub-sistem untuk mendukung platform keamanan siber yang cerdas dan menyeluruh (*holistic*), yang sedang dikembangkan di *Networked Computing Lab*, Program studi Matematika Pertahanan, Universitas Pertahanan. Platform ini diproyeksikan untuk digunakan oleh institusi pemerintahan mahupun swasta.

Keterbatasan model PCA-MPM adalah keterbatasan umum model pembelajaran mesin, karena model ini termasuk pendekatan pembelajaran unsupervised, sepanjang masa, dan berkesinambungan, dimana PCA-MPM ini melaksanakan pembelajaran dari data user dengan perilaku normal.

DAFTAR PUSTAKA

BUDIARTO R., ALQARNI A., ALZAHRANI M.Y., PASHA M.F., FIRDOUS M., STIAWAN D., 2022, User behaviour analytics tool using simplified predictive-memory concept, Materials & Continua (CMC), vol.70, no.2, pp.2679-2698, doi: 10.32604/cmc.2022.019847.

CHAKRAVARTY S., CHEN Y.Y., and CAPLAN J.B., Predicting memory from study-related brain activity, Journal of Neurophysiology, 124:6, 2060-2075, 2020.

CINALLI D.A. Jr, COHEN S.J., Guthrie K. and Stackman R.W. Jr, Object recognition memory: distinct yet complementary roles of the mouse CA1 and perirhinal cortex. Front. Mol. Neurosci. 13:527543, 2020. doi: 10.3389/fnmol.2020.527543

CUI Y., AHMAD S, dan HAWKINS J., 2016, Continuous online sequence learning with an unsupervised neural network model, Neural Computation, vol. 28, no. 11, pp. 2474–2504.

DENG K., XING L., ZHENG L., WU H., XIE P. et al., 2019, A user identification algorithm based on user behavior analysis in social networks, IEEE Access, vol. 7, pp. 47114–47123.

EICHENBAUM H., 2010, Memory systems, WIREs Cognitive Science, vol. 1, no. 4, pp. 478–490.

GU Y. K., XU B., HUANG H., dan QIU G., 2020, A Fuzzy Performance Evaluation Model for a Gearbox System Using Hidden Markov Model, IEEE Access, vol. 8, pp. 30400–30409, 2020, doi: 10.1109/ACCESS.2020.2972810.

HAWKINS J. dan BLAKESLEE S., 2015, On Intelligence, New York, USA: Owl Book.

HAWKINS J., LEWIS M., KLUKAS M., PURDY S. dan AHMAD S., 2019, A framework for intelligence and cortical function based on cells in the neocortex , Frontiers in Neural Circuits, vol. 12, article ID: 121.

SANTHAKUMAR K. and KASAEI H., Lifelong 3D object recognition and grasp synthesis using dual memory recurrent self-organization networks, Neural Networks, vol. 150, 2022, pp. 167-180.

LI G., SHEN Y., ZHAO P., LU X., LIU J. et al., 2019, Detecting cyberattacks in industrial control systems using online learning algorithms, Neurocomputing, vol. 364, pp. 338–348.

LOSING V., HAMMER B. dan WERSING H., 2018, Incremental on-line learning: A review and comparison of state of the art algorithms, Neurocomputing, vol. 275, pp. 1261–1274.

MACCDC 2012 dataset, 2021. [Online]. Tersedia: https://maccdc.org/2012-agenda/ (last accessed: 08/07/2022).

MOHAMAD S. dan BOUCHACHIA A., 2020, Deep online hierarchical dynamic unsupervised learning for pattern mining from utility usage data, Neurocomputing, vol. 390, pp. 359–373.

PASHA M. F., BUDIARTO R., RAMADASS S. dan SYUKUR M., 2018, A sequential hierarchical superset implementation of neocortex memory system and its case study of automated network forensic analysis, International Conference on Artificial Intelligence, Las Vegas, USA, pp. 490–495.

PERICHAPPAN K., 2018, Greedy algorithm based deep learning strategy for user behavior prediction and decision making support, Journal of Computer and Communications, vol. 6, no. 6, pp. 45–53.

SHARIPUDDIN, PURNAMA B., KURNIABUDI, WINANTO E.A, STIAWAN D., DARMAWIJOYO, HANAPI, BUDIARTO R., 2020, Features extraction on IoT intrusion detection system using principal components analysis (PCA), 7th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, October 1-2, 2020, pp. 114-118.

SHARIPUDDIN, E.A. WINANTO, B. PURNAMA, KURNIABUDI, D. STIAWAN, D. HANAPI, M.Y. IDRIS, B. KERIM, R. BUDIARTO, Enhanced Deep Learning Intrusion Detection in IoT Heterogeneous Network with Feature Extraction, Indonesian Journal of Electrical Engineering and Informatics (IJEEI), Vol. 9, No. 3, pp. 747-757, 2021.

SHAUKAT K., LUO S., CHEN S. dan LIU D., 2020, Cyber threat detection using machine learning techniques: A performance evaluation perspective, 2020 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, pp. 1–6.

SHAUKAT K, LUO S., VARADHARAJAN V., HAMEED I. A. dan XU M., "A survey on machine learning techniques for cyber security in the last decade," IEEE Access, vol. 8, pp. 222310–222354, 2020.

SHAUKAT K., ALAM T.M., LUO S., SHABBIR S., HAMEED I. A, et al., A Review of time-series anomaly detection techniques: A step to future perspectives," In: Arai K. (eds) Advances in Information and Communication (FICC 2021). Advances in Intelligent Systems and Computing, Springer, Cham, vol. 1363, pp. 865–877, 2021.

STIAWAN D., ABDULLAH A. H. dan IDRIS M. Y., 2010, Classification of habitual activities in behavior-based network detection, Journal of Computing, vol. 2, no. 8, pp. 1–7.

D. STIAWAN, A. HERYANTO, A. BERDADI, D.P. RINI, I.M.I SUBROTO, KURNIABUDI, M.Y. IDRIS, A.H. ABDULLAH, B. KERIM, R. BUDIARTO, An approach for optimizing ensemble intrusion detection systems, IEEE Access, vol. 9, pp. 6930-6947, 2021. doi: 10.1109/ACCESS.2020.3046246.

D. STIAWAN, SUSANTO, A. BIMANTARA, M.Y. IDRIS, AND R. BUDIARTO, IoT botnet attack detection using deep autoencoder and artificial neural network, KSII Transactions on Internet and Information Systems, vol. 17, no. 5, May 2023, pp. 1310-1338, 2023.

STIAWAN D., BARDADI A., AFIFAH N., MELINDA L., HERYANTO A., SEPTIAN T.W., IDRIS M.Y. , SUBROTO I.M.I, LUKMAN dan BUDIARTO, R., An improved LSTM-PCA ensemble classifier for SQL injection and XSS attacks detection, Computer Systems Science and Engineering,Vol. 46, No. 2, pp. 1759-1774, 2023.

SUN Z., WANG Y., ZHOU H., JIAO J. dan OVERSTREET R.E., 2019, Travel behaviours, user characteristics, and social-economic impacts of shared transportation: a comprehensive review, International Journal of Logistics Research and Applications, vol. 24, no. 1, pp. 51–78.

Yan N. and Au O.T-S., Online learning behavior analysis based on machine learning, Asian Association of Open Universities Journal, vol. 14, no. 2, pp. 97-106, 2019.

ZHANG H., WANG M., YANG L. dan ZHU H., 2019, A novel user behavior analysis and prediction algorithm based on mobile social environment, Wireless Network, vol. 25, no. 2, pp. 791–803.

Halaman ini sengaja dikosongkan