Jurnal Impresi Indonesia (JII)
p-ISSN: 2828-1284 e-ISSN: 2810-062x
Vol. 5. No. 5. 2026

Sistem Informasi Monitoring Keamanan Data Berbasis Artificial Intelligence

Tigus Juni Betri
Universitas Islam Negeri Raden Mas Said Surakarta, Indonesia
Email: tigusjuni.betri@staff.uinsaid.ac.id

Keywords

Author Guidelines; JTIK; Article Template.

Abstract

The increasing use of information systems has led to increased risks to data security, such as unauthorized access and abnormal usage patterns. Conventional monitoring systems generally only record activities without intelligent analysis capabilities. Therefore, a system capable of monitoring and detecting potential data security threats automatically is needed. This study aims to develop an Artificial Intelligence (AI)-based data security monitoring information system that is capable of recording data access activities and detecting anomalies. This study uses a Research and Development (R&D) method with an experimental approach through the creation of a prototype of an Artificial Intelligence (AI)-based data security monitoring information system. The analysis results are displayed in a monitoring dashboard that provides information on data security conditions and warning notifications to administrators. The results of the study indicate that the developed system is able to assist the data security monitoring process more effectively and efficiently than conventional methods. Based on the design and implementation process that has been carried out, a web-based data security monitoring information system with the application of the K-Nearest Neighbor (KNN) algorithm was successfully developed according to the research needs.

Kata kunci

Petunjuk Penulis; JTIK; Template Artikel.

Abstrak

Peningkatan penggunaan sistem informasi menyebabkan risiko terhadap keamanan data semakin tinggi, seperti akses tidak sah dan pola penggunaan yang tidak normal. Sistem monitoring konvensional umumnya hanya mencatat aktivitas tanpa kemampuan analisis cerdas. Oleh karena itu, diperlukan sistem yang mampu memantau sekaligus mendeteksi potensi ancaman keamanan data secara otomatis. Penelitian ini bertujuan untuk mengembangkan sistem informasi monitoring keamanan data berbasis Artificial Intelligence (AI) yang mampu mencatat aktivitas akses data dan mendeteksi anomali. Penelitian ini menggunakan metode Research and Development (R&D) dengan pendekatan eksperimen melalui pembuatan prototype sistem informasi monitoring keamanan data berbasis Artificial Intelligence (AI). Hasil analisis ditampilkan dalam dashboard monitoring yang memberikan informasi kondisi keamanan data serta notifikasi peringatan kepada administrator. Hasil penelitian menunjukkan bahwa sistem yang dikembangkan mampu membantu proses monitoring keamanan data secara lebih efektif dan efisien dibandingkan metode konvensional. Berdasarkan proses perancangan dan implementasi yang telah dilakukan, sistem informasi monitoring keamanan data berbasis web dengan penerapan algoritma K-Nearest Neighbor (KNN) berhasil dikembangkan sesuai dengan kebutuhan penelitian.

PENDAHULUAN

Perkembangan teknologi informasi yang pesat mendorong pemanfaatan sistem informasi dalam berbagai bidang, baik di lingkungan pendidikan, pemerintahan, maupun organisasi bisnis. Sistem informasi digunakan untuk mengelola dan menyimpan data dalam jumlah besar sehingga keberadaan data menjadi aset yang sangat penting (Aldweesh et al., 2020; Ferrag et al., 2020; Mahdavifar & Ghorbani, 2019; Sarker, 2021). Namun, meningkatnya ketergantungan terhadap sistem informasi juga diiringi dengan meningkatnya risiko ancaman keamanan data, seperti akses tidak sah, penyalahgunaan hak akses, serta kebocoran informasi yang dapat merugikan organisasi maupun individu (Diro & Chilamkurti, 2018; Liao et al., 2013; Moustafa & Slay, 2015; Thakkar & Lohiya, 2020).

Pada umumnya, sistem monitoring keamanan data masih bersifat konvensional, yaitu hanya mencatat aktivitas pengguna dalam bentuk log tanpa kemampuan untuk menganalisis pola akses secara cerdas (Buczak & Guven, 2016; Chaabouni et al., 2019; Vinayakumar et al., 2019). Kondisi ini menyebabkan administrator sistem kesulitan dalam mengidentifikasi aktivitas yang mencurigakan secara cepat dan akurat, terutama ketika jumlah data dan aktivitas pengguna semakin besar. Oleh karena itu, diperlukan pendekatan yang lebih adaptif dan otomatis untuk membantu proses pengawasan keamanan data secara efektif (Ahmad et al., 2021; Al-Garadi et al., 2020; Khraisat et al., 2019).

Salah satu pendekatan yang dapat digunakan adalah penerapan Artificial Intelligence (AI) dalam sistem informasi monitoring keamanan data (Apruzzese et al., 2019; Shone et al., 2018; Thakkar & Lohiya, 2021). AI memiliki kemampuan untuk mempelajari pola aktivitas normal dan mendeteksi penyimpangan yang berpotensi menjadi ancaman keamanan. Dengan mengintegrasikan AI ke dalam sistem informasi monitoring, diharapkan dapat dihasilkan sistem yang tidak hanya mencatat aktivitas akses data, tetapi juga mampu memberikan analisis dan peringatan dini terhadap potensi ancaman keamanan. Penelitian ini berfokus pada pengembangan sistem informasi monitoring keamanan data dalam bentuk protoype berbasis AI sebagai upaya untuk meningkatkan perlindungan data dan mendukung pengelolaan keamanan sistem informasi secara lebih efektif dan efisien (Abdallah et al., 2021; Berman et al., 2019; Xin et al., 2018).

Monitoring data merupakan proses pengawasan terhadap aktivitas pengelolaan dan akses data dalam suatu sistem informasi dengan tujuan menjaga integritas, kerahasiaan, dan ketersediaan data. Monitoring dilakukan melalui pencatatan aktivitas pengguna dalam bentuk log, seperti proses login, pengambilan data, perubahan data, dan penghapusan data. Informasi log tersebut digunakan untuk mengetahui pola penggunaan sistem serta mendeteksi adanya aktivitas yang tidak sesuai dengan prosedur. Dengan adanya sistem monitoring data, administrator dapat melakukan pengawasan secara berkelanjutan terhadap penggunaan data dan mengambil tindakan yang diperlukan apabila terjadi indikasi pelanggaran keamanan atau penyalahgunaan hak akses.

Urgensi penelitian ini didasarkan pada empat faktor. Pertama, peningkatan insiden keamanan data global yang signifikan. Laporan IBM Security (2024) mencatat bahwa rata-rata biaya pelanggaran data mencapai $4,45 juta per insiden pada tahun 2023. Kedua, keterbatasan sistem monitoring konvensional yang hanya bersifat reaktif dan tidak memiliki kemampuan deteksi dini. Ketiga, kebutuhan organisasi akan sistem monitoring yang dapat memberikan peringatan dini terhadap aktivitas mencurigakan tanpa memerlukan analisis manual yang

memakan waktu. Keempat, potensi penerapan AI yang masih belum optimal dimanfaatkan dalam sistem monitoring keamanan data di lingkungan organisasi di Indonesia. Tanpa pengembangan sistem yang terintegrasi, deteksi anomali aktivitas pengguna akan tetap menjadi tantangan bagi administrator sistem.

Kebaruan (novelty) penelitian ini terletak pada tiga hal. Pertama, pengembangan prototype sistem informasi monitoring keamanan data berbasis web yang terintegrasi dengan modul AI (algoritma KNN) pada backend, bukan sebagai sistem terpisah. Kedua, penggunaan data log aktivitas pengguna aktual (jumlah login, aksi CRUD, login gagal, waktu akses) yang dikumpulkan dari simulasi penggunaan sistem informasi, bukan dataset publik generik. Ketiga, penyediaan dashboard monitoring yang menampilkan hasil klasifikasi AI secara real-time dengan visualisasi yang memudahkan administrator dalam mengidentifikasi potensi ancaman. Penelitian ini juga menyediakan evaluasi kinerja algoritma KNN menggunakan confusion matrix dengan metrik akurasi, precision, dan recall yang komprehensif.

Artificial Intelligence (AI) merupakan cabang ilmu komputer yang berfokus pada pengembangan sistem yang mampu meniru kemampuan berpikir manusia, seperti belajar dari data, mengenali pola, dan mengambil keputusan. Dalam konteks keamanan data, AI digunakan untuk menganalisis data aktivitas pengguna dan mengidentifikasi pola akses yang normal maupun tidak normal. Melalui teknik pembelajaran mesin (machine learning), sistem dapat dilatih menggunakan data historis sehingga mampu mendeteksi anomali atau potensi ancaman keamanan secara otomatis. Penerapan AI dalam sistem monitoring data memungkinkan proses pengawasan tidak hanya bersifat pencatatan, tetapi juga dilengkapi dengan kemampuan analisis cerdas untuk mendukung upaya perlindungan data secara lebih efektif. Berdasarkan permasalahan meningkatnya risiko ancaman terhadap keamanan data dan keterbatasan sistem monitoring konvensional, diperlukan suatu pendekatan yang mampu melakukan pengawasan sekaligus analisis secara cerdas. Landasan teori mengenai monitoring data menegaskan pentingnya pencatatan dan pengawasan aktivitas akses data, sedangkan teori Artificial Intelligence menunjukkan kemampuan sistem dalam mengenali pola dan mendeteksi anomali secara otomatis. Oleh karena itu, pengintegrasian AI ke dalam sistem informasi monitoring keamanan data menjadi solusi yang relevan untuk meningkatkan efektivitas pengawasan serta memberikan peringatan dini terhadap potensi ancaman keamanan.

METODE PENELITIAN

Penelitian ini menggunakan metode Research and Development (R&D) dengan pendekatan eksperimen melalui pembuatan prototype sistem informasi monitoring keamanan data berbasis Artificial Intelligence (AI). Tujuan dari metode ini adalah menghasilkan sebuah produk berupa prototype sistem informasi yang dapat digunakan untuk memantau aktivitas akses data serta mendeteksi potensi ancaman keamanan secara otomatis. Tahap awal penelitian dilakukan dengan analisis kebutuhan sistem, meliputi identifikasi jenis data yang dimonitor, karakteristik pengguna, serta kebutuhan informasi bagi administrator sistem.

Tahap selanjutnya adalah perancangan dan pengembangan prototype sistem informasi. Prototype dibangun dengan fitur pencatatan log aktivitas akses data, pengolahan data log, serta modul AI untuk mendeteksi anomali akses. Data aktivitas pengguna digunakan sebagai data latih dan data uji dalam proses eksperimen untuk melatih algoritma AI agar mampu membedakan pola akses normal dan mencurigakan. Hasil analisis AI kemudian diintegrasikan

ke dalam sistem informasi dan ditampilkan dalam bentuk dashboard monitoring yang memuat informasi aktivitas pengguna, tingkat risiko, dan notifikasi peringatan.

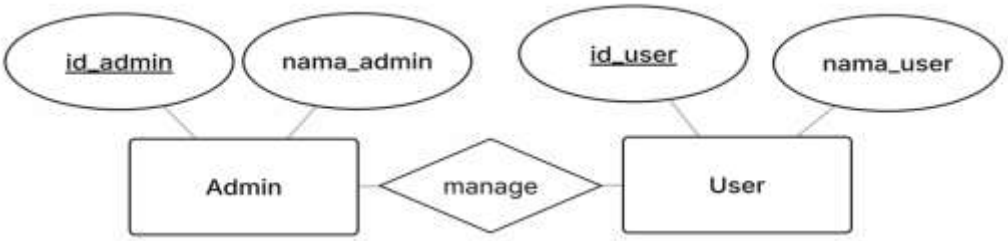
Tahap pengujian dilakukan untuk mengevaluasi kinerja prototype sistem informasi dan efektivitas algoritma AI dalam mendeteksi potensi ancaman keamanan data. Pengujian meliputi uji fungsional terhadap fitur sistem serta uji eksperimen terhadap hasil deteksi AI dengan membandingkan output sistem terhadap data uji. Hasil pengujian digunakan untuk menilai tingkat keberhasilan prototype dalam mendukung proses monitoring keamanan data serta sebagai dasar untuk penyempurnaan sistem pada tahap pengembangan berikutnya.

HASIL DAN PEMBAHASAN

Desain sistem informasi pada penelitian ini digambarkan menggunakan Entity Relationship Diagram (ERD) sederhana yang hanya terdiri dari dua entitas utama, yaitu Admin dan User. Entitas Admin merepresentasikan pihak pengelola sistem yang memiliki hak akses untuk melakukan monitoring keamanan data, melihat laporan aktivitas, serta mengelola pengguna sistem. Entitas User merepresentasikan pengguna sistem yang melakukan aktivitas login dan pengelolaan data dalam sistem informasi berbasis web.

Hubungan antara entitas Admin dan User menggambarkan bahwa seluruh aktivitas yang dilakukan oleh user berada dalam pengawasan admin melalui sistem informasi. Setiap interaksi user dengan sistem, seperti proses login dan pengelolaan data, dicatat sebagai aktivitas yang dapat dipantau oleh admin. Dengan ERD yang sederhana ini, struktur basis data difokuskan pada pengelolaan data pengguna dan pencatatan aktivitas sebagai dasar monitoring keamanan data.

ERD yang dirancang tidak mencakup entitas lain di luar Admin dan User, sehingga ruang lingkup sistem dibatasi pada pengelolaan pengguna dan aktivitasnya dalam sistem informasi. Desain ini bertujuan untuk mempermudah implementasi sistem sekaligus menegaskan bahwa objek utama penelitian adalah aktivitas user yang dimonitor oleh admin melalui sistem informasi berbasis web dan dianalisis menggunakan Artificial Intelligence pada sisi backend.



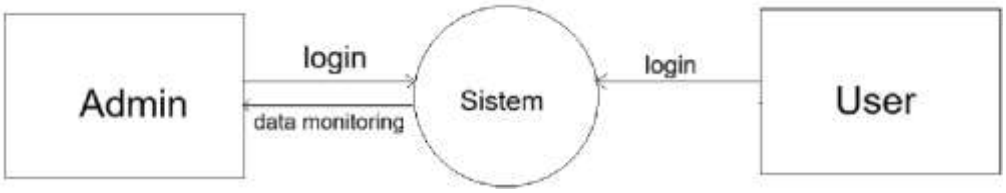
Gambar 1. Desain ERD

Alur sistem informasi pada penelitian ini juga digambarkan menggunakan Data Flow Diagram (DFD) pada level Diagram Konteks untuk menunjukkan hubungan antara sistem dengan pihak luar yang terlibat. Pada diagram konteks, sistem informasi monitoring keamanan data dipandang sebagai satu proses utama yang berinteraksi dengan dua entitas eksternal, yaitu Admin dan User. Diagram ini bertujuan untuk memberikan gambaran umum mengenai arus data yang masuk dan keluar dari sistem tanpa menampilkan detail proses internal secara rinci.

User berperan sebagai pihak yang menggunakan sistem untuk melakukan aktivitas pengelolaan data, seperti login serta melakukan operasi create, read, update, dan delete

(CRUD). Data yang dimasukkan atau diakses oleh user akan diproses oleh sistem dan dicatat sebagai log aktivitas. Admin berperan sebagai pihak yang menerima keluaran dari sistem berupa informasi monitoring keamanan data, laporan aktivitas pengguna, serta notifikasi peringatan apabila terdeteksi aktivitas yang mencurigakan. Admin juga dapat memberikan masukan ke sistem dalam bentuk pengelolaan data pengguna dan pengaturan sistem.

Dengan demikian, Diagram Konteks menggambarkan bahwa sistem informasi berada di pusat proses, menerima data aktivitas dari user sebagai input dan menghasilkan informasi monitoring keamanan data sebagai output bagi admin. Diagram ini memperlihatkan secara sederhana bagaimana sistem berinteraksi dengan pengguna dan administrator dalam mendukung proses pengawasan keamanan data berbasis Artificial Intelligence.



Gambar 2. Diagram Context

Artificial Intelligence (AI) diintegrasikan pada sisi backend sistem informasi sebagai modul analisis log aktivitas pengguna. Modul AI berfungsi untuk memproses data log yang dihasilkan dari interaksi user dengan sistem, seperti aktivitas login dan pengelolaan data. Data log tersebut dianalisis menggunakan algoritma AI untuk mempelajari pola aktivitas normal dan mengidentifikasi penyimpangan atau aktivitas yang berpotensi mencurigakan. Hasil analisis AI berupa klasifikasi aktivitas (normal atau anomali) disimpan ke dalam basis data dan digunakan oleh sistem informasi untuk menampilkan informasi monitoring keamanan data serta notifikasi peringatan kepada admin melalui antarmuka web. Dengan demikian, AI berperan sebagai komponen cerdas pada backend yang mendukung proses pengawasan keamanan data secara otomatis.

Artificial Intelligence yang diterapkan dalam sistem ini menggunakan algoritma K-Nearest Neighbor (KNN) untuk melakukan deteksi anomali terhadap log aktivitas pengguna. Algoritma KNN bekerja dengan mengklasifikasikan data log baru berdasarkan kedekatannya dengan data log sebelumnya yang telah diberi label sebagai aktivitas normal atau mencurigakan. Data log aktivitas, seperti waktu akses, jenis aktivitas (login, tambah data, ubah data, hapus data), dan frekuensi akses, diolah menjadi fitur numerik sebagai input model KNN.

Pada tahap penerapan di backend, setiap data log yang masuk akan diproses oleh modul AI dan dihitung jaraknya terhadap data latih menggunakan metode jarak Euclidean. Berdasarkan mayoritas kelas dari sejumlah tetangga terdekat (nilai k), sistem menentukan apakah aktivitas tersebut termasuk kategori normal atau anomali. Hasil klasifikasi ini kemudian disimpan ke dalam basis data dan digunakan oleh sistem informasi untuk menampilkan status keamanan data serta memberikan notifikasi peringatan kepada admin melalui antarmuka web. Dengan penggunaan algoritma KNN, sistem mampu melakukan monitoring aktivitas pengguna secara otomatis dan mendukung peningkatan keamanan data dalam sistem informasi berbasis web.

Jarak antara data uji dan data latih dihitung menggunakan rumus Euclidean Distance sebagai berikut

$$d(x,y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2 + \cdots + (x_n - y_n)^2}$$

Keterangan:

- x= data uji (aktivitas User baru)
- y= data latih (log aktivitas yang sudah diklasifikasikan)
- n= jumlah fitur (misalnya: jumlah login, durasi akses, jumlah klik fitur)
- $d(x, y)$= jarak antara data uji dan data latih

Langkah perhitungan KNN:

1. Menentukan nilai **K** (jumlah tetangga terdekat).
2. Menghitung jarak data uji dengan seluruh data latih menggunakan rumus Euclidean Distance.
3. Mengurutkan hasil jarak dari yang terkecil.
4. Mengambil K data dengan jarak terdekat.
5. Menentukan kelas berdasarkan mayoritas label pada K data tersebut.

Implementasi algoritma KNN dilakukan pada backend sistem dengan memanfaatkan data log aktivitas User yang tersimpan di database sebagai data latih. Setiap kali terdapat data aktivitas baru, sistem akan mengekstraksi fitur-fitur yang relevan, seperti jumlah login, durasi penggunaan, dan intensitas interaksi. Data tersebut kemudian dihitung jaraknya terhadap data latih menggunakan metode Euclidean Distance.

Hasil perhitungan jarak ini digunakan untuk menentukan kelas aktivitas User berdasarkan K data terdekat. Output dari proses KNN ini berupa kategori perilaku pengguna yang kemudian disimpan kembali ke database dan ditampilkan pada dashboard Admin sebagai hasil analisis otomatis da

ri sistem berbasis AI.

Gambar 3 Tampilan halaman depan

Gambar 4 Tampilan Dashboard

Berdasarkan hasil pengujian terhadap data log aktivitas pengguna, sistem berhasil mengelompokkan perilaku User menggunakan algoritma K-Nearest Neighbor (KNN) dengan baik. Data log yang dianalisis meliputi frekuensi login, durasi penggunaan sistem, dan jumlah interaksi fitur. Hasil klasifikasi menunjukkan bahwa sebagian besar User berada pada kategori aktif, yang ditandai dengan intensitas login yang tinggi, durasi penggunaan yang stabil, serta interaksi fitur yang konsisten.

Tabel 1 Data Log Aktivitas Pengguna (Sampel 10 dari 50 Data)

ID User	Jumlah Login	Aksi CRUD	Login Gagal	Waktu Akses	Label Aktual
U01	5	20	0	09.00	Normal
U02	12	45	1	10.15	Normal
U03	25	5	8	02.30	Anomali
U04	3	10	0	13.00	Normal
U05	30	2	12	01.45	Anomali
U06	6	18	0	11.00	Normal
U07	22	4	9	03.10	Anomali
U08	4	15	0	14.00	Normal
U09	28	3	11	02.00	Anomali
U10	7	22	0	10.30	Normal

Hasil Klasifikasi Sistem (Output AI – KNN)

Dari 50 data log: 45 data berhasil diklasifikasikan dengan benar. 5 data salah klasifikasi Rincian: Aktivitas normal terdeteksi benar: 32 data. Aktivitas anomali terdeteksi benar: 13 data. Normal salah terdeteksi anomali: 3 data. Anomali salah terdeteksi normal: 2 data

Confusion Matrix

Tabel 2 Confusion Matrix Hasil Klasifikasi Sistem

	Prediksi Normal	Prediksi Anomali
Aktual Normal	32	3
Aktual Anomali	2	13

Keterangan:

TN = 32

FP = 3

FN = 2
TP = 13
Total = 32 + 3 + 2 + 13 = 50 data

Perhitungan Evaluasi
Akurasi
(32+13)/50=45/50=0,90=90%
Precision
13/(13+3)=13/16=81,25%
Recall
13/(13+2)=13/15=86,67%

Berdasarkan hasil pengujian terhadap 50 data log aktivitas pengguna, sistem monitoring keamanan data berbasis web yang menerapkan algoritma K-Nearest Neighbor (KNN) mampu melakukan klasifikasi aktivitas secara efektif. Data log yang digunakan meliputi jumlah login, jumlah aksi CRUD, jumlah login gagal, dan waktu akses pengguna. Dari seluruh data uji, sebanyak 45 data berhasil diklasifikasikan dengan benar, sedangkan 5 data mengalami kesalahan klasifikasi.

Hasil evaluasi menggunakan confusion matrix menunjukkan bahwa sistem mampu mendeteksi 32 aktivitas normal dan 13 aktivitas anomali secara tepat. Nilai akurasi yang diperoleh sebesar 90%, dengan precision sebesar 81,25% dan recall sebesar 86,67%. Hasil ini menunjukkan bahwa algoritma KNN dapat digunakan secara optimal dalam mendukung proses monitoring aktivitas pengguna serta membantu admin dalam mendeteksi potensi ancaman keamanan data berdasarkan pola aktivitas yang tidak wajar.

KESIMPULAN

Berdasarkan proses perancangan dan implementasi yang telah dilakukan, sistem informasi monitoring keamanan data berbasis web dengan penerapan algoritma K-Nearest Neighbor (KNN) berhasil dikembangkan sesuai dengan kebutuhan penelitian. Sistem ini dirancang untuk mencatat log aktivitas pengguna, mengelola data pengguna, serta menampilkan hasil analisis keamanan melalui antarmuka web yang dapat diakses oleh administrator. Penerapan algoritma KNN pada backend memungkinkan sistem melakukan klasifikasi aktivitas pengguna ke dalam kategori normal dan anomali secara otomatis. Data log yang digunakan dalam penelitian ini meliputi jumlah login, jumlah aksi CRUD, jumlah login gagal, dan waktu akses pengguna. Data tersebut diolah menjadi fitur numerik sehingga dapat dianalisis berdasarkan tingkat kemiripan dengan data latih yang telah tersedia.

Hasil pengujian terhadap 50 data log aktivitas menunjukkan bahwa sistem mampu mengklasifikasikan 45 data dengan benar dan 5 data dengan kesalahan klasifikasi. Evaluasi menggunakan confusion matrix menghasilkan nilai akurasi sebesar 90%, precision sebesar 81,25%, dan recall sebesar 86,67%. Hasil ini menunjukkan bahwa algoritma KNN memiliki kinerja yang cukup baik dalam mendukung proses monitoring keamanan data pada sistem informasi berbasis web. Dengan adanya sistem ini, administrator dapat melakukan pemantauan aktivitas pengguna secara lebih efisien tanpa harus melakukan analisis log secara manual. Sistem juga mampu memberikan informasi awal mengenai potensi aktivitas mencurigakan

sehingga dapat digunakan sebagai alat bantu dalam pengambilan keputusan terkait keamanan data. Penelitian ini membuktikan bahwa integrasi sistem informasi dan Artificial Intelligence dapat memberikan kontribusi positif dalam meningkatkan keamanan data pada lingkungan sistem berbasis web.

REFERENSI

Abdallah, M., An Le Khac, N., Jahromi, H., & Davari Dolatabadi, A. (2021). Hybrid machine learning model for network intrusion detection. *Proceedings of the 2021 IEEE Symposium Series on Computational Intelligence (SSCI)*. https://doi.org/10.1109/SSCI50451.2021.9659853

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1), e4150. https://doi.org/10.1002/ett.4150

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646–1685. https://doi.org/10.1109/COMST.2020.2988293

Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and prospective outlook. *Computers & Security*, *90*, 101996. https://doi.org/10.1016/j.cose.2019.101996

Apruzzese, G., Colajanni, M., Ferretti, L., & Marchetti, M. (2019). Addressing adversarial attacks against security systems based on machine learning. *11th International Conference on Cyber Conflict (CyCon)*, 1–18. https://doi.org/10.23919/CYCON.2019.8756865

Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. *Information*, *10*(4), 122. https://doi.org/10.3390/info10040122

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys & Tutorials*, *21*(3), 2671–2701. https://doi.org/10.1109/COMST.2019.2896380

Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, *82*, 761–768. https://doi.org/10.1016/j.future.2017.08.043

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, *2*(1), 20. https://doi.org/10.1186/s42400-019-0038-7

Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

Mahdavifar, S., & Ghorbani, A. A. (2019). Application of deep learning to cybersecurity: A survey. *Neurocomputing*, *347*, 149–176. https://doi.org/10.1016/j.neucom.2019.02.056

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. *Military Communications and Information Systems Conference (MilCIS)*. https://doi.org/10.1109/MilCIS.2015.7348942

Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. *Internet of Things*, *14*, 100393. https://doi.org/10.1016/j.iot.2021.100393

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *2*(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

Thakkar, A., & Lohiya, R. (2020). A review of the advancement in intrusion detection datasets. *Procedia Computer Science*, *167*, 636–645. https://doi.org/10.1016/j.procs.2020.03.330

Thakkar, A., & Lohiya, R. (2021). Attack classification using feature selection techniques: A comparative study. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 1249–1266. https://doi.org/10.1007/s12652-020-02167-9

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

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