Identifikasi Pengguna Berbasiskan Biometrik Keystroke Menggunakan MVMCNN

1st Muhammad Abdullah Azzam
Fakultas Informatika
Univeristas Telkom
Bandung, Indonesia
abdazzam@student.telkomuniversity.ac.id

2nd Prasti Eko Yunanto, S.T., M.Kom
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
gpras@telkomuniversity.ac.id

3rd Dr. Mahmud Dwi Sulistiyo
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
mahmuddwis@telkomuniversity.ac.id

***Abstrak* — Keamanan akses pengguna daring menjadi isu krusial di era digital. Identifikasi berbasis biometrik, seperti keystroke dynamics, dianggap lebih aman dibandingkan metode konvensional. Penelitian ini mengimplementasikan Multi-Voter Multi-Commission Nearest Neighbor Classifier (MVMCNN) untuk identifikasi pengguna melalui keystroke dynamics. MVMCNN dipilih karena kemampuannya mengatasi kelemahan KNN dengan skema multi-voter dan pendekatan Local Mean Probabilistic Neural Network (LMPNN). Dataset keystroke dari Universitas Telkom digunakan dengan fitur UD, DD, DU, UU, dan Duration. Eksperimen meliputi tiga skenario: (1) menentukan panjang vektor optimal (N=4, 8, 12, 16, 20, 24), (2) penyederhanaan fitur menjadi rata-rata dan median, serta (3) seleksi fitur menggunakan Variance Threshold (0.1). Evaluasi menggunakan F1-Score. Hasil menunjukkan skenario pertama dengan N=20 menghasilkan F1-Score tertinggi (0.6911). Penyederhanaan fitur menurunkan performa, dengan F1-Score terbaik 0.3031 (mean, k=9) dan 0.3257 (median, k=3), menandakan pentingnya kekayaan informasi dalam fitur. Seleksi fitur menggunakan Variance Threshold tidak banyak mengubah performa, menunjukkan distribusi data sudah optimal. Temuan ini menegaskan bahwa granularitas data berperan penting dalam akurasi sistem identifikasi berbasis keystroke dynamics.**

***Kata kunci*— biometrik, keystroke, identifikasi, mvmcnn, f1-score.**

I. PENDAHULUAN

Dewasa ini, keamanan pengguna menjadi sangat penting, terutama dalam hal mengakses informasi dan layanan daring [1]. Identifikasi berbasis biometrik dianggap sebagai solusi yang lebih aman dan mudah dibandingkan dengan metode tradisional seperti kata sandi atau (personal identification number) PIN [2]. Dengan meningkatnya ancaman keamanan seperti akses ilegal, dibutuhkan pendekatan yang lebih baik dalam pengamanan pengguna [1], [3], [4]. Biometrik adalah konsep yang merujuk pada beragam karakteristik fisik dan perilaku manusia yang dapat digunakan untuk mengidentifikasi individu tetapi tidak terbatas pada sidik jari, ciri wajah, iris, dan suara [5], [6]. Dalam konteks ini, identifikasi berbasis keystroke hadir sebagai alternatif yang menjanjikan, mengingat keunikan pola mengetik individu yang dapat dijadikan sebagai identitas unik. Dibandingkan dengan metode tradisional seperti kata sandi, pendekatan biometrik keystroke memiliki tingkat keamanan yang lebih tinggi karena sulit untuk diretas atau disalin oleh pihak yang tidak sah [2]. Oleh karena itu, memahami lebih dalam bagaimana keystroke bisa digunakan sebagai identitas pengguna menjadi hal yang penting, terutama untuk menghadapi ancaman keamanan yang semakin beragam di era digital ini.

Sejumlah penelitian telah dilakukan untuk mengeksplorasi keystroke dynamics-based identification. Contohnya adalah metode yang digunakan oleh Ioannis Tsimperidis [7], yang memanfaatkan dataset IKDD dalam pengujian klasifikasi pengguna berbasis keystroke. Penelitian ini menggunakan algoritma Support Vector Machine (SVM) untuk membangun model klasifikasi. Hasil evaluasi menunjukkan bahwa model SVM mampu mencapai F1-score terbaik sebesar 0,76. Penelitian lain dilakukan oleh B. Radha Krishna [8], yang mengkaji penggunaan algoritma K-Nearest Neighbors (KNN) untuk tugas klasifikasi berbasis keystroke dynamics. Dalam penelitian ini, pendekatan KNN diterapkan pada data keystroke, dan hasil evaluasi menggunakan metrik F1-score menunjukkan bahwa algoritma ini mencapai F1-score terbaik sebesar 0,62. Hal ini memperlihatkan bahwa KNN juga dapat digunakan untuk tugas klasifikasi. Meskipun penelitian menggunan KNN memiliki hasil yang cukup baik, namun banyak kekurangan yang dimiliki oleh algoritma KNN [9]. Pada algoritma KNN nilai ukuran tetangga (k) memiliki sensivitas yang sangat berpengaruh [9], [10]. Dimana nilai k yang tidak tepat dapat memengaruhi kinerja algoritma, terutama dalam menghadapi outlier, apalagi ketika KNN dihadapi dengan volume dataset yang besar [9], [10]. Pada KNN tidak selalu menghasilkan klasifikasi yang robust terhadap outlier, karena aturan mayoritas suara (nilai) dari tetangga terdekat dapat dipengaruhi oleh data yang tidak representatif [9]. Untuk mengatasi masalah-masalah ini, penggunaan multi-voter multi-commission nearest neighbor classifier (MVMCNN), yang merupakan modifikasi dari KNN, dapat menjadi solusi yang potensial. Dari total 30 dataset yang diuji, 17 di antaranya menunjukkan hasil yang bagus ketika menggunakan MVMCNN [9]. Hal ini menunjukkan sekitar 57% dari dataset yang dievaluasi berhasil memberikan hasil yang baik dengan model MVMCNN daripada KNN, Local Mean-based Probabilistic

Neural Network (LMPNN), dan Bonferroni Mean Fuzzy K-Nearest Neighbors (BM-FKNN) [9].

Berdasarkan latar belakang di atas, penelitian ini bertujuan mengimplementasikan MVMCNN pada sistem identifikasi pengguna berbasis keystroke biometrik untuk meningkatkan keamanan. Selain itu, penelitian ini menganalisis performansi klasifikasi MVMCNN pada Biomey Keystroke Dataset. Terakhir, penelitian ini mengevaluasi keunggulan MVMCNN dibandingkan metode sebelumnya dalam mengatasi kelemahan KNN, seperti sensitivitas terhadap nilai k dan outlier.

Penelitian ini memiliki beberapa batasan untuk menyederhanakan ruang lingkup. Pertama, penelitian hanya berfokus pada identifikasi pengguna, bukan verifikasi atau autentikasi. Kedua, dataset yang digunakan adalah Biomey Keystroke Dataset dengan 40 partisipan dari Universitas Telkom. Ketiga, evaluasi performa model dilakukan menggunakan metrik F1-score sebagai parameter utama. Terakhir, penelitian tidak menganalisis setiap fitur secara mendalam, tetapi hanya menggunakan fitur dasar press dan release time untuk menghasilkan lima fitur utama: UD, DD, DU, UU, dan Duration.

II. KAJIAN TEORI

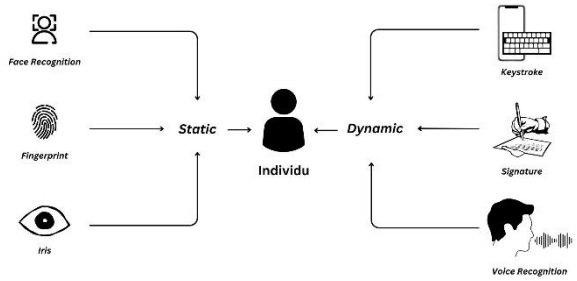
Menyajikan dan menjelaskan teori-teori yang berkaitan dengan variabel-variabel penelitian. Poin subjudul ditulis dalam abjad.

A. Evaluasi Penelitian Klasifikasi *Keystroke*

Penelitian terkait keystroke biometrik telah menggunakan berbagai algoritma klasifikasi untuk identifikasi pengguna. Ioannis Tsimperidis dkk. [7] mengevaluasi SVM, Random Forest, dan MLP pada dataset IKDD, dengan SVM mencapai F1-score tertinggi 0.705 untuk pengenalan kelompok usia. Yohan Muliono dkk. [11] meneliti SVM dengan berbagai kernel untuk otorisasi kata sandi, dengan kernel linear mencapai akurasi 0.712, sedangkan B. Radha Krishna dan Dr. M. Srihari Varma [8] menganalisis KNN dan XGB, di mana kombinasi KNN-XGB memperoleh F1-score tertinggi 0.75 dengan Fold tiga.

B. Biometrik

Biometrik adalah metode identifikasi atau autentikasi yang memanfaatkan karakteristik unik individu, baik fisik seperti sidik jari dan wajah, maupun perilaku seperti pola mengetik dan cara berjalan [6], [12]. Dibandingkan metode tradisional seperti kata sandi, biometrik lebih aman karena sulit dipalsukan dan tidak memerlukan penghafalan informasi tertentu [13], [14], [15]. Biometrik terbagi menjadi statis, yang mencakup ciri fisik tetap seperti sidik jari dan iris mata, serta dinamis, yang meliputi perilaku seperti pola mengetik dan suara [17], [18]. Meski lebih variabel, biometrik dinamis memiliki tingkat keamanan lebih tinggi karena sulit untuk direplikasi [12].



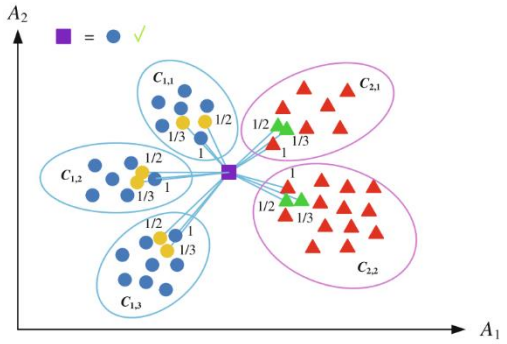
Gambar 1. Jenis Biometrik

C. User Adaptive Feature Extraction

Keystroke biometric adalah metode identifikasi atau autentikasi berbasis perilaku yang memanfaatkan pola unik seseorang saat mengetik, termasuk kecepatan, jeda antar karakter, dan tekanan tombol [18], [20]. Metode ini praktis karena tidak memerlukan perangkat keras tambahan dan dapat diterapkan pada perangkat yang sudah dimiliki pengguna, seperti komputer atau ponsel [21]. Data keystroke dapat dikategorikan menjadi monograph (Press dan Release) dan digraph (UD, UU, DU, DD, dan Duration), yang merepresentasikan waktu antar peristiwa tekan dan lepas tombol [21], [22]. User-Adaptive Feature Extraction digunakan untuk menyesuaikan karakteristik mengetik pengguna dengan mengelompokkan waktu pada digraph menjadi vektor n-dimensi, sehingga meningkatkan efektivitas identifikasi pengguna [22].

D. Multi-Voter Multi-Commission Nearest Neighbor

KNN memiliki kelemahan dalam menangani outlier karena keputusan klasifikasinya dipengaruhi oleh mayoritas tetangga terdekat yang mungkin tidak representatif [9], [10]. MVMCNN mengatasi masalah ini dengan menggabungkan skema multi-voter dan bobot tetangga dari LMPNN, serta membagi setiap kelas menjadi beberapa klaster (comission) untuk meningkatkan akurasi klasifikasi [11]. Dengan menghitung jarak total pada setiap comission dan memilih kelas dengan jarak terendah, MVMCNN lebih robust terhadap data yang kompleks dan beragam [11].



Gambar 2. Cara Kerja MVMCNN pada k=3

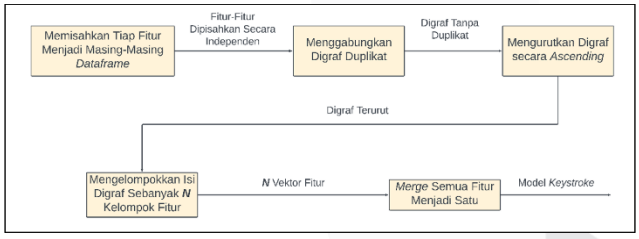
III. METODE

Memberikan gambaran rancangan penelitian yang meliputi prosedur atau langkah-langkah penelitian, waktu penelitian, sumber data, cara perolehan data dan menjelaskan metode yang akan digunakan dalam penelitian [10 pts].

A. Registrasi dan Identifikasi

Proses awal pengolahan dataset keystroke dimulai dengan membentuk monograf, yang merepresentasikan setiap tombol yang ditekan dan dilepaskan, lalu diubah ke dalam bentuk digraf untuk menganalisis interaksi antar tombol [22]. Dengan format digraf, fitur seperti UD, DD, DU, UU, dan Duration dapat dihitung untuk menggambarkan pola mengetik secara lebih representatif dan digunakan dalam proses user-adaptive [22].

B. User-Adaptive Feature Extraction



Gambar 3. Alur Sistem Keystroke MVMCNN

Tahap pertama dalam User-Adaptive Feature Extraction adalah memisahkan setiap fitur keystroke (UD, DD, DU, UU, dan Duration) ke dalam dataframe yang berbeda untuk memastikan setiap fitur dapat diproses secara terpisah tanpa saling mempengaruhi, sehingga masing-masing dapat merepresentasikan aspek spesifik dari pola mengetik pengguna, seperti waktu antar tombol dilepaskan (UU) atau waktu dari tombol pertama ditekan hingga tombol kedua dilepaskan.

Tabel 1. Contoh Digraf Duplikat

Digraf	UD (ms)	DD (ms)	DU (ms)	UU (ms)	Duration (ms)
(l, u)	100	89	421	871	254
(u, l)	167	221	187	341	431
(l, u)	312	135	793	123	627
(u, s)	812	766	421	111	331
...	...	..	...	...	...
(d, e)	1239	890	631	312	287

Pada Tabel 2, digraf yang muncul lebih dari sekali, seperti (l, u), dihitung rata-ratanya untuk menghasilkan satu nilai yang mewakili seluruh kemunculan.

Tabel 2. Digraf yang Sudah Dirata-ratakan

Digraf	UD (ms)	DD (ms)	DU (ms)	UU (ms)	Duration (ms)
(l, u)	206	112	607	497	440.5
(u, l)	167	221	187	341	431
(u, s)	812	766	421	111	331
...	...	..	...	...	...
(d, e)	1239	890	631	312	287

Kemudian digraf diurutkan secara ascending dan dilakukan pengelompokan berdasarkan masing-masing fitur secara individu. Setelah itu, dikelompokkan berdasarkan fitur-fitur dan dilakukan pengelempokkan N panjang vektor.

Tabel 3. Digraf Diurutkan Tiap Fitur.

Digraf	UD (ms)
(SPASI, c)	92
(u, l)	187
(u, s)	421
(c, u)	451
(l, u)	607
(s, SPASI)	631

Digraf	UU (ms)
(u, s)	111
(SPASI, c)	123
(s, SPASI)	312
(u, l)	341
(c, u)	387
(l, u)	497

Tabel 4. Contoh User-Adaptive yang Dikelompokkan Berdasarkan N.

F1	F2	F3
(SPASI, c)	(c, u)	(m, l)
(u, l)	(l, u)	
(u, s)	(s, SPASI)	

Tabel 5. Contoh User-Adaptive yang Berisi Value dari Tiap Fitur.

F1	F2	F3
92	451	689
187	607	
421	631	

Tabel 6. Contoh User-Adaptive yang Sudah Selesai.

F1	F2	F3
233.33	563	689

IV. HASIL DAN PEMBAHASAN

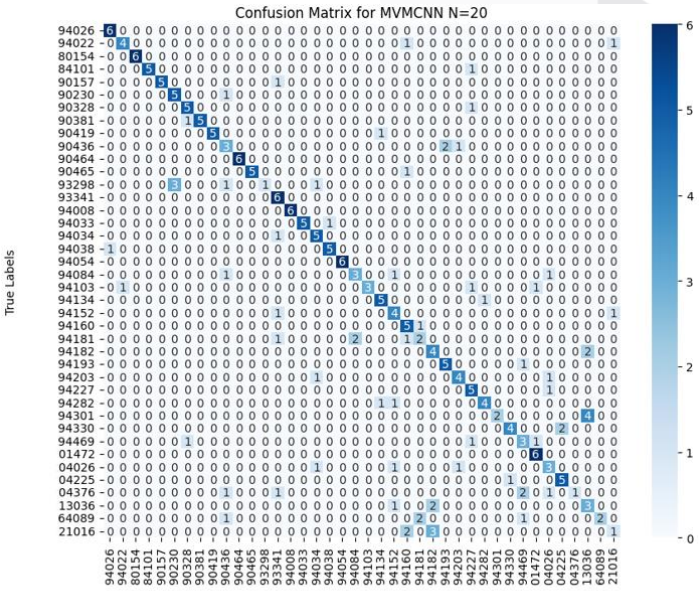
Evaluasi performansi sistem dilakukan menggunakan F1-Score untuk menilai keseimbangan precision dan recall dalam klasifikasi keystroke dynamics, dengan dataset terbagi 80% untuk pelatihan dan 20% untuk pengujian. Clustering menggunakan silhouette score dengan jumlah cluster maksimum sesuai jumlah sesi dalam data train. Tiga skenario pengujian diterapkan: (1) mengukur pengaruh jumlah data terhadap performa model, (2) menyederhanakan fitur waktu menjadi nilai rata-rata dan median untuk menilai dampaknya terhadap F1-Score, dan (3) menerapkan Variance Threshold (0.1) untuk seleksi fitur guna mengurangi dimensi data, diuji dengan k = 3, 5, 7, dan 9 dalam MVMCNN.

A. Skenario 1

Pengujian skenario pertama mengevaluasi nilai N optimal dengan membandingkan F1-Score pada variasi panjang vektor N (4, 8, 12, 16, 20, 24) dan menggunakan Silhouette Score untuk memperbaiki clustering lokal. Hasil menunjukkan bahwa MVMCNN mencapai F1-Score tertinggi pada N = 20 (0.691), sementara jumlah komisi bervariasi di setiap fitur, dengan optimasi yang lebih baik pada N = 8 dan 20. Detail hasil F1-Score dan jumlah komisi disajikan pada Tabel 7.

Tabel 7. Hasil Pengujian Skenario 1

N	***F1-Score***					
	UD	**DD**	**DU**	**UU**	***Duration***	**MVMCNN**
4	0.306240	0.362651	0.353718	0.306603	0.229554	0.601488
8	0.410851	0.450618	0.424053	0.404853	0.263170	0.667489
12	0.454911	0.448891	0.435501	0.408721	0.240446	0.646561
16	0.441514	0.461135	0.446586	0.392875	0.264230	0.645048
20	0.416272	0.440469	0.444954	0.429119	0.278066	**0.691136**
24	0.414310	0.481708	0.448877	0.418156	0.291885	0.684065



Gambar 4. Confussion Matrix Hasil Skenario 1

B. Skenario 2

Pengujian skenario kedua mengevaluasi dampak penyederhanaan fitur waktu menggunakan rata-rata dan median terhadap performansi model dengan N=20 dan variasi k (3, 5, 7, 9). Hasil F1-Score menunjukkan bahwa metode median umumnya lebih unggul dibandingkan mean, dengan nilai tertinggi pada k=3 (0.3257). Detail hasil pengujian disajikan pada Tabel 8.

Tabel 8. Hasil Pengujian Skenario 2

***N* = 20**		
k	***F1-Score* MVMCNN**	
	Median	**Mean**
3	0.325728	0.273221
5	0.271526	0.270943
7	0.260282	0.293241
9	0.247686	0.303099

C. Skenario 3

Skenario ketiga mengevaluasi dampak seleksi fitur menggunakan Variance Threshold (0.1) terhadap performansi model dengan N=20 dan variasi k (3, 5, 7, 9). Hasil F1-Score menunjukkan peningkatan akurasi dibandingkan skenario pertama, dengan nilai tertinggi pada k=5 (0.6913). Detail hasil pengujian disajikan pada Tabel 9.

Tabel 9. Hasil Pengujian Skenario 3

***N* = 20**	
k	**F1-Score MVMCNN with Feature Selection**
3	0.677285
5	**0.691282**
7	0.680233
9	0.667844

D. Analisis

Penambahan panjang vektor N dalam skenario pertama meningkatkan performa model, dengan F1-Score tertinggi (0.6911) pada N=20. Namun, peningkatan lebih lanjut (N=24) menyebabkan sedikit penurunan akibat noise dan redundansi fitur yang mengganggu pola klasifikasi. Clustering dengan Silhouette Score membantu dalam distribusi lokal fitur, tetapi jumlah komisi tidak selalu meningkat secara linier dengan N. Hasil ini menunjukkan bahwa N=20 memberikan keseimbangan optimal antara kompleksitas data dan informasi yang dibutuhkan model, menghindari overfitting sekaligus mempertahankan keakuratan prediksi.

Penyederhanaan fitur pada skenario kedua, menggunakan mean dan median, menyebabkan penurunan F1-Score karena hilangnya informasi granular yang penting dalam keystroke dynamics. Model kehilangan variasi temporal antar individu, mengurangi kemampuannya dalam membedakan pola unik. Sebaliknya, skenario ketiga yang menerapkan Variance Threshold (0.1) menunjukkan hasil hampir sama dengan skenario pertama, menandakan bahwa fitur yang dipertahankan sebelumnya sudah optimal. Ini menunjukkan bahwa seleksi fitur berbasis variabilitas tidak memberikan

peningkatan signifikan, karena model telah bekerja dengan informasi yang cukup tanpa fitur dengan variabilitas rendah.

V. KESIMPULAN

Penelitian ini berhasil mengimplementasikan metode MVMCNN pada sistem identifikasi pengguna berbasis keystroke dynamics menggunakan Biomey Keystroke Dataset dari Universitas Telkom. Model dievaluasi dengan F1-Score, mencapai nilai terbaik 0.6911 pada skenario pertama dengan panjang vektor N=20. Penyederhanaan fitur waktu pada skenario kedua menurunkan performa model karena hilangnya granularitas data, sementara seleksi fitur dengan Variance Threshold (0.1) pada skenario ketiga tidak memberikan peningkatan signifikan. Hasil ini menunjukkan bahwa granularitas data berperan penting dalam performa model dan bahwa penyederhanaan fitur tidak selalu meningkatkan akurasi. MVMCNN terbukti sebagai alternatif efektif untuk autentikasi biometrik, menawarkan solusi keamanan adaptif dibandingkan metode konvensional.

.

REFERENSI

[1] A. Tarter, "Importance of Cyber Security," in Community Policing - A European Perspective: Strategies, Best Practices and Guidelines, R. and A. B. and M. G. Bayerl P. Saskia and Karlović, Ed., Cham: Springer International Publishing, 2017, pp. 213–230. doi: 10.1007/978-3-319-53396-4_15.

[2] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," Future Generation Computer Systems, vol. 16, no. 4, pp. 351–359, 2000, doi: https://doi.org/10.1016/S0167-739X(99)00059- X.

[3] T. Sendjaja, Irwandi, E. Prastiawan, Y. Suryani, and E. Fatmawati, "Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks," International Journal of Science and Society, vol. 6, pp. 1008–1019, Jan. 2024, doi: 10.54783/ijsoc.v6i1.1098.

[4] R. Verma, "CYBERSECURITY CHALLENGES IN THE ERA OF DIGITAL TRANSFORMATION," 2024, p. 187. doi: 10.25215/9392917848.20.

[5] D. Gunetti and C. Picardi, "Keystroke analysis of free text," ACM Trans. Inf. Syst. Secur., vol. 8, no. 3, pp. 312–347, Aug. 2005, doi: 10.1145/1085126.1085129.

[6] A. Jain, P. Flynn, and A. Ross, Handbook of Biometrics. 2008. doi: 10.1007/978-0-387-71041-9.

[7] I. Tsimperidis, O.-D. Asvesta, E. Vrochidou, and G. A. Papakostas, "IKDD: A Keystroke Dynamics Dataset for User Classification," Information, vol. 15, no. 9, 2024, doi: 10.3390/info15090511.

[8] B. R. Krishna and M. S. Varma, "Enhancing User-Level Security: Performance Analysis of Machine Learning Algorithms for Dynamic Keystroke Analysis," J Theor Appl Inf Technol, vol. 101, no. 13, pp. 5313– 5323, 2023, [Online]. Available: http://www.jatit.org

[9] S. Suyanto, P. E. Yunanto, T. Wahyuningrum, and S. Khomsah, "A multi voter multi-commission nearest neighbor classifier," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 8, Part B, pp. 6292–6302, 2022, doi: https://doi.org/10.1016/j.jksuci.2022.01.018.

[10] S. Zhang, "Challenges in KNN Classification," IEEE Trans Knowl Data Eng, vol. 34, no. 10, pp. 4663–4675, Oct. 2022, doi: 10.1109/TKDE.2021.3049250.

[11] Y. Muliono, H. Ham, and D. Darmawan, "Keystroke Dynamic Classification using Machine Learning for Password Authorization," 39 Procedia Comput Sci, vol. 135, pp. 564–569, 2018, doi: https://doi.org/10.1016/j.procs.2018.08.209.

[12] S. Simske, "Dynamic biometrics: The case for a real-time solution to the problem of access control, privacy and security," in 2009 1st IEEE International Conference on Biometrics, Identity and Security, BIdS 2009, Jan. 2009, pp. 1–10. doi: 10.1109/BIDS.2009.5507535.

[13] J. Kim and P. Kang, "Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features," Pattern Recognit, vol. 108, p. 107556, 2020, doi: https://doi.org/10.1016/j.patcog.2020.107556.

[14] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz, "Quantifying the security of graphical passwords: The case of Android unlock patterns," in Proceedings of the ACM Conference on Computer and Communications Security, Jan. 2013, pp. 161–172. doi: 10.1145/2508859.2516700.

[15] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, "Secure Biometrics: Concepts, Authentication Architectures, and Challenges," IEEE Signal Process Mag, vol. 30, no. 5, pp. 51–64, Sep. 2013, doi: 10.1109/msp.2013.2261691.

[16] S. Dadakhanov, "Analyze and Development System with Multiple Biometric Identification," 2020. [Online]. Available: https://arxiv.org/abs/2004.04911

[17] B. Ducray, S. Cobourne, K. Mayes, and K. Markantonakis, "Comparison of dynamic biometrie security characteristics against other biometrics," Jan. 2017, pp. 1–7. doi: 10.1109/ICC.2017.7996938.

[18] P. S. Teh, A. B. J. Teoh, and S. Yue, "A survey of keystroke dynamics biometrics," ScientificWorldJournal, vol. 2013, p. 408280, 2013, doi: 10.1155/2013/408280.

[19] I. M. Al Anshori, Evaluasi User-Adaptive Fitur dalam Keystroke Biometric menggunakan Beragam Metode Distance Similarity. Bandung, Indonesia: Universitas Telkom, 2023.

[20] H. A. Boz, M. Gürkan, and B. Yanıkoğlu, "Keystroke Dynamics Based Biometric Identification," in 2020 28th Signal Processing and Communications Applications Conference (SIU), Oct. 2020, pp. 1–4. doi: 10.1109/SIU49456.2020.9302273.

[21] R. A. C. P. Hutomo, Multimodal Biometrik pada Keystroke User-Adaptive Feature dan Mahalanobis Distance. Katalog: Skripsi (S1), 2023.

[22] J. Kim, H. Kim, and P. Kang, "Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection," Appl Soft Comput, vol. 62, pp. 1077– 1087, 2018, doi: https://doi.org/10.1016/j.asoc.2017.09.045. 40

[23] D. J. Hand, P. Christen, and N. Kirielle, "F*: An Interpretable Transformation of the F-measure," 2021. [Online]. Available: https://arxiv.org/abs/2008.00103

[24] P. Christen, D. J. Hand, and N. Kirielle, "A Review of the F-Measure: Its History, Properties, Criticism, and

Alternatives," ACM Comput. Surv., vol. 56, no. 3, Oct. 2023, doi: 10.1145/3606367.

P. Yunanto and A. Barmawi, "Bimodal Keystroke Dynamics-Based Authentication for Mobile Application Using Anagram," Jurnal Ilmu Komputer dan Informasi, vol. 15, pp. 81–91, Jan. 2022, doi: 10.21609/jiki.v15i2.1015.