# BIBLIOGRAFÍA


[1] J. Pato y O. C. Center, "Identity management: Setting context," *Hewlett-Packard, Cambridge, MA*, 2003.

[2] B. F. Skinner, *Science and human behavior*, 92904. Simon y Schuster, 1953.

[3] M. Sidman, *Tactics of scientific research*. Basic Books, Incorporated, Pub., 1960.

[4] A. G. Martín, A. Fernández-Isabel, I. M. de Diego y M. Beltrán, "A survey for user behavior analysis based on machine learning techniques: current models and applications," *Applied Intelligence*, pp. 1-27, 2021.

[5] E. Gurarie, C. Bracis, M. Delgado, T. D. Meckley, I. Kojola y C. M. Wagner, "What is the animal doing? Tools for exploring behavioural structure in animal movements," *Journal of Animal Ecology*, vol. 85, n.º 1, pp. 69-84, 2016.

[6] J. Pacheco y S. Hariri, "Anomaly behavior analysis for IoT sensors," *Transactions on Emerging Telecommunications Technologies*, vol. 29, n.º 4, pp. 1-15, 2018.

[7] M. Pantic, A. Pentland, A. Nijholt y T. S. Huang, "Human computing and machine understanding of human behavior: a survey," en *Artifical Intelligence for Human Computing*, Springer, 2007, pp. 47-71.

[8] J. Navarro, I. M. de Diego, P. C. Pérez y F. Ortega, "Outlier detection in animal multivariate trajectories," *Computers and Electronics in Agriculture*, vol. 190, pp. 1-6, 2021.

[9] M. Xie, S. Han, B. Tian y S. Parvin, "Anomaly detection in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 34, n.º 4, pp. 1302-1325, 2011.

[10] M. Bohge y W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks," en *Proceedings of the 2nd ACM workshop on Wireless security*, ACM, 2003, pp. 79-87.

[11] R. A. LeVine, *Culture, behavior, and personality: An introduction to the comparative study of psychosocial adaptation*. Routledge, 2018.

[12] I. Carter, *Human behavior in the social environment: A social systems approach*. Routledge, 2017.

[13] W. Li y C. J. Mitchell, "Analysing the Security of Google's implementation of OpenID Connect," en *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, 2016, pp. 357-376.

[14] M. Miculan y C. Urban, "Formal analysis of Facebook Connect single sign-on authentication protocol," en *SOFSEM*, Citeseer, vol. 11, 2011, pp. 22-28.

[15] *Financial-grade API (FAPI)*, https://openid.net/wg/fapi/, Visitado: 2022-0504.

[16] D. Fett, R. Küsters y G. Schmitz, "The web sso standard openid connect: In-depth formal security analysis and security guidelines," en *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, IEEE, 2017, pp. 189-202.

[17] J. Navas y M. Beltrán, "Understanding and mitigating OpenID Connect threats," *Computers & Security*, vol. 84, pp. 1-16, 2019.

[18] A. G. Martín y M. Beltrán, "Mejora de la seguridad de esquemas de gestión de identidades federados mediante técnicas de User Behaviour Analytics," en *V Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2019)*, UEX, 2019, pp. 159-166.

[19] D. Recordon y D. Reed, "OpenID 2.0: a platform for user-centric identity management," en *Proceedings of the second ACM workshop on Digital identity management*, 2006, pp. 11-16.

[20] D. Hardt et al., *The OAuth 2.0 authorization framework*, 2012.

[21] N. Sakimura, J. Bradley, M. Jones, B. De Medeiros y C. Mortimore, "Openid connect core 1.0," *The OpenID Foundation*, pp. 1-85, 2014.

[22] E. Bertino y K. Takahashi, *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

[23] D. Gollmann, "Computer security," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 2, n.º 5, pp. 544-554, 2010.

[24] S. Samonas y D. Coss, "The CIA strikes back: Redefining confidentiality, integrity and availability in security.," *Journal of Information System Security*, vol. 10, n.º 3, 2014.

[25] A. Ometov, S. Bezzateev, N. Makitalo, S. Andreev, T. Mikkonen e Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, n.° 1, pp. 1-31, 2018.

[26] S. Ayeswarya y J. Norman, "A survey on different continuous authentication systems," *International Journal of Biometrics*, vol. 11, n.º 1, pp. 67-99, 2019.

[27] G. Saunders, M. Hitchens y V. Varadharajan, "An analysis of access control models," en *Australasian Conference on Information Security and Privacy*, Springer, 1999, pp. 281-293.

[28] S. Smalley, C. Vance y W. Salamon, "Implementing SELinux as a Linux security module," *NAI Labs Report*, vol. 1, n.º 43, pp. 1-58, 2001.

[29] M. Laurent y S. Bouzefrane, *Digital identity management*. Elsevier, 2015.

[30] K. Zeilenga et al., "Lightweight directory access protocol (ldap): Technical specification road map," RFC 4510, June, inf. téc., 2006.

[31] S. P. Miller, B. C. Neuman, J. I. Schiller y J. H. Saltzer, "Kerberos authentication and authorization system," en *In Project Athena Technical Plan*, Citeseer, 1988.

[32] C. Rigney, S. Willens, A. Rubens y W. Simpson, *Remote authentication dial in user service (RADIUS)*, 2000.

[33] E. Maler y D. Reed, "The venn of identity: Options and issues in federated identity management," *IEEE security & privacy*, vol. 6, n.º 2, pp. 16-23, 2008.

[34] A. Anderson y H. Lockhart, "SAML 2.0 profile of XACML," *OASIS, September*, vol. 51, n.º 1.4, 2004.

[35] E. Hammer-Lahav, D. Recordon y D. Hardt, "The oauth 1.0 protocol," RFC 5849, April, inf. téc., 2010.

[36] C. Mainka, V. Mladenov, J. Schwenk y T. Wich, "SoK: single sign-on security—an evaluation of openID connect," en *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2017, pp. 251-266.

[37] F. Yang y S. Manoharan, "A security analysis of the OAuth protocol," en *2013 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PA-CRIM)* , IEEE, 2013, pp. 271-276.

[38] E. Y. Chen, Y. Pei, S. Chen, Y. Tian, R. Kotcher y P. Tague, "Oauth demystified for mobile application developers," en *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, 2014, pp. 892-903.

[39] P. Hu, R. Yang, Y. Li y W. C. Lau, "Application impersonation: problems of OAuth and API design in online social networks," en *Proceedings of the second ACM conference on Online social networks*, 2014, pp. 271-278.

[40] R. Yang, G. Li, W. C. Lau, K. Zhang y P. Hu, "Model-based security testing: An empirical study on oauth 2.0 implementations," en *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 2016, pp. 651-662.

[41] J. Singh y N. K. Chaudhary, "OAuth 2.0: Architectural design augmentation for mitigation of common security vulnerabilities," *Journal of Information Security and Applications*, vol. 65, pp. 1-11, 2022.

[42] S. G. Morkonda, S. Chiasson y P. C. van Oorschot, "Empirical Analysis and Privacy Implications in OAuth-based Single Sign-On Systems," en *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, 2021, pp. 195-208.

[43] H. Halpin, "NEXTLEAP: Decentralizing identity with privacy for secure messaging," en *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1-10.

[44] R. Weingärtner y C. M. Westphall, "A design towards personally identifiable information control and awareness in OpenID Connect identity providers," en *2017 IEEE International Conference on Computer and Information Technology (CIT)*, IEEE, 2017, pp. 37-46.

[45] J. Werner y C. M. Westphall, "A model for identity management with privacy in the cloud," en *2016 IEEE Symposium on Computers and Communication (ISCC)*, IEEE, 2016, pp. 463-468.

[46] C. Villarán y M. Beltrán, "Protecting End User's Privacy When using Social Login through GDPR Compliance," 2021.

[47] G. Zachmann, "Mytoken-OpenID Connect Tokens for Long-term Authorization," Tesis doct., Karlsruher Institut für Technologie (KIT), 2021.

[48] A. Sharif, R. Carbone, G. Sciarretta y S. Ranise, "Best current practices for OAuth/OIDC Native Apps: A study of their adoption in popular providers and top-ranked Android clients," *Journal of Information Security and Applications*, vol. 65, pp. 1-18, 2022.

[49] Z. Cao, C. Chi, R. Hao e Y. Xiao, "User behavior modeling and traffic analysis of IMS presence servers," en *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*, IEEE, 2008, pp. 1-5.

[50] X. Kong, M. Li, T. Tang, K. Tian, L. Moreira-Matias y F. Xia, "Shared subway shuttle bus route planning based on transport data analytics," *IEEE Transactions on Automation Science and Engineering*, vol. 15, n.º 4, pp. 1507-1520, 2018.

[51] N. Ding, Q. He, C. Wu y J. Fetzer, "Modeling traffic control agency decision behavior for multimodal manual signal control under event occurrences," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, n.º 5, pp. 2467-2478, 2015.

[52] R. Faria, J. Sousa, A. Martins y J. Lagarto, "Modeling the strategic behavior of the iberian electricity market producers using time series analysis," en *2013 10th International Conference on the European Energy Market (EEM)*, IEEE, 2013, pp. 1-5.

[53] Y. Wang, Q. Chen, C. Kang y Q. Xia, "Clustering of electricity consumption behavior dynamics toward big data applications," *IEEE transactions on smart grid*, vol. 7, n.º 5, pp. 2437-2447, 2016.

[54] H. Alemdar, C. Tunca y C. Ersoy, "Daily life behaviour monitoring for health assessment using machine learning: bridging the gap between domains," *Personal and Ubiquitous Computing*, vol. 19, n.º 2, pp. 303-315, 2015.

[55] M. Manca, P. Parvin, F. Paterno y C. Santoro, "Detecting anomalous elderly behaviour in ambient assisted living," en *Proceedings of the ACM SIGCHI Symposium on Engineering Interactive Computing Systems*, 2017, pp. 63-68.

[56] A. Lotfi, C. Langensiepen, S. M. Mahmoud y M. J. Akhlaghinia, "Smart homes for the elderly dementia sufferers: identification and prediction of abnormal behaviour," *Journal of ambient intelligence and humanized computing*, vol. 3, n.º 3, pp. 205-218, 2012.

[57] N. Arbabzadeh y M. Jafari, "A data-driven approach for driving safety risk prediction using driver behavior and roadway information data," *IEEE transactions on intelligent transportation systems*, vol. 19, n.º 2, pp. 446-460, 2017.

[58] W. Zhang y Q. Fan, "Identification of abnormal driving state based on driver's model," en *ICCAS 2010*, IEEE, 2010, pp. 14-18.

[59] A. K. Sahu y P. Dwivedi, "User profile as a bridge in cross-domain recommender systems for sparsity reduction," *Applied Intelligence*, vol. 49, n.º 7, pp. 2461-2481, 2019.

[60] T. Bai, W. X. Zhao, Y. He, J.-Y. Nie y J.-R. Wen, "Characterizing and predicting early reviewers for effective product marketing on e-commerce

websites," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, n.º 12, pp. 2271-2284, 2018.

[61] M. Frank, R. Biedert, E. Ma, I. Martinovic y D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE transactions on information forensics and security*, vol. 8, n.º 1, pp. 136-148, 2013.

[62] C. Shen, Y. Li, Y. Chen, X. Guan y R. A. Maxion, "Performance analysis of multimotion sensor behavior for active smartphone authentication," *IEEE Transactions on Information Forensics and Security*, vol. 13, n.º 1, pp. 48-62, 2017.

[63] I. Firdausi, A. Erwin, A. S. Nugroho et al., "Analysis of machine learning techniques used in behavior-based malware detection," en *2010 second international conference on advances in computing, control, and telecommunication technologies*, IEEE, 2010, pp. 201-203.

[64] F. Pérez-Bueno, L. García, G. Maciá-Fernández y R. Molina, "Leveraging a Probabilistic PCA Model to Understand the Multivariate Statistical Network Monitoring Framework for Network Security Anomaly Detection," *IEEE/ACM Transactions on Networking* , 2022.

[65] P. Ravisankar, V. Ravi, G. R. Rao e I. Bose, "Detection of financial statement fraud and feature selection using data mining techniques," *Decision support systems*, vol. 50, n.º 2, pp. 491-500, 2011.

[66] U. Mahbub y R. Chellappa, "PATH: person authentication using trace histories," en *Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE Annual*, IEEE, 2016, pp. 1-8.

[67] C. Giuffrida, K. Majdanik, M. Conti y H. Bos, "I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics," en *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, 2014, pp. 92-111.

[68] Y. Li, H. Hu y G. Zhou, "Using data augmentation in continuous authentication on smartphones," *IEEE Internet of Things Journal*, vol. 6, n.º 1, pp. 628-640, 2018.

[69] H. T. Nguyen, C. L. Walker y E. A. Walker, *A first course in fuzzy logic*. CRC press, 2018.

[70] I. Brosso, A. La Neve, G. Bressan y W. V. Ruggiero, "A continuous authentication system based on user behavior analysis," en *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, IEEE, 2010, pp. 380-385.

[71] Y. Cai, H. Jiang, D. Chen y M.-C. Huang, "Online learning classifier based behavioral biometrie authentication," en *2018 IEEE 15th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, IEEE, 2018, pp. 62-65.

[72] L. Hernández-Álvarez, J. M. De Fuentes, L. González-Manzano y L. H. Encinas, "SmartCAMPP- Smartphone-based continuous authentication leveraging motion sensors with privacy preservation," *Pattern Recognition Letters*, vol. 147, pp. 189-196, 2021.

[73] J. M. de Fuentes, L. Gonzalez-Manzano y A. Ribagorda, "Secure and Usable User-in-a- Context Continuous Authentication in Smartphones Leveraging Non-Assisted Sensors," *Sensors*, vol. 18, n.º 4, p. 1219, 2018.

[74] C. Liu y J. He, "Access control to web pages based on user browsing behavior," en *Communication Software and Networks (ICCSN), 2017 IEEE 9th International Conference on*, IEEE, 2017, pp. 1016-1020.

[75] H. Gomi, S. Yamaguchi, K. Tsubouchi y N. Sasaya, "Continuous Authentication System Using Online Activities," en *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, IEEE, 2018, pp. 522-532.

[76] P. Zhao, C. Yan y C. Jiang, "Authenticating Web User's Identity through Browsing Sequences Modeling," en *Data Mining Workshops (ICDMW), 2016 IEEE 16th International Conference on*, IEEE, 2016, pp. 335-342.

[77] I. Molloy, L. Dickens, C. Morisset, P.-C. Cheng, J. Lobo y A. Russo, "Risk-based security decisions under uncertainty," en *Proceedings of the second ACM conference on Data and Application Security and Privacy*, ACM, 2012, pp. 157-168.

[78] Z. Lu e Y. Sagduyu, "Risk assessment based access control with text and behavior analysis for document management," en *Military Communications Conference, MILCOM 2016-2016 IEEE*, IEEE, 2016, pp. 37-42.

[79] B. Rožac, R. Sernec, A. Košir y A. Kos, "User behavior analysis based on Identity management systems' log data," *Machine learning*, vol. 143, pp. 1-5, 2012.

[80] M. Misbahuddin, B. Bindhumadhava y B. Dheeptha, "Design of a risk based authentication system using machine learning techniques," en *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*, IEEE, 2017, pp. 1-6.

[81] R. S. Gaines, W. Lisowski, S. J. Press y N. Shapiro, "Authentication by keystroke timing: Some preliminary results," Rand Corp Santa Monica CA, inf. téc., 1980.

[82] S. Bleha, C. Slivinsky y B. Hussien, "Computer-access security systems using keystroke dynamics," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 12, n.º 12, pp. 1217-1222, 1990.

[83] S. Cho, C. Han, D. H. Han y H.-I. Kim, "Web-based keystroke dynamics identity verification using neural network," *Journal of organizational computing and electronic commerce*, vol. 10, n.º 4, pp. 295-307, 2000.

[84] F. Monrose y A. Rubin, "Authentication via keystroke dynamics," en *Proceedings of the 4th ACM Conference on Computer and Communications Security*, 1997, pp. 48-56.

[85] K. S. Killourhy y R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," en *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*, IEEE, 2009, pp. 125-134.

[86] A. Alsultan, K. Warwick y H. Wei, "Non-conventional keystroke dynamics for user authentication," *Pattern Recognition Letters*, vol. 89, pp. 53-59, 2017.

[87] J. Kim, H. Kim y P. Kang, "Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection," *Applied Soft Computing*, vol. 62, pp. 1077-1087, 2018.

[88] K. S. Balagani, V. V. Phoha, A. Ray y S. Phoha, "On the discriminability of keystroke feature vectors used in fixed text keystroke authentication," *Pattern Recognition Letters*, vol. 32, n.º 7, pp. 1070-1080, 2011.

[89] O. Alpar, "Frequency spectrograms for biometric keystroke authentication using neural network based classifier," *Knowledge-Based Systems*, vol. 116, pp. 163-171, 2017.

[90] L. Xiaofeng, Z. Shengfei e Y. Shengwei, "Continuous authentication by free-text keystroke based on CNN plus RNN," *Procedia computer science*, vol. 147, pp. 314-318, 2019.

[91] Y. Sun, H. Ceker y S. Upadhyaya, "Shared keystroke dataset for continuous authentication," en *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, IEEE, 2016, pp. 1-6.

[92] J. Huang, D. Hou, S. Schuckers, T. Law y A. Sherwin, "Benchmarking keystroke authentication algorithms," en *2017 IEEE Workshop on Information Forensics and Security (WIFS)*, IEEE, 2017, pp. 1-6.

[93] B. Ayotte, M. Banavar, D. Hou y S. Schuckers, "Fast Free-text Authentication via Instance-based Keystroke Dynamics," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 2, n.º 4, pp. 377-387, 2020.

[94] R. A. Everitt y P. W. McOwan, "Java-based internet biometric authentication system," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, n.º 9, pp. 1166-1172, 2003.

[95] A. A. E. Ahmed e I. Traore, "A new biometric technology based on mouse dynamics," *IEEE Transactions on dependable and secure computing*, vol. 4, n.º 3, pp. 165-179, 2007.

[96] P. Chong, Y. Elovici y A. Binder, "User authentication based on mouse dynamics using deep neural networks: A comprehensive study," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1086-1101, 2019.

[97] C. Shen, Z. Cai, X. Guan, Y. Du y R. A. Maxion, "User authentication through mouse dynamics," *IEEE Transactions on Information Forensics and Security*, vol. 8, n.º 1, pp. 16-30, 2012.

[98] D. Qin, S. Fu, G. Amariucai, D. Qiao e Y. Guan, "MAUSPAD: Mouse-based Authentication Using Segmentation-based, Progress-Adjusted DTW," en *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, IEEE, 2020, pp. 425-433.

[99] T. Hu, W. Niu, X. Zhang, X. Liu, J. Lu e Y. Liu, "An insider threat detection approach based on mouse dynamics and deep learning," *Security and Communication Networks*, vol. 2019, 2019.

[100] A. Ross y A. Jain, "Information fusion in biometrics," *Pattern recognition letters*, vol. 24, n.º 13, pp. 2115-2125,2003.

[101] S. Mondal y P. Bours, "A study on continuous authentication using a combination of keystroke and mouse biometrics," *Neurocomputing*, vol. 230, pp. 1-22, 2017.

[102] L. Fridman et al., "Multi-modal decision fusion for continuous authentication," *Computers & Electrical Engineering*, vol. 41, pp. 142-156, 2015.

[103] S. Salmeron-Majadas, R. S. Baker, O. C. Santos y J. G. Boticario, "A machine learning approach to leverage individual keyboard and mouse interaction behavior from multiple users in real-world learning scenarios," *IEEE Access*, vol. 6, pp. 39 154-39 179, 2018.

[104] J. Solano, L. Camacho, A. Correa, C. Deiro, J. Vargas y M. Ochoa, "Combining behavioral biometrics and session context analytics to enhance risk-based static authentication in web applications," *International Journal of Information Security*, vol. 20, n.º 2, pp. 181-197,2021.

[105] A. Harilal et al., "The Wolf Of SUTD (TWOS): A Dataset of Malicious Insider Threat Behavior Based on a Gamified Competition.," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 9, n.º 1, pp. 54-85, 2018.

[106] X. Wang, Q. Zheng, K. Zheng y T. Wu, "User Authentication Method Based on MKL for Keystroke and Mouse Behavioral Feature Fusion," *Security and Communication Networks*, vol. 2020, 2020.

[107] K. O. Bailey, J. S. Okolica y G. L. Peterson, "User identification and authentication using multi-modal behavioral biometrics," *Computers & Security*, vol. 43, pp. 77-89, 2014.

[108] Y. Li, B. Zou, S. Deng y G. Zhou, "Using feature fusion strategies in continuous authentication on smartphones," *IEEE Internet Computing*, vol. 24, n.º 2, pp. 49-56, 2020.

[109] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi e I. Lai, "Combining mouse and keystroke dynamics biometrics for risk-based authentication in web environments," en *2012 fourth international conference on digital home*, IEEE, 2012, pp. 138-145.

[110] A. G. Martín, M. Beltrán, A. Fernández-Isabel e I. M. de Diego, "An approach to detect user behaviour anomalies within identity federations," *Computers & Security*, vol. 1-18, p. 102356, 2021.

[111] L. Hernández-Álvarez, J. M. de Fuentes, L. González-Manzano y L. Hernández Encinas, "Privacy-preserving sensor-based continuous authentication and user profiling: a review," *Sensors*, vol. 21, n.º 1, pp. 92-115, 2020.

[112] A. Vastel, P. Laperdrix, W. Rudametkin y R. Rouvoy, "Fp-scanner: The privacy implications of browser fingerprint inconsistencies," en *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 135-150.

[113] M. Beltrán, "Identifying, authenticating and authorizing smart objects and end users to cloud services in Internet of Things," *Computers & Security*, vol. 77, pp. 595-611, 2018.

[114] R. Magán-Carrión, J. Camacho, G. Maciá-Fernández y Á. Ruíz-Zafra, "Multivariate Statistical Network Monitoring-Sensor: An effective tool for real-time monitoring and anomaly detection in complex networks and systems," *International Journal of Distributed Sensor Networks*, vol. 16, n.º 5, pp. 1-14, 2020.

[115] A. Gómez-Boix, P. Laperdrix y B. Baudry, "Hiding in the crowd: an analysis of the effectiveness of browser fingerprinting at large scale," en *Proceedings of the 2018 world wide web conference*, 2018, pp. 309-318.

[116] P. Laperdrix, N. Bielova, B. Baudry y G. Avoine, "Browser fingerprinting: A survey," *ACM Transactions on the Web (TWEB)*, vol. 14, n.º 2, pp. 1-33, 2020.

[117] M. Abuhamad, A. Abusnaina, D. Nyang y D. Mohaisen, "Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey," *IEEE Internet of Things Journal*, vol. 8, n.º 1, pp. 65-84, 2020.

[118] M. Bhatnagar, R. K. Jain y N. S. Khairnar, "A Survey on Behavioral Biometric Techniques: Mouse vs Keyboard Dynamics," *Int. J. Comput. Appl*, vol. 975, pp. 1-5, 2013.

[119] C. Chio y D. Freeman, *Machine learning and security: Protecting systems with data and algorithms*. .ºReilly Media, Inc.", 2018.

[120] V. Kozitsin, I. Katser y D. Lakontsev, "Online Forecasting and Anomaly Detection Based on the ARIMA Model," *Applied Sciences*, vol. 11, n.º 7, pp. 1-13, 2021.

[121] S. Hariri, M. C. Kind y R. J. Brunner, "Extended isolation forest," *IEEE Transactions on Knowledge and Data Engineering*, vol. 33, n.º 4, pp. 1479-1489, 2019.

[122] Z. Cheng, C. Zou y J. Dong, "Outlier detection using isolation forest and local outlier factor," en *Proceedings of the conference on research in adaptive and convergent systems*, 2019, pp. 161-168.

[123] E. Schubert, J. Sander, M. Ester, H. P. Kriegel y X. Xu, "DBSCAN revisited, revisited: why and how you should (still) use DBSCAN," *ACM Transactions on Database Systems (TODS)*, vol. 42, n.º 3, pp. 1-21, 2017.

[124] T. Shimshon, R. Moskovitch, L. Rokach e Y. Elovici, "Clustering di-graphs for continuously verifying users according to their typing patterns," en *2010 IEEE 26-th Convention of Electrical and Electronics Engineers in Israel*, IEEE, 2010, pp. 445-449.

[125] B. Tang, Q. Hu y D. Lin, "Reducing false positives of user-to-entity first-access alerts for user behavior analytics," en *2017 IEEE International Conference on Data Mining Workshops (ICDMW)*, IEEE, 2017, pp. 804-811.

[126] J. Yan, Y. Qi, Q. Rao y S. Qi, "Towards a user-friendly and secure hand shaking authentication for smartphones," en *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, IEEE, 2018, pp.1170-1179.

[127] Z. C. Lipton, C. Elkan y B. Narayanaswamy, "Thresholding classifiers to maximize F1 score," *Machine Learning and Knowledge Discovery in Databases*, vol. 8725, pp. 225-239, 2014.

[128] S. Eberz, K. B. Rasmussen, V. Lenders e I. Martinovic, "Evaluating behavioral biometrics for continuous authentication: Challenges and metrics," en *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017, pp. 386-399.

[129] I. M. De Diego, A. R. Redondo, R. R. Fernández, J. Navarro y J. M. Moguerza, "General Performance Score for classification problems," *Applied Intelligence*, 2022.

[130] A. G. Martín, I. M. de Diego, A. Fernández-Isabel, M. Beltrán y R. R. Fernández, "Combining user behavioural information at the feature level to enhance continuous authentication systems," *Knowledge-Based Systems*, pp. 1-13, 2022.

[131] Y. Sun, J. Li, J. Liu, B. Sun y C. Chow, "An improvement of symbolic aggregate approximation distance measure for time series," *Neurocomputing*, vol. 138, pp. 189-198, 2014.

[132] P. Geurts, D. Ernst y L. Wehenkel, "Extremely randomized trees," *Machine learning*, vol. 63, n.º 1, pp. 3-42, 2006.

[133] F. Moosmann, B. Triggs y F. Jurie, "Fast discriminative visual codebooks using randomized clustering forests," en *Twentieth Annual Conference on Neural Information Processing Systems (NIPS'06)*, MIT Press, 2006, pp. 985-992.

[134] M. G. Baydogan y G. Runger, "Learning a symbolic representation for multivariate time series classification," *Data Mining and Knowledge Discovery*, vol. 29, n.º 2, pp. 400-422, 2015.

[135] M. P. Van der Loo et al., "The stringdist package for approximate string matching.," *R J.*, vol. 6, n.º 1,pp. 1-13,2014.

[136] H. Li y N. Homer, "A survey of sequence alignment algorithms for next-generation sequencing," *Briefings in bioinformatics*, vol. 11, n.º 5, pp. 473-483, 2010.

[137] C. Trapnell y M. C. Schatz, "Optimizing data intensive GPGPU computations for DNA sequence alignment," *Parallel computing*, vol. 35, n.º 8-9, pp. 429-440, 2009.

[138] J. Cheetham, F. Dehne, S. Pitre, A. Rau-Chaplin y P. J. Taillon, "Parallel clustal w for pc clusters," en *International Conference on Computational Science and Its Applications*, Springer, 2003, pp. 300-309.

[139] X. Huang y K.-M. Chao, "A generalized global alignment algorithm," *Bioinformatics*, vol. 19, n.º 2, pp. 228-233, 2003.

[140] H. Abdi, "Metric multidimensional scaling (MDS): analyzing distance matrices," *Encyclopedia of measurement and statistics*, pp. 1-13, 2007.

[141] F. Klinker, "Exponential moving average versus moving exponential average," *Mathe- matische Semesterberichte*, vol. 58, n.º 1, pp. 97-107, 2011.

[142] *let's chat*, https://sdelements.github.io/lets-chat, Visitado: 2022-05-04.

[143] M. Cantelon, M. Harter, T. Holowaychuk y N. Rajlich, *Node. js in Action*. Manning Greenwich, 2014.

[144] *Mongodb*, https://www.mongodb.com/, Visitado: 2022-05-04.

[145] L. A. Leiva y R. Vivó, "Web browsing behavior analysis and interactive hypervideo," *ACM Transactions on the Web (TWEB)*, vol. 7, n.º 4, pp. 1-28, 2013.

[146] *OpenAM*, https://backstage.forgerock.com/docs/openam/13.5/, Visitado: 2022-05-04.

[147] Martín, Alejandro G and Beltrán, Marta and Fernández-Isabel, Alberto and de Diego, Isaac Martín, "Keystroke and Mouse Dynamics for UEBA Dataset, Mendeley Data, v2," 2020.

[148] J. Ho y D.-K. Kang, "One-class Naïve Bayes with duration feature ranking for accurate user authentication using keystroke dynamics," *Applied Intelligence*, vol. 48, n.º 6, pp. 1547-1564, 2018.

[149] Y. Zhao, "Learning user keystroke patterns for authentication," *Proceedings of the world academy of science, engineering and technology*, vol. 14, pp. 65-70, 2006.

[150] M. Malkauthekar, "Analysis of Euclidean distance and Manhattan distance measure in Face recognition," en *Third International Conference on Computational Intelligence and Information Technology (CIIT 2013)*, IET, 2013, pp. 503-507.

[151] T. Lodderstedt, S. Dronia y M. Scurtescu, *OAuth 2.0 token revocation*, 2013.