REFERENCES

[1] M. Akintolu and S. E. Adewoye, "Systematic Review of the Role of Open and Distance Education in Achieving the Sustainable Development Goals (SDGs)," *Int. J. Learn. Teach. Educ. Res.*, vol. 23, no. 12, pp. 113–129, Dec. 2024.

[2] A. Afolabi, H. A. Fatoye, A. Abiodun, and A. A. Adewole, "Emerging opportunities in the open and distance education and e-learning platforms in Nigeria," in *Proc. Int. Stakeholders' Conf. Enhancing Inclusive Equitable Quality Educ. Through Open Distance Educ.*, Ibadan, Nigeria, Dec. 2021,

[3] A. Qayyum and O. Zawacki-Richter, *Open and Distance Education in a Digital Age* (SpringerBriefs in Education). Cham, Switzerland: Springer, 2018, pp. 1–8.

[4] "Assessing large cohorts," Bristol Inst. Learn. Teach. Blog, Oct. 14, 2019. [Online]. Available: https://bilt.online/assessing-large-cohorts-2/ (accessed Feb. 12, 2025).

[5] P. van Vliet, "Scaling up student assessment: Issues and solutions," DigitalCommons@University of Nebraska - Lincoln, 2018. [Online]. Available: http://digitalcommons.unl.edu/ipts/27 (accessed Feb. 12, 2025).

[6] O. L. Holden, M. E. Norris, and V. A. Kuhlmeier, "Academic integrity in online assessment: A research review," *Front. Educ.*, vol. 6, pp. 1–13, Jul. 2021.

[7] J. R. Young, "Online Classes See Cheating go high-tech," *Chron. High. Educ.*, Jun. 2012. [Online]. Available:https://www.chronicle.com/article/online-classes-see-cheating-go-high-tech/

[8] J. Adkins, C. Kenkel, and C. L. Lim, "Deterrents to online academic dishonesty," *Int. J. Learn. High. Educ.*, vol. 1, no. 1, pp. 17–22, Jan. 2005. [Online]. Available:https://digitalcommons.butler.edu/cgi/viewcontent.cgi?article=1190&context=cob_papers

[9] D. Vincent, "Promoting Academic Integrity in Assessment in Online Distance Learning," Technology-Mediated Learning, Sep. 22, 2013. [Online]. Available: https://journals.library.mun.ca/index.php/TML/article/view/835

[10] T. B. Michael and M. A. Williams, "Student equity: Discouraging cheating in online courses," *Admin. Issues J. Educ. Pract. Res.*, vol. 3, no. 2, pp. 1–12, Oct. 2013.

[11] N. Chadaga, "Lockdown browser," HackerEarth, 2024. [Online]. Available: https://www.hackerearth.com/recruit/glossary/lockdown-browser/ (accessed Mar. 15, 2024).

[12] K. Mugambi, J. Sansa-Otim, and T. Bulega, "Student and e-assessment authentication in distance learning," *RUFORUM Working Document Series*, no. 14, pt. 3, pp. 65–70, 2016.

[13] D. Temoshok, J. Fenton, Y.-Y. Choong, N. Lefkovitz, A. Regenscheid, R. Galluzzo, and J. Richer, *Digital Identity Guidelines - Authentication and Authenticator Management*, NIST Special Publication SP 800-63B-4, Jul. 2025.

[14] N. Chourasia and P. Joeg, "Authenticate user by keystroke dynamics," *Int. J. Eng. Res. Technol. (IJERT)*, vol. 3, no. 4, pp. 1239–1241, Apr. 2014.

[15] A. A. E. Ahmed and I. Traoré, "A new biometric technology based on mouse dynamics," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 3, pp. 165–179, Jul.–Sep. 2007.

[16] C. A. Fidas, M. Belk, A. Constantinides, D. Portugal, P. Martins, A. M. Pietron, A. Pitsillides, and N. Avouris, "Ensuring academic integrity and trust in online learning environments: A longitudinal study of an AI-centered proctoring system in tertiary educational institutions," *Educ. Sci.*, vol. 13, no. 6, p. 566, Jun. 2023.

[17] B. Fang, "Addressing academic dishonesty in the age of ubiquitous technology," EDUCAUSE Rev., Sep. 5, 2012. [Online]. Available: https://er.educause.edu/articles/2012/9/addressing-academic-dishonesty-in-the-age-of-ubiquitous-technology (accessed Jan. 3, 2025).

[18] D. L. McCabe, L. K. Trevino, and K. D. Butterfield, "Cheating in academic institutions: A decade of research," *Ethics Behav.*, vol. 11, no. 3, pp. 219–232, 2001.

[19] A. R. But, Z. Ahmad, R. F. Ali, and Q. Iqbal, "Academic integrity: A five-decade journey, from cheating to a lack of understanding of academic dishonesty," *J. Excell. Soc. Sci.*, vol. 3, no. 3, pp. 211–231, 2024.

[20] T. Bretag, S. Mahmud, M. Wallace, R. Walker, C. James, M. Green, J. East, U. McGowan, and L. Patridge, "Core elements of exemplary academic integrity policy in Australian higher education," *Int. J. Educ. Integr.*, vol. 7, no. 2, pp. 3–12, 2011.

[21] K. Sevnarayan and K. B. Maphoto, "Exploring the dark side of online distance learning: Cheating behaviours, contributing factors, and strategies to enhance the integrity of online assessment," *J. Acad. Ethics*, vol. 22, pp. 51–70, 2024.

[22] K. Mate and J. Weidenhofer, "Considerations and strategies for effective online assessment with a focus on the biomedical sciences," *FASEB Bioadv.*, vol. 4, no. 1, pp. 9–21, Oct. 2021.

[23] C. M. Kell, Y. Thandar, A. K. Bhundoo, F. Haffejee, B. Mbhele, and J. Ducray, "Academic integrity in the information age: insights from health sciences students at a South African University," *J. Appl. Res. High. Educ.*, vol. 17, no. 7, pp. 16–28, 2025.

[24] C. L. Huang, X. Shao, C. Wu, and S. C. Yang, "Navigating the digital learning landscape: insights into ethical dilemmas and academic misconduct among university students," *Int. J. Educ. Technol. High. Educ.*, vol. 22, Art. no. 29, 2025.

[25] C. K. Y. Chan, "Is AI changing the rules of academic misconduct? An in-depth look at students' perceptions of 'AI-giarism,'" *arXiv preprint arXiv:2306.03358*, 2023.

[26] National Center for Education Statistics, "Testing Integrity: Issues and Recommendations for Best Practice," U.S. Department of Education, Washington, DC, USA, Rep. NCES 2013-454, Feb. 2013. [Online]. Available: https://ies.ed.gov/use-work/resource-library/report/issue-brief/testing-integrity-issues-and-recommendations-best-practice

[27] S. Pudasaini, L. Miralles-Pechuán, D. Lillis, and M. L. Salvador, "Survey on plagiarism detection in large language models: The impact of ChatGPT and Gemini on academic integrity," *arXiv preprint arXiv:2407.13105*, 2024.

[28] D. Kundu, A. Mehta, R. Kumar, N. Lal, A. Anand, A. Singh, and R. R. Shah, "Keystroke dynamics against academic dishonesty in the age of LLMs," *arXiv preprint arXiv:2406.15335*, 2024.

[29] F. Sabrina, S. Azad, S. Sohail, and S. Thakur, "Ensuring academic integrity in online assessments: A literature review and recommendations," *Int. J. Inf. Educ. Technol.*, vol. 12, no. 1, pp. 60–68, Jan. 2022.

[30] R. Hamaamin, O. A. Ali, and S. Kareem, "Biometric systems: A comprehensive review," *Basrah J. Sci.*, vol. 42, no. 1, pp. 146–167, Apr. 2024.

[31] *Biometrics and Standards*, ITU-T Technology Watch Report, International Telecommunication Union, Geneva, Switzerland, Dec. 2009.

[32] F. Galton, "Personal identification and description," *J. Anthropol. Inst. Great Britain Ireland*, vol. 18, pp. 177–191, 1889.

[33] F. Galton, *Finger Prints*. London, UK: Macmillan & Co., 1892, p. 3. 1892

[34] R. B. Hill and R. L. Laub, "Method of identifying individuals by means of the pattern of blood vessels of the retina," U.S. Patent 3,937,953, Feb. 10, 1976.

[35] L. Flom and A. Safir, "Iris recognition system," U.S. Patent 4,641,349, Feb. 3, 1987.

[36] I. Alsaadi, "Physiological biometric authentication systems, advantages, disadvantages and future development: A review," *Int. J. Sci. Technol. Res.*, vol. 4, no. 12, pp.285-289, Oct. 2015.

[37] J. Galbally, J. Fierrez, R. Cappelli, and G. Marcialis, "Introduction to presentation attack detection in fingerprint biometrics," in *Handbook of Biometric Anti-Spoofing*, S. Marcel, J. Fierrez, and N. Evans, Eds. Cham, Switzerland: Springer, Seattle, WA, USA, 2022, pp. 3–16.

[38] M. Sharma and H. Elmiligi, "Behavioral biometrics: Past, present and future," in *Recent Advances in Biometrics*, BoD – Books on Demand, Mar.2022, ch. 4, pp. 1–20. DOI: 10.5772/intechopen.102841

[39] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: a survey and classification," *Int. J. Biom.*, vol. 1, no. 1, pp. 81–113, 2008.

[40] "Behavioural biometrics," ENISA, Europa.eu, 2025. [Online]. Available: https://www.enisa.europa.eu/publications/behavioural-biometrics (accessed Aug. 13, 2025).

[41] M. El-Abed, R. Giot, B. Hemery, and C. Rosenberger, "A study of users' acceptance and satisfaction of biometric systems," in *Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST)*, Location Unknown, Oct. 2010, pp. 170–178. doi.org/10.1504/IJBM.2008.018665

[42] P. S. Teh, A. B. J. Teoh, and S. Yue, "A survey of keystroke dynamics biometrics," *Sci. World J.*, vol. 2013, pp. 1–24, 2013.

[43] M. Helander, *A Guide to Human Factors and Ergonomics*. Boca Raton, FL, USA: CRC Press, 2005.

[44] O. Ciobanu, C. C. Gavat, and R. Cozmei, "The keyboard remains the least ergonomically designed computer device," in *Proc. 5th IEEE Int. Conf. E-Health Bioeng. (EHB)*, Iasi, Romania, Nov. 2015, pp. 1–4.

[45] S. P. Banerjee and D. L. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," *J. Pattern Recognit. Res.*, vol. 7, no. 1, pp. 116–139, Jan. 2012.

[46] R. Giot, M. El-Abed, and C. Rosenberger, "Keystroke dynamics overview," ResearchGate, Jun. 2011. [Online]. Available: https://www.researchgate.net/publication/221912833_Keystroke_Dynamics_Overview (accessed Feb. 12, 2025).

[47] H. Nonaka and M. Kurihara, "Sensing pressure for authentication system using keystroke dynamics," in *Proc. Int. Conf. Comput. Intell. (ICCI)*, Istanbul, Turkey, Dec. 2004, pp. 19-22.

[48] P. H. Pisani and A. C. Lorena, "A systematic review on keystroke dynamics," *J. Brazilian Comput. Soc.*, vol. 23, no. 5, pp. 428–440, Jul. 2013.

[49] B. Sayed, I. Traore, I. Woungang, and M. Obaidat, "Biometric authentication using mouse gesture dynamics," *IEEE Syst. J.*, vol. 7, no. 2, pp. 262–274, Jun. 2013.

[50] S. Khan, C. Devlen, M. Manno, and D. Hou, "Mouse dynamics behavioral biometrics: A survey,"*ACM Computing Surveys*, vol. 56, no. 6, Art. no. 154, Aug. 2022, pp.1-33, [Online]. Available: https://doi.org/10.1145/364031

[51] H. Gamboa and A. L. N. Fred, "A behavioral biometric system based on human-computer interaction," in *Proc. SPIE - Int. Soc. Opt. Eng.*, vol.5404, Aug. 2004, pp. 381-392.doi: 10.1117/12.541419.

[52] T.-Y. Chang, J. C. Tsai, Y.-J. Yang, and P.-C. Cheng, "User authentication using rhythm click characteristics for non-keyboard devices," in *Proc. Int. Conf. Asia Agriculture Animal (IPCBEE)*, Hong Kong, Jan. 2011, pp. 114-118.

[53] S. Cho, C. Han, D. H. Han, and H.-I. Kim, "Web based keystroke dynamics identity verification using neural network," *J. Organ. Comput. Electron. Commerce*, vol. 10, no. 4, pp. 295–307, Dec. 2000.

[54] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in *Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Lisbon, Portugal, Aug. 2009, pp. 23–32.

[55] A. Wahab, D. Hou, and S. Schuckers, "A user study of keystroke dynamics as second factor in web MFA," in *Proc. 13th ACM Conf. Data Appl. Secur. Privacy (CODASPY '23)*, Charlotte, NC, USA, Apr. 2023, pp. 61–72.

[56] B. Glass, G. Jenkinson, Y. Liu, M. A. Sasse, and F. Stajano, "The usability canary in the security coal mine: A cognitive framework for evaluation and design of usable authentication solutions," *arXiv preprint arXiv:1607.03394*, 2016.

[57] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," *Future Gener. Comput. Syst.*, vol. 16, no. 4, pp. 351–359, Feb. 2000.

[58] R. Giot, M. El-Abed, and C. Rosenberger, "Keystroke dynamics with low constraints SVM based passphrase enrollment," in *Proc. IEEE 3rd Int. Conf. Biom.: Theory, Appl. Syst. (BTAS)*, Washington, DC, USA, 2009, pp. 1–6.

[59] I. Sluganovic, A. Karlovic, P. Bosilj, S. Horvat, and M. Sare, "User authentication based on keystroke dynamics analysis," in *Proc. 35th Int. Conv. MIPRO*, Opatija, Croatia, May 2012, pp. 2136–2141.

[60] L. C. F. Araújo, L. H. R. Sucupira, M. G. Lizarraga, L. L. Ling, and J. B. T. Yabu-Uti, "User authentication through typing biometrics features," *IEEE Trans. Signal Process.*, vol. 53, no. 2, pp. 851–855, Feb. 2005.

[61] A. K. Jain, S. C. Dass, and K. Nandakumar, "Soft biometric traits for personal recognition systems," in *Biometric Authentication* (ICBA 2004), D. Zhang and A. K. Jain, Eds. (Lecture Notes in Computer Science, vol. 3072). Berlin, Heidelberg, Germany: Springer, 2004, pp.731-738.

[62] O. Arigbabu, S. Ahmad, W. Adnan, S. Yussof, V. Iranmanesh, and F. Malalla, "Estimating body related soft biometric traits in video frames," *The Scientific World Journal*, vol. 2014, Art. no. 460973, Jul. 2014.

[63] R. Giot and C. Rosenberger, "A new soft biometric approach for keystroke dynamics based on gender recognition," *Int. J. Inf. Technol. Manage.*, vol. 11, no. 1/2, pp. 35-49, Jan. 2012.

[64] A. A. Buker, A. Vinciarelli, and G. Roffo, "Type like a man! Inferring gender from keystroke dynamics in live-chats," *IEEE Intell. Syst.*, vol. 34, no.6, pp. 53–59, Nov.-Dec. 2019. doi: 10.1109/MIS.2019.2948514.

[65] A. Pentel, "High precision handedness detection based on short input keystroke dynamics," Aug. *2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA)*, Larnaca, Cyprus, 2017, pp. 1-5, doi: 10.1109/IISA.2017.8316380.

[66] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics database: A benchmark for keystroke dynamics biometric systems," in *Proc. Int. Conf. Biometrics Special Interest Group* (BIOSIG), Darmstadt, Germany, Jan. 2013, pp. 1–8.

[67] A. Kumar, A. Patwari, and S. Sabale, "User authentication by typing pattern for computer and computer based devices," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 3, no. 10, pp. 8132–8134, Oct. 2014.

[68] I. Tsimperidis, P. Yoo, K. Taha, A. Mylonas, and V. Katos, "R2BN: An adaptive model for keystroke-dynamics-based educational level classification," *IEEE Trans. Cybern.*, vol. 50, no. 11, pp. 4736–4746, Nov. 2020.

[69] C. Epp, M. Lippold, and R. L. Mandryk, "Identifying emotional states using keystroke dynamics," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.* (CHI), Vancouver, BC, Canada, May 2011, pp. 715–724.

[70] R. Giot, M. El-Abed, and C. Rosenberger, "Keystroke dynamics authentication for collaborative systems," in *Proc. IEEE Int. Symp. Collaborative Technol. Syst.* (CTS), Baltimore, MD, USA, Nov. 2009, pp. 172–179.

[71] R. Shadaman, A. Wahab, M. Manno, M. Lukaszewski, D. Hou, and F. Hussain, "Keystroke dynamics: Concepts, techniques, and applications," *arXiv preprint arXiv:2303.11186*, Mar. 2023.

[72] K. Niinuma and A. K. Jain, "Continuous user authentication using temporal information," in *Proc. SPIE 7667, Biometric Technology for Human Identification VII*, Orlando, FL, USA, Apr. 2010, Art. no. 76670A.

[73] I. C. Stylios, O. Thanou, I. Androulidakis, and E. Zaitseva, "A review of continuous authentication using behavioral biometrics," in *Proc. SouthEast Eur. Design Autom. Comput. Eng. Comput. Netw. Soc. Media Conf.* (SEEDA-CECNSM), Kastoria, Greece, Sep. 2016, pp. 1–8.

[74] C. C. Tappert, M. Villani, and S.-H. Cha, "Keystroke biometric identification and authentication on long-text input," in *Behavioral Biometrics for Human Identification: Intelligent Applications*, L. Wang and J. Geng, Eds. Hershey, PA, USA: IGI Global, Jan. 2009, pp. 342–367.

[75] H. Çeker and S. Upadhyaya, "User authentication with keystroke dynamics in long-text data," in *Proc. IEEE 8th Int. Conf. Biometrics Theory Appl. Syst.* (BTAS), Niagara Falls, NY, USA, 2016, pp. 1–6, doi: 10.1109/BTAS.2016.7791182.

[76] P. Bours and H. Barghouthi, "Continuous authentication using biometric keystroke dynamics," in *Proc. Norwegian Inf. Secur. Conf.* (NISK), Oslo, Norway, 2009, pp. 1–12.

[77] E. Alsolamy, "An examination of keystroke dynamics for continuous authentication," Doctoral dissertation, Inf. Secur. Inst., Queensland Univ. of Technol., Brisbane, QLD, Australia, 2012.

[78] T. Sim and R. Janakiraman, "Are digraphs good for free-text keystroke dynamics?," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.* (CVPR), Minneapolis, MN, USA, Jul. 2007, pp. 1–6.

[79] H. Al-Assam, H. Sellahewa, and S. Jassim, "Accuracy and security evaluation of multi-factor biometric authentication," *Int. J. Inf. Secur. Res.*, vol. 1, no. 1, pp. 11–19, Mar. 2011.

[80] R. Giot, M. El-Abed, and C. Rosenberger, "GREYC keystroke: A benchmark for keystroke dynamics biometric systems," in *Proc. IEEE 3rd Int. Conf. Biometrics: Theory Appl. Syst.* (BTAS), Washington, DC, USA, 2009, pp. 1–6.

[81] T. Sim, "Continuous authentication - Still a thing after 20 years?," IEEE Biometrics Council Webinar, Jan. 17, 2024. [Online video]. Available: https://youtu.be/LOdowYjNDZA (accessed Feb. 15, 2025).

[82] P. Bours and S. Mondal, "Performance evaluation of continuous authentication systems," *IET Biometrics*, vol. 4, no. 4, pp. 220–226, Jun. 2015.

[83] D. Senarath, S. Tharinda, M. Vishvajith, S. Rasnayaka, S. Wickramanayake, and D. Meedeniya, "Re-evaluating keystroke dynamics for continuous authentication," in *Proc. 3rd Int. Conf. Adv. Res. Comput.* (ICARC), Belihuloya, Sri Lanka, 2023, pp. 202–207.

[84] M. Trojahn, F. Arndt, and F. Ortmeier, "Authentication with keystroke dynamics on touchscreen keypads-effect of different n-graph combinations," in *Proc. 3rd Int. Conf. Mobile Services, Resources, and Users* (Mobility), Lisbon, Portugal, Jan. 2013, pp. 69–74.

[85] N. Ahmad, A. Szymkowiak, and P. A. Campbell, "Keystroke dynamics in the pre-touchscreen era," *Front. Hum. Neurosci.*, vol. 7, Art. no. 835, Dec. 2013.

[86] I. Buhan and P. Hartel, "The state of the art in abuse of biometrics," Centre for Telematics and Information Technology (CTIT), University of Twente, Enschede, The Netherlands, Tech. Rep. TR-CTIT-05-34, Sep. 2005.

[87] C. Gottschlich, "Skilled impostor attacks against fingerprint verification systems and its remedy," *arXiv preprint arXiv:1503.04729*, 2015.

[88] S. Coghlan, T. Miller, and J. Paterson, "Good proctor or 'big brother'? Ethics of online exam supervision technologies," *Philos. Technol.*, vol. 34, no. 4, pp. 1581–1606, Dec. 2021.

[89] K. Becker and H. Meng, "Identifying statistically actionable collusion in remote proctored exams," *J. Appl. Test. Technol.*, vol. 23, no. S1, pp. 54–61, Mar. 2022.

[90] D. L. McCabe and L. K. Treviño, "Academic dishonesty: Honor codes and other contextual influences," *J. High. Educ.*, vol. 64, no. 5, pp. 522–538, Sep. 1993.

[91] J. Liebers, C. Burschik, U. Gruenefeld, and S. Schneegass, "Exploring the stability of behavioral biometrics in virtual reality in a remote field study: Towards implicit and continuous user identification through body movements," *arXiv preprint arXiv:2310.15003*, Oct. 2023.

[92] R. Giot, B. Dorizzi, and C. Rosenberger, "Analysis of template update strategies for keystroke dynamics," in *Proc. IEEE Workshop Comput. Intell. Biometrics Identity Manage.* (CIBIM), Paris, France, May 2011, pp. 1–8.

[93] P. H. Pisani, A. C. Lorena, and A. C. P. L. F. de Carvalho, "Adaptive biometric systems using ensembles," *IEEE Intell. Syst.*, vol. 33, no. 2, pp. 19–28, Mar./Apr. 2018.

[94] N. Poh, A. Rattani, and F. Roli, "Critical analysis of adaptive biometric systems," *IET Biometrics*, vol. 1, no. 4, pp. 191–199, Dec. 2012.

[95] H. Bhatt, S. Bharadwaj, R. Singh, M. Vatsa, A. Noore, and A. Ross, "On co-training online biometric classifiers," in *Proc. IEEE Int. Joint Conf. Biometrics* (IJCB), Washington, DC, USA, Oct. 2011, pp. 1–7.

[96] T. Susnjak and T. McIntosh, "ChatGPT: The end of online exam integrity?," *Educ. Sci.*, vol. 14, no. 6, Art. no. 656, Jun. 2024.

[97] P. Santoki, "Design and implementation of detection of key logger," *Int. J. Eng. Dev. Res.*, vol. 2, no. 2, pp. 1999–2017, Jun. 2014.

[98] S. P. Bejo, B. Kumar, P. Banerjee, P. Jha, A. N. Singh, and M. K. Dehury, "Design, analysis and implementation of an advanced keylogger to defend cyber threats," *International Journal of Computer Sciences and Engineering*, vol. 11, no. 3, pp. 12–18, Mar. 2023.

[99] A. Bhardwaj and S. Goundar, "Keyloggers-silent cyber security weapons," *Netw. Secur.*, vol. 2021, no. 7, pp. 13–19, Jul. 2021.

[100] R. M. Martín and M. Apfelthaler, "A task segment framework to study keylogged translation processes," *Int. J. Transl. Interpreting Res.*, vol. 14, no. 2, pp. 8–31, Jul. 2022.

[101] C. Ritzer, "German court: Monitoring of employees by key logger is not allowed," Data Protection Report, Aug. 08, 2017. [Online]. Available: https://www.dataprotectionreport.com/2017/08/german-court-monitoring-of-employees-by-key-logger-is-not-allowed/ (accessed Apr. 29, 2025).

[102] A. Wengelin and V. Johansson, "Investigating writing processes with keystroke logging," in *Digital Writing Technologies in Higher Education: Theory, Research, and Practice*, M. Leijten and L. Van Waes, Eds. Cham, Switzerland: Springer, 2023, pp. 405–420.

[103] Y. Atoum, L. Chen, A. X. Liu, S. D. H. Hsu, and X. Liu, "Automated online exam proctoring," *IEEE Trans. Multimedia*, vol. 19, no. 7, pp. 1609–1624, Jul. 2017.

[104] O. Holden, M. E. Norris, and V. A. KUKuhlmeier, "Academic integrity in online assessment: A research review," *Front. Educ.*, vol. 6, Art. no. 639814, Mar. 2021.

[105] M. Torrance and D. Galbraith, "The processing demands of writing," in *Handbook of Writing Research*, C. MacArthur, S. Graham, and J. Fitzgerald, Eds. New York, NY, USA: Guilford Publications, 2006, pp. 67–80.

[106] Y. Deng and Y. Zhong, "Keystroke dynamics user authentication based on Gaussian mixture model and deep belief nets," *ISRN Signal Process.*, vol. 2013, Art. no. 565843, Jan. 2013.

[107] C. Boutin, Ed., "NIST to turn atomic clocks ahead one second on June 30," National Institute of Standards and Technology, Tech. Rep., Aug. 06, 2009. [Online]. Available: https://www.nist.gov/pml/time-and-frequency-division/time-realization/leap-seconds (accessed Aug. 13, 2024).

[108] B. Keating, "Letter frequencies in the English language," University of Notre Dame. [Online]. Available: https://www3.nd.edu/~busiforc/handouts/cryptography/Letter%20Frequencies.html (accessed Jul. 04, 2024).

[109] J. Huang, D. Hou, S. Schuckers, T. Law, and A. Sherwin, "Benchmarking keystroke authentication algorithms," in *Proc. IEEE Workshop Inf. Forensics Secur.* (WIFS), Rennes, France, 2017, pp. 1–6.

[110] MathWorks, "Choosing the best machine learning classification model and avoiding overfitting," MathWorks Corporate Website, 2024. [Online]. Available: https://www.mathworks.com/campaigns/offers/next/choosing-the-best-machine-learning-classification-model-and-avoiding-overfitting.html (accessed Feb. 15, 2025).

[111] M. Awad and R. Khanna, *Efficient Learning Machines: Theories, Concepts, and Applications for Engineers and System Designers*. Berkeley, CA, USA: ApressOpen, 2015.

[112] G. Tubin, "Keylogging: How it works, impact, and 5 defensive measures," Cynet, Jul. 22, 2024. [Online]. Available: https://www.cynet.com/cybersecurity/keylogging-how-it-works-impact-and-5-defensive-measures/ (accessed Feb. 15, 2025).

[113] C. Murphy, J. Huang, D. Hou, and S. Schuckers, "Shared dataset on natural human-computer interaction to support continuous authentication research," in *Proc. IEEE Int. Joint Conf. Biometrics* (IJCB), Denver, CO, USA, 2017, pp. 525–530.

[114] Y. Sang, H. Shen, and P. Fan, "Novel impostors detection in keystroke dynamics by support vector machine," in *Proc. 5th Int. Conf. Parallel Distrib. Comput. Appl. Technol.* (PDCAT), Singapore, Dec. 2004, pp. 624–628.

[115] E. Yu and S. Cho, "Keystroke dynamics identity verification - Its problems and practical solutions," *Comput. Secur.*, vol. 23, no. 5, pp. 428–440, Jul. 2004.

[116] K. S. Balagani, V. V. Phoha, A. Ray, and S. Phoha, "On the discriminability of keystroke feature vectors used in fixed text keystroke authentication," *Pattern Recognit. Lett.*, vol. 32, no. 8, pp. 1070–1080, Jun. 2011.

BIBLIOGRAPHY

[1] R. Kumar, *Research Methodology: A Step-by-Step Guide for Beginners*. New Delhi, India: Sage Publications India Pvt. Ltd., 2014.

[2] T. Lucey, *Quantitative Techniques*, 5th ed. UK: ELST, 2001.

[3] K. Thompson and D. M. Ritchie, *UNIX Programmer's Manual*, 3rd ed. Bell Telephone Laboratories Inc., Feb. 1973.

[4] P. Sharma, *Fundamentals of Web Technology*, 1st ed. S K Kataria & Sons, 2013.

[5] D. Goodman and M. Morrison, *JavaScript Bible*, 5th ed. USA: Wiley Publishing Inc., 2004.

[6] G. Crisp, *The e-Assessment Handbook*, 1st ed. New York, NY, USA: Continuum International Publishing Group, 2008.

- END -