[8] Dwivedi, S. (2018). In A Week, Aadhaar Data Of 70 Lakh Children On Andhra Pradesh Government Sites. https://www.ndtv.com/indianews/despite-laws-no-action-against-government-agencies-displaying-aadhaardata-1844747.
[9] Fernandes, J. (2023) Aadhaar data Leak; Personal information of 81.5 crore Indians on dark web. Available via https://www.livemint.com/news/india/aadhaardata-leak-personal-information-of-81-5-crore-indians-on-dark-web-top-7-things-toknow-11698737674480.html.
[10] Ganjoo, S. (2018). Quora reports massive data breach, data of 100 million users stolen. https://www.indiatoday.in/technology/news/story/quorareports-massive-data-breach-data-of-100-million-users-stolen-1401950-2018-12-04.
[11] Garg, R. (2022): A Technological Approach to Address Deficiencies in UID (Aadhaar). 3rd International Conference on Big Data, Blockchain and Security,Copenhagen Denmark. doi (Vol 10).
[12] Ghosh, D. (2023a). Rise in number of aadhaar fraud cases. https://timesofindia. indiatimes.com/city/kolkata/rise-in-number-of-aadhaarfraud-cases/articleshow/ 102817460.cms.
[13] Ghosh, D. (2023b). Aadhaar frauds in a month keep kolkata-cops on toes. https://timesofindia.indiatimes.com/city/kolkata/37-aadhaar-frauds-in-a-monthkeep-kolkata-cops-on-toes/articleshow/ 103544825.cms.
[14] Jain, M. (2019). The Aadhaar card: cybersecurity issues with India's biometric experiment. https://jsis.washington.edu/news/the-aadhaar-cardcybersecurity-issues-with-indias-biometric-experiment.
[15] Jha, R. (2023). How crooks are exploiting gaps in Aadhaar system in Delhi. https://timesofindia.indiatimes.com/city/delhi/how-crooks-are-exploiting-gaps-in-aadhaar-system-in-delhi/articleshow/98744284.cms.
[16] KumarShrestha, A.; Singh Maharajan, P.; Paudel, S. (2015): Identification and illustration of insecure direct object references and their countermeasures. International Journal of Computer Applications 114(18), pp. 39-44.
[17] Liu, Y.; He, D.; Obaidat, M.S.; Kumar, N.; Khan, M.K.; Choo, K.R. (2020): Blockchain-based identity management systems: A review. Journal of network and computer applications 166: 102731.
[18] Maulik, R.;Chaki, N. (2009): PhishNet: Enhancing the Security Aspect of IMS Users.In: 2009 First International Conference on Networks & Communications, Chennai,India, Dec 2009. doi:10.1109/NetCoM.2009.34.
[19] Menon, S. (2017): Aadhaar-based biometric authentication for PDS and food security: Observations on implementation in Jharkhand's Ranchi District. Indian Journal of Human Development 11(3), pp. 387-401.
[20] Moneylife (2023). Jeevan Pramaan Life Certificate: BBDB Manch Warns about AePS and Phishing Frauds. https://www.moneylife.in/article/jeevan-pramaan-life-certificate-bbdbmanch-warns-about-aeps-and-phishing-frauds/72512.html.
[21] Murdoch S.J.; Danezis G. (2005): Low-cost traffic analysis of Tor. In 2005 IEEE Symposium on Security and Privacy (S&P'05), pp 183-195.
[22] Nohl, K.; Kribler, S.; Lehl, J. (2014): BadUSB-on accessories that turn evil.Black HatUSA 1(9):1-22.
[23] Outlook Money (2023) Massive Aadhaar Data Breach of 815 Million Indians: Here's How To Keep Your Details Safe. https://business.outlookindia.com///news/massive-aadhaar-data-breach-of-815-million-indians-heres-how-to-keep-your-details-safe.
[24] PTI (2023). Easy Address Change Process in Aadhaar Major Cause of Cyber Fraud: Police. https://www.outlookindia.com/national/easy-address-change-process-in-aadhaar-major-cause-of-cyber-fraud-police-news-273848.
[25] Raghava, M. (2023). Another victim loses money to aadhaar-enabled payment system fraud following registration of document at Mangaluru City sub-registrar's office. https://www.thehindu.com/news/cities/Mangalore/another-victim-losesmoney-to-aadhaar-enabled-payment-system-fraud-following-registration-of-landdocument-at-mangaluru-sub-registrars-office/article67408249.ece.
[26] Ramya, K.; Sumathi, A. (2019). Big Data Applications in Aadhar Card Fraud Detection. IJCSE 7(3) 5:865-867. doi:10.26438/ijcse/v7i3.86586.
[27] Sarasvati, N.T. (2023). What Made It Easier for Fraudsters to Access People's Biometrics, Aadhaar Details in Kolkata? https://www.medianama.com/2023/10/223-aadhaar-enabled-payment-systemfraud-kolkata.
[28] Sarasvati, N.T. (2024). Aadhaar-enabled Payment System Frauds Contributed to 11% of Financial Cybercrimes: I4C Data. https://www.medianama.com/2024/01/223-aadhaar-enabled-payment-systemaeps-financial-frauds-i4c-data.
[29] SNS (2023). Kolkata-police-commissioner warns of rising biometric-data-theft-bank-fraud-cases. https://www.thestatesman.com/bengal/kolkatapolice-commissioner-warns-of-rising-biometric-data-theft-bank-fraud-cases-1503223209.html.
[30] Srinivasan, J.; Bailur, S.; Schoemaker, E.; Seshagiri, S. (2018): Privacy at the margins— The poverty of privacy: Understanding privacy trade-offs from identity infrastructure users in India. International Journal of Communication 12, 2.
[31] Sukhtankar, S.; Niehaus, P.; Muralidharan, K. (2022): Integrating Biometric Authentication in India's Welfare Programs: Lessons from a Decade of Reforms.
[32] Weber, H. (2018). Politics of 'leaving no one behind': contesting the 2030 Sustainable Development Goals agenda. In the Politics of Destination in the 2030 Sustainable Development goals, pp. 399-414.

Authors Profile

Reshmi Maulik is an Assistant Professor in Meghnad Institute of Technology, Techno India Group, Kolkata, India. She received her Master's degree in Economics from University of Calcutta in 2000. She then completed C level (equivalent to M.Tech. in Computer Science) from DOEACC Society, Government of India, in 2005. She has also worked in the software industry for 3 years before returning to academia. She has authored several research papers in Journals and International conferences. She is currently pursuing PhD in Computer Science and Engineering from MAKAUT. Her current research focuses on cyber security and finding the ways to minimize the bug resolution time in software engineering.