REVIEW ARTICLE

Deepfakes and Aadhaar: An Unexplored Cybersecurity Challenge in India

Vivekananth. P*, Navneet Sharma
Department of Computer Science & IT, IIS (deemed to be University), Jaipur

Abstract

While India's Aadhaar system, the world's largest biometric identity platform, has demonstrated robustness, the rapid evolution of DeepFake technology presents a potential, yet unexplored, cybersecurity challenge. This technology uses AI to create hyper-realistic synthetic faces, fingerprints, and even iris images. This mini scoping review examines how Deepfakes could potentially bypass Aadhaar's security measures. By analyzing recent research and security incidents, the review explores how Deepfakes could threaten Aadhaar's security. Additionally, it proposes ways to strengthen Aadhaar's defenses and identifies areas for future research on DeepFake detection. While a DeepFake breach of Aadhaar is hypothetical, this review proactively explores potential risks and solutions, aiming to contribute to India's cybersecurity efforts and safeguard Aadhaar against future threats.

Keywords: Aadhaar, Artificial Intelligence, Cybersecurity, DeepFake technology, Generative Adversarial Networks

Introduction

Biometric authentication systems, including India's Aadhaar, are a cornerstone for securing access to essential services for billions of citizens (MC and Shanmugam, 2023). However, the rise of DeepFakes, AI-powered tools that create synthetic media with unsettling realism, poses a growing threat. DeepFakes leverage Generative Adversarial Networks (GANs), a type of advanced machine learning, to produce highly convincing forgeries of fingerprints, iris scans, or other biometric data used for authentication (Firc *et al.,* 2023). This two-part system, with a generator crafting forgeries and a discriminator refining them against real data, has significantly advanced DeepFake technology, posing a new and concerning security challenge. While initial research suggests DeepFakes could pose a threat, a comprehensive analysis of Aadhaar's vulnerabilities in this context is currently lacking. This mini scoping review aims to address this gap in knowledge by exploring how DeepFakes might threaten Aadhaar's security. We will explore current DeepFake advancements, analyze potential weaknesses within the Aadhaar system, and propose strategies to strengthen its defenses.

This review employs a well-established five-stage methodological framework to assess Aadhaar's vulnerabilities. This meticulous process involves:

- Defining the scope based on research questions.
- Identifying relevant studies published between 2018 and 2023.
- Systematically selecting studies for relevance.
- Charting and analyzing data for key themes.
- Synthesizing the data to inform security improvements.

A systematic review encompassing all pertinent research would be the most desirable approach. However, given the constraints of time and resources inherent to this mini scoping review, we opted for a focused analysis of a targeted set of less than 40 articles. This strategic approach ensured in-depth exploration of the most relevant research on DeepFake threats to Aadhaar security. Through meticulous selection based on depth, relevance to Aadhaar and DeepFake detection, and methodological rigor, we identified 36 critical articles. This foundational set of studies provides a comprehensive understanding of the multifaceted threats posed by DeepFakes. The following sections will delve into the identified research questions in detail, aiming to illuminate Aadhaar's vulnerabilities and potential mitigation strategies. By proactively addressing these challenges, we can ensure the continued security of Aadhaar and similar biometric systems.

Methodology

To efficiently assess DeepFake threats to Aadhaar's security a scoping review framework was chosen for its ability to provide a broad overview of the current literature (Pham *et al.,* 2014). This methodology adheres

*Corresponding Author Email: vivekananthp34747@iisuniv.ac.in to the established five-stage framework proposed by Arksey and O'Malley (2005) and ensures methodological rigor by following the Preferred Reporting Items for Systematic Reviews and Meta-Analysis extension for Scoping Reviews (PRISMA-ScR) guidelines.

The initial stage of the scoping review involved defining the research questions that would guide the literature search and selection process. These research questions aimed to explore the multifaceted implications of DeepFake technology on Aadhaar security:

- What are the current advancements and applications of DeepFake technology that pose a threat to biometric systems, including Aadhaar?
- What are the potential vulnerabilities within the Aadhaar system that could be exploited by DeepFakes?
- What strategic measures can be proposed to enhance the resilience of Aadhaar and similar systems against DeepFake attacks?

Following the established framework, Stage 2 centered on developing a comprehensive search strategy to identify relevant academic literature. A predefined list of keywords and search terms encompassing DeepFake technology, Aadhaar, biometrics, and cybersecurity was compiled (Table 1). These keywords were used to systematically search various academic databases, including Google Scholar, IEEE Xplore, and Semantic Scholar. Additionally, the Google search engine was employed to identify relevant news articles and reports on Aadhaar breaches. Considering the objective of a mini scoping review and the manageable workload for a two-person team, we aimed to identify a targeted set of less than 40 articles. This focus ensured in-depth analysis of the most relevant studies while remaining efficient within the project timeline.

Inclusion criteria were meticulously established to ensure the identified studies directly addressed the research questions. Peer-reviewed articles published between 2018 and 2023 were prioritized to capture the latest advancements in DeepFake technology and its security implications. Studies focusing on DeepFake applications in biometric systems, reports of Aadhaar data breaches, and articles discussing potential preventive measures were included. Exclusion criteria were set to filter out irrelevant content such as non-English articles, studies solely focused on AI technologies unrelated to DeepFakes or biometric security, and duplicate or redundant data from less reputable sources.

Stage 3 tackled systematic selection of relevant articles from the initial pool of 5562 using Rayyan, a free online review tool. Rayyan's AI capabilities (duplicate detection, pre-screening) streamlined the process for the two collaborating researchers, allowing focused analysis of a targeted pool. Rayyan's shared workspace further facilitated collaboration with blinded review and discussions. Following initial screening, detailed content assessments ensured articles addressed Aadhaar's security and potential DeepFake vulnerabilities.

Stage 4 involved meticulously charting the selected articles based on a predefined framework considering their approach, key findings, and relevance to DeepFake threats. Articles were categorized by methodological quality and the depth of information provided on DeepFake capabilities and potential Aadhaar vulnerabilities. Zotero, a reference management software, aided in data management and annotation throughout this stage. This process established a clear overview of the current research landscape on DeepFake threats to Aadhaar security.

Table 1. Distribution of search results across different databases and search engines using various search terms related to DeepFake, Aadhaar, biometrics, and Cybersecurity

Search Terms	Google Scholar	IEEE Xplore	Semantic Scholar	Google Search	Total
DeepFake and Aadhaar	0	1	2	11	14
Cybersecurity, Biometrics, and DeepFake	227	127	5	823	1185
Identity Verification, DeepFake, and Aadhaar	4	0	10	311	327
Identity Verification and DeepFake	88	22	4	503	618
Artificial Intelligence, Security Threats, and Aadhaar	49	4	6	601	661
DeepFake Detection in Biometrics	2698	19	3	177	2943
Net Total	3066	173	30	2426	**5562**

The final stage, focused on data synthesis and reporting the findings. Thematic analysis techniques were employed to identify potential vulnerabilities within Aadhaar. Real incidents of Aadhaar breaches were analyzed to construct hypothetical scenarios envisioning future DeepFake attacks, ensuring a realistic assessment of risks. Throughout the review process, we maintained a balance between methodological rigor and exploration of DeepFake's multifaceted implications for Aadhaar's security.

Results and Discussion

This mini scoping review identified 36 articles (Fig. 1) exploring the intersection of DeepFakes and Aadhaar security. Stringent criteria and in-depth analysis yielded this dataset from an initial pool of 5,562 (Fig. 1). The distribution across research questions varied as seen in the bar graph (Fig. 2). The first area focused on the general technological threats DeepFakes pose to biometric systems (12 articles). This highlights growing

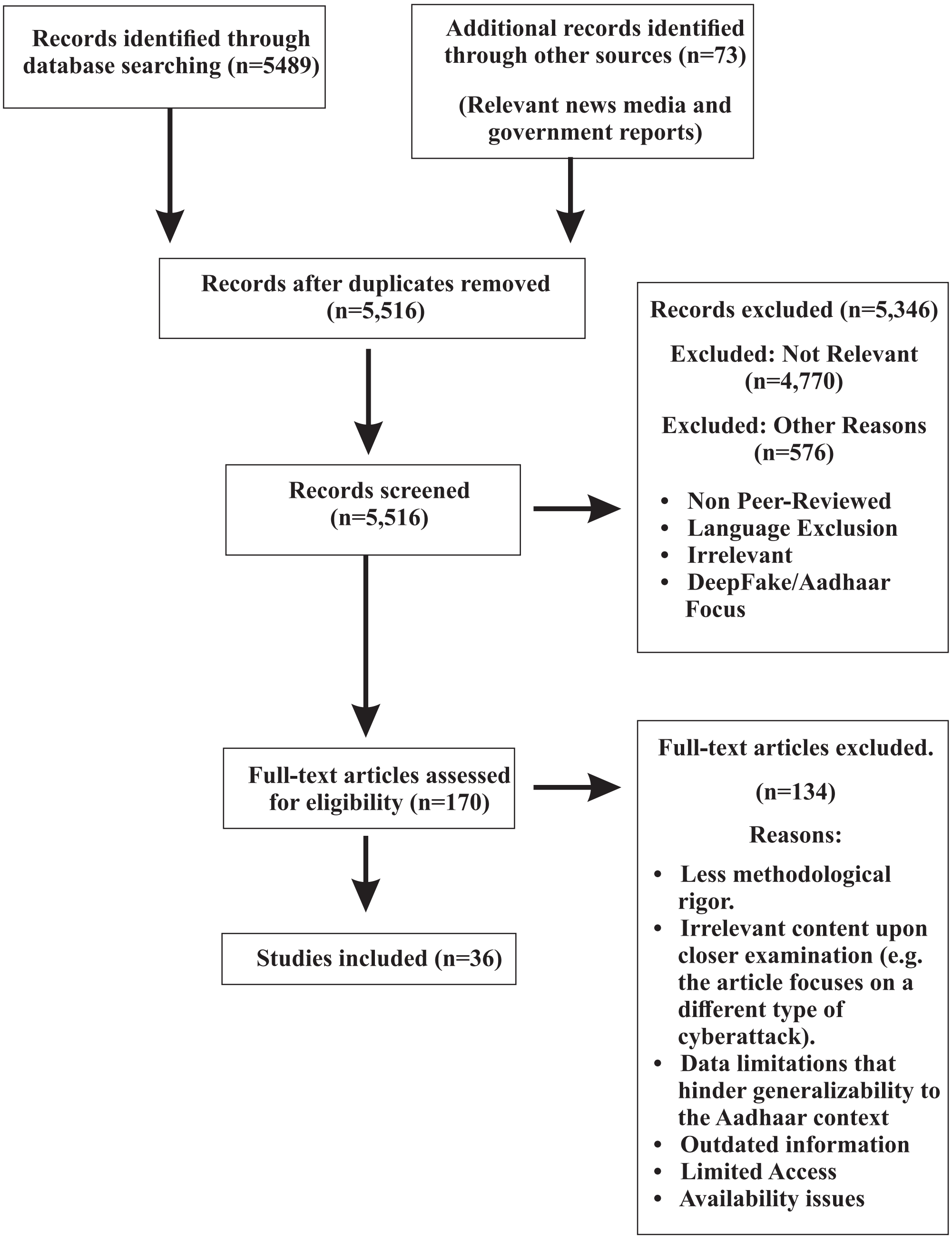
Records identified through database searching (n=5489)
Additional records identified through other sources (n=73)
(Relevant news media and government reports)
Records after duplicates removed (n=5,516)
Records excluded (n=5,346)
Excluded: Not Relevant (n=4,770)
Excluded: Other Reasons (n=576)
• Non Peer-Reviewed
• Language Exclusion
• Irrelevant
• DeepFake/Aadhaar Focus
Records screened (n=5,516)
Full-text articles assessed for eligibility (n=170)
Full-text articles excluded.
(n=134)
Reasons:
• Less methodological rigor.
• Irrelevant content upon closer examination (e.g. the article focuses on a different type of cyberattack).
• Data limitations that hinder generalizability to the Aadhaar context
• Outdated information
• Limited Access
• Availability issues
Studies included (n=36)

Fig. 1. PRISMA Flow chart of scoping review (based on framework Arksey and O'Malley,2005)

research community concern about DeepFakes' potential to bypass security measures. The second area investigated vulnerabilities specific to Aadhaar (8 articles), analyzing a mix of academic papers (5) and news reports (3). Finally, the review examined methods for countering DeepFake threats to Aadhaar security (16 articles), with a government press report included. This foundational analysis provides a framework to address the research questions, which will be explored in detail in subsequent sections, focusing on DeepFake risks to Aadhaar and mitigation strategies.

Technological Threats of DeepFake to Biometrics:

Deepfakes, blending "deep learning" and "fake," threaten biometric security, especially facial recognition (Mirsky and Lee, 2021). This concern is further amplified by research from Firc *et al.* (2023), who successfully generated "morphed identities" capable of deceiving facial recognition algorithms (Fig. 3). This figure showcases how Deepfakes can combine features from two individuals, creating a synthetic face that could bypass facial recognition security measures.

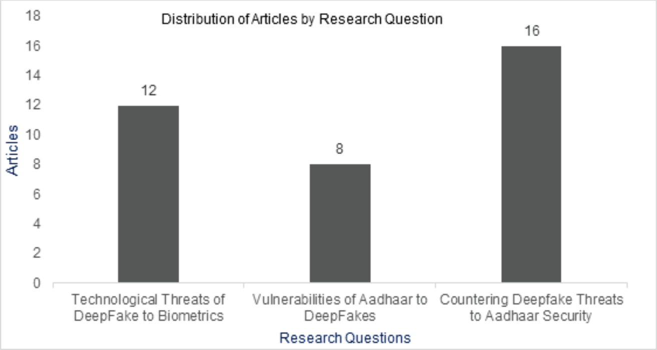

Fig. 2. Distribution of Articles by Research Question

The challenge goes beyond technical limitations. Nightingale and Farid (2022) expose a disconcerting trend: people tend to perceive AI-generated faces, termed "AI hyperrealism" by Miller *et al.* (2023), as even more trustworthy than real ones. This phenomenon can potentially manipulate human judgment and significantly intensify the deepfake challenge. This vulnerability is further compounded by the emergence of face synthesis, the ability of AI to generate entirely new, hyper-realistic faces that never existed before. Pioneering research by Karras *et al.* (2019) has pushed the boundaries of this technology using style-based generators for Generative Adversarial Networks (GANs). This allows AI to manipulate internal variables within the model to generate faces with specific features. The level of realism achieved is remarkable, often indistinguishable from real faces (Fig. 4), as showcased by websites like "ThisPersonDoesNotExist". This raises concerns about deepfakes AI contaminating facial recognition training data or injecting synthetic facial data into databases, potentially compromising accuracy and introducing biases

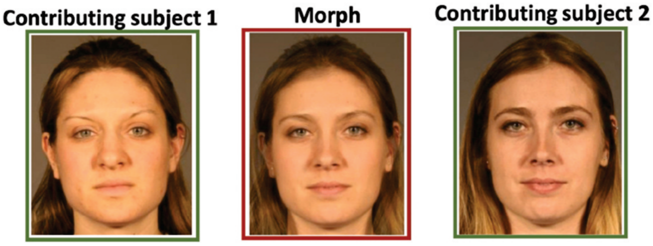

Fig. 3. An example of face morphing. Left and right-most images show the original subjects. The middle image shows the result of morphing both subjects. (Firc *et al.*, 2023)

Fig. 4. Fictional Faces synthesized using StyleGAN2 model (Source: "ThisPersonDoesNotExist")

The innovation extends further to the creation of synthetic fingerprints, known as 'MasterPrints', which can mimic real fingerprints and bypass security systems (Bontrager *et al.,* 2018). These synthetic fingerprints can be used in dictionary attacks, testing a wide array of fake prints to find matches with real users' biometrics, potentially compromising the security of these systems. Furthermore, sophisticated generative methods allow for realistic simulation of aging effects on facial images, complicating age-sensitive biometric verification systems as depicted in Fig. 5 by Georgopoulos *et al.* (2020).

DeepFake technology not only poses a threat through the creation of visually deceptive synthetic identities but also extends its capabilities to voice impersonation. Minimal computing resources can now produce convincingly artificial speech, which can be used for both beneficial and malicious purposes, posing challenges to real-time detection technologies and complicating forensic efforts to distinguish between real and synthetic voices (Amezaga and Hajek, 2022; Mcuba *et al*., 2023). Adding to this, DeepFake can generate synthetic iris images that closely mimic real biometric markers, significantly enhancing the threat to biometric security systems like iris scans, crucial for systems relying on these for authentication (Wang *et al.,* 2022; Makrushin *et al*., 2023). These advancements underscore the pressing need for sophisticated countermeasures to protect security, privacy, and digital trust.

Vulnerabilities of Aadhaar to DeepFakes

Aadhaar, India's unique digital identity system linking a twelve-digit number to a person's biometrics and demographics, is critical to the nation's digital infrastructure (MC and Shanmugam, 2023). However, a recent study by Peidro-Paredes *et al.* (2023) has exposed a troubling vulnerability: AI-generated "MasterPrints" that can bypass fingerprint scanners on some Android devices. Worryingly, their "MasterPrints" achieved a 70% success rate in fooling fingerprint scanners, highlighting a potential vulnerability in Aadhaar's fingerprint authentication system. The concern extends beyond the technology itself. The multi-layered structure of Aadhaar, involving various stakeholders like banks and mobile manufacturers, creates potential entry points for attackers (Tyagi *et al.,* 2018). Each entity collects and stores user biometric data, which is encrypted and used for verification across different agencies and devices. While regulations mandate strong network security, ensuring complete compliance across all stakeholders is a complex task. If deepfakes are used to bypass security measures, attackers could gain access to the vast amount of biometric data stored within the system.

Recent incidents expose a critical vulnerability in Aadhaar: data leaks. A news report from The Hindu (Special Correspondent, 2021) revealed a leak of 20 million Aadhaar numbers from the Tamil Nadu PDS database, highlighting the system's vulnerability due to its presence across various entities, each a potential leak point. These incidents are not isolated. Singh (2021) highlights the recurring issue of Aadhaar leaks, and Tiwari *et al.* (2022) acknowledge their prevalence in their security analysis. The sheer scale of the potential 2018 billion-record leak (Safi, 2018) underscores the gravity of the situation. Even inadvertent disclosures by individuals or officials (Singh, 2023) can contribute to this ever-growing pool of exposed data. Furthermore, recent investigations by the Delhi Police (Jha, 2023) expose even more worrying flaws. The system's

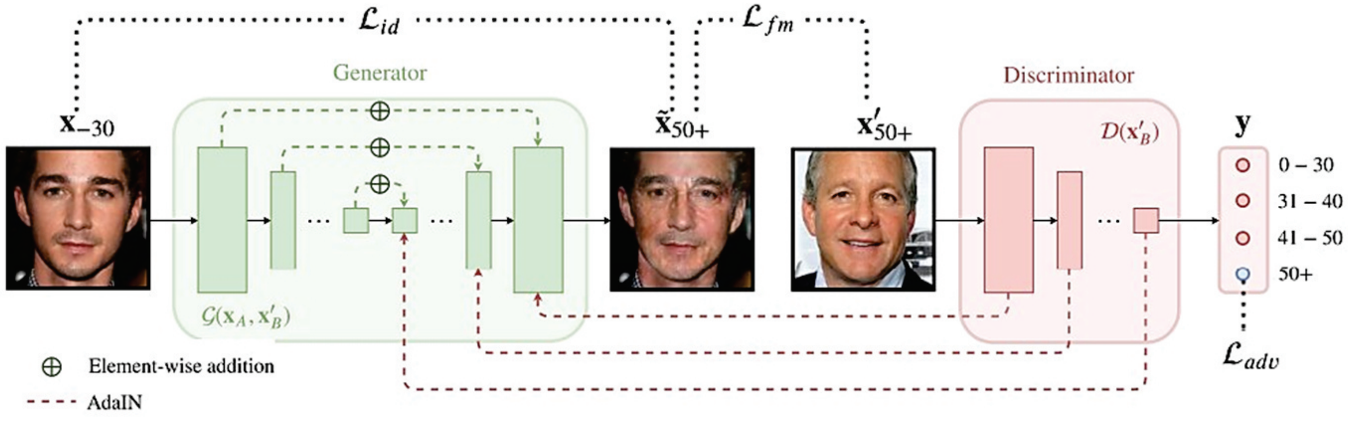

Fig. 5. Depiction of the face aging process, transforming a young individual's image to an older age group while preserving identity features, guided by age-discriminative representations and precise aging patterns. (Georgopoulos *et al.*, 2020)

limitations were exposed when individuals created multiple registrations with the same photo but different fingerprints. Scammers exploited these weaknesses further by acquiring agents' credentials and using silicon fingerprints or printed iris scans to gain unauthorized access (Jha, 2023). The system's inability to detect such forgeries – silicon fingerprints indistinguishable from real ones and printed iris scans bypassing verification – raises serious concerns. Additionally, the lack of facial recognition during registration allowed for duplicate Aadhaar cards with the same photo (Jha, 2023). This confluence of vulnerabilities – data leaks and system shortcomings – paves the way for a terrifying scenario: DeepFakes seamlessly integrated with stolen data to breach Aadhaar security and potentially wreak havoc on financial systems, social welfare programs, and even national security.

In a hypothetical scenario, inspired by real-world cases like fraudulent Aadhaar enrolment centers exposed in Ludhiana (HT Correspondent, 2021), cybercriminals form a clandestine group to exploit Aadhaar vulnerabilities with DeepFakes. Fabricating synthetic data, they create fictional identities undetectable by mimicking documented enrolment frauds (Jha, 2023). With these synthetic identities seamlessly integrated into the Aadhaar ecosystem, the cybercriminals exploit the system's weaknesses, potentially enabling various illicit activities such as terrorism, financial fraud and identity theft. This hypothetical scenario underscores the critical cybersecurity challenge posed by DeepFake technology to Aadhaar and highlights the urgent need for enhanced security measures and robust authentication protocols to mitigate such threats effectively.

Countering deepfake threats to Aadhaar security

Deepfake-generated forgeries can manipulate facial data, potentially bypassing current fingerprint checks and compromising enrollment security. Imagine a scenario where someone uses a DeepFake synthetic photo to register for a new Aadhaar card with their real fingerprints. The current system wouldn't detect this deception. To effectively counter this threat, a multi-layered defense system is crucial for both enrollment and authentication phases of Aadhaar registration process. Aadhaar's current AI implementation focuses on fingerprint liveness detection (Ministry of Electronics and IT, 2023), a valuable tool, but it only tackles one aspect of Aadhaar enrollment. During enrollment, AI can analyze specific facial points, like the corners of the eyes and mouth, to identify subtle inconsistencies indicative of manipulation (Kolagati *et al.,* 2022). These inconsistencies, often invisible to the human eye, can expose deepfakes. Additionally, Matern *et al.* (2019) propose analyzing facial data for visual artifacts during enrollment, further preventing the registration of falsified identities. Additionally, embedding invisible watermarks into facial images with distortions that raise red flags during enrollment can further strengthen defenses (Albahar and Almalki, 2019; Lv, 2021). Gaze tracking technology, which identifies unnatural eye movements, adds another layer to this comprehensive approach (Demir and Ciftci, 2021).

To strengthen Aadhaar's authentication phase against Deepfakes, advanced techniques like iFace 1.1, SegNet, and LBPNet can be implemented. iFace 1.1 excels at detecting subtle facial inconsistencies, while SegNet tackles limitations of specific forgery techniques (Mitra *et al.,* 2021; Yu *et al.,* 2022). LBPNet leverages a CNN model for detailed texture analysis through Local Binary Patterns (Kingra *et al.,* 2022). During authentication, the system can combine iFace 1.1 or SegNet for inconsistency detection with LBPNet's texture analysis, creating a multi-layered defense against Deepfakes. While implementing these advanced techniques requires careful consideration of training data, computational resources, and ethical implications, their integration can significantly fortify Aadhaar's security framework, safeguarding its integrity and user trust.

Data breaches and leaks on the dark web can expose biometric data, fueling deepfake attacks with more convincing forgeries. To counter this, a comprehensive cybersecurity strategy is essential. One approach is leveraging blockchain and IPFS technologies. These can provide tamper-proof data storage and clear data provenance (Hasan and Salah, 2019). This means if a leak occurs, authorities can trace the data back to its origin, potentially exposing dark web sales and aiding investigations. This transparency can deter attackers and make Aadhaar a less attractive target. Additionally, differential privacy techniques (Dash and Sharma, 2023) can add a layer of protection by masking user data while maintaining its usability for Aadhaar's functions.

Zero Trust security principles can also be valuable (Mahmoud *et al.,* 2022). This approach emphasizes verifying every access attempt and granting minimal privileges. In enrollment centers, Zero Trust can require multi-factor authentication for staff logins and restrict access to enrollment software functionalities. This approach hinders unauthorized modifications or deepfake data injection.

Staying ahead of deepfake advancements is crucial. Aadhaar's AI models used for authentication need regular updates with data from cutting-edge deepfake techniques (Naitali *et al.,* 2023). This can involve incorporating data like synthetic fingerprints (Bontrager *et al.,* 2018) or iris image datasets (Wang *et al.,* 2022) into the training process. By constantly learning about new deepfake methods, the AI models can effectively identify and prevent forgeries during enrollment.

Beyond technology, empowering users and personnel is another critical defense layer. Effective cybersecurity awareness training should emphasize reporting suspected deepfake attempts (Cinar, 2023). Aadhaar personnel need to understand reporting procedures and who to contact in such situations. Public awareness campaigns are equally important. Studies show users often struggle to distinguish real from deepfake content (Köbis *et al.,* 2021). Campaigns can equip individuals to recognize suspicious activities and avoid deepfake-based scams (Lacobucci *et al.,* 2021). Additionally, campaigns can educate users on how to identify and report suspicious activity related to Aadhaar. Reminding citizens not to reveal their Aadhaar numbers publicly or use them for unnecessary services can further strengthen security.

However, the battle against deepfakes is an ongoing one. Continuous advancements in deepfake technology necessitate regular updates to AI models and implementation of new detection methods. By remaining vigilant and adapting these strategies, Aadhaar can maintain its integrity as a cornerstone of India's digital identity framework.

Limitations and Future Research Considerations:

This article explores strategies to combat DeepFake threats to Aadhaar security. However, the research has limitations that point to valuable avenues for future exploration.

Firstly, the ethical implications of DeepFakes warrant a more in-depth analysis. While the paper identifies potential issues like privacy violations and misuse, a comprehensive understanding requires a nuanced evaluation of societal values and potential unintended consequences (de Ruiter, 2021).Further research involving ethicists, policymakers, and technologists is crucial to ensure responsible use of these technologies. Additionally, the paper highlights potential mitigation strategies, but lacks specifics on implementation. Determining the most practical and cost-effective ways to integrate these technologies into Aadhaar's existing infrastructure requires collaboration between security specialists, Aadhaar administrators, and developers. Future research should involve detailed feasibility studies that address training data requirements, computational resource needs, and integration challenges. Finally, while the paper acknowledges the importance of a robust legal framework, providing specific recommendations is beyond its scope. The legal landscape surrounding DeepFakes and biometric data security is constantly evolving. Examining potential legal frameworks and their effectiveness in deterring DeepFake attacks necessitates ongoing legal expertise. Future research should explore potential legal solutions in collaboration with legal scholars specializing in technology and data security law. Addressing these limitations will contribute to a more comprehensive and ethically sound approach to safeguarding Aadhaar against the evolving threat of DeepFakes.

Conclusion

This scoping review identified 36 articles that analyzed the threat DeepFake technology poses to Aadhaar, India's vast identity database. By examining research and real-world cases, it identified vulnerabilities in Aadhaar's system, such as data leaks and Aadhaar system's limitations in fingerprint and iris verification. DeepFakes' ability to create realistic synthetic faces, fingerprints, voices, and iris scans poses a significant security risk. The review proposes a multi-layered defense strategy. This includes advanced AI analysis during enrollment to detect manipulated data using techniques like analyzing facial points, embedding invisible watermarks, and tracking eye movements. Additionally, techniques like iFace 1.1, SegNet, and LBPNet can strengthen authentication by identifying inconsistencies in facial data. Furthermore, the review emphasizes the importance of a comprehensive cybersecurity strategy. This includes robust data security measures like Blockchain and IPFS, differential privacy, Zero Trust security, regular updates to AI models to stay ahead of evolving DeepFake technology, and user education initiatives to raise awareness of this cyber threat. Implementing the proposed recommendations can fortify Aadhaar against DeepFakes. However, the research acknowledges certain limitations. The ethical implications of DeepFakes, the specifics of implementing the proposed mitigation strategies, and the evolving legal landscape surrounding DeepFakes and biometric data security are areas that warrant further exploration. As DeepFake technology advances, so must our defenses. Future research should address these limitations, explore legal solutions, and stay ahead of DeepFake advancements. This review paves the way for a more secure digital future by highlighting the need for enhanced security measures and robust authentication protocols to combat DeepFakes. By staying vigilant and adapting, we can ensure the continued security of Aadhaar and similar systems.

Conflict of Interest

The Authors declare no conflict of interest.

References

Amezaga, N., Hajek, J. 2022. Availability of Voice Deepfake Technology and its Impact for Good and Evil. In Proceedings of the 23rd Annual Conference on Information Technology Education. Association for Computing Machinery, 23–28. https://doi.org/10.1145/3537674.3554742

Albahar, M., Almalki, J. (2019). Deepfakes: Threats and countermeasures systematic review. J. Theor. Appl. Inf. Technol. 97(22), 3242-3250.

Arksey, H., O'Malley, L. (2005). Scoping studies: towards a methodological framework. Int. J. Soc. Res. Methodol. 8(1), 19–32. https://doi.org/10.1080/1364557032000119616

Bontrager, P., Roy, A., Togelius, J., Memon, N., Ross, A. 2018. DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution. In 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, pp. 1-9.

Cinar, B. 2023. Deepfakes in Cyber Warfare: Threats, Detection, Techniques and Countermeasures. Asian J. Res. Comput. Sci. 16, 178-193.

Dash, B., Sharma, P. 2023. Are ChatGPT and deepfake algorithms endangering the cybersecurity industry? A review. Int. J. Eng. Appl. Sci. 10(1), 21-39.

de Ruiter, A. 2021. The Distinct Wrong of Deepfakes. Philos. Technol. 34(4), 1311-1332. https://doi.org/10.1007/s13347-021-00459-2

Demir, I., Ciftci, U. A. 2021. Where Do Deep Fakes Look? Synthetic Face Detection via Gaze Tracking. In ACM Symposium on Eye Tracking Research and Applications. Association for Computing Machinery, Article 6, 1–11. https://doi.org/10.1145/3448017.3457387

Firc, A., Malinka, K., Hanáček, P. 2023. Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. Heliyon, 9(4). e15090.doi: 10.1016/j.heliyon.2023.e15090.

Georgopoulos, M., Oldfield, J., Nicolaou, M.A., Panagakis, Y., Pantic, M. 2020. Enhancing Facial Data Diversity with Style-based Face Aging. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 66-74.

Hasan, H. R., Salah, K. (2019) Combating Deepfake Videos Using Blockchain and Smart Contracts. IEEE Access. 7, 41596-41606. doi: 10.1109/ACCESS.2019.2905689

HT Correspondent. 2021. Fake Aadhaar enrolment center uncovered in Ludhiana, three held. Hindustan Times. URL https://www.hindustantimes.com/cities/chandigarh-news/fake-aadhaar-enrolment-centre-uncovered-in-ludhiana-three-held-101627844124266.html. (Accessed on 6. 10. 2023)

Lacobucci, S., De Cicco, R., Michetti, F., Palumbo, R., Pagliaro, S. 2021. Deepfakes Unmasked: The Effects of Information Priming and Bullshit Receptivity on Deepfake Recognition and Sharing Intention. Cyberpsychol. Behav. Soc. Netw. 24(3), 194-202

Jha, R. 2023. How crooks are exploiting gaps in Aadhaar system in Delhi. Times of India URL http://timesofindia.indiatimes.com/articleshow/98744284.cms. (Accessed on 9. 10, 2023.)

Karras, T., Laine, S., Aila, T. (2019). A style-based generator architecture for generative adversarial networks. In 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 4396-4405.

Kingra, S., Aggarwal, N., Kaur, N. 2022. LBPNet: Exploiting texture descriptor for deepfake detection. Forensic Sci. Int.: Digit. Investig. 42-43, 301452. https://doi.org/10.1016/j.fsidi.2022.301452

Kobis, N., Doležalová, B., Soraperra, I. 2021. Fooled twice - People cannot detect deepfakes but think they can. iScience, 24, 103364. https://doi.org/10.1016/j.isci.2021.103364

Kolagati, S., Priyadharshini, T., Rajam, V. M. A. 2022. Exposing deepfakes using a deep multilayer perceptron – convolutional neural network model. Int. J. Inf. Manag. Data Insights. 2(1), 100054. https://doi.org/10.1016/j.jjimei.2021.100054

Lv, L. 2021. Smart Watermark to Defend against Deepfake Image Manipulation. In 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS), Chengdu, China, pp. 380-384.

Mahmoud, A., Nyamasvisva, T., Valloo, S. 2022. Zero Trust Security Implementation Considerations in Decentralized Network Resources for Institutions of Higher Learning. International Journal of Infrastructure Research and Management. 10(1), 79-90.

Makrushin, A., Uhl, A., Dittmann, J. 2023. A Survey on Synthetic Biometrics: Fingerprint, Face, Iris and Vascular Patterns. IEEE Access, 11, 33887-33899.

Matern, F., Riess, C., Stamminger, M. 2019. Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations. In 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW), pp. 83-92. https://doi.org/10.1109/WACVW.2019.00020

MC, A., Shanmugam, K. 2023. Implementing unique identification technology: The journey and success story of Aadhaar in India. J. Inf. Technol. Teach. Cases. 0(0). https://doi.org/10.1177/20438869231200286

Mcuba, M., Singh, A., Adeyemi, I., Venter, H. (2023). The effect of deep learning methods on deepfake audio detection for digital investigation. Procedia Comput. Sci. 219, 211-219. https://doi.org/10.1016/j.procs.2023.01.283

Miller, E. J., Steward, B. A., Witkower, Z., Sutherland, C. A. M., Krumhuber, E. G., Dawel, A. (2023). AI Hyperrealism: Why AI Faces Are Perceived as More Real Than Human Ones. Psychol. Sci. 34(12), 1390-1403. https://doi.org/10.1177/09567976231207095

Ministry of Electronics & IT. 2023. UIDAI rolls out new security mechanism for robust fingerprint based Aadhaar authentication. Press Information Bureau. URL: https://pib.gov.in/PressReleasePage.aspx?PRID=1902822 (Accessed on 6. 10. 2023)

Mirsky, Y., Lee, W. 2022. The Creation and Detection of Deepfakes: A Survey. ACM Comput. Surv.54(1), Article 7. 1-41 https://doi.org/10.1145/3425780.

Mitra, A., Mohanty, S. P., Corcoran, P., Kougianos, E. 2021. iFace: A Deepfake Resilient Digital Identification Framework for Smart Cities. In: 2021 IEEE International Symposium on Smart Electronic Systems (iSES), Jaipur, India. 361-366

Naitali, A., Ridouani, M., Salahdine, F., Kaabouch, N. 2023. Deepfake Attacks: Generation, Detection, Datasets, Challenges, and Research Directions. Computers, 12(10), 216. https://doi.org/10.3390/computers12100216

Nightingale, S. J., Farid, H. 2022. AI-synthesized faces are indistinguishable from real faces and more trustworthy. Proc. Natl. Acad. Sci, U.S.A. 119(8), e2120481119. https://doi.org/10.1073/pnas.2120481119

Pham, M. T., Rajić, A., Greig, J. D., Sargeant, J. M., Papadopoulos, A., McEwen, S. A. (2014). A scoping review of scoping reviews: advancing the approach and enhancing the consistency. Res. Synth. Methods. 5(4), 371–385. https://doi.org/10.1002/jrsm.1123

Peidro-Paredes, M., De Fuentes, J. M., González-Manzano, L., Velasco-Gomez, M., 2023. Characterizing the MasterPrint threat on Android devices with capacitive sensors. In: Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). Association for Computing Machinery. 16, 1-11. https://doi.org/10.1145/3600160.3600177

Safi, M. 2018. India national ID database data leak bought online. The Guardian. URL https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar. (Accessed on 7. 10. 2023)

Singh, P. 2021. Aadhaar and data privacy: Biometric identification and anxieties of recognition in India. Inf. Commun. Soc. 24(7), 978–993. https://doi.org/10.1080/1369118X.2019.1668459

Singh, R. 2023. The curious case of tweeting an Aadhaar number: Trust/mistrust in security practices of public data infrastructures. J. Cult. Econ. 1–18. https://doi.org/10.1080/17530350.2023.2229360

Special Correspondent. 2021. Cyber startup says Tamil Nadu's PDS data breached. The Hindu. URL https://www.thehindu.com/news/national/tamil-nadu/cyber-startup-says-tamil-nadus-pds-data-breached/article35088967.ece1. (Accessed on 7. 10. 2023)

Tiwari, P. R., Agarwal, D., Jain, P., Dasgupta, S., Datta, P., Reddy, V., Gupta, D. 2022. India's "Aadhaar" Biometric ID: Structure, Security, and Vulnerabilities. Cryptology ePrint Archive, Paper 2022/481. URL: https://eprint.iacr.org/2022/481 (Accessed on 7. 1. 2023)

Tyagi, A. K., Rekha, G., Sreenath, N. 2018. Is your Privacy Safe with Aadhaar?: An Open Discussion. In 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, India, pp. 318-323.

Wang, C., He, Z., Wang, C., Tian, Q. (2022). Generating Intra- and Inter-Class Iris Images by Identity Contrast. 2022 IEEE International Joint Conference on Biometrics (IJCB), 1-7. doi: 10.1109/IJCB54206.2022.10007974.

Yu, C. M., Chen, K. C., Chang, C. T., Ti, Y. W. 2022. SegNet: a network for detecting deepfake facial videos. Multimed. Syst. 28(3) 793–814.