Generative AI in Cybercrime: A Security Analysis of Deepfakes Technologies

Morgan Brunner – Montana State University
Mentors: Dr. Clemente Izurieta & Yvette Hastings

Introduction

Deepfake technology, powered by advances in artificial intelligence and deep learning, has significantly changed how digital media is created and manipulated. Deepfakes are highly realistic synthetic images, audio, or videos that can imitate real people and events. As these technologies improve, they are becoming harder to detect and are more accessible to the public.

Recent research shows that deepfakes pose serious risks to cybersecurity, public trust, and digital communication. They are increasingly used for misinformation, identity theft, and fraud, while also damaging reputations and influencing public opinion.

In addition, studies highlight that deepfakes are spreading rapidly due to social media and can be nearly indistinguishable from real content, making them a growing threat to both individuals and organizations.

This research analyzes how deepfake technology is used in cybercrime and evaluates possible countermeasures to reduce these risks.

Research Methods

A literature review was conducted using the search string ‘Generative AI in Cybercrime’ on Google Scholar. Search criteria was: is the paper about deepfakes specifically/ is it from the 2000s/ is the paper’s topic directly related to AI security measures. After criteria was met, there were about 3870 papers, of which I read 16 abstracts and used 7 in this project.

Attack Methods [1,2,3,4,6,7]

Identity Fraud & Social Engineering
- Attackers use deepfake audio or video to impersonate trusted individuals
- Used in financial scams and phishing attacks

Disinformation & Political Manipulation
- Fake videos of public figures can influence elections and public opinion
- Deepfakes can spread quickly through social media platforms

Reputational Attacks & Harassment
- Used to create fake or harmful content targeting individuals
- Includes blackmail, defamation, and harassment

Biometric Spoofing
- Deepfakes can bypass facial recognition and voice authentication systems
- Exploits weaknesses in digital security systems

Physical Countermeasures [2]

Restricted Access to Sensitive Systems
- Limit physical access to devices used for authentication

Secure Data Collection Environments
- Prevent unauthorized recording of voice or facial data

Employee Awareness Training
- Train users to question suspicious audio/video communications

Device Monitoring & Control
- Prevent unauthorized use of cameras and microphones

Virtual Countermeasures [2,3]

Deepfake Detection Algorithms
-Use AI to identify inconsistencies in facial movement, lighting, or audio patterns
-However, detection systems can be bypassed by newer techniques

Multi-Factor Authentication (MFA)
- Reduces reliance on biometric-only systems

AI-Based Forensic Analysis
- Detects manipulation at the frame or signal level

Encryption & Secure Systems
-Protects sensitive communications from interception

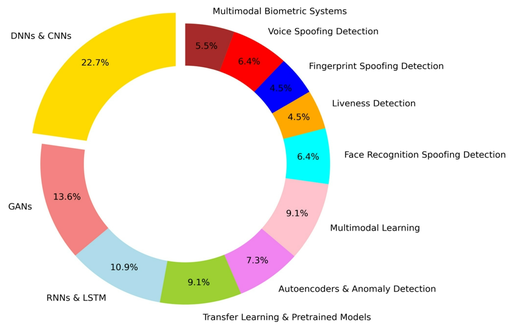

Figure 1. Shows the realistic percentages of how above mentioned technologies contribute to overall detection of deepfakes Figure from [3].

Other Countermeasures [1,3,4,5]

Legal and Policy Development
-Current laws struggle to keep up with deepfake technology
-New regulations are needed to address misuse

Platform Moderation Improvements
-Social media companies must improve detection and removal systems

Public Awareness and Education
- Educating users reduces the effectiveness of deepfake attacks

Continuous Research and Innovation
-Ongoing improvements are needed as deepfake technology evolves

Conclusion

Deepfake technology presents a growing cybersecurity threat due to its ability to manipulate realistic digital media. It is increasingly used for fraud, misinformation, and identity-based attacks, making it a large threat to cybersecurity.

Although detection tools and security measures exist, research shows that they are not always reliable and can be bypassed by advanced techniques. This creates a continuous challenge for cybersecurity professionals.

To effectively address this issue, a combination of technical solutions, physical security measures, policy development, and user awareness is required. As deepfake technology continues to evolve, organizations must remain proactive to protect digital trust and security.

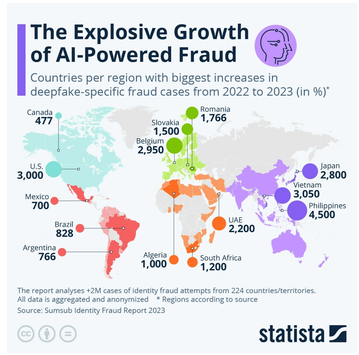

Figure 2. This chart shows the countries per region with biggest increases in deepfake-specific fraud cases. Figure from https://www.statista.com/chart/31901/countries-per-region-with-biggest-increases-in-deepfake-specific-fraud-cases/?srsltid=AfmBOor2jzc3NMRqp8JHBYn1LW_rBFUnq5Ika94Ubd6xilbXfPhvVgFx

Acknowledgements

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.

References

[1] U.S. Government Accountability Office, Deepfakes and Artificial Intelligence, 2020. https://www.gao.gov/assets/gao-20-379sp.pdf
[2] Department of Homeland Security, Increasing Threats of Deepfake Identities, 2021. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf
[3] ScienceDirect, Unmasking Digital Deceptions: Deepfake Detection and Cybersecurity Challenges, 2025. https://www.sciencedirect.com/science/article/pii/S2215016125004765
[4] ScienceDirect, Deepfakes and AI-Driven Disinformation: A Systematic Review, 2026. https://www.sciencedirect.com/science/article/abs/pii/S104732032600043X
[5] TechReg, Deep Fake Technology: Legal Framework and the Way Forward, 2024. https://www.researchgate.net/publication/381482955_DEEP_FAKE_TECHNOLOGY_ANALYSIS_OF_LEGAL_FRAMEWORK_AND_THE_WAY_FORWARD
[6] International Journal of Emerging Technolo
gies in Computer Science and IT, Deepfake Technology and Cybersecurity Implications, 2025. https://womencourage.acm.org/2025/wp-content/uploads/2025/12/Cybersecurity-and-Deepfake-technology-Challenges-and-educational-implications.pdf
[7] Journal of Cyber Security (IngentaConnect), Deepfake Threats and Countermeasures, 2025. https://www.researchgate.net/publication/391397479_Deepfake_Threats_Detection_and_Countermeasures_in_Cybersecurity