European Economic Letters
ISSN 2323-5233
Vol 15, Issue 2 (2025)
http://eelet.org.uk

# Deepfake Technology & Financial Frauds: Awareness, Risks and Prevention Strategies

**Dr. (CS) Shital Mehta**
*Dr. Shantilal K Somaiya School of Commerce and Business Studies Somaiya Vidyavihar University Vidyavihar East. Mumbai*

**Dr. Harshali Patil**
*Somaiya School of Basic and Applied Sciences Somaiya Vidyavihar University Vidyavihar East. Mumbai*

**Ms. Mehek Meghani**
*UG Student Dr. Shantilal K Somaiya School of Commerce and Business Studies Somaiya Vidyavihar University Vidyavihar East. Mumbai*

## Abstract:

This study explores public perception, awareness, and readiness towards deepfake- associated financial fraud. Although individuals are wary of scams, their knowledge of deepfake fraud is minimal, and most want more information. Most of them depend on reactive approaches, such as not responding to unfamiliar contacts, instead of employing proactive security devices or reporting a scam. Total 83 participants with varying backgrounds were assessed to evaluate awareness, attitudes towards deepfake fraud and security behaviour. The research highlights the knowledge gaps and security steps, with a focus on more rigorous education and fraud prevention.

## KeyWords:

Deepfake Technology, Artificial Intelligence, Financial Fraud

## Introduction:

Deepfake technology means the application of artificial intelligence (AI) and machine learning (ML) to produce very realistic but artificial images, videos, and audio recordings of individuals. Deepfake technology imitates an individual’s facial expressions, voice, and body movements and make it seem like they spoke or did something they never even did. They accomplish this by learning from huge databases of real media. This technology embraces machine learning software to utilize someone's face, voice, or image in artificial media to provide the illusion that they are doing things they never did.

Deepfakes are created by artificial intelligence programs that utilize a range of built-in technologies to create new audio and video content. It creates the content using overlay, altering, and mixing audio and video in such a way as to fabricate and disseminate convincing content. Deep Fakes are seen in many forms, including face reenactment where faces are altered through manipulation by a person. It also involves face generation, whereby new faces are created with no counterpart in reality. It is also possible for it to occur in the manner of face swapping, whereby someone's face is replaced with someone else's; and speech synthesis, whereby voices are rebuilt. There is also a growing threat worldwide because deepfakes have been misused to spread false information, encroach on people's privacy, and commit cybercrime.

They hold the potential tools for manipulation and misinformation. They can be utilized to impersonate corporate executives in financial scams, fabricate deceptive evidence in legal cases, or manipulate the stock market prices with false information. The ease of access and use enhances its potential harm, as it becomes more challenging to identify and distinguish between authentic and forged content. India is getting most vulnerable to deepfake attacks because of its rapidly evolving digital environment and growing access to computer technology, AI developments and extensive use of smartphones.

Terrifyingly, over 75% of Indians on the internet have been exposed to deepfake content in the past year alone, and awareness and prevention are urgently needed. Abuse of deepfakes poses a significant risk to Indian businesses, individuals, and society at large. From sulllying corporate reputations to spreading misinformation at election times, deepfakes threaten data privacy, brand reputation, and public trust. The Deepfakes Analysis Unit (DAU) under the Misinformation Combat Alliance is one of the notable initiatives in India. Started in March 2024, shortly before the Indian elections, the DAU offers a public service via an exclusive WhatsApp tipline.

This allows individuals to forward suspected deepfake content, particularly audio and video files, for analysis. The DAU has received hundreds of submissions since it was launched and has detected varying levels of AI manipulation and helped curb the spread of dangerous deepfakes. Financial fraud is a form of financial crime perpetrated when an individual takes money, capital, or otherwise damages one's financial well-being with deceitful, misleading, or other unlawful means.These schemes can range from simple scams like payment of gas bill of a minimal amount to complex operations such as pyramid schemes.Financial fraud is a financial crime perpetrated when an individual is deprived of their money, capital, or otherwise damage one's financial well-being by fraudulent, misleading, or other unlawful means. The schemes may be as straightforward as a small payment of gas bills to a well-established business like pyramid schemes. Financial fraud takes the form of Identity theft, Phishing, Investment scams, credit card fraud, Insurance fraud, tax fraud, loan scam, money laundering and likewise.

## Review of Literature:

In this study, the authors analyse the capabilities of deepfakes in crafting realistic spear phishing scenarios and assess their impact on individuals. Their findings indicate that a considerable proportion of participants are unable to recognize AI-generated audio and video as fraudulent, underscoring the risks associated with these technologies when exploited by malicious entities. The paper establishes a direct link between deepfake technology and financial fraud by illustrating how it can be employed to orchestrate misleading spear phishing attacks. The research highlights the concerning accuracy of deepfakes and their ability to mislead even the most vigilant individuals, representing a significant threat to both financial institutions and private individuals. (Kemp, Kalutarange & Al-Kadri)

The research article explores how AI-generated media manipulates images and videos, offering both positive applications (entertainment, education) and serious risks (misinformation, identity theft, and fraud). Deepfakes can erode public trust and pose security threats. In financial fraud, cybercriminals use deepfakes to impersonate executives, tricking employees into authorizing fraudulent transactions. Real cases show millions lost due to deepfake scams. This highlights the urgent need for AI-driven detection tools, stronger security protocols, and media literacy to counteract these risks. (Understanding of deepfakes, Cybersecurity Centre of Excellence).

This research focused on the dual nature of deepfake technology. The report provides a comprehensive description of how deepfakes enable financial fraud, such as impersonating corporate leaders to approve fraudulent transactions, bypassing biometric security, and influencing stock markets with false news and false statements. In addition, it discusses the application of deepfakes in blackmail, extortion, and political deception. The chapter highlights the urgent need for more effective detection techniques, regulation, and cooperation between nations to counter the mounting risks posed by deepfake technology. (Deepfakes and Their impact on business, Svetlana Volkova)

## Research Methodology:

### Identification of problem:

Deepfake technology is advancing rapidly, posing significant threats to financial security. Fraudsters exploit this technology to manipulate digital identities, deceive individuals, and conduct financial scams. The study aims to assess public awareness of deepfake threats, their perception of risks, and the effectiveness of current mitigation strategies

### Data Collection:

Sample selection is done by using convenience sampling technique. Primary Data is collected through Questionnaires and personal interviews of the respondents by the researchers. After discarding the incomplete and inappropriate responses, a total of 83 usable responses were used for the purpose of analysis.

### A Sample size :

The study collected responses from 83 respondents of a diverse group representing different age groups, professions, and levels of familiarity with financial transactions and cybersecurity. The final sample size consists of survey respondents from varied demographics.

### B. Universe of study:

The research targets individuals who engage in online financial transactions, including banking, digital payments, and investments. Respondents include students, employed professionals, and retirees.

### C. Limitations of the study:

o The study is based on self-reported survey data, which may include biases in responses.

o Limited geographic representation may not capture variations in deepfake-related financial fraud across different regions.

o The study does not include technical evaluations of deepfake detection algorithms but focuses on public perception and awareness.

o The rapidly evolving nature of deepfake technology may introduce challenges in keeping findings up-to-date.

## Objectives of study

1. To evaluate the level of awareness regarding deepfake technology and its risks.
2. To analyse public perception of existing security measures by financial institutions.
3. To identify effective strategies for preventing deepfake-related financial fraud.
4. To explore the role of regulatory frameworks and technological advancements in combating deepfake fraud.

**Hypothesis**

H1: There is a significant relation between age group and awareness of deepfake technology.
H0: There is no relationship between age group and awareness of deepfake technology.
To test the hypothesis, Chi-Square test is applied.

| Transaction Frequency | Observed contingency | | | Expected Frequencies | | |
|---|---|---|---|---|---|---|
| | No | Not Sure | Yes | No | Not Sure | Yes |
| 18-25 | 3 | 2 | 24 | 4.89 | 2.80 | 21.31 |
| 26-40 | 2 | 0 | 10 | 2.02 | 1.16 | 8.82 |
| 41-55 | 6 | 3 | 15 | 4.05 | 2.31 | 17.64 |
| Above 55 | 3 | 3 | 12 | 3.04 | 1.73 | 13.23 |

| Chi-Square test | Degree of Freedom (df) | p-value |
|---|---|---|
| 5.188 | 6 | 0.520 |

As p value > 0.05 here, we fail to reject null hypothesis. This leads to the conclusion that There is a significant relationship between age group and awareness of deepfake technology.
H2:Awareness on deepfake technology increases with higher online transaction frequency
H0: There is no association between awareness of deepfake technology and frequency of online transaction

To test the hypothesis, Chi-Square test is applied.

| Transaction Frequency | Observed contingency | | | Expected Frequencies | | |
|---|---|---|---|---|---|---|
| | No | Not Sure | Yes | No | Not Sure | Yes |
| Daily | 10 | 4 | 47 | 10.29 | 5.88 | 44.83 |
| Monthly | 0 | 1 | 3 | 0.67 | 0.39 | 2.94 |
| Never | 3 | 0 | 1 | 0.67 | 0.39 | 2.94 |
| Rarely | 0 | 1 | 0 | 0.17 | 0.10 | 0.73 |
| Weekly | 1 | 2 | 10 | 2.19 | 1.25 | 9.55 |

| Chi-Square test | Degree of Freedom (df) | p-value |
|---|---|---|
| 22.54 | 8 | 0.004 |

As p value < 0.05 here, we reject null hypothesis. This leads to the conclusion that Awareness on deepfake technology increases with higher online transaction frequency.

H3: Individuals targeted by scams are more likely to verify financial messages.

H0: There is no association between scam targeted individuals and their verification of financial messages.

To test the hypothesis, the Chi-Square test is applied.

| Targeted by Scam | Observed contingency | | | | | Expected Frequencies | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Always | Never | Often | Rarely | Sometimes | Always | Never | Often | Rarely | Sometimes |
| May be | 3 | 2 | 1 | 0 | 4 | 4.82 | 0.84 | 2.53 | 0.36 | 1.45 |
| No | 20 | 3 | 10 | 3 | 7 | 20.72 | 3.63 | 10.88 | 1.55 | 6.22 |
| Yes | 17 | 2 | 10 | 0 | 1 | 14.46 | 2.53 | 7.59 | 1.08 | 4.34 |

| Chi-Square test | Degree of Freedom (df) | p-value |
|---|---|---|
| 14.70 | 8 | 0.065 |

As p value > 0.05 here, null hypothesis is rejected.This leads to the conclusion that Individuals targeted by scams are more likely to verify financial messages.

**Conclusion:**

The findings reveal that although most individuals are aware of the dangers of financial fraud and take some precautions, their measures are more geared towards responding to scams than proactive prevention. Most people cross-check sources, avoid suspicious transactions, and ignore strange messages or calls. Fewer still take active steps like reporting frauds or adopting additional security measures. One of the important observations of the research is the general mistrust of electronic communication in financial transactions. Due to the prevalence of scam calls, emails, and messages, people have grown accustomed to a blanket distrust of any financial message. While such distrust can help avoid some disadvantages, it also increases the challenges for genuine banks and companies to establish trust with customers. The study also established that most individuals feel they lack the ability to cope with scams from deepfake technology. As much as there is keen interest in learning about such scam operations and counter-measures, the majority of them feel that the information remains insufficient. Such easy precautions as reviewing bank accounts and avoiding making known contacts are beneficial but ineffective when dealing with sophisticated scams involving faked videos and voice recordings. In order to protect themselves effectively, people need to improve their knowledge of cybersecurity technologies and anti-fraud techniques and methods, incorporating such approaches into their everyday lives. The other significant observation is the widespread skepticism about deepfakes. Most people view it only negatively, even though it can be used for detecting fraud and authenticating identities. The word "deepfake" itself is usually connected with negative connotations, so people assume that it is used only for evil purposes.

Future studies will need to uncover why previous scam exposure does not always translate to more secure financial behavior and seek out targeted intervention for low transactions. As awareness is not age-specific, far-reaching, behavior-based awareness initiatives should be accorded high priority. Moreover, creating user-friendly tools and policy-level frameworks have the potential to improve public defense against deepface-facilitated financial scams.

**References:**

1. Kemp, M., Kalutarage, H., & Al-Kadri, M. O. (2005). AI-Powered Spearphishing Cyber Attacks: Fact or Fiction. doi:10.48550/arXiv.2502.00961
2. Understanding deepfakes: how they work and why they matter. (n.d.). Cybersecurity Centre of Excellence (CCoE). https://ccoe.dsci.in/blog/understanding-deepfakes
3. A. Vig, Shinu. "Regulating Deepfakes: An Indian perspective." Journal of Strategic Security 17, no. 3 (2024) : 70-93. Doi:: https://doi.org/10.5038/1944-0472.17.3.2245
4. The Dark Side of Deepfakes: Fraud and Cybercrime, Svetlana Volkova (Vologda State University, Russia), IGI Global Scientific Publishing https://www.igi-global.com/chapter/the-dark-side-of-deepfakes/364354
5. https://www.indiancybersquad.org/post/case-study-kerala-s-first-deepfake-fraud
6. https://www.businessworld.in/article/indias-deepfake-cases-up-550-losses-may-hit-rs-70000-cr-by-2024-report-541202