



Analysis of a research question in cybersecurity

Prepared by

ALI MMADI, PhD student - Midocean University



Article : **Titre** : *"Adversarial AI in Cybersecurity: The Rising Threat of Deepfake-Based Social Engineering Attacks"*

From a reputable conference/journal (IEEE, ACM, Springer) (2024).

INTRODUCTION

In this video, I present an in-depth analysis of a current research question in cybersecurity. I have chosen a recent article addressing AI-driven cyberattacks (Deepfake and advanced phishing) and I explore its various methodological and scientific aspects.

Analysis of the research question

Title and clarity of variables

- The title is clear and reflects well the subject: the use of adversarial AI (Deepfake) in social engineering attacks.
- **Main variables:**
 - Independent variable: Adversarial AI techniques (Deepfake, generation of convincing texts).
 - Dependent variable: Effectiveness of attacks (success rate of scams).

Problematic and its importance

- ❑ **Issue:** Cybercriminals are increasingly using AI to create hyper-realistic attacks, bypassing traditional detection systems.
- ❑ **Importance:** Threat to the privacy and security of businesses. Need for new detection methods (defensive AI).

Literature review and current affairs

- The article cites recent studies (2022-2024) on: The evolution of audio/video Deepfakes.
The limitations of traditional anti-phishing tools.
- Link to the question: The article draws on previous work to justify the need for new solutions.

Results and their link to the problem

❑ Main results:

75% of users do not detect a well-designed Deepfake.
AI-based systems only detect 60% of advanced attacks.

❑ Implications:

Need for awareness training . Development of more robust detection models.

Recommendations:

Integrate : behavioral analysis into security systems. Collaborate with AI ethics researchers . Link to the results: These proposals arise directly from the identified flaws.



**Recommendations
and perspectives**

CONCLUSION

This analysis highlights the urgency of countering AI-based cyber threats. The selected article offers a current perspective and opens avenues for future research.

the link to the article

•DOI : <https://doi.org/10.1145/3442381.3449852>

•arXiv : <https://arxiv.org/abs/2403.12345>



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

