WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Detection of Synthetic Fraud Schemes

Manasa Sriram, Nidhish Nutakki, Veerabhadra Yerram

Course Based Project under Business Communication and Value Science.
Computer Science and Business Systems Department, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad India.

ABSTRACT

The rise of the sense of interconnection between people all over the world has created a medium for fraudulent activities. These fraudulent activities have crucially led to damage to various organisations and individuals. Fraudsters have evolved significantly, employing the latest cutting-edge technology in order to portray frauds. This rise in complicated and polished fraud techniques provokes the necessity to explore innovative solutions to detect and report different kinds of frauds. Artificial Intelligence has proven to be a sophisticated tool for detecting fraudulent activities, enhancing the ability to detect frauds and offering propitious capabilities to fine tune the working of fraud detection systems.

This research paper dwells deeper into the detection of Artificial Intelligence generated and based synthetic fraud schemes. It explores the pathway where fraudsters use artificial intelligence to create fake identities and doom people and influence them, making people exploitable.

KEYWORDS : Artificial Intelligence, Fake Identity, Synthetic Voices, Generative Adversarial Networks, Deepfake, Corporate Scams, Cybersecurity.

INTRODUCTION

Mankind has advanced in terms of connection with the entire world. There has been a rapid growth in various activities that could be performed with access to the internet. With increase to the exposure, fraudulent activities have poached people's pockets. Various kinds of frauds have become a critical issue in the society, causing pressing concerns to individuals, business and government organisations.This surge in digital dependency has exposed people to greater risks and encourages fraudsters to further explore vulnerabilities. Complimentarily, Artificial Intelligence has made vast strides in terms of usability by the general public. Fraudsters too have engaged in using artificial intelligence to intensify the fraudulent acts. Using AI to create fake documents and schemes, identities and video proofs. Ultimately, this forges the need to create innovative solutions to detect fraud, thereby, preventing people from getting exploited. We initiate our research by surveying how AI can, and is being used by fraudsters engaging in synthetic frauds. This ventures our thinking into how the frauds gain the people's trust. We will explore how artificial intelligence can be detected effectively. Further, ideas on different types of frauds that exist and how new frauds could possibly be created uplifts the interest on limiting such open-minded pathways.

LITERATURE SURVEY

In the modern technologized Era, AI-powered Fraud is a most concerning challenge, where the criminals use artificial intelligence and create fake identities, fake voice and documents. We are unable to detect the following systems since they are very realistic.

1. Synthetic identity frauds

AI can generate realistic identities which can't be even detected in verification checks, biometrics and other graphical analysis. Identity thefts are a very rare cause of these. The frauds use the IDs to impersonate others and to access accounts and services in their name. The criminals enter other countries with fake IDs and it is one of the causes for destruction. The fake IDs are used for multiple purposes like entering properties, labs, military bases and many other areas and stealing the information, which misleads them.

2. AI forged documents

The GANs(Generative Adversarial Networks) are used to create fake documents making it difficult to identify if it's fake or not. The forensic tools are also not able to detect AI generated forgeries. These documents are then used to mislead the companies, industries or any working areas. Fraud payments can be made using documents. The frauds can gain unauthorized access to resources which leads to financial loss. The criminals can open accounts, obtain loans and get credits using the fake docs.

3. Deep Fake voices and fraud videos

The advanced technologies have a lot of impact on financial frauds, corporate scams and misleading information. The frauds make fake calls to detect our voices and then record it. After recording they use AI to create very similar audio features and use our voices elsewhere. They also use our face identity to create fraud videos and use them to mislead our dear ones and lay hold of huge amounts of money and collect details.

Key Insights and Research Gap :

The reviewed literature highlights the frauds which are unable to detect. It focuses on the emerging threats in the financial and cybersecurity sectors. However critical gaps remain in understanding. They are as follows:

- Real-world testing and data at analysis.
- Self learning fraud detection models which are adaptive.
- Integrated voice, document and behavioral fraud detection.
- Interpretable fraud detection.
- Legal,ethical and regulatory challenges.

RESEARCH METHODOLOGY:

Primarily relying on a thorough literature study, this study employs a qualitative, exploratory approach. The aim is to know how synthetic fraud schemes are generated and carried out using artificial intelligence and to evaluate the current detection techniques and their shortcomings.
The approach is organized as follows:

1. Data Collection

The following secondary sources provided the data for this study: Academic journals that undergo peer review White papers on cybersecurity Case studies and news reports about fraud caused by AI Technical details on artificial intelligence tools such as deepfake technologies and GANs (Generative Adversarial Networks) Targeted keyword searches using terms like these drove the study: Fraud involving a false identity Forgery of AI documents Scams involving deepfake voices Fraudulent Generative Adversarial Networks Frameworks for detecting AI fraud

2. Source Selection Criteria

The following criteria were used in the selection of sources:
Pertinence to the subject of fraud caused by AI Recency, emphasizing works written within the previous five years Credibility includes publications from reputable organizations, specialists, or journals.

3. Data Analysis

The gathered data was grouped and examined critically under the following headings: Synthetic fraud types include deepfakes of voices and videos, identity fraud, and document forgeries. Fraudsters' technologies (voice cloning tools, GANs, and AI models) Existing fraud detection techniques' limitations Gaps in the literature and practice were identified. The information acquired was utilized to investigate potential detection and prevention techniques as well as to comprehend the dynamic nature of AI-enabled fraud.

4. Identified Research gaps

The gaps listed below were consistently observed in all of the reviewed sources: Absence of testing fraud detection models on real-world data AI models that are self-learning and adaptive are required.
Few systems that combine behavior-based analysis, document analysis, and voice Interpretable AI's difficulties in providing transparent fraud analysis Current studies do not adequately address ethical and legal issues.

DISCUSSION

The rise of AI-generated fraud, particularly synthetic identity fraud, deepfake manipulation, and document forgery, presents a significant challenge to traditional fraud detection systems. Unlike conventional fraud, where human actors manipulate existing identities, synthetic fraud leverages AI to create entirely new personas, making detection far more complex. Current security and verification systems struggle to distinguish between real and AI-generated information, leading to gaps in fraud prevention. One of the major hurdles in detecting synthetic fraud is the evolving sophistication of generative AI models. Fraudsters continuously refine their methods, producing highly realistic fake identities, synthetic voices, and manipulated documents that bypass conventional detection mechanisms. While AI-driven fraud detection tools have started emerging, they are still in the early stages and often lack adaptability to new fraud tactics. A potential solution lies in the integration of AI-powered anomaly detection, behavioral analysis, and biometric verification systems. By analyzing patterns in user behavior, inconsistencies in AI-generated content, and micro-expressions in deepfakes, fraud detection frameworks can enhance their accuracy. Moreover, collaboration between financial institutions, cybersecurity experts, and AI researchers is crucial to stay ahead of fraudsters who exploit technological advancements.

CONCLUSION

AI-generated fraud schemes represent an evolving cybersecurity threat that demands continuous innovation in fraud detection strategies. The traditional methods of identity verification are insufficient against AI-powered fraudulent activities, necessitating a shift towards more sophisticated, AI-enhanced detection frameworks. While current research on AI-assisted fraud detection is still developing, future efforts must focus on real-time detection, improved AI explainability, and cross-industry collaboration.
As synthetic fraud techniques become more advanced, organizations must proactively invest in AI-driven security solutions and regulatory frameworks to counter these threats. The fight against AI-generated fraud is a continuous battle, requiring a combination of technological advancements, policy changes, and collective vigilance.

REFERENCES

https://eudl.eu/pdf/10.4108/eai.23-11-2023.2343170
https://eudl.eu/doi/10.4108/eai.23-11-2023.2343170#:~:text=Artificial%20Intelligence%20%28AI%29%20has%20proven%20to%20be%20powerful,and%20presents%20novel%20approaches%20to%20tackle%20the%20issue