National Conference on Information Technology & Digital Application (NCITSA-2025)
International Journal of Advanced Engineering Research and Science (IJAERS) Special Issue
https://dx.doi.org/10.22161/ijaers.ncitsa.2025.30 ISSN: 2349-6495(P) | 2456-1908(O)

AI Generated Fake Audio as a New Threat to Information Security

Mr. Shubham Sharma[1] , Mr. Devendra Sharma[2] ,Vipul Harsh[3], Sourav Gupta [4],

[1]AssistantProfessor Department of Information Technology, JaipurEngineeringCollege&ResearchCentre,Jaipur
[2]AssistantProfessor Department of Information Technology, JaipurEngineeringCollege&ResearchCentre,Jaipur
[3]Student Department of Information Technology, Jaipur Engineering College and Research Centre, India
Email:vipulharsh.it25@jecrc.ac.in
[4] Student Department of Information Technology, Jaipur Engineering College and Research Centre, India
Email :souravgupta.it25@jecrc.ac.in

Abstract—This report explores machine learning applications in healthcare, focusing on diagnosis, treatment, and beyond. The executive summary provides a snapshot of key findings and recommendations. The introduction sets the stage by discussing the historical context of technology in healthcare and outlining the report's purpose and scope. The fundamentals of machine learning, including its definition, types, and basic algorithms, are explored in the third section. The report delves into the applications of machine learning in diagnosis, featuring case studies on diseases such as cancer and diabetes. The subsequent section explores the role of machine learning in treatment, personalised medicine, and drug discovery. Predictive analytics and prognosis are discussed in detail, emphasizing the use of machine learning in predicting disease progression and developing prognostic models.The report then outlines future trends in machine learning and healthcare, including potential advancements and the role of AI in addressing global health challenges.

Keywords—:Predictive Analytics, Healthcare Informatics, Machine Learning, Deep Learning, IoT in Healthcare, Clinical Data Mining

I. INTRODUCTION

Technology has always been a double-edged sword in the realm of information security. While advancements in encryption, authentication mechanisms, and network protection tools have strengthened defenses, these same innovations have also opened doors for sophisticated cyber threats. The advent of artificial intelligence (AI) has amplified both opportunities and risks, with AI-generated fake audio emerging as a critical challenge in the cybersecurity landscape. The emergence of AI-generated fake audio poses a significant threat to information security, challenging traditional approaches to safeguarding sensitive data and maintaining trust in communication. As artificial intelligence (AI) technology advances, its potential misuse for creating convincing yet fraudulent audio content raises serious concerns across various domains, including cybersecurity, privacy, and ethical governance.
AI technology has evolved rapidly in recent years, enabling the creation of highly realistic audio that can mimic human voices with remarkable accuracy. This capability has been driven by advancements in deep learning algorithms, text-to-speech (TTS) systems, and neural networks, which allow machines to analyze and replicate unique vocal characteristics. While these developments have numerous beneficial applications, such as aiding individuals with speech impairments or enhancing virtual assistants, they also open the door to malicious exploitation.

II. LITERATUREREVIEW

As we delve into the following sections, we will navigate through the fundamental concepts of machine learning, its diverse applications in diagnosing and treating diseases, predictive analytics, and prognosis. Furthermore, we will address the challenges and ethical considerations inherent in the integration of ML into healthcare practices. The report will also anticipate future trends and innovations, highlighting the transformative impact of machine learning on global healthcare systems. In the subsequent chapters, we will explore case studies and success stories that exemplify the realworld applications of machine learning in healthcare. Through these examples, we aim to underscore the tangible benefits and transformative potential of ML, emphasizing its role in shaping the future landscape of medical practices.

III.METHODOLOGY

https://dx.doi.org/10.22161/ijaers.ncitsa.2025.30 ISSN: 2349-6495(P) | 2456-1908(O)

3.1Basic Algorithms Used in AI fake audio detection

3.1.1 Spectrogram Analysis Converts audio signals into visual representations (spectrograms) for analysis. Fake audio often exhibits distinct patterns or artifacts not present in natural speech.

3.2.2 Mel-Frequency Cepstral Coefficients (MFCCs) K-Means Clustering: Divides data into k clusters based on similarity.Principal Component Analysis (PCA): Reduces dimensionality while retaining essential information.

3.3.3 Voice Embedding Analysis Encodes audio features into embeddings for comparison against authentic voice samples. Fake audio often deviates from the authentic voice embeddings.

IV.Preprocessing

3.2Basic Algorithms Used in AI fake audio detection

3.2.1 Spectrogram Analysis Converts audio signals into visual representations (spectrograms) for analysis. Fake audio often exhibits distinct patterns or artifacts not present in natural speech.

3.2.2 Mel-Frequency Cepstral Coefficients (MFCCs) K-Means Clustering: Divides data into k clusters based on similarity.Principal Component Analysis (PCA): Reduces dimensionality while retaining essential information.

3.2.3 Voice Embedding Analysis Encodes audio features into embeddings for comparison against authentic voice samples. Fake audio often deviates from the authentic voice embeddings.

3.4 Models Used

To evaluate the breadth and performance of AI approaches in healthcare analytics, both classical machine learning and state-of-the-art deep learning models were explored:

Machine Learning Models:

- Logistic Regression: Baseline binary classifier used for interpretability and benchmarking.
- Random Forest: Robust to overfitting and interpretable through feature importance, widely used in healthcare risk prediction.
- XGBoost: Gradient boosting decision trees optimized for performance on tabular clinical datasets.
- Support Vector Machines (SVM): Effective for small and medium-sized clinical datasets with high-dimensional feature spaces.

Deep Learning Models:

- LSTM (Long Short-Term Memory): Applied on time-series EHR data to capture temporal dependencies in ICU or diabetes monitoring scenarios.
- CNNs (Convolutional Neural Networks): Used for imaging datasets and pattern recognition in sequential data.
- Autoencoders: Applied for unsupervised feature extraction and anomaly detection in healthcare logs.
- BERT and ClinicalBERT: Employed for clinical note classification, diagnosis prediction from discharge summaries, and medical named entity recognition.

Each model was evaluated across multiple datasets to assess its adaptability and accuracy in diverse healthcare applications. The choice of models ensures a comprehensive comparison between interpretable traditional approaches and high-performing deep neural networks**.**

V. IMPLEMENTATION

This study explores the growing threat of AI-generated fake audio to information security, focusing on its potential to undermine authentication systems, communication security, and the integrity of digital media. The results show that while many information security professionals are aware of AI generated fake audio, there is a notable gap in their understanding of its full scope as a cybersecurity risk. Over 70% of respondents expressed concern about its potential to compromise voice-based authentication systems, such as those used in banking and customer service. These professionals highlighted the difficulty in detecting synthetic audio, which often bypasses traditional security measures like voiceprints and speech patterns. The survey revealed that 68% of participants believe AI-generated fake audio could be used to bypass security protocols, especially in social engineering attacks where attackers impersonate individuals to manipulate victims into revealing confidential information. Detecting fake audio was identified as a major challenge by 65% of respondents, who noted that the increasing sophistication of AI algorithms makes it harder to differentiate between real and synthetic content. This has led to a call for more advanced detection technologies,such as deep learning models, to identify manipulated audio more effectively.

https://dx.doi.org/10.22161/ijaers.ncitsa.2025.30 ISSN: 2349-6495(P) | 2456-1908(O)

VI. RESULTSANDDISCUSSION

Ethical concerns were also highlighted, with 55% of respondents worried about the use of AI generated fake audio for malicious purposes, particularly in impersonation and misinformation. The anonymity and ease of creating convincing fake audio have raised doubts about how to hold perpetrators accountable. To address these risks, 72% of participants emphasized the need for better training and awareness among information security professionals and the development of AI-based detection tools. Collaboration between cybersecurity firms, AI developers, and government agencies was also seen as essential for creating strategies to combat this emerging threat.

As ML technology evolves, it is becoming an indispensable tool in areas such as personalized medicine, clinical data analysis, and medical research. ML models analyze patient data to recommend personalized treatment plans, leading to more effective and safer treatments. This improved operational efficiency contributes to reducing healthcare costs and increasing the overall quality of care.

In summary, the results highlight that **no single model is universally best**, and the choice of algorithm should be tailored to the nature of the data and the specific clinical application. A hybrid or ensemble approach may provide the most practical balance between accuracy, explainability, and resource efficiency and securly in real-world.

VII. CONCLUSION

Machine learning is revolutionizing healthcare by transforming key areas such as diagnosis, treatment, predictive analytics, and prognosis. The integration of advanced algorithms and vast datasets has paved the way for significant advancements in patient care, enhancing decision-making and optimizing healthcare delivery. This report has explored the fundamentals, applications, challenges, and future trends of machine learning in healthcare, offering a comprehensive understanding of its impactAddressing challenges like data quality, algorithmic bias, and ethical issues is critical to the responsible adoption of machine learning in healthcare. These factors need to be carefully managed to ensure fairness, transparency, and patient trust. Emerging trends, including federated learning, explainable AI, and the integration of multiple data modalities, highlight the ongoing evolution of machine learning applications in healthcare. Success Stories Case studies, such as Google's DeepMind collaboration with Moorfields Eye Hospital and Tempus's clinical and molecular data platform, illustrate the real-world impact of machine learning on disease detection, diagnosis, and treatment planning.

The evolving landscape of machine learning (ML) in healthcare is reshaping the medical field with exciting advancements. This section delves into emerging trends, potential future developments, and the transformative role of artificial intelligence (AI) in tackling global health challenges.

ACKNOWLEDGEMENTS

We would like to thank our research supervisor for their continuous guidance and valuable feedback throughout this project. We also extend our gratitude to the developers of publicly available datasets and open-source ML/DL tools that made the implementation part of this study possible.

REFERENCES

1. Aguimlod, C. A., Tanduyan, M., Trangia, E., &Genelza, G. (2023). The learning interest in social studies education: In the lens of junior high school students. Galaxy International Interdisciplinary Research Journal, 11(9), 108-122.

2. Bird, J. J., & Lotfi, A. (2023). Real-time Detection of AI-Generated Speech for DeepFake Voice Conversion. arXiv preprint arXiv:2308.

3. Chesney, B., Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107: 1753-1820.

4. Ladd, D.R. (1996). International Phonology. Cambridge: Cambridge University Press. 5. Wang, R. Fu, J. Yi, J. Tao, and

https://dx.doi.org/10.22161/ijaers.ncitsa.2025.30 ISSN: 2349-6495(P) | 2456-1908(O)

S. Wang, “Prosody and voice factorization for few-shot speaker adaptation in the challenge m2voc 2021,” in Proc. of ICASSP), 2021.