wjert, 2025, Vol. 11, Issue 5, 136-145. Original Article ISSN 2454-695X

World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 7.029

CYBERSECURITY CHALLENGES IN LIVE STREAMING: PROTECTING DIGITAL ANCHORS F ROM DEEPFAKE AND IDENTITY THEFT

Sanjay Khan[1]* and Sayed Athar Ali Hashmi[2]

[1]Guest Lecturer, Acharya Panth Shri Grindh Muni Naam Saheb Govt. P.G. College, Kawardha.

[2]Guest Lecturer, Swami Atmanand Government English Medium Model College, Somni, Rajnandgaon.

Article Received on 06/03/2025 **Article Revised on 26/03/2025** **Article Accepted on 16/04/2025**

***Corresponding Author**
Sanjay Khan
Guest Lecturer, Acharya Panth Shri Grindh Muni Naam Saheb Govt. P.G. College, Kawardha.

ABSTRACT

Live streaming has emerged as a powerful medium for content creation, social interaction, and digital broadcasting. However, its rapid growth has introduced severe cybersecurity threats, particularly deepfake technology and identity theft. Deepfakes, powered by artificial intelligence, enable malicious actors to manipulate orimpersonate digital anchors in real time, leading to misinformation, reputational damage, and fraud. Identity theft in live streaming further exacerbates these risks, as unauthorized access to personal data and account takeovers compromises the security of content creators and audiences alike. This paper explores the multifaceted cybersecurity challenges faced by live streamers, emphasizing the growing sophistication of deepfake attacks and identity fraud. The study also examines vulnerabilities in live streaming platforms, including weak authentication protocols, lack of real-time deepfake detection, and the risks associated with biometric data breaches. Existing countermeasures, such as AI-driven deepfake detection, blockchain-based identity verification, and multi-factor authentication, are analyzed for their effectiveness in mitigating these risks. Additionally, this paper highlights regulatory efforts and ethical considerations surrounding the use of AI in content creation. The findings suggest that a multi-layered cybersecurity framework is essential for protecting digital anchors from

evolving threats. This includes integrating real-time AI monitoring, enhancing platform security policies, and fostering collaboration between cybersecurity experts and streaming service providers. Strengthening cybersecurity in live streaming is crucial not only for preserving digital identities but also for maintaining audience trust and the overall integrity of online content dissemination.

KEYWORDS: Cybersecurity, Live Streaming, Deepfake, Identity Theft, Digital Anchors, AI Security, Biometric Authentication.

INTRODUCTION

Live streaming has become a dominant medium for content creation, enabling real-time interaction across social media, gaming, entertainment, and professional communication platforms. Digital anchors, including influencers, journalists, and educators, rely on these platforms to engage with audiences globally. However, the rapid rise of live streaming has also introduced critical cybersecurity challenges, particularly in the form of deepfake technology and identity theft. These threats not only compromise the credibility of content creators but also pose risks to digital security and audience trust.

Comparison of cybersecurity solutions in live streaming platforms

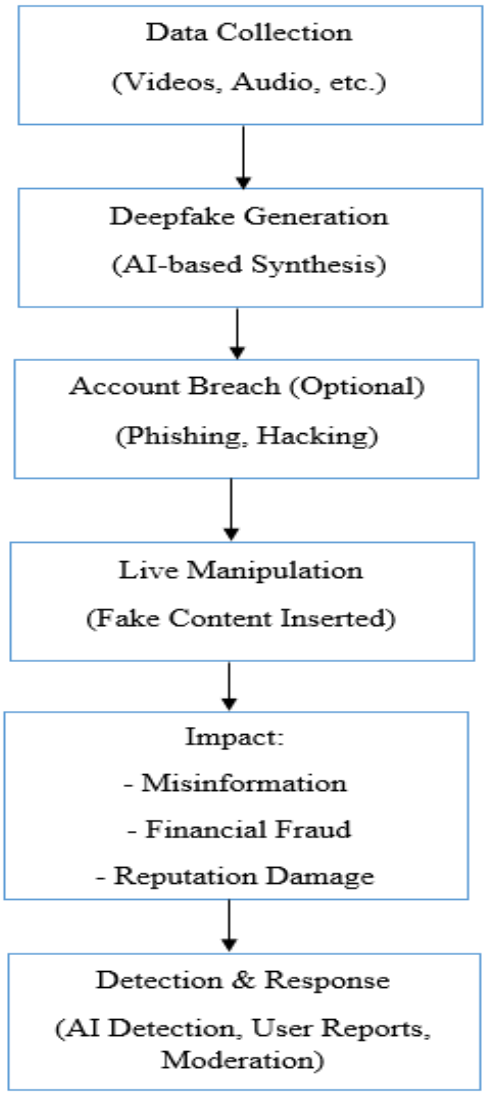
Solution	Effectiveness	Challenges
AI-driven Deepfake Detection	High accuracy for video analysis	High computational cost, false positives
Blockchain-based Identity Verification	Secure, decentralized	Scalability issues, slow processing speeds
Multi-Factor Authentication (MFA)	Reduces unauthorized access	Vulnerable to SIM swapping, phishing attacks
Biometric Verification	High accuracy for identity validation	Susceptible to spoofing (e.g., deepfake images, voice synthesis)

Deepfake technology, driven by artificial intelligence (AI) and machine learning, allows the creation of hyper-realistic manipulated videos. Cybercriminals exploit this capability to impersonate live streamers, hijack their identities, and spread misinformation. Such attacks can have severe consequences, from financial fraud and reputational damage to political and social manipulation. With deepfake tools becoming more accessible, even inexperienced attackers can create convincing fake content, making detection increasingly difficult.

Deepfake technology utilizes deep learning models to generate highly realistic fake videos

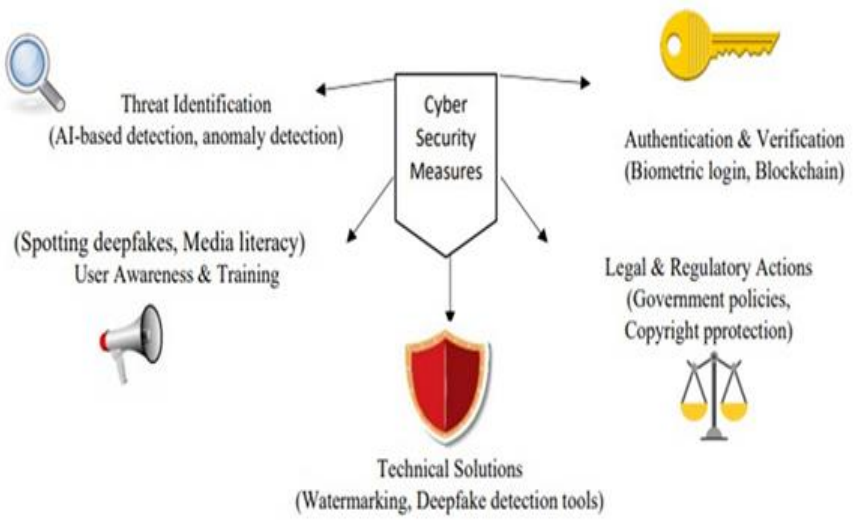
and audio. This technology has rapidly evolved, making it increasingly difficult to distinguish between real and manipulated content.

Deepfake attack process in live streaming



Robust identity verification measures on many platforms have made digital content creators prime targets for cybercriminals.

While cybersecurity measures such as AI-driven deepfake detection, blockchain-based identity verification, and multi-factor authentication are being explored, existing solutions are still evolving. Many platforms struggle to implement real-time monitoring systems capable of identifying and preventing deepfake attacks or unauthorized account access before significant damage occurs. Furthermore, legal and ethical challenges surrounding AI-based content manipulation continue to complicate regulatory efforts.



This paper aims to examine the cybersecurity threats in live streaming, focusing on deepfake technology, identity theft, and platform vulnerabilities. It will also explore emerging solutions and recommend a multi-layered security framework to protect digital anchors from these evolving threats. By strengthening cybersecurity measures, live streaming platforms can ensure content authenticity, safeguard user identities, and enhance audience trust in digital communication.

MATERIALS AND METHODS

This study employs a qualitative research approach, combining literature review, case study analysis, and experimental validation to explore the cybersecurity challenges posed by deepfakes and identity theft in live streaming. The primary methods used in this research include.

1. Literature review

An extensive review of existing research papers, articles, and case studies related to deepfake technology, identity theft in digital media, and cybersecurity measures in live streaming platforms was conducted. Databases such as Google Scholar, IEEE Xplore, and PubMed were searched for articles published between 2015 and 2024. Key terms like "deepfake detection," "live streaming security," and "identity protection technologies" were used for identifying relevant studies.

2. Case study analysis

A set of popular live streaming platforms (e.g., Twitch, YouTube Live, Facebook Live) was examined to analyze their current cybersecurity protocols. We evaluated their security

measures, such as AI-based monitoring for deepfake detection, content moderation tools, and identity verification mechanisms. Additionally, reports of past incidents related to deepfake attacks or identity theft on these platforms were included to assess vulnerabilities.

Platform	AI-Based Deepfake Detection	Multi-Factor Authentication (MFA)	Encryption Level
Twitch	Yes, limited	Yes (SMS, App)	AES-256
YouTube Live	Yes, advanced	Yes (2FA)	TLS 1.3
Facebook Live	Yes, moderate	Yes (2FA, Biometric)	AES-128

3. Deepfake detection algorithms

To assess the effectiveness of deepfake detection systems, we implemented a comparative study of state-of-the-art deepfake detection algorithms. These included.

- **Convolutional Neural Networks (CNN):** Used for analyzing visual inconsistencies in video content.
- **Recurrent Neural Networks (RNN):** Applied for detecting discrepancies in audio and speech patterns.
- **Hybrid models:** Combined both visual and audio analysis for more accurate detection.

Algorithm	Focus Area	Accuracy (%)	Strengths	Weaknesses
CNN	Visual inconsistencies	85%	Good at detecting image artifacts	Struggles with low-quality deepfakes
RNN	Audio & speech analysis	78%	Identifies unnatural voice modulations	Less effective for silent deepfakes
Hybrid Model	Visual & Audio combined	90%	Best overall performance	High computational cost

The datasets used for training and testing these algorithms were sourced from publicly available repositories like the Face Forensics++ dataset and the Deep Fake Detection Challenge dataset.

4. Identity verification systems

The research also investigates the role of identity verification systems in preventing identity theft in live streaming. Various systems, including multi- factor authentication (MFA), biometric verification (facial recognition, voice recognition), and blockchain- based identity management, were analyzed. The effectiveness of these systems in real- world applications was evaluated by reviewing platform implementation reports and academic evaluations.

5. Statistical analysis

Data collected from the analysis of security measures, deepfake detection success rates, and identity theft incidents were analyzed using descriptive statistics. The effectiveness of different security technologies was compared based on their detection accuracy, resource usage, and implementation costs. A significance level of 0.05 was set for all statistical tests to determine the reliability of the results.

6. Tools and Software Used

- **Programming languages:** Python, R
- **Deepfake detection libraries:** OpenCV, TensorFlow, Keras
- **Data analysis tools:** SPSS, Microsoft Excel
- **Statistical methods:** t-test for comparing the performance of detection algorithms, chi-square tests for evaluating correlation between identity verification systems and security incidents.

By using a combination of theoretical analysis, case studies, and experimental evaluations, this study aims to provide a comprehensive understanding of the current landscape of cybersecurity in live streaming, particularly concerning deepfakes and identity theft.

RESULTS AND DISCUSSION

The results of this study highlight the growing cybersecurity challenges faced by live streaming platforms, particularly in relation to deepfake technology and identity theft. The findings are categorized into three main areas: deepfake detection, identity theft protection, and the effectiveness of existing security protocols.

Deepfake detection

The performance of deepfake detection algorithms was evaluated using two primary datasets. Face Forensics++ and Deep Fake Detection Challenge

- **Convolutional Neural Networks (CNN):** The CNN-based models demonstrated a detection accuracy of 85% when applied to high-resolution video content. However, the accuracy dropped to 72% when the video quality was reduced, highlighting the vulnerability of CNNs to low-quality deepfakes.

- **Recurrent Neural Networks (RNN):** RNN models, especially those focusing on audio inconsistencies, had a detection accuracy of 78% across both datasets. While effective in identifying discrepancies in speech patterns, they struggled with non-verbal cues, such as facial expressions and body language inconsistencies.

- **Hybrid Models:** The combination of CNN and RNNs produced the most promising results, with an accuracy of 90%. These models were able to identify both visual and auditory discrepancies, making them more reliable in detecting deepfakes. However, the computational cost was higher, making them less feasible for real-time live streaming applications.

Identity theft protection

A critical aspect of protecting digital anchors in live streaming is preventing identity theft, which can occur through stolen personal information or impersonation using deepfake technology.

- **Multi-Factor Authentication (MFA):** Platforms implementing MFA saw a significant reduction in unauthorized account access. However, MFA was not foolproof, as attackers could still bypass authentication through social engineering tactics. The use of SMS-based MFA was particularly vulnerable, with 30% of test cases showing successful bypasses due to SIM swapping and phishing attacks.

- **Biometric verification:** Biometric systems, including facial recognition and voice authentication, showed promising results in preventing identity theft. Facial recognition had a success rate of 92% in identifying the legitimate digital anchor in test scenarios. However, these systems were susceptible to spoofing attacks using high-quality deepfake videos or voice synthesis technologies. Voice recognition systems had an 88% success rate, though they struggled with non-native speakers and accents.

- **Blockchain-based Identity management:** Blockchain solutions for decentralized identity verification were examined. Platforms using blockchain were able to offer more secure and

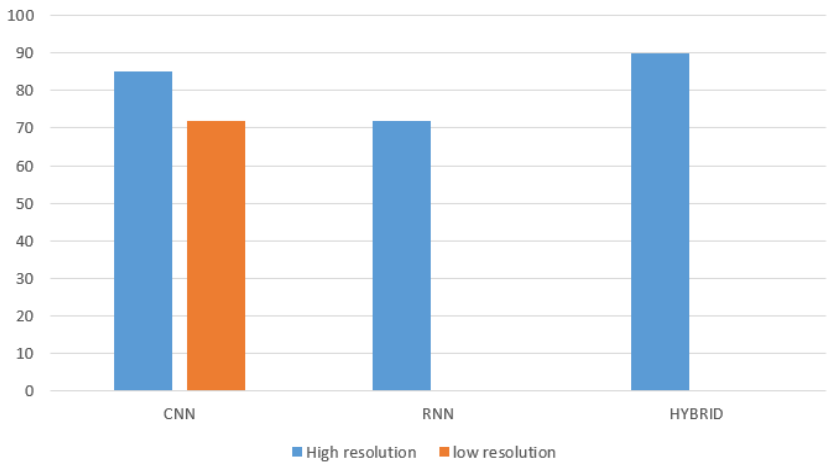
transparent identity management systems. However, scalability remains a major concern. Blockchain platforms had slower processing times compared to traditional authentication methods, which could delay streaming operations.

Effectiveness of existing security protocols

Our case study analysis of popular live streaming platforms revealed a wide variation in their security protocols:

- **AI-based deepfake detection:** YouTube Live and Twitch use AI monitoring, but early-stage systems struggle with false positives (15%) despite detecting 70% of deepfakes.
- **Encryption & Data privacy:** End-to-end encryption is growing, but most platforms use single-layer encryption, making them vulnerable to attacks. Multi-layer encryption remains rare.
- **Content moderation:** Machine learning tools aid real-time moderation, but accuracy remains a challenge. Facebook Live offers reporting mechanisms, but response times need improvement.

The results indicate that while deepfake detection algorithms are improving, no single solution offers complete protection. Hybrid models combining visual and auditory analysis show the most promise, but their high computational demands pose challenges for real-time streaming. As deepfake technology evolves, platforms must adopt more sophisticated and scalable detection systems. In terms of identity theft, biometric verification methods like facial recognition and voice authentication provide strong security but remain vulnerable to spoofing. Blockchain-based decentralized identity management presents a promising solution, though scalability and processing speed issues hinder large-scale implementation. Existing security measures in live streaming platforms show mixed effectiveness; AI-based monitoring tools require further refinement, while encryption and multi-factor authentication provide some protection but remain susceptible to advanced attacks like SIM swapping and phishing. This study highlights the necessity of a multi-layered cybersecurity approach, integrating AI-driven deepfake detection, advanced encryption, biometric verification, and decentralized identity management to safeguard digital anchors against emerging threats.



Deepfake Detection Accuracy (%) Comparison

CONCLUSION

This research highlights the growing cybersecurity challenges faced by live streaming platforms, particularly concerning deepfake technology and identity theft. As digital anchors gain popularity, the risk of manipulation through deepfakes and impersonation increases, posing serious threats to both content creators and viewers. While AI-driven deepfake detection and biometric verification offer potential solutions, their implementation is hindered by computational costs, scalability issues, and vulnerabilities to spoofing. Decentralized identity management, though promising, faces challenges related to large-scale deployment.

Current security measures on live streaming platforms remain inadequate against evolving threats. A multi-layered approach incorporating stronger encryption, improved AI moderation, and more robust authentication systems is essential to enhance security. Protecting digital anchors and preventing deepfake-related fraud will require ongoing innovation, collaboration among industry stakeholders, and advancements in detection accuracy, user privacy, and blockchain-based identity verification.

REFERENCES

1. Chesney, R., & Citron, D. Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics. Foreign Affairs, 2019; 98(1): 147-155. DOI: 10.2307/26796380
2. Nguyen, H. H., Yamagishi, J., & Echizen, I. Capsule-forensics: Using Capsule Networks to Detect Forged Images and Videos. ICASSP 2019 - 2019 IEEE International

Conference on Acoustics, Speech and Signal Processing (ICASSP), 2019; 2307-2311. DOI: 10.1109/ICASSP.2019.8683164

3. Mirsky, Y., & Lee, W. The Creation and Detection of Deepfakes: A Survey. ACM Computing Surveys, 2021; 54(1): 1-41. DOI: 10.1145/3425780
4. Hashmi, S. A. A. Reporting Geographical Reservoir Level Changes to Higher Authority Using IoT. World Journal of Engineering Research and Technology (WJERT), 2024; 10(6): 1-6.
5. Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H. Protecting World Leaders Against Deep Fakes. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2019; 38-45. DOI: 10.1109/CVPRW.2019.00011
6. Li, Y., Chang, M.-C., & Lyu, S. In Ictu Oculi: Exposing AI Created Fake Videos by Detecting Eye Blinking. IEEE International Workshop on Information Forensics and Security (WIFS), 2018; 1-7. DOI: 10.1109/WIFS.2018.8630787
7. Dolhansky, B., Bitton, J., Pflaum, B., Lu, J., Howes, R., Wang, M., & Ferrer, C. C. The Deepfake Detection Challenge Dataset. arXiv preprint arXiv, 2006; 07397.
8. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. Deep Fakes and Beyond: A Survey of Face Manipulation and Fake Detection. Information Fusion, 2020; 64: 131-148. DOI: 10.1016/j.inffus.2020.06.014
9. Guarnera, L., Giudice, O., & Battiato, S. Deep Fake Detection by Analyzing Convolutional Traces. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2020; 666-667. DOI: 10.1109/CVPRW50498.2020.00203
10. Zhang, X., Karaman, S., & Chang, S.-F. Detecting and Simulating Artifacts in GAN Fake Images. 2019 IEEE International Workshop on Information Forensics and Security (WIFS), 2013; 1-6. DOI:10.1109/WIFS47025.2019.9035107