IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144108

AI-Generated Deepfakes for Cyber Fraud and Detection

Mohammed Aasimuddin[1], Shahnawaz Mohammed[2]

Campbellsville University, KY, USA[1]

Trine University, MI, USA[2]

Abstract: The fast-evolving strides of artificial intelligence, specifically using generative adversarial networks (GANs), have ushered in the era of deepfakes—artificial media capable of replicating human faces, voices, and actions with comparative ease. Although the technology has revolutionary and positive applications across the domains of filmmaking and accessibility, it equally bears colossal risks if used for cyber fraud. Deepfakes are being used more and more by cybercriminals for impersonation, identity theft, business email compromise (BEC), and various other types of deception. Impersonation of CEOs over video calls, audio message fakes to approve illegal fund transfers, and evading biometric security controls using synthetic faces and voices with a hyper-realistic appearance are now achievable by fraudsters.

The existing reality of deepfakes as a tool for cybercrime is examined in this paper. It discusses actual events where deepfakes were utilized to take advantage of, deceive, or financially exploit individuals and groups. Moreover, it has a detailed description of the detection methods created to help counter this emerging threat. These include some of them being passive detection methods like artifact and frequency analysis, deep learning classifiers, and biological signal detection, and others being active detection methods like liveness checks, watermarking, and blockchain-based content verification.

Despite concerted efforts, the race between deepfake generation and detection remains on an upward trajectory. Attackers continue to adapt to remain undetected, and conventional forensic mechanisms become less effective with time. The paper concludes on a note highlighting the importance of hybrid detection systems, robust regulatory frameworks, and global cooperation to enable ethical and secure use of AI-generated content.

Keywords: Artificial Intelligence, Deepfakes, Cyber Fraud, Generative Adversarial Networks (GANs), Deepfake Detection, Identity Theft, Liveness Detection, Biometric Security, AI Forensics, Cybersecurity.

I. INTRODUCTION

Artificial intelligence has come a long way in recent years, especially with the emergence of deep learning models such as Generative Adversarial Networks (GANs) [1]. One of the most unsettling side effects of this technology is the production of deepfakes—fake media in which a subject in a current image, audio, or video is swapped with another's face or voice in a manner that seems to be genuinely real. At first, an interesting technological curiosity, deepfakes have quickly become a double-edged sword, with deep-seated implications for privacy, security, and digital trust.

Although deepfake technology promises future applications in filmmaking, gaming, accessibility, and virtual communication, it is turning into a burgeoning trend in cybercrime abuse. Deepfakes are being used by spammers and cybercriminals to steal identities, perform social engineering, enable financial fraud, conduct disinformation operations, and modify digital evidence [2]. For instance, spammers can use fake voices to impersonate business executives during phone calls or video conferencing and manipulate employees into approving unauthorized transactions. Others will use deepfake images or videos to bypass facial recognition software and gain unauthorized access to secure platforms or buildings.

Deepfakes unleashed on cyber deception is a serious threat increase. Phishing or spoofing attacks traditionally are text-based deception-dependent, but deepfakes add a new dimension of realism and psychological tricks [3]. Targets are going to believe what they hear and see, and detection and prevention are going to be more difficult.

This paper seeks to examine the nexus of deepfake technology and cyber fraud by probing the attacker's tools and techniques, providing examples of actual attacks, and classifying detection methods employed. Both passive (forensic) methods, which scan content for recognizing features of manipulation, and active (interactive) methods, which authenticate users through real-time challenges or hidden metadata, are considered [4].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144108

Moreover, the paper addresses the technical, ethical, and regulatory difficulties in deepfake detection and proposes future research and development trends.

In an age where digital authenticity is increasingly being challenged, it is crucial to know how deepfakes are employed in cyber fraud—and how to detect and counter them—in order to stay ahead of threats.

II. BACKGROUND AND TECHNOLOGY

2.1. Generative Adversarial Networks (GANs)

GANs form the backbone of deepfake technology. Invented in 2014 by Ian Goodfellow, a GAN is two neural networks, the discriminator and the generator, racing each other in a loop [5]. The generator generates fake data (e.g., faces), and the discriminator attempts to distinguish real data from fake data. Through loop-based training, the generator gets better at producing output until the discriminator cannot tell. It is by this method that GANs can create extremely realistic counterfeit images, videos, and audio.

2.2. Autoencoders and Variational Autoencoders (VAEs)

Autoencoders are neural networks that use unsupervised learning to successful coding's. Autoencoders are also applied to face-swapping operations in the creation of deepfakes [6]. Variational Autoencoders (VAEs) take it a step further by learning latent distributions, thus applying effectively in creating smooth, diverse facial expressions or video deepfake alterations.

2.3. Categories of Deepfakes

Deepfakes exist in various forms, each based on unique AI models:

- **Video Deepfakes**: Face reanimation in video or face swapping through GANs or encoder-decoder models [7].
- **Audio Deepfakes**: Created using text-to-speech models and voice cloning technology, usually trained on a few minutes of audio.
- **Text Deepfakes**: Created by large language models for the purpose of imitating writing styles or generating phishing emails.
- **Multimodal Deepfakes**: Use visual, audio, and textual information to make more realistic deception [8].

2.4. Deepfake Generation Tools

Deepfakes have been democratized through open-source and commercial tools. Some of the most popular platforms include:

- **Deep Face Lab** (open-source, video-based face swapping)
- **Descript Overdub** (voice cloning)
- **Face Swap, Zao, and Reface** (mobile apps for facial animation)

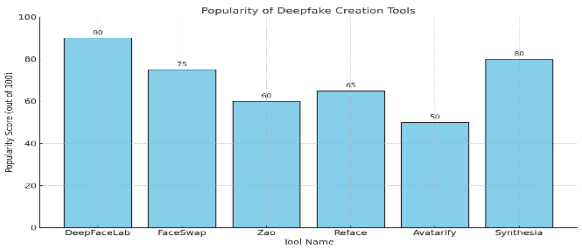

Figure 1: Deepfake Generation Tools

III. DEEPFAKES IN CYBER FRAUD

Deepfake technology use in cybercrime is a radical new direction in the methods used by attackers (8). Deepfakes enable advanced impersonation tactics far more advanced than the usual phishing or spoofing techniques. Deepfakes are used by cybercriminals to manipulate, deceive, and trick individuals, organizations, and institutions, taking advantage of human trust in visual and audio information.

3.1. Attack Vectors

Deepfakes are used in various cyber fraud situations, such as:

- **Business Email Compromise (BEC) Amplification:** Phishing emails are supplemented by deepfake video or audio of executives making urgent wire transfer demands [9].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144108

- **Synthetic Identity Fraud:** Deepfake images or videos are used by attackers to create imposter but legitimate-looking identities that can evade facial recognition technology at banks, KYC processes, and access controls.
- **CEO Deepfake in Video Conferences:** CEOs are replicated with deepfake videos in video conferences to approve payments, release confidential information, or implement strategic business moves.
- **Voice Phishing (Vishing):** Deepfake voice calls replicate the tone and voice of a well-known entity, convincing victims to act under the pretense that is delusory [10].

3.2. Incidents in Reality

Some high-profile cases have depicted the criminal side of deepfakes in frauds:

- **2019 UK-Based Company Fraud:** A deepfake voice of the CEO was utilized by criminals to trick an employee into sending $243,000 to a fake account [11].
- **2022 Tech Conference Scam:** A deepfake video of a keynote speaker was utilized by hackers to phish conference attendees into opening malicious links.
- **2023 Hong Kong Deepfake Heist:** Staff members were tricked using a deepfake video of their CFO during a virtual meeting via Zoom, and more than $25 million was lost [12].

Table 1: Deepfake in Cyber Scams

Type of Fraud	Deepfake Used	Impact	Real-World Example
Business Email Compromise	Deepfake audio/video	Fraudulent wire transfers	2019 CEO voice scam in the UK
Synthetic Identity Fraud	Face-swapped images/videos	Access to accounts, loans, or documents	Fake KYC processes in digital banks
Executive Impersonation	Real-time video deepfake	Strategic manipulation, data theft	2023 Hong Kong virtual meeting impersonation
Vishing (Voice Phishing)	AI-generated voice clones	Convincing victims into revealing credentials	Targeted phone scams using cloned voices

IV. MECHANISMS TO DETECT

As the sophistication and realism of deepfakes grow, there is greater need than ever for efficient detection mechanisms [13]. Detection mechanisms can be broadly classified into passive and active mechanisms. Passive mechanisms scan content for anomalies without the user's involvement, whereas active mechanisms are based on interactive or proactive mechanisms of authentication.

4.1. Passive Detection (Forensic Approaches)

Passive detection methods examine media content to detect inconsistencies or artifact traces of manipulation that occur when creating deepfakes [14]. The techniques don't need to know the origin of the media in advance or access additional metadata.

4.1.1. Frequency and Artifact Analysis

Media generated by GANs usually consists of frequency-domain artifacts that are not found in natural images or videos. Forensics on images and videos, like Discrete Fourier Transform (DFT) and JPEG compression artifact detection, can identify alterations through unnatural texture or pixel discordance [15].

4.1.2. Temporal Inconsistencies

Unusual blinking, lip-sync inconsistency, and abnormal head movements are usual in deep faked videos. Temporal analysis of video frames assists in finding inconsistencies in movement and expression flow [16].

4.1.3. Biological Signal Analysis

Some detection systems are based on physiological signals such as eye movements, breathing patterns, or even heart rates (detectable as micro-fluctuations of skin colour) [17]. Such biological signals are difficult to replicate and can be used as a good indicator of genuineness.

4.1.4. Deep Learning-Based Classifiers

Machine learning models, particularly Convolutional Neural Networks (CNNs) and Transformers, are trained on high volumes of data (e.g., Face Forensics++, Celeb-DF) to identify real from manipulated media [18]. The models learn to identify manipulation-induced patterns and textures.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144108

4.2. Active Detection (Challenge-Response Systems)

Active detection approaches employ user input or built-in systems that test for authenticity during live communication [19].

4.2.1. Liveness Detection

Systems make users execute arbitrary facial movements—such as blinking, smiling, or tilting their head—so static or pre-rendered deepfakes are unable to react suitably in real-time [20].

4.2.2. Digital Watermarking and Provenance

Media can be watermarked with imperceptible digital watermarks or cryptographic hashes during production [21]. They can then be used to verify the origin and integrity of the media.

4.2.3. Blockchain Verification

Blockchain platforms hold metadata and creation timestamps of media on a distributed ledger [22]. This provides tamper-evidence and traceability of the digital asset, making it easier to make authenticity claims.

V. DETECTION TOOL EVALUATION

Deepfake detection tool functionality depends on a number of important parameters like accuracy, generalization, scalability, usability, and robustness [23]. As deepfake technology evolves at a frenetic speed, method evaluation to maintain confidence in digital content and protect people and institutions from cyber deceit is paramount.

5.1. Precision and Accuracy

Most new detection tools, particularly deep learning-based tools (such as CNNs and Transformers), have a high level of precision in testing environments (24). Tools that have already been pre-trained on face data such as Face Forensics++, Celeb-DF, and DFDC attain precision scores of more than 90% when detecting previously known deepfake patterns [25]. They fail in precision when encountering previously unseen forms of distortion as well as real distortions like compression and noise.

5.2. Generalization Across Domains

Generalization is still one of the largest limitations. A model that is trained on synthetically generated video data will not necessarily work on audio deepfakes or cross-platform media. Cross-domain transfer learning and data augmentation methods are being investigated to enhance model robustness on other forms of deepfakes [26]. Yet, a lot of tools are not yet able to generalize without retraining or fine-tuning on novel datasets.

5.3. Real-Time Performance and Scalability

Real-time detection technology like Microsoft's Video Authenticator and Intel's Fake Catcher are promising but are still constrained by processing burden (27). Such technology causes latency in real-time video applications like conference calls or biometric authentication mechanisms. Additionally, putting such technology to mass deployment—like social networking sites—takes enormous computation power and cloud-optimized infrastructure.

5.4. Usability and Accessibility

The majority of sophisticated detection tools are used by researchers or security experts. Tools like Deep ware Scanner and Sensity AI, which are publicly available, can be accessed via APIs or browser extensions, but consumer-grade is not yet as accurate as enterprise-grade systems [28]. There is also no uniform user interface and integration feature for non-experts.

Table 2: Comparative Analysis

Tool	Type	Accuracy	Real-Time?	Open Access
Microsoft Authenticator	Video	~85%	Yes	No
Fake Catcher (Intel)	Video (Biological)	~90%	Yes	Limited
Deep ware Scanner	Video/Audio	~75%	No	Yes
Sensity AI	Multi-format	~88%	Partial	API access

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144108

VI. CHALLENGES AND LIMITATIONS

With the immense progress in deepfake detection, the fast development of generative AI continues to pose new challenges [29]. With deepfakes getting increasingly realistic and ubiquitous, detection approaches face technological, operational, and ethical obstacles compromising their effectiveness.

6.1. Deepfake Evasion and Adaptability

Deepfake generation algorithms are also becoming increasingly sophisticated to counter detection algorithms [30]. Attackers can also parameter-optimize generative models to hide artifacts on which detection relies. For example, adversarial examples and style transfer can be utilized to manipulate deepfakes such that it is wiser than classifiers optimized on traditional datasets.

6.2. Generalization and Dataset Bias

Several detection models generalize weakly. One-style or dataset-based models (such as Face Forensics++) would not generalize to new architectures or unseen manipulation styles [31]. Dataset bias and overfitting on certain training data attributes are largely the reason, since this restricts their use in real-world.

6.3. Real-Time Detection Failure

Deepfake detection in real time is a significant technical issue. Labelling and classification of deepfake audio or video streams with high accuracy may require significant computational resources, leading to unacceptable latency for real-time use like video conferencing or biometric authentication systems [32].

6.4. Data Sparsity and Annotation Cost

There should be high-quality, diverse, and up-to-date datasets to train detection models [33]. However, construction of such datasets requires considerable laborious manual annotation and ethical questions, especially if real people's likenesses are used.

6.5. Ethical, Privacy, and Legal Issues

One of the detection methods, particularly those using biometric tracking or blockchain authentication, constitute privacy issues [34]. The balance in ensuring safety and maintaining the freedom of an individual is subtle and intricate. Additionally, the body of legislation relating to regulation of deepfake material and imposition of sanctions on its misuse is scattered among jurisdictions.

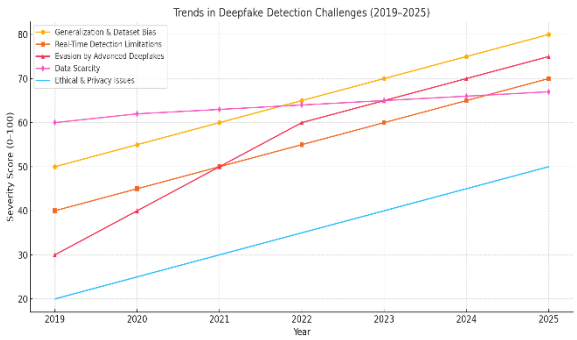

Figure 2: Trends in Deepfake Detection Challenges

VII. FUTURE DIRECTION

As deepfakes improve and become more ubiquitous, detection and mitigation in the future will be based on a multi-faceted approach combining technology, policy, cooperation, and public education [35] The most important future directions for preventing deepfake-based cyber fraud are listed below.

7.1. Improved Detection Algorithms

Future deepfake detection will rely on multimodal AI models processing not only visual or audio cues, but also contextual, behavioural, and biometric signals. Neuro-symbolic AI, that latest generation of technology that combines symbolic reasoning and neural networks, will definitely enhance interpretability and robustness for detecting synthetic content [36]. Zero-shot and few-shot learning techniques may enable detectors to learn to generalize across hitherto unseen classes of deepfakes with comparatively minimal training needs.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144108

7.2. Integration with Cybersecurity Infrastructure

Real-time deepfake detection will most likely be built into future cybersecurity systems [37]. Deepfake detection engines may be incorporated into email clients, social networks, video conferencing software, and identity verification systems in the attempt to automatically mark suspicious media before presenting it to users. Integration would also need low-latency algorithms capable of working properly in real-world environments.

7.3. Decentralized Media Provenance Systems

Blockchain technology presents a great avenue to verifying originality of content with tamper-proof digital ledgers [38]. Next-generation content platforms can ideally timestamp and record videos, images, or audio files on decentralized networks so that downstream users are able to verify originality and identify tampering.

7.4. Legislative and Policy Developments

Authorities are finally starting to sit up and take notice of the threat from deepfakes, and future legal measures will in all likelihood mandate transparency of AI-created content [39]. Steps could demand digital watermarking of fake media, criminalize the creation of malicious deepfakes, and make platforms responsible for facilitating the dissemination of deceptive content. International cooperation will be needed to arrest cross-border abuse.

7.5. Public Awareness and Digital Literacy

Education is a future prevention strategy. Individuals must be educated—particularly in business, media, and education fields—to recognize and challenge suspicious content [40, 41]. Online literacy must be encouraged in future campaigns, educating users on the dangers of deepfakes and empowering them with techniques to validate.

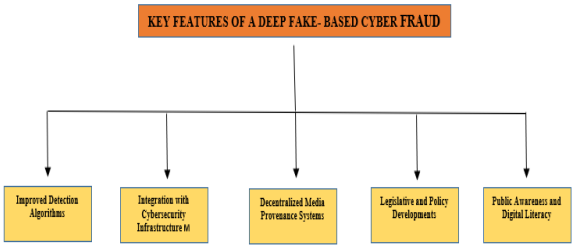

Figure 3: Deepfake – Based Cyber Fraud

VIII. CONCLUSION

The emergence of AI-driven deepfakes has posed a previously unseen challenge to the world of cybersecurity. Those good old days of innocent discovery and art are long gone as deepfakes have now become tools of sinister misdirection with a possible capability to mimic voices, faces, and behaviour at ghastly heights of accuracy. As cybercrooks are increasingly using this technology for purposes of fraud, which range from creation of synthetic identities and voice phishing to impersonation of executives and disinformation campaigns, trust and authenticity of digital communication are under grave threat.

This paper has described how deepfakes are being used to weaponize cyber fraud, included real-world examples, and discussed a thorough survey of detection methodologies. Although ongoing detection processes—passive as well as active—yield optimistic outcomes, these have also undergone several limitations in the form of dataset bias, scalability, as well as difficulties in real-time deployment. Because the creation of deepfake models is adaptive, detection systems continuously need to develop in order to be one step ahead of increasingly more advanced forgeries.

Existing solution comparison pointed to the reality that even though some solutions have shown high accuracy if they are run under test cases, there isn't much in the way of usefulness when taken into real contexts. This is what necessitates deeper embedding into large-scale cyber defence frameworks alongside generalization using algorithms.

In the next few years, the fight against deepfake-enabled cyber fraud will be more than about technical prowess. It will involve a coordinated, multidisciplinary effort by AI researchers, cybersecurity professionals, legislators, and the general public. Regulations need to be reinforced to punish unlawful use of deepfakes, and education in schools needs to acquaint the public with the dangers and telltale signs of cyber deception.

DOI: 10.17148/IJARCCE.2025.144108

Short, deepfakes are equally a technological wonder and an imminent cybersecurity risk. Through the advancement of stronger detection technologies, the imposition of ethical norms on AI, and enhancing digital literacy, society can prevent the dangers and ensure the preservation of trust to thrive in the digital world.

REFERENCES

[1]. Khadri, W., Reddy, J. K., Mohammed, A., & Kiruthiga, T. (2024, July). The Smart Banking Automation for High Rated Financial Transactions using Deep Learning. In 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC) (pp. 686-692). IEEE.

[2]. Mohammed, A. K., & Ansari, M. A. (2024). The Impact and Limitations of AI in Power BI: A Review. International Journal of Multidisciplinary Research and Publications (IJMRAP),. Pp. 23-27, 2024., 7(7), 24–27.

[3]. Donnelly, K. J. (2023). Perpetual Realism: Mediating Fantasy and Reality. In *The McGurk Universe: The Physiological and the Psychological in Audiovisual Culture* (pp. 57-106). Cham: Springer International Publishing.

[4]. Alhaidery, M. M. A., & Taherinia, A. H. (2022). A passive image forensic scheme based on an adaptive and hybrid techniques. *Multimedia Tools and Applications*, *81*(9), 12681-12699.

[5]. Aggarwal, A., Mittal, M., & Battineni, G. (2021). Generative adversarial network: An overview of theory and applications. *International Journal of Information Management Data Insights*, *1*(1), 100004.

[6]. Mohammed, A., Sultana, G., Aasimuddin, F. M., & Mohammed, S. (2025). Leveraging Natural Language Processing for Trade Exception Classification and Resolution in Capital Markets: A Comprehensive Study. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 14-18.

[7]. Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward. *Applied intelligence*, *53*(4), 3974-4026.

[8]. Khalid, H., Tariq, S., Kim, M., & Woo, S. S. (2021). FakeAVCeleb: A novel audio-video multimodal deepfake dataset. *arXiv preprint arXiv:2108.05080*.

[9]. Papathanasiou, A., Germanos, G., Kolokotronis, N., & Glavas, E. (2023, November). Cognitive Email Analysis with Automated Decision Support for Business Email Compromise Prevention. In *2023 8th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)* (pp. 1-5). IEEE.

[10]. Ashfaq, S., Chandre, P., Pathan, S., Mande, U., Nimbalkar, M., & Mahalle, P. (2023, June). Defending against vishing attacks: A comprehensive review for prevention and mitigation techniques. In *International Conference on Recent Developments in Cyber Security* (pp. 411-422). Singapore: Springer Nature Singapore.

[11]. Almalki, K. (2022). *Factors engendering corporate fraud and mechanisms for enhancing the detection and prevention of fraudulent financial practices in the UK retail industry* (Doctoral dissertation, University of Sheffield).

[12]. Chittoju, S. R., & Ansari, S. F. (2024). Blockchain's Evolution in Financial Services: Enhancing Security, Transparency, and Operational Efficiency. International Journal of Advanced Research in Computer and Communication Engineering, 13(12), 1–5. https://doi.org/10.17148/IJARCCE.2024.131201

[13]. Rieger, M., Boe, S. G., Ingram, T. G., Bart, V. K., & Dahm, S. F. (2024). A theoretical perspective on action consequences in action imagery: Internal prediction as an essential mechanism to detect errors. *Psychological Research*, *88*(6), 1849-1858.

[14]. Gupta, S., Mohan, N., & Kaushal, P. (2022). Passive image forensics using universal techniques: a review. *Artificial Intelligence Review*, *55*(3), 1629-1679.

[15]. Jenkins, W. K. (2022). Fourier series, Fourier transforms and the DFT. In *Mathematics for Circuits and Filters* (pp. 83-111). CRC Press.

[16]. Balammagary, S., Mohammed, N., Mohammed, S., & Begum, A. (2025). AI-Driven Behavioural Insights for Ozempic Drug Users. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 10-13.

[17]. Begum, A., Mohammed, N., & Panda, B. B. (2024). Leveraging AI in health informatics for early diagnosis and disease monitoring. IARJSET, 11(12), 71–79. https://doi.org/10.17148/iarjset.2024.111205

[18]. Janamolla, K., Balammagary, S., & Mohammed, A. Blockchain Enabled Cybersecurity to Protect LLM Models in FinTech.

[19]. Mittal, G., Hegde, C., & Memon, N. (2024, July). GOTCHA: Real-time video deepfake detection via challenge-response. In *2024 IEEE 9th European Symposium on Security and Privacy (EuroS&P)* (pp. 1-20). IEEE.

[20]. Khairnar, S., Gite, S., Kotecha, K., & Thepade, S. D. (2023). Face liveness detection using artificial intelligence techniques: A systematic literature review and future directions. *Big Data and Cognitive Computing*, *7*(1), 37.

[21]. Sanivarapu, P. V., Rajesh, K. N., Hosny, K. M., & Fouda, M. M. (2022). Digital watermarking system for copyright protection and authentication of images using cryptographic techniques. *Applied Sciences*, *12*(17), 8724.

[22]. Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. *Sensors*, *22*(4), 1304.

DOI: 10.17148/IJARCCE.2025.144108

[23]. Rana, M. S., Nobi, M. N., Murali, B., & Sung, A. H. (2022). Deepfake detection: A systematic literature review. *IEEE access*, *10*, 25494-25513.

[24]. Dowd, P. A. (2023). Accuracy and Precision. In *Encyclopedia of Mathematical Geosciences* (pp. 1-4). Cham: Springer International Publishing.

[25]. Lamichhane, B., Thapa, K., & Yang, S. H. (2022). Detection of image level forgery with various constraints using DFDC full and sample datasets. *Sensors*, *22*(23), 9121.

[26]. Mohammed, S., Sultana, G., Aasimuddin, F. M., & Chittoju, S. S. R. AI-Driven Automated Malware Analysis.

[27]. Nash, A., Studiawan, H., Grispos, G., & Choo, K. K. R. (2023, November). Security analysis of google authenticator, microsoft authenticator, and authy. In *International Conference on Digital Forensics and Cyber Crime* (pp. 197-206). Cham: Springer Nature Switzerland.

[28]. Khadri Syed, W., & Janamolla, K. R. (2023). Fight against financial crimes – early detection and prevention of financial frauds in the financial sector with application of enhanced AI. IJARCCE, 13(1), 59–64. https://doi.org/10.17148/ijarcce.2024.13107

[29]. Mohammed, S., DDS, Dr. S. T. A., Mohammed, N., & Sultana, W. (2024). A review of AI-powered diagnosis of rare diseases. International Journal of Current Science Research and Review, 07(09). https://doi.org/10.47191/ijcsrr/v7-i9-01

[30]. Subudhi, B. N. (2024). Adaptive Meta-Learning for Robust Deepfake Detection: A Multi-Agent Framework to Data Drift and Model Generalization. *arXiv preprint arXiv:2411.08148*.

[31]. Teney, D., Abbasnejad, E., Lucey, S., & Van den Hengel, A. (2022). Evading the simplicity bias: Training a diverse set of models discovers solutions with superior ood generalization. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 16761-16772).

[32]. Shaaban, O. A., Yildirim, R., & Alguttar, A. A. (2023). Audio deepfake approaches. *IEEE Access*, *11*, 132652-132682.

[33]. Schmarje, L., Grossmann, V., Zelenka, C., Dippel, S., Kiko, R., Oszust, M., ... & Koch, R. (2022). Is one annotation enough?-a data-centric image classification benchmark for noisy and ambiguous label estimation. *Advances in Neural Information Processing Systems*, *35*, 33215-33232.

[34]. Syed, W. K., Mohammed, A., Reddy, J. K., & Dhanasekaran, S. (2024, July). Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures. In 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC) (pp. 1331-1336). IEEE.

[35]. John Luan, R., & Narayanan, R. (2024). Enhancing student engagement with authentic assessment in technology-based program: A multi-faceted approach.

[36]. Mohammed, S., Vali, M. Q., & Mohammed, A. R. Securing Healthcare IT Systems: Addressing Cybersecurity Threats in a Critical Industry.

[37]. Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security*, *30*(2), 255-279.

[38]. Gad, A. G., Mosa, D. T., Abualigah, L., & Abohany, A. A. (2022). Emerging trends in blockchain technology and applications: A review and outlook. *Journal of King Saud University-Computer and Information Sciences*, *34*(9), 6719-6742.

[39]. Mohammed, Shanavaz. "The Impact of AI on Clinical Trial anagement."(2024b).

[40]. Ahmed, M. I., Mohammed, A. R., Ganta, S. K., Kolla, S. K., & Kashif, M. K. (2025). AI-Driven Green Construction: Optimizing Energy Efficiency, Waste Management and Security for Sustainable Buildings. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 37-41.

[41]. Mohammed, Z., Mohammed, N. U. M., Mohammed, A., Gunda, S. K. R., & Ansari, M. A. A. (2025). AI-Powered Energy Efficient and Sustainable Cloud Networking. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 31-36.