Intelligent Detection of Malicious Digital Identities Using Artificial intelligence (Ai)-Driven Approach

Dr. Sunita Dixit
Professor
Department of Computer Science & Engineering at St. Andrews
Institute of Technology & Management
Gurgaon
bhardwajsunita23@gmail.com

To Cite this Article
Dr. Sunita Dixit, "Intelligent Detection of Malicious Digital Identities Using Artificial intelligence (Ai)-Driven Approach ", Journal of Science Engineering Technology and Management Science, Vol. 03, Issue 08, August 2026, pp: 633-639, DOI: http://doi.org/10.64771/jsetms.2026.v03.i08.pp633-639
Submitted: 19-07-2026 *Accepted: 02-08-2026* *Published: 08-08-2026*

Abstract- Digital identity is now an integral part of the digital ecosystem and is essential for safe access to the Internet, communication, financial systems, health, and e-government services. As digital technology has expanded, so have the opportunities for identity theft, fake accounts, phishing, deepfakes, impersonation and other forms of identity-based cyber-attacks and cannot prevent these new types of attacks with traditional security methods and require intelligent and adaptive detection. Artificial Intelligence (AI) has come to the rescue with the possibility of automated identity verification, behavioral analysis, biometric authentication, anomaly detection and real-time threat identification. This study presents a comprehensive literature analysis on intelligent detection of harmful digital identities using artificial intelligence. Topics covered include digital identity basics, several kinds of harmful digital identities, methods for verifying digital identities, deep learning and machine learning, large language models, generative AI, and intrusion detection systems based on artificial intelligence. According to the reviewed literature, AI has a major influence on improving detection accuracy, automation, scalability, and resilience to sophisticated cyberattacks. The results underscore the importance of AI in creating trustworthy, secure, and privacy-protecting digital identity management systems, as well as potential avenues for further research and development that could improve intelligent cybersecurity solutions.

Keywords—Artificial Intelligence, Malicious Digital Identities, Machine Learning, Deep Learning, Identity Fraud Detection.

I. INTRODUCTION

Digital identity is essential to the ways people interact, transact and present themselves digitally. The significance of digital identity has grown much more significant in the era where there is constant exchange, storage, and analysis of personal information. It's not only about users being identified online, but also about their digital traces from their actions. These footprints are not solely about customization, but can also be of great security relevance (e.g., security of personal data). In industries like online banking, e-commerce, healthcare, and government services, digital identity is crucial for safeguarding sensitive data and facilitating trusted online interactions [1][2][3]. Therefore, it is the duty and responsibility of individuals and organizations to actively protect digital identities in order to help keep the digital ecosystem private, secure and trustworthy [4].

Digital identity is the set of attributes that defines a person or thing online. The security of digital identities has always been difficult and is becoming even more complex with the emergence of new cyber threats, identity theft, fake accounts, impersonation attacks, synthetic identities, and new technologies that have complicated the authentication process [5]. Digital identity security is also very complicated, with issues regarding cloud environments, standardized environments, privacy preservation, and secure identity management, necessitating advanced and intelligent protection mechanisms.

The digital transformation has created a much wider surface area for attack for malicious actors as businesses, social platforms, financial systems and critical infrastructure are increasingly relying on digital services [6]. Advanced assaults on digital identities cannot be detected by using typical security methods such as rule-based systems, static firewalls, or signature-based detection. The use of AI-driven solutions has proven to be a successful solution, as they facilitate intelligent identity verification, anomaly detection, behavioral analysis, continuous authentication, and real-time identification of malicious digital identities. Moreover, AI enhances adaptive security in Cloud Computing, IoT, and Zero Trust (ZT) settings by continuously analyzing access requests, user activities, and potential threats from user identities [7][8].

Automated threat detection, intelligent fraud prevention, behavioral biometrics, and real-time risk assessment are just a few of the areas where AI can help strengthen digital identity security. AI-driven techniques can accurately identify malicious digital identities, reduce false positives, and improve identity verification practices [9]. Therefore, the potential application of AI and modern cybersecurity solutions is an intriguing possibility for uncovering fraudulent online identities and protecting digital ecosystems from emerging threats.

The paper structure is as follows: **Section II** introduces digital identity concepts and fundamentals. **Section III** discusses malicious digital identities. **Section IV** describes AI-based detection techniques. **Section V** provides a literature overview of current works, while **Section VI** provides suggestions for further research.

II. DIGITAL IDENTITY: CONCEPTS AND FUNDAMENTALS

The idea of a person's "digital identity" has evolved from its physical counterpart. In the digital realm, it is simple to make comparisons, even when they don't necessarily hold water or have any practical utility [10]. The digital translation has mostly eradicated the shared sense of identity. This process can be shown by looking at its setting, which is very different from the last one, and the unique features of digital identity.

A. Identity Lifecycles

A digital identity is generated for each lifecycle 'creation' step to serve as a distinct identifier in a record system [11]. Its creation can be done covertly as part of a user's journey (customer identity) or as part of a corporate procedure (workforce or device identity). Digital identities have the ability to facilitate digital transactions at any point in time via the accounts and privileges that are associated with them. Despite the document's presentation of a lifetime as a continuum, it is expected that:

• In most businesses, there are several technological solutions that might handle the digital identity lifecycle.

• There are certain lifecycle processes that happen more often than others. For example, authenticate and use happen more often than combine and delete.

B. Components of Digital Identity

A digital identity is formed by a collection of attributes and credentials that uniquely represent an individual, organization, or device in the digital environment. These components are used to establish identity, authenticate users, and authorize access to digital services while ensuring security and privacy.

- **Personal Identifiers*:*** A person's biometric data, including fingerprints, height, weight, and date of birth, as well as their legally issued identifiers, such a national security number (NSN), are all part of their personal identity that is formed at birth. An individual's social identity is the sum of their life experiences as they have unfolded through time, as recorded in their biographical narrative.
- **Biometric Identifiers:** The word "biometric" describes a method of establishing a person's identification through the measurement and statistical analysis of their biological characteristics. Physical qualities include things like fingerprints and iris/retina patterns as well as hand geometry. Behavioral traits include things like voice, handwriting, and stride [12].
- **Social Identifiers:** An individual's social and psychological contexts are both taken into account by social identity theories. According to the psychological perspective, a person's social identity and their interactions with the people and things around them are defined. For sociologists, the most important kinds of interpersonal connections are those based on roles, such as those between teachers and their students or between employers and their employees.

III. MALICIOUS DIGITAL IDENTITIES

A wide variety of misleading and destructive internet organizations, each with its own unique traits and goals, are collectively known as "malicious digital identities" in the field of cybersecurity [13]. Automated programs that attempt to imitate human behavior online are known as bots, and they are a common kind of fraudulent account.

A. Types of Malicious Digital Identities

Malicious digital identities are fraudulent or deceptive online personas created to impersonate legitimate users, automate malicious activities, or exploit digital platforms for financial gain, misinformation, cyberattacks, or identity theft. Understanding the different types of malicious digital identities:

- **Bots:** A "bot" is a computer program that can do repetitive, automated tasks more quickly than a human [14].
- **Botnet:** A botnet is a collection of compromised machines that are controlled by an infection-riddled "bot master" using C&C channels [15]. There are usually three different kinds of software that form a botnet.
- **Fake Profile:** false users are those who use social media to impersonate other people; false profiles are the online homes of these imposters [16].
- **Sockpuppet:** A sockpuppet identity starts with a scaffold – name, age, location and appearance. The operator chooses information to ensure the credibility and accessibility of the story [17]. They might include a picture of a real person (identity theft), a stock photo or, more recently, an AI-generated headshot that cannot be found through a reverse-image search.
- **Phishing:** The goal of these deceptive communications is to get people to provide sensitive information (such as passwords, credit card details, or other sensitive data) [18]. Phishing attacks can be extremely risky and lead to identity theft or monetary loss.

B. Data Breaches and Their Implications for Malicious Digital Identities

The fact that data leaks are common in digital identity is a huge problem for individuals and organizations alike. Research into this has revealed that consumers' unease in providing their personal (sensitive) information to corporations has an impact on their willingness to provide such information [4]. Additionally, transparency has been identified as one of the essential elements that can contribute to reducing suspicion and fostering trust in data management procedures. Security breaches have financial consequences as well as privacy implications. The impact of cyber intrusions on market performance has been witnessed for the companies involved, especially in the economic sector.

C. Phishing and Fraud Detection

Cyberspace can be prone to long-term threats like phishing attacks and fraud schemes [19] that pose risks to people and businesses around the world. The goal of these tactics is to persuade users to do financial transactions or provide personal information that would benefit the attacker. Tried and tested methods such as phishing and fraud detection may be difficult to use, as hackers can target unexpected locations [20]. However, new strategies that more successfully minimize these challenges may emerge as a result of AI's proactive and reactive strategies [21]. Through the application of deep algorithms and ML techniques, these systems powered by AI are able to detect phishing and fraud trends, anomalies, and behavioral norms. AI can identify phishing, fraudulent operations, and other suspicious activities by analyzing the sender's behavior, content, transactional patterns, and user activity.

D. Identity Deception Attacks on Social Media

Identity deception attacks occur when attackers exploit or create digital identities to trick, defraud, deceive, steal personal information, and disrupt trust on social media platforms. The attacks exploit the openness and interconnectedness of social networks, and are increasingly difficult to identify. Common examples include fake profiles, identity theft and identity cloning, all of which use varying tactics to trick the user and carry out an ulterior motive. Table I shows a detailed classification of the malicious digital identities in social network platforms. It defines the many forms of identity-related assaults, including bogus profiles, theft, and cloning, and describes the motivations, methods, outcomes, and most targeted social media platforms. This classification gives an understanding of the features and the effects of the various identity deception attacks.

TABLE I. CLASSIFICATION OF MALICIOUS DIGITAL IDENTITIES AND THEIR CHARACTERISTICS IN SOCIAL NETWORKS

Attack Category	Attack Type	Purpose	Procedure	Outcome	Target Network
Fake Profile	Sybil Attack	Using a plethora of false identities to damage or undermine a social media reputation.	The enemy creates a plethora of false identities.	Getting an outsized amount of influence and control on social media and maintaining or expanding that influence.	Peer-to-peer networks, Microblogging, and social media sites.
Fake Profile	Sock puppet	In order to back an argument or to get around limitations.	The person signs up for one false identity.	Defying limitations or unfairly gaining support for an opinion.	Microblogging, Collaborative projects, and Blogs.
Fake Profile	Social Botnet	With the goal of automating the attack's scope.	Malicious information and interactions with social media users are generated by computer algorithms.	The attack's sphere of influence grows.	All types of social media.
Identity Theft	Compromised	The intentional dissemination of incorrect information, abuse of valid accounts, or defamation of a social media user.	Phishing and other forms of social engineering try to get people to reveal sensitive information or take advantage of the fact that most people don't bother to change their passwords on all of their social media accounts.	There is a lack of complete control over the account for the original user because both the account owner and the adversary have access to it.	All types of social media.
Identity Theft	Hijacked	The same as when someone's identity is stolen.	The same as when someone's identity is stolen.	There is a problem with the original user's account.	All types of social media.
Identity Cloning	Single-site or Cross-site	Intentionally misleading or slandering someone while stealing their personal information.	The victim's identity is stolen and used to build a duplicate profile on the same or other social media platforms. The victim's pals get the invitation to become friends. Their level of trust determines whether or not a friend request is approved.	The victim sets up a new network, and the attacker has access to all of the shared private data.	All types of social media.

IV. ARTIFICIAL INTELLIGENCE FOR MALICIOUS DIGITAL IDENTITY DETECTION

AI improves biometric identification systems by making face, iris, fingerprint, and voice recognition faster, more accurate, and more effective. ML is the key to AI's ability to process complex biometric signals and spot subtle changes that humans would miss. For instance, AI can improve face recognition accuracy despite lighting, angle, and emotion variations [22]. Similarly, AI can enhance the capacity to distinguish between authentic and false inputs in terms of fine details and intricate patterns for iris and fingerprint identification.

A. AI-based intrusion detection system

The widespread reliance on data and the internet has made security an absolute must. Research toward creating an automated mechanism to identify suspicious traffic is continuing [23]. Cloud computing has just emerged, and more and more sectors are making the transition. Cybersecurity concerns have been on the rise in tandem with this development. Consequently, suitable answers are necessary to guarantee the network and cloud function correctly. An alluring approach to assault detection and classification is AI-based intrusion detection.

B. AI Detection Approaches for Malicious Digital Identities

The detection techniques are the bedrock of the intrusion detection system's functionality. There are currently two main varieties of IDS that identify intrusions: those that rely on anomalies and those that use signatures. Two acronyms for these terms are AIDS and SIDS.

- **Signature-intrusion detection system (SIDS):** The word "signature" refers to a pattern that characterizes a single danger that has already been identified and documented in the dataset [24]. Comparing the present network traffic to the harmful signatures stored in the dataset is the fundamental mechanism of SIDS. When the patterns align, the alert is set to affirmative, allowing for the detection and prevention of harmful behavior.
- **Anomaly-intrusion detection system (AIDS):** AIDS is another example of an infectious disease. Anomaly detection is the foundation of AIDS. An unusual amount of SNMP traffic or a large volume of Telnet connections in a short amount of time are examples of anomalous traffic. Studying typical traffic at various times would be the initial step in the AIDS detection process, and the results would provide a baseline profile. Using the profile as a baseline, AIDS would then start monitoring traffic after the study.

C. Artificial Intelligence Technologies for Malicious Digital Identity Detection

AI has become a key technology for detecting malicious digital identities by analyzing user behaviour, profile characteristics, social interactions, and network

activities to identify fraudulent accounts and suspicious behaviour. AI-driven methods increase the precision of detection, allow for live monitoring, and boost the scalability of ID verification solutions.

- **Machine Learning (ML):** ML is a branch of AI that focuses on improving performance and making predictions using data acquired from various sources, such as human-curated training sets or data obtained from the real world.

1. Supervised Learning: As a cybersecurity education tool, this is among the most tried-and-true formats [25]. It relies on labeled data, with each instance being labeled as normal or malicious, allowing the model to learn decision boundaries that can correctly classify new, unseen data.
2. Unsupervised Learning: Unsupervised learning is also a key application in cybersecurity for anomaly detection, which involves identifying patterns of behavior that deviate from those the system is used to. Unsupervised methods are generally more efficient and can be used in dynamic and evolving environments because they do not need labeled data.
3. Semi-Supervised Learning: Combining supervised and unsupervised learning methods with both labeled and unlabeled data is known as semi-supervised learning. In fields like cybersecurity, where labeled data is scarce but unlabeled data abounds, this method might prove useful.

- **Deep Learning (DL):** DL models learn complex representations automatically from large-scale identity data. The profile attributes, behavioral patterns, temporal activities, and social network relationships are all analyzed to detect malicious identities, where architectures like CNNs, RNNs/LSTMs, GNNs, and Transformers are widely employed [26][27].
- **Large Language Model (LLM):** A massive AI model or Gen AI subset taught to understand and produce human language from massive datasets. When it comes to text-based tasks (such as translation, categorization, and text production), LLMs are highly capable since they are taught utilizing designs like Transformers.
- **Gen AI:** GenAI can also support the cybersecurity function by generating synthetic data for model training, augmenting threat simulation, assisting security analysts in identifying new identity-based attacks and improving automated detection systems[28].

D. AI Threat Detection and Prevention

E. AI-Based Digital Identity Verification Techniques

The applicant's identification is checked for validity and consistency using the identity verification module, which incorporates different ML models. Figure 1 shows how document analysis, biometric authentication, behavioral analytics, and decision-making are combined in an AI-powered identity verification workflow to validate identities and identify fraudulent verification attempts.

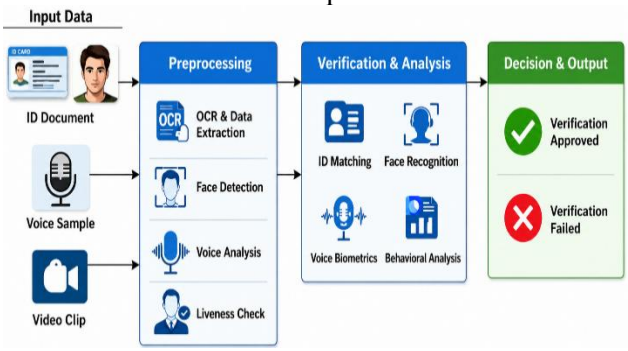

Figure 1: AI-Based Digital Identity Verification Framework

- Document Verification: Document Verification is extracting text information from documents. CNNs for the Detection of Tampering Patterns and Artifacts of Forgery.
- Biometric Authentication: An example of a deep metric learning model used for biometric verification is a Siamese network, which can recognize faces and match ID photos with selfies [29]. Spoofing attacks can be lessened with the use of liveness-detecting tools.
- Behavioral and Device Analytics: Analyzing patterns of behavior such device fingerprint consistency, typing speed, and geolocation stability is done using sequence-based ML models. An ICS is created by combining the outputs of various sub-modules using ensemble learning.

F. Data Preprocessing and Feature Extraction

Raw inputs are first preprocessed to enhance data quality and noise reduction:

- OCR & Text Normalization: Removes name, DOB, ID number from the documents.
- Face Detection & Alignment: Region detection and alignment of face.
- Voice Signal Processing: Noise removal, MFCC: Feature extraction.
- Liveness Check: The liveness check is a pre-processing stage to reduce the possibility of spoofing based on motion and depth cues, ensuring consistency and reliability across modalities.

V. LITERATURE REVIEW

The section outlines the latest research for intelligent identification of malicious digital identities through AI, including AI-based malware analysis, blockchain-based identity management, secure authentication, phishing detection, deepfake identification, and privacy-preserving identity verification.

S. Khan, H. Raza, and M. Alam (2026) is an extensive survey of Malware analysis and detection using AI, particularly ML and LLMs. The article discusses the idea of using AI for both static and dynamic malware analysis, new trends like federated learning, and growing issues including adversarial assaults, model transparency, and resource restrictions [30].

S. Krithika *et. al* (2026) proposed UPI Connect, a blockchain-based SSI solution for safe and private cross-site identity management. After a person is verified, a UPI is given to them and safely stored on the blockchain. ML algorithms determine if third-party platforms are reliable, while models like DT and ANN categorize websites. When users access sensitive information on untrusted websites, Zero-Knowledge Proof (ZKP) ensures that their authentication process remains safe [31].

X. Liu *et al.*, (2025) developed a secure computer protocol called SPSLD using the NTRU algorithm, which uses additive homomorphism for encryption. Models that are semi-honest or malicious can use it. The experimental results demonstrate that the semi-honest protocol offers secure and efficient protection for WSN environments, reducing computational complexity by at least 85% and execution time by 32%-46% compared to Paillier-based schemes. Additionally, the malicious model outperforms comparable attack-resistant schemes by 12% [32].

R. Pandey and R. Pandey (2025) Deepfake technology manipulates facial expressions, lip movements, or entire identities to create incredibly lifelike fake videos using powerful AI, namely DL. While digital media editing tools have many harmless applications, deepfakes can also be used maliciously to deceive, defame, or damage an individual's reputation through manipulated images and videos[33].

U. Gulzar (2025) introduces Personhood Credentials (PHCs), a digital identity to establish a genuine person without risking privacy or being identified as a bot or fake account. PHCs are issued by trusted sources such as governments or organizations and are local or international (but not biometric). The growing ability of AI to mimic human behavior and its scalability only reinforces the importance of these identity verification tools [34].

I. Naseer (2024) Phishing attacks are a kind of cybercrime that targets individuals by having them divulge personal information by making the perpetrator appear to be a legitimate website or organization. Conventional cybersecurity solutions are becoming increasingly ineffective due to the ever-changing nature of phishing methods. To improve cybersecurity, AI, and machine learning in particular, are essential for analyzing massive volumes of data, identifying attack trends, and detecting threats in real-time; this allows for more accurate and adaptive phishing detection [35].

The reviewed studies have been summarized in Table II, which presents information on the objective of the study, the method employed, the major conclusions, the weaknesses of the previous investigations, and the suggestions for future research.

TABLE II. SUMMARY OF THE STUDY OF INTELLIGENT DETECTION OF MALICIOUS DIGITAL IDENTITIES USING ARTIFICIAL INTELLIGENCE

Reference	Study Focus	Approach / Methodology	Key Findings	Challenges / Limitations	Future Directions
S. Khan, H. Raza, and M. Alam (2026)	AI-driven malware analysis and detection	Comprehensive survey of AI, ML, LLMs, static & dynamic malware analysis	AI significantly improves malware detection; highlights federated learning and explainable AI	Adversarial attacks, lack of model transparency, resource constraints	Develop ethical, explainable, and robust AI-based malware detection frameworks
S. Krithika et al. (2026)	Decentralized digital identity verification	Blockchain-based Self-Sovereign Identity (SSI), ML, Decision Tree, ANN, Zero-Knowledge Proof (ZKP)	Enables secure, privacy-preserving identity verification and trusted cross-site authentication	Blockchain complexity, computational overhead, scalability	Enhance decentralized identity systems with lightweight AI and scalable blockchain solutions
X. Liu et al. (2025)	Secure malicious node detection in WSN	NTRU encryption, homomorphic computation, SPSLD protocol, cut-and-choose security	Reduces computational complexity by 85% and improves execution efficiency while resisting malicious attacks	Additional computational overhead under malicious model	Optimize secure computation protocols for large-scale IoT and wireless sensor networks
R. Pandey and R. Pandey, (2025)	Deepfake detection	Deep learning-based analysis of manipulated images and videos	Demonstrates AI's capability to detect sophisticated deepfake content and identity impersonation	Rapid evolution of deepfake generation techniques	Develop more robust real-time multimodal deepfake detection systems
U. Gulzar (2025)	Personhood Credentials (PHCs) for digital identity	Privacy-preserving digital identity framework using Personhood Credentials	Verifies human users without revealing personal information, reducing fake accounts and bots	Adoption challenges and increasing sophistication of AI-generated identities	Standardize PHC frameworks and integrate them with AI-driven identity verification
I. Naseer(2024)	AI-based phishing detection	Machine Learning for email, URL, and sender behavior analysis	AI improves phishing detection, including zero-day threats, through real-time analysis	Constantly evolving phishing techniques and high-quality data requirements	Develop adaptive AI models capable of detecting emerging phishing attacks in real time

Conclusion And Future Work

Digital identity is a crucial aspect of protecting people, institutions and digital services in the digital era. Cyber risks have changed over time and become smarter and more flexible. This means that need a smarter and more flexible security system that can find malicious digital identities as quickly and accurately as possible. The concepts of digital identity, malicious digital identity, and recent AI-based approaches to digital identity detection and verification have been reviewed. It explored how ML, DL, LLM, generative AI, biometric authentication, intrusion detection, phishing detection and behavioral analytics can be used to bolster digital identity security. The literature explored shows that AI has the potential to greatly improve the way identities are verified, threats are detected, fraud is prevented, and incidents are automatically answered, to mention a few, while also increasing scalability and minimizing false positives. The findings point to AI-powered approaches as a potential roadmap for creating reliable digital identity management systems that can tackle the expanding cybersecurity requirements and threats.

Future work should extend to creating explainable, privacy-preserving and computationally efficient AI models for detection of malicious digital identities. The incorporation of federated learning, blockchain, multimodal biometric authentication, and large language models can further enhance the scalability, robustness, real-time detection, and resilience against emerging cyber threats based on identities.

REFERENCES

[1] M. Mittal, "AI IN HEALTHCARE: THE NEXT FRONTIER IN MEDICAL DIAGNOSIS," *Int. J. Inf. Technol. Manag. Inf. Syst.*, vol. 16, no. 2, pp. 1448–1455, Mar. 2025, doi: 10.34218/IJITMIS_16_02_091.

[2] A. Joon, S. A. Pahune, S. Mathur, and S. Rongala, "Designing Predictive Analytics Frameworks with ML for ERP-Supported E-Commerce Systems," in *2025 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC)*, 2025, pp. 1–6. doi: 10.1109/ASSIC64892.2025.11158452.

[3] R. Kant, R. R. Thallada, B. Pandey, and P. Srivastava, "AI-Based Cybersecurity in Healthcare: A Data-Driven, Governance-Aware Framework for Secure Clinical Systems," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, Houston, TX, USA: IEEE, 2026, pp. 1–5, February. doi: 10.1109/ICAIC67076.2026.11395836.

[4] M. N. Ghadge, "Digital Identity in the Age of Cybersecurity: Challenges and Solutions," *Glob. J. Comput. Sci. Technol.*, vol. 24, no. 1, pp. 1–9, 2024, doi: 10.34257/ljrcstvol24is1pg1.

[5] N. Ghadge, "Challenges with Securing Digital Identity," *Int. J. Cybern. Informatics*, vol. 13, no. 4, pp. 01–08, 2024, doi: 10.5121/ijci.2024.130401.

[6] R. Rao Thallada, "AI-Driven Business Continuity and Disaster Recovery in Financial Services: Minimizing Downtime through Predictive Intelligence and Autonomous Response Systems," *J. Bus. Manag. Stud.*, vol. 7, no. 6, pp. 09–14, October, 2025, doi: 10.32996/jbms.

[7] G. Sunkara, "AI-Driven Cybersecurity: Advancing Intelligent Threat Detection and Adaptive Network Security in the Era of Sophisticated Cyber Attacks," *Well Test.*, vol. 31, no. 1, pp. 185–198, 2022.

[8] S. Kumara and M. Shah, "Securing national connectivity infrastructure through identity resilience: implications for zero trust," *Futur. Technol. Open Access J.*, vol. 5, no. 3, pp. 276–286, August, 2026, doi: 10.55670/fpll.futech.5.3.24.

[9] A. Awadallah *et al.*, "Artificial Intelligence-Based Cybersecurity for the Metaverse: Research Challenges and Opportunities," *IEEE Commun. Surv. Tutorials*, 2025, doi: 10.1109/COMST.2024.3442475.

[10] M. Robles-Carrillo, "Digital identity: an approach to its nature, concept, and functionalities," *Int. J. Law Inf. Technol.*, vol. 32, 2024, doi: 10.1093/ijlit/eaae019.

[11] A. Cameron and O. Grewe, "An Overview of the Digital Identity Lifecycle (v2)," *IDPro Body Knowl.*, vol. 1, 2022, doi: 10.55621/idpro.31.

[12] J. Blue, J. Condell, and T. Lunney, "A Review of Identity, Identification and Authentication," *Int. J. Inf. Secur. Res.*, vol. 8, no. 2, pp. 794–804, 2018, doi: 10.20533/ijisr.2042.4639.2018.0091.

[13] S. Salloum, "Detecting Malicious Accounts in Cyberspace: Enhancing Security in ChatGPT and Beyond," 2024, pp. 653–666. doi: 10.1007/978-3-031-52280-2_42.

[14] M. Aljabri, R. Zagrouba, A. Shaahid, F. Alnasser, A. Saleh, and D. M. Alomari, *Machine learning-based social media bot detection: a comprehensive literature review*, vol. 13, no. 1. Springer Vienna, 2023. doi: 10.1007/s13278-022-01020-5.

[15] K. C. Hwa, S. Manickam, and M. A. Al-Shareeda, "Review of Peer-to-Peer Botnets and Detection Mechanisms," 2022. doi: https://doi.org/10.48550/arXiv.2207.12937.

[16] P. G. Bharti, Nasib Singh Gill, "Exploring machine learning techniques for fake profile detection in online social networks," 2023, doi: 10.11591/ijece.v13i3.pp2962-2971.

[17] Jonathan Altice, "SockPuppets: The Double-Edged Sword of Cyber Operations – A Developmental Case Study," 2025.

[18] V. K. Jethani, V. Pathak, and V. Shrivastava, "Spam and fake account detection using machine learning: A review," *Int. J. Recent Res. Rev.*, vol. XVIII, no. 1, pp. 230–240, March, 2025.

[19] S. P. Sivashanmugam, S. Kumara, A. Mohile, and D. R. Suram, "Improving Detection Accuracy of Phishing Attacks with Feature Selection and Machine Learning Techniques in Cybersecurity," in *2026 1st International Conference on Emerging Trends in Advancements and Applications of Computational Intelligence Techniques (ETAACT)*, Bhubaneswar, India: IEEE, 2026, pp. 1–6, April. doi: 10.1109/ETAACT69135.2026.11542138.

[20] S. R. Somula, "INTELLIGENT FRAUD PREVENTION: IMPLEMENTING AML SOLUTIONS FOR MCCA REIMBURSEMENT CLAIMS PROTECTION," *Int. J. Comput. Eng. Technol.*, vol. 16, no. 1, pp. 3609–3622, Feb. 2025, doi: 10.34218/IJCET_16_01_249.

[21] A. Al Siam, M. Alazab, A. Awajan, and N. Faruqui, "A Comprehensive Review of AI's Current Impact and Future Prospects in Cybersecurity," IEEE, 2025, pp. 14029–14050. doi: 10.1109/ACCESS.2025.3528114.

[22] S. Mandru, "How AI can Improve Identity Verification and Access Control Processes," *J. Artif. Intell. Cloud Comput.*, vol. 1, pp. 1–5, 2022, doi: 10.47363/JAICC/2022(1)E101.

[23] T. Sowmya and E. A. Mary Anita, "A comprehensive review of AI-based intrusion detection system," *Meas. Sensors*, 2023, doi: 10.1016/j.measen.2023.100827.

[24] M. Ni, "A review on machine learning methods for intrusion detection system," *Appl. Comput. Eng.*, vol. 27, no. 1, pp. 57–64, 2023, doi: 10.54254/2755-2721/27/20230148.

[25] M. T. Karatu, I. M. Mungadi, and A. Shehu, "Machine Learning Techniques for Cybersecurity Threat Detection : A Systematic Review," *Int. J. Innov. Sci. Res. Technol.*, vol. 11, no. 3, pp. 2992–2998, 2026.

[26] A. Aguirre and L. Salazar, "A Systematic Review of Artificial Intelligence Techniques for Phishing Detection," *Adv. Artif. Intell. Mach. Learn.*, p. 231, 2025, doi: 10.54364/AAIML.2025.53231.

[27] K. Muskan, "Deep Learning-Based Malware Detection : A Systematic Review with Explainable Artificial Intelligence Perspectives," vol. 010277, pp. 1–5, 2026.

[28] H. Cheng *et al.*, "Generative AI for Requirements Engineering: A Systematic Literature Review," *Softw. Pract. Exp.*, vol. 56, pp. 141–170, 2025, doi: 10.1002/spe.70029.

[29] P. Malik, K. Raghuwanshi, M. Jain, M. Rajput, and M. Dehlvi, "Digital Identity Verification Using Machine Learning to Reduce Fraud in Micro-Lending and Enhance Credit Risk Assessment," vol. 14, pp. 10–25, 2026.

[30] S. Khan, H. Raza, and M. Alam, "AI-Driven Malware Analysis and Detection: A Comprehensive Survey of Techniques, Trends and Challenges," *J. Informatics Web Eng.*, vol. 1, no. 5, p. 106, 2026, doi: 10.33093/jiwe.2026.5.1.7.

[31] S. Krithika, E. S. Praveena, R. Subhashini, and N. V. Tamil Selvi, "UPI Connect: Centralized Access Point for Decentralized Identity Verification and Secure Cross-Site Registration," in *2026 Fourth International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, 2026, pp. 746–752. doi: 10.1109/ICAISS68683.2026.11526621.

[32] X. Liu *et al.*, "Malicious Node Detection Scheme in WSN Based on Secure Computation of Spatially Parallel Straight-Line Distance," *IEEE Internet Things J.*, vol. 12, no. 24, pp. 53520–53537, 2025, doi: 10.1109/JIOT.2025.3616959.

[33] R. Pandey and R. Pandey, "Deepfake Detection: State-of-the-Art Techniques and Emerging Trends," in *2025 2nd International Conference on Electronic Circuits and Signaling Technologies (ICECST)*, 2025, pp. 1101–1105. doi: 10.1109/ICECST66106.2025.11307586.

[34] U. Gulzar, "Digital Identity and Personhood Safeguarding Privacy in a Machine World," in *2025 2nd International Conference on Intelligent Systems for Cybersecurity (ISCS)*, 2025, pp. 1–4. doi: 10.1109/ISCS69371.2025.11385997.

[35] I. Naseer, "The role of artificial intelligence in detecting and preventing cyber and phishing attacks," *Eur. J. Eng. Sci. Technol.*, vol. 11, no. 09, pp. 82–86, October, 2024.