International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

AI in Cybersecurity and Digital Forensics: A Comparative Review of Techniques, Applications, and Research Gaps

Hensei Patel[1], Jay Pathak[2]

[1]KPGU University, Krishna School of Diploma Studies, Varnama, Vadodara, Gujarat
Email: *hensei13122000[at]gmail.com*

[2]KPGU University, Krishna School of Diploma Studies, Varnama, Vadodara, Gujarat
Email: *pathakjay2506[at]gmail.com*

Abstract: ***Cybersecurity and digital forensics are experiencing serious challenges as a consequence of a sharp rise in cyber risks and cybercrimes driven on by the rapid growth of digital technologies, cloud computing, and connected services. A great deal of digital evidence produced by contemporary systems are becoming too much for manual forensic methods and conventional security technologies to manage. To overcome these limitations, artificial intelligence (AI) methods such as machine learning (ML), deep learning (DL), convolutional neural networks (CNN), generative adversarial networks (GAN), natural language processing (NLP), reinforcement learning, and federated learning have shown promise. This review's goals are to identify performance trends, highlight unresolved issues, and offer a thorough review of current AI-driven research in cybersecurity and digital forensics. 19 investigations covering intrusion detection, malware analysis, phishing identification, smart grid security, cloud forensics, multimedia evidence analysis, generative AI security, and human-focused cybersecurity that were published between 2020 and 2026 were carefully selected from major scientific databases, including IEEE Xplore, Springer, Elsevier, ScienceDirect, ACM Digital Library, and SSRN. The contrast shows that while generative AI and NLP enhance forensic capabilities through threat simulation and automated analysis, deep learning models-particularly CNN-based architectures—achieve detection accuracy above 98% in intrusion detection and forensic categorisation tasks. The black-box nature of AI models, adversarial vulnerability, dataset scarcity, poor cross-domain generalisation, privacy issues, and high processing cost are some of the enduring challenges, however. Also, future directions for Explainable AI (XAI) research are provided in the paper.***

Keywords: Artificial Intelligence, Cybersecurity, Digital Forensics, Machine Learning, Deep Learning, Convolutional Neural Networks, Generative AI, Intrusion Detection System, Explainable AI.

1. Introduction

With abilities far exceeding those of traditional rule-based protection mechanisms, artificial intelligence (AI) has emerged as a vital advancement in the domains of cybersecurity and digital forensics. Rapid advancements in technological advances, cloud computing, the Internet of Things (IoT), smart devices, and online communication platforms have greatly broadened the attack surface and raised the volume and sophistication of assaults. The capabilities of conventional security solutions like firewalls, signature-based intrusion detection systems, and human forensic analysis are now exceeded by threats such ransomware and phishing campaigns, deepfakes, Advanced Persistent Threats (APTs), and AI-generated cyberattacks. For the purpose to enhance cyber protection and update digital forensic investigations, companies, investigators, and researchers are starting to employ AI-driven strategies.

Artificial intelligence (AI) techniques such as machine learning (ML), deep learning (DL), natural language processing (NLP), reinforcement learning (RL), and generative AI have shown positive results in phishing classification, threat intelligence, anomaly detection, detection of malware, user behaviour analysis, and automated incident response. AI speeds up and enhances the accuracy of investigations in digital forensics by helping investigators with evidence gathering, multimedia analysis, pattern recognition, activity classification, and large-scale data processing. Additionally, real-time threat monitoring and prediction defence are made feasible by AI-powered systems, which enable companies to detect and reduce cyber risks proactively rather than reactively.

Despite these changes, a number of important issues are still unsolved. Many AI models' interpretability and legal validity in forensic decision-making are limited by their "black-box" nature. Large-scale execution is nevertheless hindered by ethical and privacy issues, adversarial attack vulnerability, a lack of suitable real-world datasets, and restricted cross-domain adaptability. These issues highlight the necessity of a systematic assessment that summarises recent advances in AI, assesses its pros and cons, and determines the research paths required for effective AI-based cyber security and forensics. Even though a number of reviews on AI in cybersecurity have been published recently, such as those by Goni et al. [6], Al Siam et al. [3], Kayode et al. [4], and Swetha et al. [17], most of them either concentrate on a particular AI technique or on cybersecurity or digital forensics independently. In contrast, this article covers both domains concurrently, incorporates recent studies from 2024–2026, and provides a comparative analysis that clearly connects AI techniques to their application areas, performance characteristics, and unsolved challenges.

2. Literature Study

Reem Almarwani [1] proposed a user-centered cybersecurity framework focusing on AI-driven synthetic threats such as deepfakes and AI-generated deception. The study integrated

cognitive security and behavioral analysis to evaluate user awareness and protective behavior, highlighting the importance of detection competence in defending against AI-powered cyber threats.

Afrin et al. [2] conducted a systematic review of AI-powered cybersecurity in smart grid communication systems. The study analyzed ML and DL-based intrusion detection models and discussed federated learning, blockchain integration, and adversarial robustness for securing cyber-physical smart grid infrastructures.

Al Siam et al. [3] reviewed the role of Artificial Intelligence in cybersecurity using machine learning, deep learning, NLP, and anomaly detection approaches. The paper emphasized AI's effectiveness in malware detection, phishing identification, and behavioural analysis while discussing future improvements and integration challenges.

Kayode et al. [4] examined emerging trends and opportunities in AI-driven cybersecurity. The study explored supervised learning, anomaly detection, reinforcement learning, and autonomous response systems while addressing adversarial attacks, explainability issues, and governance frameworks for responsible AI deployment.

Khaga et al. [5] surveyed machine learning and deep learning-based intrusion detection systems for proactive cloud security. The study highlighted adaptive IDS frameworks, cooperative detection mechanisms, and intelligent cloud monitoring systems to improve defense against evolving cyber threats in distributed cloud environments.

Goni et al. [6] presented a systematic review of machine learning applications in cybersecurity and cyber forensics. The paper discussed the role of ML and DL in threat detection, digital evidence analysis, and cybercrime investigation while recommending future exploration of computational intelligence methods.

McCarthy et al. [7] proposed a machine learning-based forensic activity classification system using digital traces from iPhones. The research demonstrated how sensor-generated smartphone data can assist forensic investigations by identifying user activities and reconstructing timelines using AI-based likelihood analysis.

Mirsadeghi et al. [8] investigated the class imbalance problem in machine learning-based intrusion detection systems for software-defined networking (SDN). The study evaluated GANs, Random Forest, SMOTE, and Siamese Neural Networks to improve minority attack detection and intrusion classification accuracy.

Whittaker et al. [9] explored the use of open-source software and interdisciplinary teaching methods to improve digital forensics accessibility and education. The study emphasized sustainable learning, competency-based training, and understanding AI-assisted forensic image processing techniques in higher education.

Ekhande et al. [10] reviewed deep learning approaches in digital forensics, particularly CNN-based techniques for image, video, and audio analysis. The study concluded that convolutional neural networks provide high accuracy in forensic investigations and multimedia evidence classification.

Qadir and Varol [11] discussed the role of machine learning in digital forensics and behavioral investigation. The study highlighted how AI can process large-scale digital evidence, identify criminal patterns, and support predictive forensic analysis for cybercrime prevention.

Englbrecht and Pernul [12] proposed a privacy-aware digital forensic investigation framework for enterprises. The study introduced entropy-based identification techniques to protect sensitive information during forensic analysis while maintaining compliance with privacy regulations such as GDPR.

Zziwa et al. [13] analyzed the integration of cloud computing and AI in cybersecurity forensics. The paper highlighted AI-driven threat detection, real-time anomaly analysis, automated forensic workflows, and scalable cloud-based forensic systems for enhanced incident response.

Emehin et al. [14] explored the opportunities and ethical implications of Generative AI in forensic data analysis. The study discussed AI-assisted reconstruction, predictive analytics, and cloud-based investigations while addressing concerns regarding bias, fabricated evidence, and privacy violations.

Uddin et al. [15] presented a comprehensive review of Generative AI applications in cybersecurity operations and threat intelligence. The study examined autonomous threat detection, anomaly analysis, and AI-assisted security management while discussing risks such as malicious AI misuse and model vulnerabilities.

Shakil et al. [16] proposed MARINERNet, a deep learning-based intrusion detection system for maritime radar networks. The model achieved high accuracy in detecting sophisticated maritime cyberattacks using convolutional layers and residual learning for real-time anomaly detection.

Swetha et al. [17] reviewed AI applications in cybersecurity, focusing on machine learning, deep learning, phishing detection, malware analysis, and intrusion detection systems. The paper discussed adversarial threats, data scarcity, explainable AI, and future technologies like predictive analytics and quantum computing.

Villegas-Ch et al. [18] investigated AI techniques for enhancing efficiency and accuracy in digital forensic analysis. The study applied convolutional neural networks, NLP, and supervised learning to process massive forensic datasets and improve evidence analysis precision.

Oladipo et al. [19] reviewed machine learning-based digital forensics techniques for object detection and image recognition. The paper categorized forensic applications and identified convolutional neural networks as state-of-the-art methods for forensic image analysis and crime scene reconstruction.

3. Methodology

The methodology adopted in this review follows a structured, analytical approach to examine recent advances in the application of Artificial Intelligence (AI) in cybersecurity and digital forensics. The review process consisted of three main stages: (i) identification of relevant research sources, (ii) application of selection criteria, and (iii) thematic and comparative analysis of the selected studies.

(i) Identification of Sources

Relevant studies from reputable scientific databases, like IEEE Xplore, Springer, Elsevier, ScienceDirect, ACM Digital Library, and SSRN Electronic Journal, were collected between 2020 and 2026. Combinations of terms such as "Artificial Intelligence in Cybersecurity," "Machine Learning Intrusion Detection," "Deep Learning Digital Forensics," "Generative AI Cybersecurity," "AI-based Malware Detection," and "Cloud Forensics AI" were utilised in the search. To capture recent and broad advances in the subject, both major research articles and review papers were taken into account.

(ii) Selection Criteria.

Studies which (a) applied AI, ML, DL, or related techniques to cybersecurity or digital forensics; (b) were published between 2020 and 2026 in peer-reviewed journals, respected conferences, or indexed open-access venues; and (c) provided novel approaches, comparative analyses, or systematic reviews were included. Studies that (a) failed to focus on AI-based methods, (b) lacked technical or analytical depth, or (c) were duplicates or publications composed in language other than English were eliminated. Nineteen studies in all were chosen for an in-depth look based on these criteria.

(iii) Analytical Approach.

Major application domains, including intrusion detection, malware analysis, cloud security, smart grid security, digital forensic investigation, generative AI security, privacy-aware forensics, and human-centered cybersecurity, were utilised for organising the studies selected. Machine Learning (ML), Deep Learning (DL), Convolutional Neural Networks (CNN), Random Forest (RF), Natural Language Processing (NLP), Generative Adversarial Networks (GANs), Reinforcement Learning (RL), and Federated Learning (FL) make up the AI techniques evaluated in these studies. The application of AI techniques, application focus, stated strengths, and identified limitations were taken into account when analysing each study. The cross-cutting trends, recurrent flaws, and unmet research gaps that drive the open issues and future directions addressed in upcoming sections were made possible by this structure.

Comparative Analysis and Findings

The comparative analysis of the nineteen reviewed studies, summarized in Table 1, reveals clear trends in how Artificial Intelligence is currently applied across cybersecurity and digital forensics. Deep Learning, particularly Convolutional Neural Networks (CNN) and hybrid CNN-based architectures, dominate the most performance-critical applications, including smart grid intrusion detection [2] and maritime radar network protection [16], where reported detection accuracy exceeds 98%. CNN and NLP-based models similarly drive multimedia forensic analysis [10], [18], [19], achieving strong performance in image, video, and audio evidence classification. Machine Learning and ensemble methods remain widely used in behavioural forensics [11], cloud security IDS [5], and class-imbalance handling for software-defined networks [8], while Generative AI and Reinforcement Learning are increasingly applied to threat simulation, autonomous incident response, and forensic data reconstruction [4], [14], [15].

Across the reviewed studies, AI-based systems consistently outperform traditional security and forensic methods along four key dimensions: accuracy, automation, scalability, and predictive capability. AI-driven intrusion detection systems enable real-time monitoring and automated mitigation in distributed cloud, IoT, and industrial environments [2], [5], [13]. Forensic systems built on CNN and NLP allow large-scale evidence processing, multimedia classification, and activity reconstruction that would be infeasible through manual analysis [7], [10], [18]. Generative AI further extends forensic capabilities through predictive analysis, evidence reconstruction, and threat-scenario simulation [14], [15], while human-centered frameworks address emerging risks such as deepfakes and AI-generated deception by combining behavioural analysis with detection [1], [4].

Despite these advances, the comparative analysis exposes recurring limitations across the reviewed literature. The black-box nature of deep learning models restricts interpretability and limits the legal admissibility of AI-driven forensic decisions [10], [16], [18]. Adversarial vulnerability and class imbalance remain unresolved problems in intrusion detection [2], [4], [8], [17], while privacy concerns and ethical risks associated with generative AI continue to grow [12], [14], [15]. High computational cost and weak cross-domain adaptability further restrict deployment in resource-constrained and heterogeneous environments [7], [10], [16]. Collectively, these findings indicate that while AI techniques achieve strong accuracy in controlled settings, significant additional research is required to make them robust, interpretable, and operationally trustworthy in real-world cyber defence and forensic practice.

4. Result Analysis

By improving threat detection, intrusion prevention, and forensic investigation protocols, AI has significantly transformed cybersecurity and digital forensics. The reviewed research show that machine learning (ML) and deep learning (DL) addresses are frequently employed to identify malware, phishing attempts, cyberattacks, and suspicious network activity. For intelligent grids and maritime intrusion detection systems (ID studies like Afrin et al. (2026) and Shakil et al. (2026) used CNN-GRU as well as deep learning models to achieve an accuracy above 98%. In a similar vein, Ekhande et al. (2022) highlighted the value of Convolutional Neural Networks (CNN) in multimedia forensic analysis, particularly for the classification of picture and video information. Additionally, real-time threat monitoring, automated incident response, predictive analytics, and activity reconstruction in digital investigations are all backed up by AI-based solutions. Additionally, threat a simulation, cloud forensic analysis, and smart security operations were enhanced with the help of

generative artificial intelligence and NLP models. These developments show that, in comparison to traditional approaches, AI enhances efficacy, speed, and scalability of cybersecurity and forensics systems.

Given these advances, a comparative analysis of the evaluated studies reveals a number of limitations. Since many AI systems function as "black-box" models, it can be difficult to clarify and legally justify their judgements in forensic investigations. High complexity of computation, limited actual data sets, adversarial attacks, and privacy concerns remain to be significant obstacles. In addition, a number of studies found that AI models with low cross-domain adaptability perform poorly across various cybersecurity domains if trained for one environment. In addition, the deployment of deep learning systems in IoT and edge environments is difficult due to their high computing resource requirements. Additionally, ethical AI governance and focused on people cybersecurity have not received enough attention. Overall, even though AI has impressive potential in security and digital forensics, future research must concentrate on developing strong, scalable, explainable, and privacy-preserving AI frameworks suitable for real cyber defence and forensics.

Table 1: Comparative Analysis of AI Techniques in Cybersecurity and Digital Forensics

Domain	AI Technique	Strengths	Limitation
Intrusion Detection	CNN, DL, RF GAN, FL	High accuracy, real-time detection	Adversarial attacks, high cos
Multimedia Forensics	CNN, NLP, Supervised ML	Image/video/audio classification	Complexity, poo generalization
Cloud Security	ML, DL-IDS, Anomaly Detection	Scalable detection, fast response	Latency, resource intensive
Generative AI Security	LLMs, GANs	Threat simulation, analytics	Bias, misuse, privacy issues
Human-Centered Security	Behavioral AI, RL	Deepfake detection, governance	Explainability gaps
AI Review Frameworks	ML, DL, NLP	Malware/phishing analysis	Older methods, limited datasets

Table-2: Strengths and Challenges of AI Approaches in Cybersecurity and Digital Forensics

AI Approach	Strengths	Challenges
Machine Learning (ML)	Fast threat detection and automated pattern analysis	Requires high-quality datasets and may produce false positives
Deep Learning (DL)	High accuracy in intrusion detection and malware analysis	High computational cost and lack of explainability
Convolutional Neural Networks (CNN)	Effective for image, video, and multimedia forensic analysis	Needs large datasets and powerful hardware resources
Natural Language Processing (NLP)	Useful for phishing detection and threat intelligence analysis	Difficulty handling multilingual and context-based attacks
Generative AI	Supports predictive analysis, threat simulation, and automated investigation	Ethical risks, fake content generation, and malicious misuse

5. Research Gaps & Open Challenges

The comparative study highlights a number of current research gaps that limit the maturity, reliability, and practical execution of existing AI-driven systems, even though the analysed studies show significant improvements in the use of AI to cybersecurity and digital forensics. These gaps were found by tracking recurrent defects across application areas and by looking at the restrictions that were explicitly identified in the nineteen reviewed studies.

Gap-1: Lack of Explainability in AI Models.
Deep learning architectures like CNNs and hybrid CNN-GRU models, what role as black-box predictors, are employed by most of the surveyed AI-based cybersecurity and forensic systems [2], [10], [16], and [18]. Given their great accuracy, these models lacked interpretable data to support their conclusions, which limits their legal legitimacy in forensic investigations and undermines trust in operational security settings. The current AI-driven protective frameworks examined in this article hardly ever incorporate explainable AI (XAI) methods.

Gap-2: Adversarial Vulnerability & Robustness.
Existing AI models are vulnerable to adversarial attacks, when properly constructed inputs result in misclassification, based on several research [2], [4], [17]. Still, only few of the looked at papers use defensive methods like adversarial training or assess adversarial resilience. Since attackers may deliberately try to avoid AI-based detectors, this gap is particularly critical for intrusion detection, malware analysis, and smart grid security.

Gap-3: Class Imbalance and Dataset Limitations. Class imbalance is an important obstacle to intrusion detection, particularly for minority attack classes in software-defined networking and IoT contexts, based on reviewed studies [8]. Furthermore, the majority of AI models are trained on outdated, artificial, or domain-specific datasets that fail to reflect current attack patterns or zero-day threats. One ongoing issue in cybersecurity and forensic research is the lack of high-quality, real-world, and frequently updated datasets.

Gap-4: Weak Cross-Domain Generalization.
The vast majority of surveyed models are created and tested in a specific field, such as smart grids [2], maritime networks [16], or iPhone-based forensic data [7], and their performance substantially reduces in other contexts. A few studies assess cross-dataset or cross-domain performance, and the lack of transferable AI frameworks that operate consistently across various cybersecurity and forensic settings remains to be a major issue.

Gap-5: Privacy and Ethical Concerns.
Privacy-preserving forensic and security frameworks remain underdeveloped in the reviewed literature. Only a small number of studies explicitly address privacy-aware investigation [12] or examine the ethical risks associated with generative AI [14], [15]. Concerns such as data leakage, regulatory compliance with frameworks like GDPR, and the dual-use nature of generative AI- usable for both cyber

defence and cyberattack- have not been systematically addressed.

Gap-6: High Computational Cost and Limited Edge Deployment.
Deep learning models used in forensic analysis and intrusion detection require substantial computational resources [10], [16]. This limits their applicability in resource-constrained environments such as IoT devices, edge networks, and embedded forensic systems, where lightweight, energy-efficient, and real-time AI models are needed for practical deployment.

Gap-7: Limited Integration of Human-Centred and Generative AI Defences.
Human-centered defence mechanisms that combine behavioural analysis, cognitive security, and AI-driven detection are still a few in the reviewed literature, given the growing sophistication of AI-generated synthetic threats like deepfakes and AI-assisted phishing [1], [14], and [15]. Few frameworks integrate automated cybersecurity response, generative AI threat detection, and user awareness into one architecture.

Together, these gaps indicate that future research must move beyond accuracy-focused performance metrics and address the deeper requirements of trustworthiness, robustness, fairness, privacy protection, and operational readiness in AI-driven cybersecurity and digital forensics.

6. Conclusion

This review has presented a structured analysis of how Artificial Intelligence (AI) techniques are reshaping cybersecurity and digital forensics. Drawing on nineteen studies published between 2020 and 2026, the work examined the role of Machine Learning, Deep Learning, Convolutional Neural Networks, Generative Adversarial Networks, Natural Language Processing, Reinforcement Learning, and Federated Learning across major application domains, including intrusion detection, malware analysis, phishing identification, smart grid security, cloud forensics, multimedia evidence analysis, and human-centered cybersecurity.

The reviewed literature demonstrates that AI-driven approaches significantly outperform traditional signature-based and rule-driven techniques. Deep learning models, particularly CNN-based architectures, achieved detection accuracy above 98% in intrusion detection for smart grid and maritime networks, while CNN and NLP-based systems showed strong performance in multimedia forensic analysis and digital evidence classification. Generative AI further introduced new capabilities for threat simulation, predictive forensic reconstruction, and automated incident response. In parallel, human-centered frameworks emphasized that detection competence and user awareness remain essential against AI-generated synthetic threats such as deepfakes and AI-assisted deception.

At the same time, the comparative analysis exposed several persistent limitations across the surveyed studies. The lack of explainability in deep learning models continues to challenge the legal admissibility of AI-driven forensic decisions. Class imbalance, adversarial attacks, dataset scarcity, and weak cross-domain generalization remain unresolved technical concerns, while privacy preservation, ethical governance, and high computational cost limit deployment in real-world cloud, IoT, and edge environments. These limitations indicate that, although AI has already transformed cyber defence and forensic investigation, current solutions are not yet fully reliable, interpretable, or scalable for operational use.

The contributions of this review are threefold: (i) it consolidates recent AI techniques applied to cybersecurity and digital forensics into a structured comparative framework; (ii) it identifies common strengths, limitations, and performance trends across major AI approaches; and (iii) it outlines open research challenges that must be addressed for the next generation of intelligent and trustworthy cyber defence systems. Future progress in this field will depend on developing AI frameworks that are robust against adversarial manipulation, explainable to forensic investigators and courts, privacy-preserving by design, and adaptable across heterogeneous cybersecurity environments.

References

[1] R. Almarwani, M. Almarwani, and F. Almarwani, "AI-Driven Synthetic Threats in Cybersecurity: A User-Centered Framework for Awareness, Detection, and Protective Behavior," IEEE Access, vol. 14, 2026.
[2] S. Afrin, M. R. Al Muttaki, A. I. A. Anil, and S. Hasan, "AI-Powered Cybersecurity for Smart Grid Communication: A Systematic Review of Intrusion Detection and Threat Mitigation Systems," Energy Conversion and Management: X, vol. 29,2026.
[3] A. Al Siam, M. M. Hassan, and T. Bhuiyan, "Artificial Intelligence for Cybersecurity: A State of the Art," in Proc. 4th IEEE International Conference on AI in Cybersecurity (ICAIC), 2025.
[4] B. Kayode, N. T. Adebola, S. Akerele, O. Fagbohun, C. Agbo, O. Bantale, and L. C. Nwokocha, "The State of AI-Driven Cybersecurity: Trends, Challenges and Opportunities," Journal of Artificial Intelligence, Machine Learning and Data Science, vol. 3, no. 2,2025.
[5] S. Y. Khaga, R. T. Avireneni, S. H. Koneru, and N. K. K. R. Yelkoti, "Towards Proactive Cloud Security: A Survey on ML and Deep Learning-Based Intrusion Detection Systems," Journal of Contemporary Education Theory and Artificial Intelligence, vol,2025.
[6] I. Goni, J. M. Gumpy, T. U. Maigari, and M. Mohammad, "Cybersecurity and Cyber Forensics: Machine Learning Approach Systematic Review," Semiconductor Science and Information Devices, vol. 2, no. 2, 2020.
[7] C. McCarthy, J. P. van Zandwijk, M. Worring, and Z. Geradts, "Forensic Activity Classification Using Digital Traces from iPhones: A Machine Learning-Based Approach," in Proc. DFRWS EU 2026.
[8] S. M. H. Mirsadeghi, H. Bahsi, R. Vaarandi, and W. Inoubli, "Learning From Few Cyber-Attacks: Addressing the Class Imbalance Problem in Machine Learning-Based Intrusion Detection in Software-Defined Networking," IEEE Access, vol. 11,2023.

[9] I. C. Whittaker, J. Thomson, M. Dilley-Salter, R. Adams, E. A. Breeds, M. C. Roffin, L. Shaw, and R. S. Bolton-King, "Using Open-Source Software and Interdisciplinary Teaching to Increase Digital Forensics Accessibility and Inclusivity," Forensic Science International: Synergy,2025.
[10] S. Ekhande, U. Patil, and K. V. Kulhalli, "Review on Effectiveness of Deep Learning Approach in Digital Forensics," International Journal of Electrical and Computer Engineering (IJECE), vol. 12, no. 5, 2022.
[11] A. M. Qadir and A. Varol, "The Role of Machine Learning in Digital Forensics," in Proc. 8th International Symposium on Digital Forensics and Security (ISDFS), 2020.
[12] L. Englbrecht and G. Pernul, "A Privacy-Aware Digital Forensics Investigation in Enterprises," in Proc. 15th International Conference on Availability, Reliability and Security (ARES), 2020.
[13] I. Zziwa, A. Ilolo, K. C. Nwafor, and D. O. T. Ihenacho, "Cloud Computing and AI in Cybersecurity Forensics: Leveraging Data Analytics for Enhanced Threat Detection and Incident Response," International Journal of Research Publication and Reviews, vol. 5, no. 10,2024.
[14] O. Emehin, I. Emeteveke, O. J. Adeyeye, and I. Akanbi, "Generative AI in Forensic Data Analysis: Opportunities and Ethical Implications for Cloud-Based Investigations," International Journal of Research Publication and Reviews, vol. 5, no. 10,2024.
[15] M. Uddin, M. S. Irshad, I. A. Kandhro, F. Alanazi, F. Ahmed, M. Maaz, S. Hussain, and S. S. Ullah, "Generative AI Revolution in Cybersecurity: A Comprehensive Review of Threat Intelligence and Operations," Artificial Intelligence Review, vol. 58,2025.
[16] M. M. N. Shakil, M. A. Hossain, M. S. Islam, and N. V. D. S. S. V. P. Raju, "A Novel Deep Learning Approach for Intrusion Detection in Maritime Radar Networks," Scientific Reports, vol. 16,2026.
[17] T. Swetha, U. Kumaran, V. P. Meena, and I. A. Hameed, "Leveraging AI for Enhanced Cybersecurity: A Comprehensive Review," Discover Applied Sciences, vol. 7,2025.
[18] W. Villegas-Ch, R. Gutierrez, and A. Maldonado Navarro, "Artificial Intelligence Techniques for Enhancing Accuracy and Efficiency in Digital Forensic Analysis," Discover Artificial Intelligence, vol. 6, 2026.
[19] F. O. Oladipo, E. E. Ogbuju, A. F. Samson, and A. E. Musa, "The State of the Art in Machine Learning-Based Digital Forensics," SSRN Electronic Journal, 2020.