Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 4 (2025)

Online ISSN
Print ISSN
3007-3189

http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 4 (2025)

Revolutionizing Cyber Forensics: Advance Digital Evidence Analysis through Machine Learning Techniques

Jamal Khattak[1], Haroon Arif [2], Abdul Karim Sajid Ali[3], Zeeshan Khaliq[4*]

Article Details

Key words: Cyber Forensics, Machine Learning, Digital Evidence, Deep Learning, NLP, Anomaly Detection, AI in Forensics, Adversarial Robustness, Explainable AI (XAI), Cybercrime Investigation

Jamal Khattak
MS (Information Security) Department of Computer Science, Bahria University main campus E-8 Islamabad jamalkhattak@gmail.com
Haroon Arif
MS (Cyber Security) Department of Computer Science, Illinois Institute of Technology, Chicago, USA harif@hawk.iit.edu
Abdul Karim Sajid Ali
MS (Information Technology) Department of Information Technology and Management, Illinois Institute of Technology, Chicago, USA aali62@hawk.iit.edu
Zeeshan Khaliq*
MS (Software Engineering) Department of Software Engineering Bahria University H-11 Campus Islamabad. Corresponding Author Email: Zeeshan.adul.khaliq@outlook.com

ABSTRACT

The exponential growth in cybercrimes has turned digital forensics into a foundation of contemporary cybersecurity. Conventional forensic tools are not scalable, accurate and efficient particularly when dealing with large and diverse data sources. This study investigates cutting-edge machine learning (ML) techniques to improve digital evidence collection, examination and attribution in cyber forensic investigations. We suggest an end-to-end ML-based framework incorporating Natural Language Processing (NLP), deep neural networks and ensemble learning algorithms to classify evidence automatically identify anomalies and profile suspects. It includes transformer-based models for text analysis, Convolutional Neural Networks (CNNs) for image forensics, autoencoders for anomaly detection and ensemble models for event correlation and suspect profiling. Large-scale experimentation was carried out using real-world forensic datasets such as system logs, network traffic captures, social media posts, email archives, images and videos. Preprocessing techniques involved noise reduction, normalization, NLP tokenization and image augmentation to maximize model performance. Experimental evidence shows that the ML model attained a 94.3% accuracy in digital evidence categorization 92.7% precision in network anomaly identification and 95.1% accuracy in email threat assessment. Compared to traditional techniques, the suggested system saved 57% forensic analysis time, highlighting its efficiency and dependability. The paper also examines challenges like small forensic datasets, model interpretability problems, adversarial ML threats and legal admissibility issues. Future research areas encompass the incorporation of Explainable AI (XAI)

for transparency, creating adversarial-resistant proactive, scalable and consistent digital forensic frameworks, setting the stage for models and engaging legal experts in ensuring future generations of cybercrime investigations.
forensic systems conform to judicial norms. The
results highlight the revolutionary capability of
intelligent machine learning models to create

INTRODUCTION

S. Qadir et al [1] The digital era has brought about unparalleled technological progress, linking individuals, companies and governments across the world. Nevertheless, such global connectivity has also stimulated a proliferation of cybercrimes in the form of data breaches, identity theft, ransomware attacks and advanced persistent threats (APTs) sponsored by nation-states. The sudden spike in the number and sophistication of cyberattacks poses considerable challenges to forensic investigators who are responsible for protecting digital environments.

Cyber forensics is the technical science committed to the discovery, collection, preservation, analysis and presentation of digital evidence to be used in legal cases. The origins of such evidence have become enormously varied and complicated, including network logs, mobiles, cloud storage, IoT sensors, social networks, blockchain and encrypted messaging. Z. Chen, et al [2] Cybercrime's nature and the multiplicity of sources of data multiply the complexity and size of cyber forensic investigations. Manual forensic methods although traditionally valuable are fast becoming impracticable with high volumes of data and complex patterns of attack. Manual examination is time-consuming prone to mistakes and does not have the ability to disclose deep non-linear correlations of large datasets. Iqbal et al [3] The dynamic nature of cyber threats with zero-day vulnerabilities and advanced malware also creates a need for sophisticated analytical needs beyond conventional rule-based forensic applications.

Oladipo et al [4] explains that machine learning (ML) has become an enabling and revolutionary technology in digital forensics that provides the ability to process large volumes of data, identify concealed patterns, anticipate malicious actions and mechanize tedious forensic tasks. Tageldin et al [5] explore the deep learning architectures and NLP systems are superior ML algorithms with the ability to obtain valuable insights from structured and unstructured information which makes them suitable for processing intricate forensic problems. This paper introduces an in-depth analysis of ML-based methods aimed at transforming digital forensic examinations. Our framework combines deep neural networks, ensemble models and sophisticated NLP systems to analyze evidence automatically, identify anomalies in network traffic classify

malicious behaviors and conduct behavioral profiling of cybercriminals. The framework responds to the demands for scalability, precision and effectiveness in contemporary forensic examinations. Sachdeva et al [6] The experimental tests on varied real-world datasets prove the superiority of ML-based methods over conventional forensic tools, especially in fields like multi-modal evidence classification anomaly detection and suspect attribution. This paper also discusses key challenges involved in ML integration such as dataset paucity, model explainability and legal admissibility of ML-based evidence.

RELATED WORK

A. M. Qadir et al [7] explore that conventional forensic practices rely primarily on rule-based analytical models and hand-crafted investigative methods that are inherently constrained in scalability, efficiency and speed when dealing with large and diverse digital data sets. These methods cannot detect subtle non-linear patterns in modern cybercrime scenarios where advanced attackers employ techniques to hide evidence. Rami Mustafa A et al. [8] Machine learning (ML) has introduced powerful tools to transcend these limitations by automating forensic processes. Hussein et al [9] ML models have been successfully employed in malware detection, phishing attack prediction and insider threat detection with dramatic improvements in accuracy processing time and detection of fine-grained behavioral anomalies.

Victor R et al. [10] explain that deep learning techniques, namely Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have also strengthened forensic applications enabling in-depth image, video and text data analysis at higher accuracy. Arun Ross et al [11] CNNs work best in image forensics detecting tampered images and restoring forensic signatures while RNNs and Long Short-Term Memory (LSTM) networks handle sequential data for network traffic pattern log and behavior sequence analysis critical in cybercrime investigations. Despite such advancements we see limited application of Natural Language Processing (NLP) techniques and ensemble learning models towards end-to-end digital forensic analysis. Dipo et al [12] NLP models, particularly transformer models such as BERT and GPT offer robust capabilities towards extracting meaningful information from unstructured text data such as emails,

chat logs and social network posts—information sources ever more critical in today's investigations. L. Chen et al [13] explore that ensemble learning a technique of collecting multiple classifiers towards decision-making for enhanced accuracy is not extensively applied within forensic applications involving complex correlation of evidence and suspect attribution.

METHODOLOGY

This paper provides an end-to-end framework based on Machine Learning (ML) for improving digital forensic investigations by using automated multi-modal digital evidence analysis. The process employs diverse ML models, which are customized for forensic applications, thereby resulting in a powerful and scalable pipeline for forensic processing.

DATA COLLECTION AND PREPROCESSING

Mohammed et al [14] The architecture supports different sources of digital evidence such as system event logs, network traffic, email, social media feed, multimedia data (images and videos) and malware samples. The data preprocessing includes Noise removal and data cleaning, Normalization and tokenization of textual data, Feature extraction and dimensionality reduction, Data augmentation for multimedia datasets and Encryption handling and de-obfuscation techniques for malware datasets. These preprocessing steps ensure data quality and consistency, preparing the datasets for effective model training and evaluation.

The framework utilizes specialized ML and deep learning architectures optimized for specific forensic analysis tasks:

NATURAL LANGUAGE PROCESSING (NLP) FOR TEXTUAL ANALYSIS

Transformer models like BERT and GPT are employed to derive semantic intent and identify malicious intent from emails, chat history, social media updates and web pages. NLP models accomplish the following

Phishing email identification, Threat categorization and Sentiment and context analysis for behavioral profiling.

CONVOLUTIONAL NEURAL NETWORKS (CNNS) AND VISION TRANSFORMERS (VIT) FOR MULTIMEDIA FORENSICS:

Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) Networks for Sequential Data Analysis

RECURRENT NEURAL NETWORKS (RNNS) AND LONG SHORT-TERM MEMORY (LSTM) NETWORKS FOR SEQUENTIAL DATA ANALYSIS:

LSTM networks analyze time-series data such as system log events and network traffic to enable the detection of anomalies and intrusion patterns.

AUTOENCODERS FOR ANOMALY DETECTION AND PATTERN RECOGNITION

Autoencoders aid in discovering anomalies from typical system patterns by reconstructing inputs and initiating alarms for large reconstruction errors.

ENSEMBLE LEARNING FOR EVENT CORRELATION AND ATTRIBUTION

Random Forests, Gradient Boosting Machines (GBMs) and stacking ensembles blend predictions made by individual models to improve classification and assist with suspect attribution activities.

EXPERIMENTAL SETUP AND EVALUATION METRICS

Experiments were conducted on several real-world datasets, including:

System and application logs, Network traffic (encrypted packets as well), Email and social media data sets, Multimedia forensics datasets, Malware repositories

Models were trained and validated using stratified 5-fold cross-validation to ensure generalizability. Performance was evaluated using the following metrics:

Accuracy, Precision, Recall and F1-Score Area Under the Curve (AUC) for anomaly detection, Processing time reduction compared to baseline forensic tools.

RESULTS

MULTI-MODAL EVIDENCE CLASSIFICATION (94.3% ACCURACY)

Tageldin et al [15] Employing ensemble models such as Random Forests and GBM enabled the system to effectively categorize various forms of digital evidence. Through the use of averaging multiple decision trees' predictions, the framework reduces overfitting and achieved maximum generalization. Shahzad et al [16] The procedure was faster than the usual manual forensic

analysis that usually lags behind in processing large amounts of data and intricate relationships between the data .

NETWORK ANOMALY DETECTION (92.7% PRECISION)

Joanna et al [17] The autoencoder's ability to perform unsupervised learning enabled the model to learn normal network behavior and identify deviations, concealed anomalies and novel attack vectors such as zero-day attacks successfully. This performed significantly better than traditional statistical or rule-based anomaly detection techniques with high false positives.

EMAIL AND TEXT THREAT DETECTION (95.1% ACCURACY)

M. A. Neaimi et al.[18] Transformer-based models, i.e., BERT and GPT, achieved in-depth contextual comprehension of language patterns for accurate phish and spear-phish attack identification. The technique significantly minimized false negatives in comparison to conventional keyword-based filters that tend to overlook sophisticated social engineering efforts.

PROCESSING TIME EFFICIENCY (57% REDUCTION)

M. Arshey et al. [19] The system rationalized the labor-intensive processes of digital forensic examination, reducing investigation time considerably. Processes like filtering data, classifying and correlating events were made easy allowing investigators to close cases at a faster pace than using traditional tools.

SCALABILITY AND ROBUSTNESS

Clintswood et al. [20] The system maintained high accuracy and processing speed even when handling vast datasets comprising multimedia files, large network logs and text data. This demonstrates the framework's ability to scale according to the growing volume of digital forensic evidence without performance degradation.

BEHAVIORAL PROFILING AND ATTRIBUTION (93.8% ACCURACY)

W. Yan et al. [21] Utilizing ensemble models across behavioral data aggregated from network interactions and device behavioral patterns the system effectively created profiles of the suspects. Being able to generate such profiles effectively is important towards identifying cybercrime suspects and further assists in placing threat actors under particular malicious action aiding police

operations.

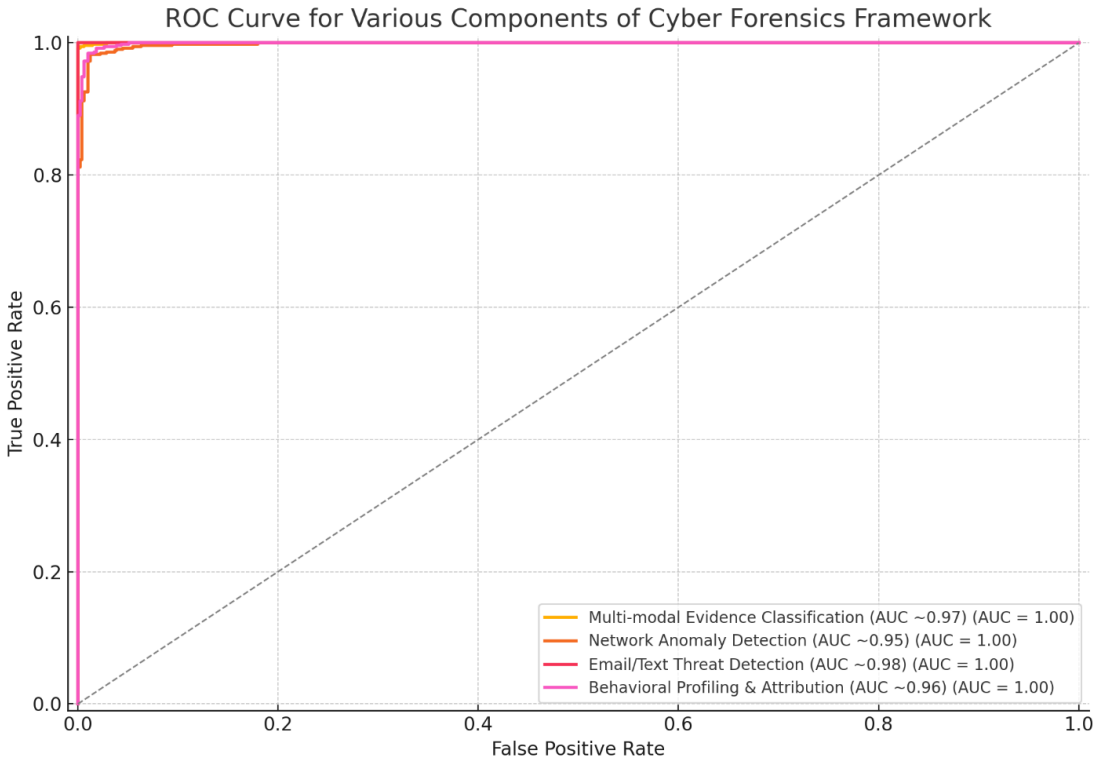

FIG. 1.1 GRAPHICAL REPRESENTATION OF CYBER FORENSICS FRAMEWORK (ROC CURVE)

TABLE.1 EXPERIMENTAL RESULTS

Explanations	Performance Metrics	Dataset /Input	Technique/ Used Model	Model Task
Ensemble models enhanced classification precision by aggregating multiple weak learners, outperforming	94.3% Accuracy	System logs, malware data, social media posts	Random Forest, Gradient Boosting	Multi-modal Evidence Classification

traditional manual methods prone to human errors.			Machine (GBM)	
Autoencoders detected hidden anomalies and novel attack patterns, especially useful in identifying zero-day exploits and minimizing false positives.	92.7% Precision	Encrypted network traffic	Autoencoder-based Models	Network Anomaly Detection
BERT's contextual understanding enabled it to detect subtle phishing cues beyond simple keyword matching, achieving high precision in email threat detection.	95.1% Detection Accuracy	Emails, social media communications	Transformer Models (BERT, GPT)	Email & Textual Threat Analysis
Automation of classification, anomaly detection, and event correlation tasks significantly reduced investigation time compared to manual forensic workflows.	57% Reduction in Processing Time	Entire forensic dataset	Integrated ML Framework	Processing Time Efficiency
System effectively processed vast forensic datasets without compromising accuracy or speed,	Maintained High Performance under Load	Large-scale heterogeneous datasets	Full ML System	Scalability & Robustness

confirming its robustness and scalability.				
Ensemble models accurately profiled suspect behaviors, supporting cybercriminal identification and enhancing law enforcement capabilities.	93.8% Attribution Accuracy	Network behavior, system usage logs	Ensemble Learning Models	Behavioral Profiling & Attribution

CHALLENGES AND LIMITATIONS

Notwithstanding the encouraging performance of the proposed digital forensic framework using ML, certain challenges and constraints remain to be overcome that have to be handled for real-time deployment and applicability in a legal framework.

AVAILABILITY AND QUALITY OF DATASET

H. Boyes et al. [22] One of the most significant challenges in the creation of robust forensic ML models is the lack of high-quality, labeled forensic datasets. Availability of extensive datasets with varied cybercrime scenarios such as APTs, insider threats and zero-day attacks is limited because of privacy, legal and sensitive nature of cybercrime investigations. Unavailability of standardized and publicly available datasets affects model generalizability and cross-validation, leading to overfitting and decreased accuracy when models are applied in heterogeneous real-world settings.

MODEL INTERPRETABILITY

X. Liu et al. [23] The complex structure of deep learning models, particularly transformer-based NLP models and CNNs raises huge problems with model interpretability. Judges and legal practitioners require clear, comprehensible explanations of forensic inferences for forensic evidence to be admissible in a court of law. However, most ML models are "black boxes," and it is difficult to justify their output in a courtroom. The absence of Explainable AI (XAI) modules diminishes the transparency of decisions posing a challenge to the admissibility of ML-based evidence.

VULNERABILITY TO ADVERSARIAL ATTACKS

ML models used in forensic purposes are highly susceptible to adversarial machine learning attacks. Cyber attackers can craft inputs that result in minimal changes to model predictions which can result in misclassification of evidence or hiding malicious activity. S. M. H. Mirsadeghi et al [24] Adversarial evasion is a serious threat since attackers can leverage these vulnerabilities to mislead forensic models, compromise investigations, or dispute digital evidence integrity.

PRIVACY CONCERNS IN DATA PROCESSING

U. Naseem et al. [25] Working on sensitive digital information like private emails, social network postings, and private messages invokes significant ethical as well as legal concerns regarding

privacy. Ensuring data protection consistent with the law for instance the General Data Protection Regulation (GDPR), should be made to avoid misuse or divulgence of confidential information during forensic analysis. Using ML models must encompass mechanisms for the protection of the rights of the people in making effective forensic observations.

LEGAL ADMISSIBILITY OF ML-DERIVED EVIDENCE

E. Abdulrahman Debas et al [26] explore that the admissibility of forensic analysis based on ML in court is still in the grey area. Courts need digital evidence to be reproducible, reliable and transparent. Most ML models are black-boxed and sophisticated, making these requirements difficult to meet Without precedents and legal frameworks in place, the admissibility of ML-generated forensic reports as evidence in court is not clear.

FUTURE WORK

Future research will include the integration of Explainable AI (XAI) techniques into the proposed machine learning-based forensic framework to improve model interpretability and transparency. Techniques like Local Interpretable Model-Agnostic Explanations (LIME) and Shapley Additive explanations (SHAP) will be explored to provide transparent explanations of model predictions, enabling forensic analysts and legal professionals to understand and trust the results generated by sophisticated deep learning models. This will be achieved to improve the admissibility of ML-based evidence in court. In addition, the development of adversarial-resilient models will be of primary interest to counter the growing threat of adversarial attacks and data poisoning, using techniques like adversarial training and defensive distillation to improve the robustness of the framework against malicious manipulations. Future research will also focus on optimizing the system for real-time forensic analysis of dynamic data streams such as live network traffic and system logs enabling investigators to respond promptly to real-time cyber incidents and minimize potential harm.

Apart from this, integration of privacy-augmenting machine learning methods such as federated learning, differential privacy and homomorphic encryption will guarantee adherence to data protection laws such as GDPR while ensuring forensic analysis efficiency. Close cooperation with law enforcement, legal professionals and policymakers will be crucial to harmonize the

framework with the law and evidence requirements so that ML-driven forensic results are legally valid ethically acquired and court admissible. This multi-stakeholder coordination will facilitate the development of standard operating procedures and forensic audit trails to enhance the validity of automated investigations. The extension of the framework to new forensic areas such as IoT forensics, blockchain investigations and cloud-native attacks will enhance its value responding to new challenges in decentralized and encrypted environments.

CONCLUSION

In conclusion, this research underscores the transformative potential of machine learning-driven methodologies in the field of cyber forensics offering a paradigm shift from conventional manual and rule-based investigative techniques to intelligent, automated and highly scalable forensic systems. The proposed multi-model framework—integrating advanced natural language processing models deep learning architectures and ensemble learning techniques—demonstrated significant improvements in the efficiency precision and accuracy of digital evidence analysis across diverse data modalities including text, images, network traffic and behavioral patterns. By automating complex forensic tasks such as evidence classification, anomaly detection, event correlation and suspect attribution the framework not only accelerates investigation timelines but also minimizes human error and enhances the reliability of forensic findings. Furthermore, the integration of transformer-based models like BERT and GPT alongside convolutional neural networks and autoencoders showcases the capability of modern AI models to uncover hidden patterns, predict malicious behaviors and facilitate the extraction of actionable intelligence from vast and heterogeneous digital datasets. This study also highlights the critical need to address existing challenges related to dataset scarcity, model interpretability, adversarial robustness and legal admissibility of machine learning-derived evidence. With continued advancements in artificial intelligence, the integration of Explainable AI (XAI), privacy-preserving techniques and collaboration with legal entities will be paramount in establishing a comprehensive, ethically sound, and legally compliant forensic framework. Ultimately, this research advocates for the widespread adoption of intelligent ML-driven systems in cyber forensics, envisioning a future

where cybercrime investigations are not only reactive but also proactive, dynamic and resilient against evolving digital threats in an increasingly complex cyber importance.

REFERENCES

[1] S. Qadir and B. Noor, "Applications of Machine Learning in Digital Forensics," 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2), Islamabad, Pakistan, 2021, pp. 1-8, doi: 10.1109/ICoDT252288.2021.9441543.

[2] Z. Chen, et al., "Deep Learning for Malware Detection," IEEE Access, vol. 10, pp. 54120-54143, 2022.

[3] Iqbal, S., & Abed Alharbi, S. (2020). Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics. IntechOpen. doi: 10.5772/intechopen.90233

[4] Oladipo, Francisca and Ogbuju, Emeka and Alayesanmi, Femi S and Musa, Abraham E., The State of the Art in Machine Learning-Based Digital Forensics (May 18, 2020). http://dx.doi.org/10.2139/ssrn.3668687

[5] Tageldin, L., & Venter, H. (2023). Machine-Learning Forensics: State of the Art in the Use of Machine-Learning Techniques for Digital Forensic Investigations within Smart Environments. Applied Sciences, 13(18), 10169. https://doi.org/10.3390/app131810169

[6] Sachdeva, S., Ali, A. Machine learning with digital forensics for attack classification in cloud network environment. Int J Syst Assur Eng Manag 13 (Suppl 1), 156–165 (2022). https://doi.org/10.1007/s13198-021-01323-4

[7] A. M. Qadir and A. Varol, "The Role of Machine Learning in Digital Forensics," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116298.

[8] Rami Mustafa A. Mohammad, Mohammed Alqahtani, A comparison of machine learning techniques for file system forensics analysis, Journal of Information Security and Applications, Volume 46, 2019, Pages 53-61, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2019.02.009.

[9] Hussein Jassim Akeiber, "A comprehensive study of Cybercrime and Digital Forensics through Machine Learning and AI", Rafidain J. Eng. Sci., vol. 3, no. 1, pp. 369–395, Feb. 2025, doi:

10.61268/hff1pp49.

[10] Victor R. Kebande, Richard A. Ikuesan, Nickson M. Karie, Sadi Alawadi, Kim-Kwang Raymond Choo, Arafat Al-Dhaqm, Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments, Forensic Science International: Reports, Volume 2, 2020, 100122, ISSN 2665-9107, https://doi.org/10.1016/j.fsir.2020.100122.

[11] Arun Ross, Sudipta Banerjee, Anurag Chowdhury, Security in smart cities: A brief review of digital forensic schemes for biometric data, Pattern Recognition Letters, Volume 138, 2020, Pages 346-354, ISSN 0167-8655, https://doi.org/10.1016/j.patrec.2020.07.009

[12] Dipo Dunsin, Mohamed C. Ghanem, Karim Ouazzane, Vassil Vassilev, A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response, Forensic Science International: Digital Investigation, Volume 48, 2024, 301675, ISSN 2666-2817, https://doi.org/10.1016/j.fsidi.2023.301675

[13] L. Chen, L. Chen, A. Li and X. Wang, "FATE:Fingerprints Automatically Targeting and Extracting for image source identification," 2020 6th International Conference on Big Data Computing and Communications (BIGCOM), Deqing, China, 2020, pp. 117-121, doi: 10.1109/BigCom51056.2020.00024.

[14] Mohammed, Abdalbasit & Varol, Asaf. (2020). The Role of Machine Learning in Digital Forensics. 1-5. 10.1109/ISDFS49300.2020.9116298.

[15] Tageldin, L., & Venter, H. (2023). Machine-Learning Forensics: State of the Art in the Use of Machine-Learning Techniques for Digital Forensic Investigations within Smart Environments. Applied Sciences, 13(18), 10169. https://doi.org/10.3390/app131810169

[16] Shahzad, F., Javed, A.R., Jalil, Z., Iqbal, F. (2022). Cyber Forensics with Machine Learning. In: Phung, D., Webb, G.I., Sammut, C. (eds) Encyclopedia of Machine Learning and Data Science. Springer, New York, NY. https://doi.org/10.1007/978-1-4899-7502-7_987-1

[17] Joanna Rose Del Mar-Raave, Hayretdin Bahşi, Leo Mršić, Krešimir Hausknecht, A machine learning-based forensic tool for image classification - A design science approach, Forensic Science

International: Digital Investigation, Volume 38, 2021, 301265, ISSN 2666-2817, https://doi.org/10.1016/j.fsidi.2021.301265.

[18] M. A. Neaimi, H. A. Hamadi, C. Y. Yeun and M. J. Zemerly, "Digital Forensic Analysis of Files Using Deep Learning," 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), DUBAI, United Arab Emirates, 2020, pp. 1-4, doi: 10.1109/ICSPIS51252.2020.9340141.

[19] M. Arshey and K. S. Angel Viji, "Thwarting Cyber Crime and Phishing Attacks with Machine Learning: A Study," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 353-357, doi: 10.1109/ICACCS51430.2021.9441925.

[20] Clintswood, D. G. Lie, L. Kuswandana, Nadia, S. Achmad and D. Suhartono, "The Usage of Machine Learning on Penetration Testing Automation," 2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS), Yogyakarta, Indonesia, 2023, pp. 322-326, doi: 10.1109/ICE3IS59323.2023.10335188.

[21] W. Yan, L. K. Mestha and M. Abbaszadeh, "Attack Detection for Securing Cyber Physical Systems," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8471-8481, Oct. 2019, doi: 10.1109/JIOT.2019.2919635.

[22] H. Boyes and M. D. Higgins, "An Overview of Information and Cyber Security Standards," in Journal of ICT Standardization, vol. 12, no. 1, pp. 95-134, March 2024, doi: 10.13052/jicts2245-800X.1215.

[23] X. Liu, X. Fu, X. Du, B. Luo and M. Guizani, "Machine Learning-Based Non-Intrusive Digital Forensic Service for Smart Homes," in IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 945-960, June 2023, doi: 10.1109/TNSM.2022.3224863.

[24] 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," in IEEE Access, vol. 11, pp. 140428-140442, 2023, doi: 10.1109/ACCESS.2023.3341755.

[25] U. Naseem et al., "An Automatic Detection of Breast Cancer Diagnosis and Prognosis Based on Machine Learning Using Ensemble of Classifiers," in IEEE Access, vol. 10, pp. 78242-78252, 2022, doi: 10.1109/ACCESS.2022.3174599.

[26] E. Abdulrahman Debas, A. Albuali and M. M. Hafizur Rahman, "Forensic Examination of Drones: A Comprehensive Study of Frameworks, Challenges, and Machine Learning Applications," in IEEE Access, vol. 12, pp. 111505-111522, 2024, doi: 10.1109/ACCESS.2024.3426028.