Journal of Theoretical and Applied Information Technology
30th November 2025. Vol.103. No.22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE USE OF ARTIFICIAL INTELLIGENCE SYSTEMS TO SUPPORT FORENSIC ACTIONS IN COMPUTER CRIMES INVESTIGATIONS

VIACHESLAV KULIUSH[1], YULIIA CHORNOUS[2], OLEKSII KHARKEVYCH[3], OKSANA VASYLOVA[4], VITALII MATSAK[5]

[1]Cyber Police Department of the National Police of Ukraine, Ukraine

[2]National Academy of Internal Affairs, Department of Criminalistics and Forensic Medicine, Ukraine

[3]Interregional Academy of Personnel Management, Department of Law Enforcement and Anti-Corruption Activities, Ukraine

[4]Yuriy Fedkovych Chernivtsi National University, Department of Criminal Law, Ukraine

[5]Department of Internal and Personal Security of the State Border Guard Service of Ukraine, Ukraine

E-mail: [1]petromboy@gmail.com, [2]chornousyuliia@gmail.com, [3]kharkevych.o@gmail.com, [4]vasylovaoksana@chnu.edu.ua, [5] matsakv41@gmail.com

ABSTRACT

The relevance of the study is determined by the increasing number of computer crimes and the need for a normatively permissible, explainable, and integrated implementation of artificial intelligence (AI) systems in digital forensics. *The aim of the research* is to develop an optimized model for the AI use in computer crime investigations, taking into account explainability, auditability, and legal admissibility. The study employed the following methods: integrative stratification system of the typology of computer crimes, inter-normative comparative-procedural analysis of regulations, procedural modelling of the AI application scenario, synthesis of an optimized multi-agent model based on decomposition and normative analysis. The generalized results of the study showed that the integration of AI into forensics is limited by algorithmic opacity, regulatory fragmentation, and lack of procedural admissibility. The proposed optimized model with multi-agent architecture, explainability, auditability, and legal traceability minimizes algorithmic bias, formalizes forensic admissibility, and justifies the need to revise regulations and implement forensically explainable AI standards. *The academic novelty* is the formalization of an explainable AI-based forensic framework that integrates multi-agent analytics, legal traceability mechanisms, and standardized validation protocols, thereby advancing cognitive interpretability, regulatory admissibility, and institutional scalability of AI-evidence in criminal proceedings. *The prospects for further research* include conducting controlled empirical tests to verify the legal admissibility, interpretability, and procedural efficiency of the optimized procedural model.
Keywords: *Criminal Justice; Legal System; Rule of Law; Explainability; Legal Traceability*

1. INTRODUCTION

The transformational challenges of European integration, in particular in the area of building a security landscape for the EU financial sector, countering terrorist threats, and managing international migration, make the need to adapt innovative technologies to public law and forensic practices more urgent [1]. AI is increasingly considered as a tool for improving the effectiveness of anti-corruption management, strengthening financial and economic security, and optimizing law enforcement procedures in the fight against cybercrime [2]. In this context, public administration plays a key role, in particular in terms of forming a regulatory environment for the incorporation of AI, developing human capital, and ensuring compliance of automated analysis tools with the requirements of jurisdictional admissibility [3].

In view of the rapid growth in the number and complexity of computer crimes, the study is aimed at substantiating and formalizing the use of AI systems to support investigative actions in the

field of digital forensics, taking into account the technical, procedural, and regulatory aspects of their implementation.

The aim of the study is to form a structurally optimized model for the use of AI systems in forensic investigations of computer crimes with an emphasis on explainability, auditability, and legal traceability within the framework of regulatory and procedural admissibility.

Research objectives:

1 Stratify the computer crimes typology to build a classification model with the separation of technical and forensic parameters of AI application.

2 Conduct a comparative and procedural analysis of regulations on admissibility, explainability and incorporation of AI into forensics.

3 Formalize a typical scenario for the use of AI in digital investigations through procedural modelling.

Synthesize an optimized AI integration model taking into account multi-agent architecture and the principles of explainability, auditability, and legal traceability.

2. LITERATURE REVIEW

The increasing complexity of cybercrime necessitates an academic analysis of the potential of AI/ML solutions to support investigative actions in digital forensics, taking into account technological, methodological, and regulatory aspects.

The first step in shaping the modern paradigm of digital forensics was the research of Qiu [4], who empirically studied special units for combating cybercrime and demonstrated that AI-generated offences create a new level of forensic complexity, in particular in the aspects of attribution, evidence and legal qualification. It was established that the key barriers to investigative actions are regulatory backwardness, a deficit of technical and legal competencies, and the unpredictability of the evolution of algorithmic threats.

Continuing the problem of regulatory and technical mismatch, El-Kady [5] found that the use of machine learning (ML) algorithms and clustering methods in digital forensics provides effective attribution of crypto transactions, verification of digital traces, and identification of subjects in the dark web environment. The author emphasized the critical importance of blockchain forensics in the context of anonymized currency circulation and the shortage of host-oriented forensic solutions.

Studying the technical aspect of event reconstruction, Stephen [6] found that AI anomaly detection tools — specifically DBSCAN and DeepLog — enhanced the accuracy of forensic identification of cyber incidents, particularly in cloud infrastructures. The study demonstrated the relevance of ML models for forensic attack attribution, deepfake detection, and digital crime reconstruction.

Jain et al. [7] similarly focused on the forensic validity of digital artifacts, demonstrating that integrating AI algorithms into cyber forensics improved the accuracy of attack attribution, digital incident reconstruction, and the detection of complex malicious patterns. The effectiveness of AI solutions in malware detection, crime prediction, and forensic validation of digital evidence was confirmed based on real-world cases.

At the same time, Shamoo [8] focused on cyber fraud as one of the key vectors of the modern digital threat, finding that the use of AI tools — in particular, ML algorithms, NLP systems, and computer vision modules —increased the accuracy and speed of detecting fraudulent actions, tracing digital artifacts, and identifying behavioural deviations. The effectiveness of AI technologies in detecting complex cyber fraud schemes, implementing predictive analytics, and adapting to the dynamics of threats in cyberspace was established.

In the aspect of cognitive analysis of criminal activity, Singh et al. [9] proved that the use of deep learning (DL), in particular convolutional neural networks (CNNs), provided automated segmentation of visual artifacts, forensic classification of digital traces and increased reliability of biometric identification. The applied DL models demonstrated high efficiency in the reconstruction of forensic scenes, cognitive analysis of evidence, and structural predictive modelling of criminal activity.

Akeiber [10] further developed the issue of intelligent automation of identification processes, substantiating that the implementation of AI/ML algorithms in digital forensics provided automated classification of electronic evidence, anomaly detection, and analysis of threat patterns. The analysis carried out by the author showed an increase in the efficiency of investigative actions through the use of RFM engineering, predictive analytics, and AI automation.

In turn, Merdas and Obaid [11] proved that the use of AI/ML algorithms, in particular Random

Forest, in forensic analytics provided high accuracy of crime prediction modelling (99.4%) when correlating evidentiary indicators. The authors demonstrated the effectiveness of neural network (NN) structures in the reconstruction of a criminal episode and attribution of the offender based on the processing of multi-format digital artifacts.

Special attention was paid to the processing of large-scale forensic data: Patel et al. [12] demonstrated that the use of AI tools in digital forensics optimized the identification of behavioural trajectories, decryption of encrypted communications, and forensic processing of large-scale data. The authors proved that AI modules reduce the risks of investigative error, increase the validity of the evidentiary base, and ensure the attribution of cyber incidents with a high degree of confidence. Summarizing the spectrum of forensic AI solutions, Singh [13] demonstrated that the use of machine learning (ML) architectures, including NNs and predictive analytics, in digital forensics provides cognitive profiling of network anomalies, automated incident response, and forensic verification of cyber threats. The author focused on the normative and ethical challenges of legitimizing AI detectors in transnational cybercrime investigations.

The reviewed literature confirms the increasing applicability of AI/ML technologies in digital forensics—particularly in evidence processing, crime attribution, and anomaly detection. However, a critical research gap persists in the legal admissibility, procedural integration, and explainability of AI-generated forensic outputs. Despite advancements in predictive modelling, automated trace classification, and digital artifact reconstruction (Stephen [6]; Merdas & Obaid [11]; Patel et al. [12]), there is limited systemic integration of normative verification protocols and forensic standards (e.g., explainability, traceability, auditability) necessary for evidentiary legitimacy. The core problem addressed by this research lies in the lack of a stratified, legally compliant, and cognitively interpretable AI-supported forensic model. Accordingly, this study aims to develop and validate an optimized framework for AI integration in digital forensics that ensures normative stratification, procedural transparency, and forensic admissibility of AI-based analytics.

The hypothesized problem of the study lies in the absence of institutionalized, explainability-compliant, and normatively traceable integration protocols for AI in digital forensics, which critically limits the procedural допустимість, evidentiary robustness, and legal applicability of AI-generated outputs in criminal proceedings. Although prior research confirms the operational efficacy of AI/ML architectures in trace attribution, anomaly detection, and forensic reconstruction, persistent barriers—algorithmic opacity, regulatory fragmentation, semantic ambiguity, and deficit of auditability mechanisms—undermine their forensic legitimacy. The study hypothesizes that only through the formalization of a multi-agent explainable AI framework, incorporating adaptive analytics, legal traceability, and standardized validation, can these limitations be overcome and AI evidence gain admissibility in adversarial and transjurisdictional legal contexts.

3. METHODS

3.1. Research Design

The research design involved the following steps (Figure 1).

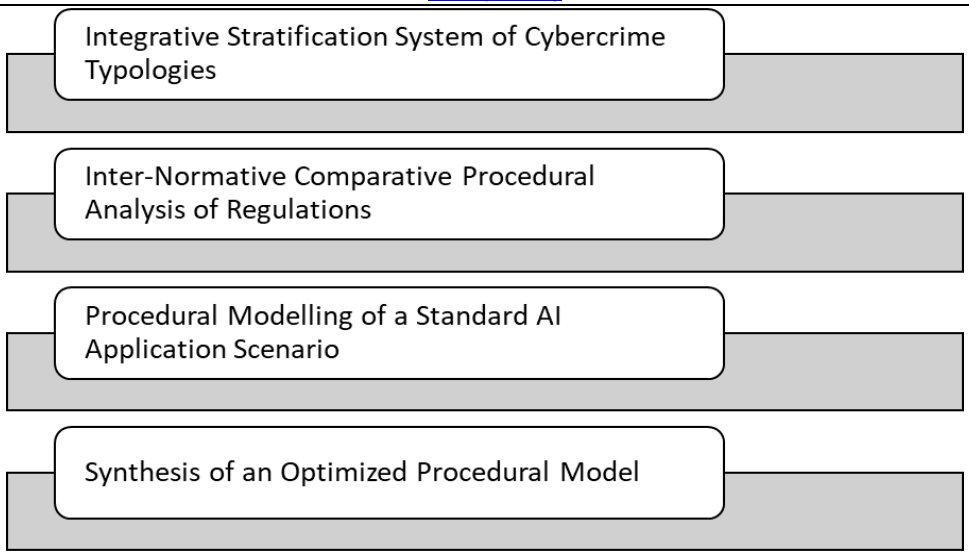

Figure 1: Research stages
Source: created by the authors

3.2. Methods

The research methodology encompasses four complementary approaches aimed at formalizing, normative assessment, and optimizing the application of AI in digital forensics.

The integrative stratification system of the computer crimes typology was used to build a classification model (Table 1), which provided a decomposition of the subject area with the separation of technical characteristics of incidents and procedural forensic parameters of AI application (Table 3).

The inter-normative comparative procedural analysis of regulations (Table 2) allowed comparing international and national legal acts in order to identify discrepancies in the standards of admissibility, explainability, and incorporation of AI into investigative procedures.

Procedural modelling of a typical AI application scenario (Figure 2) provided the formalization of the basic algorithm for integrating AI modules into the investigation of digital incidents, with the fixation of key phases — from initiation to verification of results.

The final stage was the synthesis of an *optimized procedural model* (Figure 3) by aggregating the results of the previous decomposition and normative analysis (Tables 3–4), which enabled the implementation of a multi-agent architecture with an emphasis on explainability, auditability, and legal traceability. The proposed approach covered the technical, procedural, and normative aspects of AI application, ensuring the formation of a cognitively relevant and procedurally integrated model of the permissible use of AI analytics in criminal proceedings.

3.3. Sample

The study summarizes the typology of digital crimes (Table 1), where the use of AI is appropriate for the detection, attribution and verification of digital artifacts in the context of forensic procedures and legal regulation.

Table 1: Comprehensive Application Of AI Systems In The Investigation Of Computer (Digital) Crimes: Mechanisms, Forensic Functions, Regulatory And Legal Regulation And Judicial Approval

Item No.	Name of computer (digital) crime	AI investigation mechanism	Procedural and forensic problems solved by AI	Regulatory and legal regulation of the use of AI in forensics	Judicial precedents of the use of AI as an evidentiary tool	Relevant academic research
1	Unauthorized access to the information system	Application of anomaly detection (ML) algorithms (unsupervised learning); profiling of	Automated detection of deviations from normative behaviour; attribution of	Budapest Convention (2001), ISO/IEC 27037:2012	U.S. v. Nosal (2012) – use of log files with AI analytics	Shami et al. [14]; Gupta et al. [15]

Item No.	Name of computer (digital) crime	AI investigation mechanism	Procedural and forensic problems solved by AI	Regulatory and legal regulation of the use of AI in forensics	Judicial precedents of the use of AI as an evidentiary tool	Relevant academic research
		user behaviour based on temporal and logical patterns	account to subject; reconstruction of the sequence of the offender's actions			
2	Phishing and sociotechnical attacks (social engineering)	NLP analysis of text messages, classification of e-mail traffic, semantic matching of fraud patterns	Detection of socio-manipulative language constructs; forensic identification of the source; construction of thematic connections between the objects of the attack	ePrivacy Directive (EU), ISO/IEC 27043:2015	R v. Adam (UK, 2017) – AI module for recognizing phishing patterns	Mohamed et al. [16]; Akeiber [17]
3	Cyber fraud (financial transactions, data substitution)	Neural networks for processing payment logs, detection of anomalous transactions; construction of graph models of cash flows	Identification of fraudulent transactions; evidential linking of transactions to the subject; construction of digital criminal connections	FATF Guidance on Digital ID (2020), ISO 22301	SEC v. LBRY (2022) – AI-crypto transaction analytics as evidence	Sood et al. [18]; Bello and Olufemi [19]
4	Distribution of malicious software (Malware)	CNN/Transformer models for analysing executable code, sandbox behaviour, and system calls	Automated classification of threat type; determination of attack vector; tracing of the source of malware	NIST SP 800-61, ENISA Threat Landscape	US v. Hutchins (2017) – AI-malware classification	Moamin et al. [20]; Gundoor and Sridevi [21]
5	Deepfake manipulations (discrediting, blackmail)	Application of AI deepfake content detectors based on computer vision (GAN analysis); verification of media authenticity	Establishing the fabrication of digital content; differentiation of real/synthetic images; forensic validation of video/audio evidence	AI Act (EU, draft 2021), ISO/IEC TR 24028:2020	State v. Melvin (2021, USA) – deepfake detection in criminal proceedings	Bhuiyan et al. [22]; Lin [23]
6	Child Cyber Exploitation (Child Sexual Abuse Material (CSAM))	Implementation of AI visual classification systems (CNN, image hashing, similarity search); automated content moderation	Identification of prohibited images; attribution of the source of distribution; prioritization of investigative actions by the degree of threat	TCOF (USA), Directive 2011/93/EU	Project VIC v. Anonymous (Interpol use case) – automated content matching	Borah et al. [24]; Wolbers et al. [25]
7	Cryptocurrency Asset Manipulation	Using clustering ML models to analyse blockchain transactions; graph analytics based on Elliptic Dataset	Deconvolution of anonymized wallets; tracing the origin of assets; building a chain of custody of transactions	Regulation (EU) 2023/1114 (MiCA), FATF Digital Assets Guide	Chainalysis datasets in U.S. v. Sterlingov (2021)	El-Kady [26]; Lin [27]
8	Destruction or Modification of Information in Information Systems	AI-monitoring of changes in system logs, hash integrity accounting, detection of unauthorized interventions	Establishing the moment and method of unauthorized change; reconstructing the digital history of the event; formalizing digital evidence of changes	ISO/IEC 27040, CC of Ukraine, Art. 361	R v. Michael K. (CA, 2020) – AI- recording of data deletion facts	Goffer et al. [28]; Deandra and Sherly [29]
9	Use of botnets	Analysis of telemetry data using RNN and attention-based models;	Detection of the control centre (C2); recognizing	EU Cybersecurity Act (2019),	US v. Andrey Ghinkul (2015) – AI-tracing of	Reza et al. [30]; Daudu and

Item No.	Name of computer (digital) crime	AI investigation mechanism	Procedural and forensic problems solved by AI	Regulatory and legal regulation of the use of AI in forensics	Judicial precedents of the use of AI as an evidentiary tool	Relevant academic research
		detection of coordinated node activity	command patterns; attributing infected systems to malicious infrastructure	CERT Guidelines	botnet control commands	Osimen [31]
10	Interference in electronic election systems	Predictive analysis models for detecting anomalous user behaviour; audit of the digital chain of events	Detection of attempts to influence the results; reconstructing the chronology of unauthorized actions; forensic preservation of digital voting logs	OSCE ODIHR standards, Council of Europe Rec(2004)11	Georgia v. Raffensperger (2021) – AI-audit of digital intervention elements	Chandra [32]; Jozaghi [33]

Source: created by the authors

The sample (Table 1) covers key categories of cybercrime in which AI systems provide an analytical and evidentiary function with a focus on relevance and procedural admissibility.

The sample of regulations (Table 2) covers multi-jurisdictional sources that determine the admissibility, validation and evidentiary relevance of AI in digital forensics.

Table 2: Legal And Technical Regulations That Determine The Legal Regime For The Use Of Ai Systems In Forensics

Item No.	Title of the regulation	Summary	Provisions on the applicability of AI in forensics
1	Budapest Convention on Cybercrime (2001)	A universal international legal act codifying the components of cybercrimes and the procedural principles of digital proceedings	Fixes the admissibility of digital evidence regardless of technical origin; legitimizes the use of automated analytical tools to collect, identify, and correlate digital traces
2	EU Artificial Intelligence Act (2021, draft)	Comprehensive regulation of the life cycle of high-risk AI systems within the EU	Identifies forensic, judicial, and law enforcement AI solutions as high-risk; establishes the mandatory validation, technical traceability, explainability, auditability, and procedural compatibility
3	OECD AI Principles (2019)	International declarative and regulatory framework for the transparent and responsible use of AI	Proclaims the accountability, technical reliability, purpose legitimacy, and ethical appropriateness of AI, including its use in forensic investigations
4	FATF Guidance on Digital Identity (2020)	Methodological document for recognition, authentication and risk assessment of digital identities	Enables the use of AI/ML modules in forensic identification, predictive transaction analytics, and behavioural correlation
5	ISO/IEC 27037:2012	Technical standard for the collection, identification, preservation, and exploitation of digital artifacts	Recognizes the legitimacy of automated evidence extraction procedures; supports the instrumental integration of intelligent systems to detect relevant information
6	ISO/IEC 27043:2015	Methodological framework for digital forensic investigations	Regulates the stages of incident analysis, where AI can be applied as a means of identifying cause-and-effect relationships and building a digital event reconstruction
7	ISO/IEC TR 24028:2020	A standard focusing on trust, reliability, and traceability of AI modules	Provides requirements for formal explainability, reasonableness of conclusions, and their validity in legally significant contexts, in particular during forensic analysis
8	NIST SP 800-61 Rev.2	American cyber incident response guideline	Provides the use of AI/ML as auxiliary mechanisms for incident monitoring, anomaly classification, and heuristic attribution of harmful effects
9	Directive 2011/93/EU	European legal framework to combat sexual exploitation of children, including online	Provides a legal basis for the use of AI-based detectors of prohibited content, image classification engines, biometric flagging in the forensic process
10	Convention 108+ (Council of Europe)	Improved version of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal	Identifies the principles of legality, proportionality, and minimization of interference when using AI to process personalized digital traces in criminal proceedings

Item No.	Title of the regulation	Summary	Provisions on the applicability of AI in forensics
		Data	
11	Criminal Procedure Code of Ukraine (Art. 84, 99, 100)	Enforces the legal regime of digital evidence in criminal proceedings	Establishes the admissibility of using digital information obtained by automated means; recognizes the relevance of electronic artifacts in the proving procedure
12	Law of Ukraine "On Protection of Information in Information and Telecommunications Systems"	Identifies requirements for confidentiality, integrity, and availability of information in ITS	Provides a technical and legal basis for the implementation of AI modules in systems for recording, verifying, and preserving digital evidentiary material

Source: created by the authors

Systematization of regulations (Table 2) revealed the dominance of the principles of explainability, admissibility, forensic reliability, and responsibility as the basis for integrating AI into criminal justice.

3.4. Instruments

Gleek.io [34] was used as a text-oriented procedural modelling tool for visualizing the phase sequence of forensic actions with the integration of AI modules into a normatively conditioned evidentiary structure.

4. RESULTS

The analytical stage involved a stratification of computer crimes and a decomposition of AI applications (Tables 1, 3) to assess the effectiveness of mechanisms according to the criteria of admissibility, interoperability, and evidentiary relevance.

Table 3: Integral Analysis Of The Effectiveness Of The AI Use In Forensic Procedures For Investigating Computer Crimes: Technical And Procedural Effectiveness, Regulatory Restrictions, And Ways Of Optimization

Name of computer (digital) crime	Aspect	Effective procedural solutions for using AI in the investigation	Disadvantages of using AI in the investigation of this type of crime	Optimization solutions for using AI in the investigation of this type of crime
Unauthorized access to an information system	Technical	Anomaly detection of behaviour (ML), attribution of user actions, automated creation of event logs	False positives; insufficient accuracy in the absence of training data	Integration of context-adaptive learning, hybridization with RBAC/ABAC mechanisms
	Procedural	Anomaly detection using ML; behavioural profiling of users	False positives; unclear legal compliance of CPC articles; limited interpretability of models	Implementation of explainable AI; validation of solutions through expert procedures; development of special norms regarding the admissibility of AI analytics
Phishing, spear-phishing and sociotechnical attacks (social engineering)	Technical	NLP analysis of message content, automatic classification of malicious patterns	Instability in detecting new linguistic fraud constructs	Regular retraining of models on domain-specific corpora
	Procedural	Semantic message analysis; email classification using NLP	The problem of differentiation of contexts; lack of regulatory definition of the boundaries of AI identification	Improving linguistic models; establishing AI phishing detection standards in procedural law
Cyber fraud (financial transactions, data spoofing)	Technical	Neural network transaction analysis; graph construction of connections between participants	Possibility of circumvention manoeuvres through proxy/transit accounts	Implementing multi-agent monitoring with deep behavioural learning
	Procedural	Transaction analysis via graph networks; detection of fraudulent patterns	Opacity of decisions; limited admissibility of AI-analytics in financial matters	Regulating forensic AI analytics procedures; expanding experts' competencies

Name of computer (digital) crime	Aspect	Effective procedural solutions for using AI in the investigation	Disadvantages of using AI in the investigation of this type of crime	Optimization solutions for using AI in the investigation of this type of crime
Malware distribution	Technical	AI classification of software signatures and behaviour; real-time sandbox analysis	Decreased accuracy in zero-day threats	Generative models for predicting the behaviour of malicious samples
	Procedural	CNN/Transformer code classification; behaviour analysis in sandbox environments	Lack of procedural certification of AI tools; developer identification issues	Institutional verification of AI systems; creation of a repository of validated AI tools
Deepfake manipulation (discreditation, blackmail)	Technical	GAN detection of visual/audio content, semantic verification of source	Limited reliability with high quality synthetic materials	Multichannel validation: facial expressions, acoustics, source
	Procedural	AI detection of synthetic content; video/audio verification	High error; legal dispute over admissibility in criminal proceedings	Formalization of reliability criteria; auditing of algorithms
Child cyber Exploitation (CSAM)	Technical	AI hashing, CNN image classification, threat prioritization	Possibility of false identification of innocent content	Use of ensemble models and human verification
	Procedural	Automated CSAM content identification; image hashing	Risk of violation of presumption of innocence; limitation of jurisdictional consistency	Ethical moderation; creation of an intergovernmental framework for the use of AI in CSAM
Cryptocurrency asset manipulation	Technical	Address clustering, AI wallet deconvolution, transaction chain tracing	Anonymization through mixers and tumblers	Combining AI with blockchain forensic metadata and legal queries
	Procedural	Transaction graph analysis; wallet clustering	High dependence on data quality; lack of clear case law	Adapting blockchain analytics to digital evidence standards; creating guidelines
Destruction or modification of information in information systems	Technical	AI change monitoring, digital trail recovery, event reconstruction	Difficulty in recovery after complete deletion or encryption	Combining AI with forensic imaging and backup systems
	Procedural	Log monitoring; change verification via hash control	Lack of procedural sensitivity to unauthorized changes; difficulty in attribution	Integrating with log authentication systems; formalizing AI audit of digital traces
Use of botnets	Technical	RNN telemetry analysis, C2 command detection, infected node classification	Masquerading network traffic as legitimate	Building behavioural profiles in correlation monitoring mode
	Procedural	C2 infrastructure detection; telemetry analysis	Lack of international agreement on AI node identification procedures; low explainability	Development of forensic analysis procedures with AI; interoperability of monitoring systems

Name of computer (digital) crime	Aspect	Effective procedural solutions for using AI in the investigation	Disadvantages of using AI in the investigation of this type of crime	Optimization solutions for using AI in the investigation of this type of crime
Interference in electronic election systems	Technical	Behavioural anomaly analysis, digital footprint audit, voice transaction verification	Political sensitivity and difficulty in validating evidence	Standardization of AI detection as part of independent audit
	Procedural	AI digital action audit; chronological anomaly detection	Political vulnerability of AI audit results; lack of legal precedents	International standardization of AI evidence in the electoral process; increasing reputational independence of algorithms

Source: created by the authors

The analysis (Table 3) revealed that despite the high potential of AI, its application in forensics is limited because of algorithmic opacity, regulatory fragmentation, and lack of procedural certification, which necessitates the need for unified regulation and standardization of the admissibility of AI evidence.

A comparative and procedural analysis of regulations (Tables 2, 4) was carried out, which determine the normative stratification, legitimacy, admissibility, and interoperability of AI in forensic procedures of digital investigations.

Table 4: Procedural Normative Analysis Of The Applicability Of AI Systems In Forensic Practices Of Computer Crime Investigation: Procedural Effectiveness, Regulatory Limitations, And Ways Of Optimization

Title of the regulation	Description of the procedure for using AI in cybercrime investigations	Regulatory shortcomings in the use of AI for cybercrime investigation	Proposals for optimizing regulatory norms for the use of AI for cybercrime investigation
Budapest Convention on Cybercrime (2001)	Defines standards for the collection, preservation, and transmission of electronic evidence; implicitly allows for automated collection of digital traces	Lack of direct legal regulation on algorithmic methods of collecting and processing evidence	Inclusion of a separate section on the admissibility of AI analytics results as evidence
EU Artificial Intelligence Act (2021, draft)	Identifies risk stratification and legal restrictions on high-risk AI systems, which include forensics	High level of restrictions for forensic AI systems; lack of detail on forensic pipelines	Clarification of requirements for explainability and auditability in the field of criminal process
OECD AI Principles (2019)	Formulates ethical and procedural principles for the AI use, including security, accountability and transparency	Has no binding legal force; no mechanism for integration into criminal procedure systems	Institutionalization of principles within the forensic regulations of the Member States
FATF Guidance on Digital Identity (2020)	Regulates the AI use for identifying individuals in the context of AML/CFT; allows the use of digital identity	Narrow financial and jurisdictional focus; insufficient justification for use in digital forensics	Extension of provisions to the areas of CSAM, phishing, crypto-fraud
ISO/IEC 27037:2012	Standardizes procedures for preserving digital evidence, including automated identification and removal	Lack of specification for the use of ML/AI algorithms	Development of an application on the use of intelligent verification tools
ISO/IEC 27043:2015	Defines the concepts of incident forensics, including the detection, response, analysis, and aftermath phases	Does not include AI modules in forensic workflows; does not support explainability	Clarification of standards for explainable AI in forensic data interpretation
ISO/IEC TR 24028:2020	Provides an overview of threats to AI systems and approaches to cybersecurity with a view to trustworthiness	No connection to forensic practices; focuses on AI protection	Inclusion of forensic-validity and evidence-admissibility components in the context of secure AI
NIST SP 800-61 Rev.2	Regulates response to cyber incidents, includes automated	Does not cover deep models of malicious	Additional section with procedural validation of AI

Title of the regulation	Description of the procedure for using AI in cybercrime investigations	Regulatory shortcomings in the use of AI for cybercrime investigation	Proposals for optimizing regulatory norms for the use of AI for cybercrime investigation
	alerting and evidence handling	behaviour analysis (DL, LLM)	solutions in the post-incident analysis phase
Directive 2011/93/EU	Regulates the investigation of crimes against the sexual integrity of children, allows for digital identification	No provisions on AI hashing, semantic classification, automated prioritization	Introduction of a toolkit of permissible AI tools for CSAM investigations
Convention 108+ (Council of Europe)	Unifies approaches to personal data protection, including data processing by AI systems	High level of requirements to limit algorithmic processing without consent	Introduction of a forensic exception with audit trail provision
Criminal Procedure Code of Ukraine (Art. 84, 99, 100)	Regulates the admissibility, collection and preservation of evidence; allows digital media	No interpretation of the concept of automated (AI) analysis as an appropriate way to generate evidence	Development of a procedural interpretation of the admissibility of AI analytics as part of an examination
Law of Ukraine "On Protection of Information in Information and Telecommunications Systems"	Establishes requirements for cyber security of information systems, including incident management	No detail on forensic use of AI in cyber defence	Introduction of changes with formalization of the use of AI tools in cyber incident response

Source: created by the authors

The analysis of regulations (Table 4) revealed the absence of standardized mechanisms for incorporating AI analytics into the evidence base, which necessitates the implementation of provisions on explainability, auditability, and forensic admissibility.

Procedural modelling (Figure 2), based on a sample of typical cybercrimes (Table 1) and the regulatory framework (Table 2), reproduces a fragmented automated model of interaction between the investigator, AI system, and expert legal environment.

The typical model (Figure 2) reflects a linear sequence of actions with significant limitations in terms of regulatory stratification, explainability, and procedural integration of AI, which indicates the need for procedural optimization for the legitimation and technological validation of such decisions.

The optimized model (Figure 3) consolidates the results of the previous analysis, eliminates regulatory and procedural dysfunctions, and formalizes a functionally efficient and legally permissible architecture for the AI use in digital forensics.

The optimized model (Figure 3) implements a multi-agent approach with context-adaptive AI analytics, expert validation, and regulatory traceability, ensuring consistency from the initiation of an investigation to the transfer of a procedurally admissible digital evidence package.

The optimized model provides higher cognitive relevance, regulatory resistance, and transparency of AI analytics, minimizing algorithmic bias and increasing the admissibility of evidence through explainability, auditability, and expert validation.

Therefore, it is appropriate to review regulations to institutionalize procedural admissibility of AI, detail forensically explainable AI standards, create a registry of certified tools for CSAM, phishing, and financial investigations, and implement audit trail requirements. The proposed model provides legal predicativity, interoperability, and cognitively transparent integration of AI.

5. DISCUSSION

The current use of AI in digital forensics is driven by the complexity of cybercrime, the growth of digital artifacts, and the demands for regulatory-compliant analytics. The focus is on explainable AI as a tool for legal traceability and verification. A critical comparison of current models of AI integration into forensic procedures is conducted, taking into account regulatory, technical, and ethical aspects.

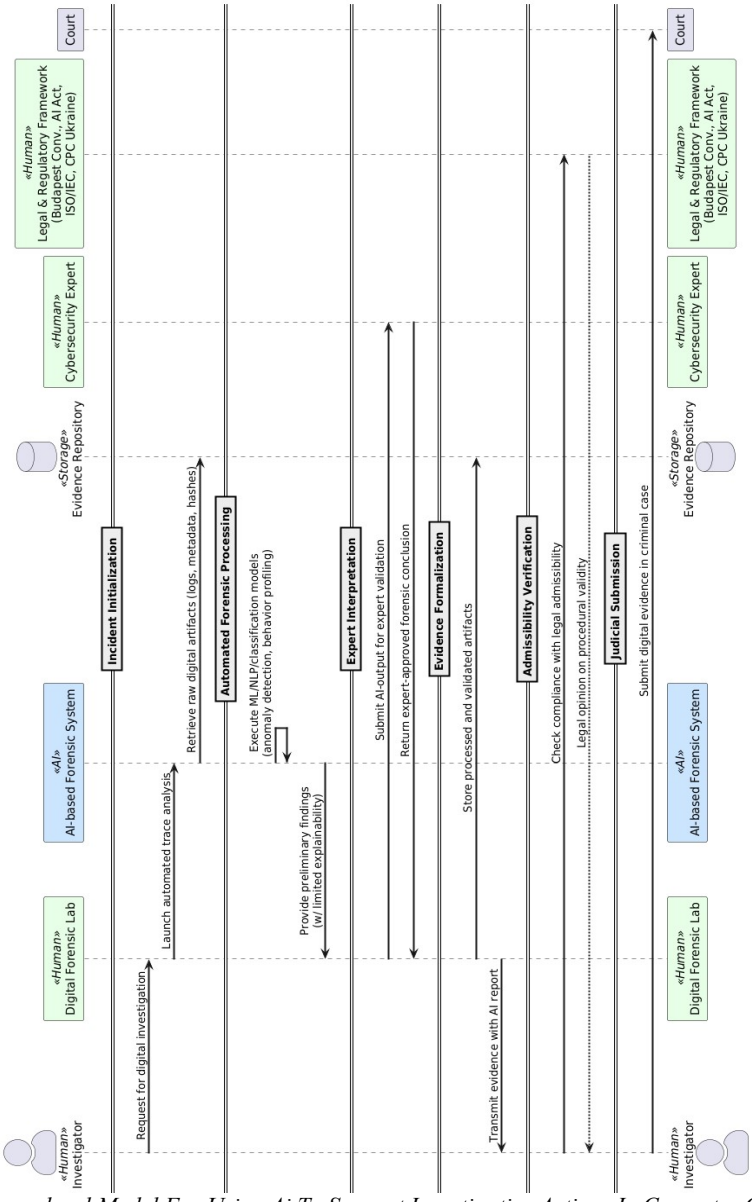

Figure 2: Typical Procedural Model For Using Ai To Support Investigative Actions In Computer Crime Investigations Source: created by the authors in Gleek.in [34]

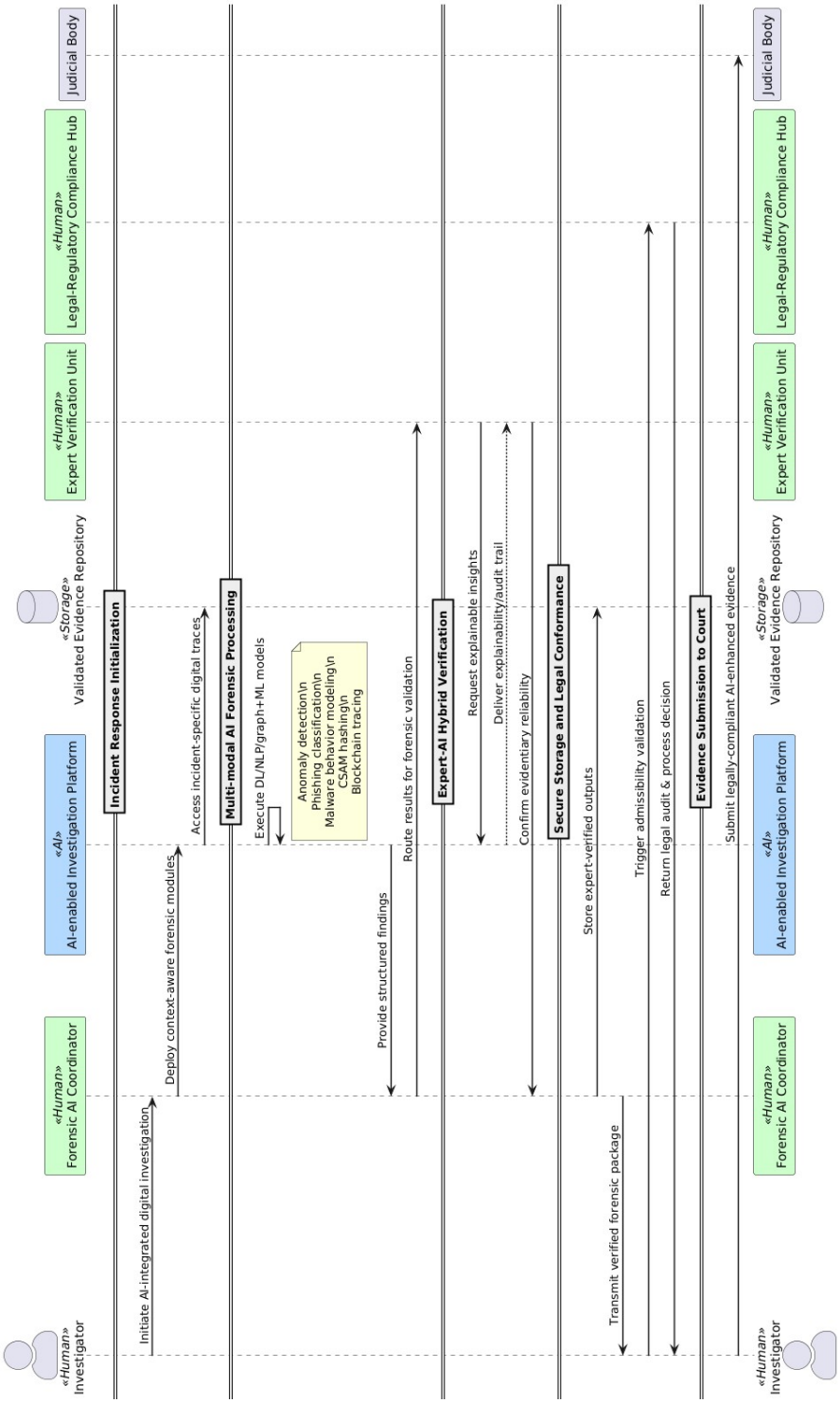

Figure 3: Optimized Procedural Model For Using AI To Support Investigative Actions In Computer Crime Investigations

Source: created by the authors in Gleek.in Gleek.io [34]

Zangana et al. [35] substantiated the effectiveness of ML/DL/NLP in cyber forensics as a means of proactive threat detection, incident management, and automated analysis of digital evidence. The same study proved the benefits of procedurally stratified implementation of

explainable AI with audit trail, legal traceability, and regulatory compliance.

Khare and Raghuwanshi [36] demonstrated the integral impact of AI on digital forensics and cybersecurity, emphasizing its role in event reconstruction, anomaly detection, and transnational response to threats. This study, in contrast to the emphasis on technical efficiency, focuses on procedural verification of AI solutions, eliminating regulatory fragmentation and formalizing the principles of auditability and responsibility in a forensic context.

Ahmed et al. [37] demonstrated the effectiveness of ML, CV, and NLP in forensic evidence processing, in particular in 3D crime scene modelling and automated analysis of biological and digital traces. Our study substantiates the appropriateness of implementing explainable AI with regulatory auditability, procedural validation, and legal admissibility in forensic cyber investigation practices.

Singh et al. [38] demonstrated the effectiveness of ML tools in cyber defence, focusing on predictive analytics and automated response. In contrast, this study proves the appropriateness of integrating explainable AI into forensic procedures, with an emphasis on legal admissibility and regulatory interoperability.

Rizal et al. [39] substantiated the use of AI in the framework of IoT-forensic readiness, with an emphasis on automated evidence collection, multi-vector attack detection and compliance with ISO/IEC 27043. In contrast, our study proves the appropriateness of procedurally validated integration of explainable AI in forensic examination of complex computer crimes, with a focus on legal admissibility, forensic traceability, and regulatory interoperability.

Malviya et al. [40] demonstrated the effectiveness of AI approaches in forensic imaging (VIRTOPSY) as a means of increasing diagnostic accuracy and evidentiary reliability. This study focuses on the procedural and normative formalization of AI analytics, in particular its admissibility, traceability, and auditability within the framework of forensic practices of computer crime investigation.

Syaakirah et al. [41] emphasized the effectiveness of classical digital forensic methods in reconstructing events and supporting judicial procedures, while acknowledging the challenges of encryption, cloud, and jurisdictional fragmentation. Instead, our study demonstrates the appropriateness of integrating explainable AI as an adaptive tool for forensic stratification of digital traces, taking into account regulatory interoperability and cognitive verification of evidence.

Shamota [42] argued for the dichotomous impact of AI in cyberspace, emphasizing its ability to both enhance the means of forensic detection of cybercrimes and complicate them by making attacks autonomous. In contrast, our study argues for the need for regulatory stratification of explainable AI in forensic procedures to ensure transnational interoperability, legal admissibility, and ethical moderation of analytics in the context of hybrid threats.

Shamoo [43] argued for the critical role of explainable AI in digital forensics, focusing on removing the opacity of black-box models and ensuring interpretability, traceability, and legal admissibility of results. This study extends this approach by demonstrating the effectiveness of XAI as a key component of an optimized procedural model that provides cognitive transparency, forensic verifiability, and regulatory interoperability of evidentiary information.

In contrast to the focus of previous research on the technical efficiency of ML/DL/NLP, the results confirm the priority of normatively stratified integration of explainable AI as a condition for legal admissibility, procedural verification, and cognitive interpretability. Such an approach minimizes the risks of inadmissibility and transforms AI analytics into a legally relevant evidentiary practice.

5.1. Limitations

A limitation of the study is the lack of empirical testing of the proposed optimized procedural model with explainable AI in real forensic scenarios.

5.2. Recommendations

It is appropriate to initiate controlled empirical tests involving digital forensics experts to verify the legal admissibility, cognitive interpretability, and procedural effectiveness of the model.

6. CONCLUSIONS

The conducted research substantiates that the integration of AI into digital forensics, despite its cognitive and analytical potential, remains constrained by algorithmic opacity, regulatory fragmentation, and lack of procedural standardization—factors that critically undermine the legal admissibility and operational integrity of AI-generated evidence. Empirical synthesis of prior

studies revealed the inadequacy of existing models in ensuring legal traceability, semantic transparency, and forensic auditability. In response, the optimized multi-agent model proposed in this study offers a structurally stratified solution, combining explainable AI modules, adaptive analytics, expert validation mechanisms, and jurisdiction-aware compliance protocols. This configuration demonstrably enhances evidentiary reliability and procedural compatibility across hybrid threat environments.

Grounded in the identified gaps in prior literature, the study supports the imperative for regulatory reformation—specifically, the institutionalization of explainability and auditability standards, the codification of forensic admissibility protocols, and the creation of a certified AI-tool register for digital investigations. This framework not only addresses the initial problem of admissibility uncertainty in AI-forensics but also formulates a normative trajectory for AI-augmented investigative practices capable of withstanding legal, ethical, and operational scrutiny.

The academic novelty of the study is the formalization of an optimized procedural model for the use of explainable AI in digital forensics, which combines multi-agent analytics, regulatory traceability, and standardized expert validation within the criminal process.

The practical significance of the research results is the development of an operationalized approach to the legitimate integration of AI analytics into forensic procedures, which ensures increased level of evidentiary admissibility, minimization of algorithmic bias, and institutional compliance with auditability, and legal traceability criteria.

REFERENCES:

[1] K. Kussainov, N. Goncharuk, L. Prokopenko, L. Pershko, B. Vyshnivska, and O. Akimov, "Anti-corruption management mechanisms and the construction of a security landscape in the financial sector of the EU economic system against the background of challenges to European integration: Implications for artificial intelligence technologies", *Economic Affairs*, Vol. 68, No. 1, 2023, pp. 509-521. doi: 10.46852/0424-2513.1.2023.20

[2] M. Kryshtanovych, L. Akimova, V. Shamrayeva, M. Karpa, and O. Akimov, "Problems of European integration in the construction of EU security policy in the context of counter-terrorism", *International Journal of Safety and Security Engineering*, Vol. 12, No. 4, 2022, pp. 501-506. doi: 10.18280/ijsse.120411

[3] O. Pavlovskyi, M. Blikhar, L. Akimova, V. Kotsur, O. Akimov, and M. Karpa, "International migration in the context of financial and economic security: The role of public administration in the development of national economy, education, and human capital", *Edelweiss Applied Science and Technology*, Vol. 8, No. 6, 2024, pp. 1492-1503. doi: 10.55214/25768484.v8i6.2265

[4] Y. Qiu, "Policing AI-generated crimes: An ethnographic study on anti-cybercrime police in China", *Security Journal*, Vol. 38, No. 1, 2025. doi: 10.1057/s41284-025-00491-3

[5] R. El-Kady, "Leveraging artificial intelligence for enhanced detection and mitigation of illicit activities on the dark web", in: *Lecture Notes on Data Engineering and Communications Technologies*. Cham: Springer Nature Switzerland, 2025a, pp. 79-89. doi: 10.1007/978-3-031-81308-5_8

[6] G. Stephen, "Investigation and prevention of cybercrimes using Artificial Intelligence", Master's thesis, Jamk University of Applied Sciences, Jyväskylä, 2025. Available in: https://www.theseus.fi/handle/10024/891045 (29.08.2025).

[7] P. Jain, P. Verma, T. Debnath, L. Heisnam, S. Chaudhary, and S. Balouria, "Cybersecurity forensics with AI", in: *Quantum Computing*. Boca Raton: Auerbach Publications, 2025, pp. 170-184. doi: 10.1201/9781003499459-10

[8] Y. Shamoo, "Cybercrime investigation and fraud detection with AI", in: *Advances in Digital Crime, Forensics, and Cyber Terrorism*. Hershey: IGI Global, 2025a, pp. 83-114. doi: 10.4018/979-8-3373-0857-9.ch004

[9] N. Singh, M. Z. Khan, B. Kaur, and A. Mishra, "Revolutionizing crime investigation", in: *Forensic Intelligence and Deep Learning Solutions in Crime Investigation*. Hershey: IGI Global, 2025, pp. 281-300. doi: 10.4018/979-8-3693-9405-2.ch014

[10] H. J. Akeiber, "A comprehensive study of cybercrime and digital forensics through machine learning and AI", *Al Rafidain Journal of Engineering Sciences*, Vol. 3, No. 1, 2025, pp. 369-395. doi: 10.61268/hff1pp49

[11] H. M. Merdas and A. M. Obaid, "From clues to convictions: The critical role of artificial intelligence in criminal investigations",

European Journal of Scientific Research and Reviews, Vol. 2, No. 2, 2025, pp. 46-56. doi: 10.5455/ejsrr.20250102031037

[12] K. Patel, H. Parikh, K. R. Dodiya, D. Patel, and A. Patel, "Evolving role of AI in forensic science and crime investigation", in: *Advances in Social Networking and Online Communities*. Hershey: IGI Global, 2025, pp. 365-388. doi: 10.4018/979-8-3373-0543-1.ch013

[13] B. Singh, "Appreciating machine learning intelligence combating cyber threats", in: *Democracy and Democratization in the Age of AI*. Hershey: IGI Global, 2025, pp. 259-284. doi: 10.4018/979-8-3693-8749-8.ch014

[14] A. Z. A. Shami, M. Saleem, and J. Ashraf, "Cybercrime and digital evidence: Investigating the challenges and opportunities in prosecuting cybercrime and handling digital evidence", *Research Consortium Archive*, Vol. 3, No. 2, 2025, pp. 401-411. doi: 10.63075/jq8yfw48

[15] M. Gupta, R. P. Sood, and R. Singh, "Artificial intelligence in criminal investigation: Transforming law enforcement and forensic analysis", in: *Rethinking the Police for a Better Future*. Cham: Springer Nature Switzerland, 2025, pp. 311-323. doi: 10.1007/978-3-031-83173-7_21

[16] N. Mohamed, H. Taherdoost, and M. Madanchian, "Enhancing spear phishing defense with AI: A comprehensive review and future directions", *ICST Transactions on Scalable Information Systems*, Vol. 12, No. 1, 2025, pp. 1-10. doi: 10.4108/eetsis.6109

[17] H. J. Akeiber, "The evolution of social engineering attacks: A cybersecurity engineering perspective", *Al Rafidain Journal of Engineering Sciences*, Vol. 3, No. 1, 2025, pp. 294-316. doi: 10.61268/r9c49865

[18] R. Sood, A. Sood, S. Sood, and S. G. Kawalkar, "Preventing online financial frauds", in: *AI and Emerging Technologies*. Boca Raton: CRC Press, 2024, pp. 69-84. doi: 10.1201/9781003501152-5

[19] O. A. Bello and K. Olufemi, "Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities", *Computer Science & IT Research Journal*, Vol. 5, No. 6, 2024, pp. 1505-1520. doi: 10.51594/csitrj.v5i6.1252

[20] S. A. H. Moamin, M. K. Abdulhameed, R. M. Al-Amri, A. D. Radhi, R. K. Naser, and L. G. Pheng, "Artificial intelligence in malware and network intrusion detection: A comprehensive survey of techniques, datasets, challenges, and future directions", *Babylonian Journal of Artificial Intelligence*, Vol. 2025, 2025, pp. 77-98. doi: 10.58496/bjai/2025/008

[21] T. Gundoor and Sridevi, "A comprehensive study on deep learning and artificial intelligence for malware analysis", in: *Next-Generation Systems and Secure Computing,* 2025, pp. 39–-59. doi: 10.1002/9781394228522.ch3

[22] E. Bhuiyan, S. Islam, A. Al-Mamun, and A. Uddin, "Cyber crime or technological epidemic? Intersecting the criminalization of sexual deepfake in domestic and international law", *OALib*, Vol. 12, No. 05, 2025, pp. 1-19. doi: 10.4236/oalib.1113311

[23] L. S. F. Lin, "Examining the role of deepfake technology in organized fraud: Legal, security, and governance challenges", *Frontiers in Law*, Vol. 4, 2025, pp. 6-17. doi: 10.6000/2817-2302.2025.04.02

[24] S. K. Borah, S. Ramaswamy, and S. Seshadri, "The online specter: Artificial intelligence and its risks for child sexual abuse and exploitation", *Journal of Indian Association for Child and Adolescent Mental Health*, Vol. 21, No. 2, 2025, pp. 107-112. doi: 10.1177/09731342251334293

[25] H. Wolbers, T. Cubitt, and M. J. Cahill, "Artificial intelligence and child sexual abuse: A rapid evidence assessment", *Trends and Issues in Crime and Criminal Justice*, Vol. 711, 2025, pp. 1-18. Available in: https://search.informit.org/doi/abs/10.3316/informit.T20250130000125016737888879 (29.08.2025).

[26] R. El-Kady, "Decoding the dark: AI and ML in the dark web cybercrime and cryptocurrency forensics", *International Cybersecurity Law Review*, Vol. 6, 2025, pp. 107-143. doi: 10.1365/s43439-025-00145-5

[27] L. S. F. Lin, "Cryptocurrencies and AI-enabled organised fraud: Emerging risks and countermeasures", in: *The 1st International Online Conference on Risk and Financial Management: Big Data, Artificial Intelligence, and Machine Learning in Finance*. 2025. Available in: https://researchoutput.csu.edu.au/en/publications/cryptocurrencies-and-ai-enabled-organised-fraud-emerging-risks-an (29.08.2025).

[28] M. A. Goffer, M. S. Uddin, J. Kaur, S. N. Hasan, C. R. Barikdar, J. Hassan, N. Das, P. Chakraborty, and R. Hasan, "AI-Enhanced cyber threat detection and response advancing national security in critical infrastructure",

Journal of Posthumanism, Vol. 5, No. 3, 2025. doi: 10.63332/joph.v5i3.965

[29] F. H. Deandra and I. M. Sherly, "Advancing digital forensic investigations: Addressing challenges and enhancing cybercrime solutions", *World Journal of Information Technology*, Vol. 3, No. 1, 2025, pp. 10-15. doi: 10.61784/wjit3018

[30] J. Reza, M. I. Khan, and S. A. Sarna, "Proactive cyber threat detection using AI and open-source intelligence", *Journal of Computer Science and Technology Studies*, Vol. 7, No. 5, 2025, pp. 558-576. doi: 10.32996/jcsts.2025.7.5.62

[31] B. O. Daudu and G. U. Osimen, "Combatting cyberthreats in African digital space with artificial intelligence", in: *Cybersecurity in Knowledge Management*. Boca Raton: CRC Press, 2025, pp. 115-–130. doi: 10.1201/9781003498094-8

[32] S. Chandra, "Exploring the role of artificial intelligence in governance", in: *Advances in Computational Intelligence and Robotics*. Hershey: IGI Global, 2025, pp. 141-168. doi: 10.4018/979-8-3693-9395-6.ch007

[33] E. Jozaghi, "National security during the first AI revolution: The case for transforming Canada's security apparatus", *Canadian Public Administration*, Vol. 68, No. 2, 2025, pp. 285-308. doi: 10.1111/capa.70020

[34] Diagram maker for developers. Gleek, 2025. Available in: https://www.gleek.io/ (29.08.2025).

[35] H. M. Zangana, M. Omar, and D. Mohammed, "Introduction to artificial intelligence in cybersecurity and forensic science", in: *Advances in Information Security, Privacy, and Ethics*. Hershey: IGI Global, 2025, pp. 1-24. doi: 10.4018/979-8-3373-0588-2.ch001

[36] P. Khare and V. Raghuwanshi, "Navigating emerging AI technologies and future trends in cybersecurity and forensics", in: *Advances in Digital Crime, Forensics, and Cyber Terrorism*. Hershey: IGI Global, 2025, pp. 321-346. doi: 10.4018/979-8-3373-0857-9.ch012

[37] S. Ahmed, M. F. Khan, B. Singh, N. Singh, and B. Sharma, "Enhancing crime scene analysis", in: *Forensic Intelligence and Deep Learning Solutions in Crime Investigation*. Hershey: IGI Global, 2025, pp. 63-84. doi: 10.4018/979-8-3693-9405-2.ch004

[38] B. Singh, C. Kaunert, and S. Chandra, "Relishing machine learning intelligence combating cyber threats", in: *Navigating Cyber Threats and Cybersecurity in the Software Industry*. Hershey: IGI Global, 2025, pp. 129-150. doi: 10.4018/979-8-3693-6250-1.ch007

[39] R. Rizal, S. R. Selamat, M. Z. Mas'ud, and N. Widiyasono, "Enhanced readiness forensic framework for the complexity of Internet of Things (IoT) investigation based on artificial intelligence", *Journal of Advanced Research in Applied Sciences and Engineering Technology*, Vol. 50, No. 1, 2025, pp. 121-135. doi: 10.37934/araset.50.1.121135

[40] R. Malviya, A. Jain, S. Lal, M. K. Arora, and S. Kumar, "Exploring artificial intelligence (AI) in forensic pathology and autopsy analysis", in: *Forensic Intelligence and Deep Learning Solutions in Crime Investigation*. Hershey: IGI Global, 2025, pp. 125-146. doi: 10.4018/979-8-3693-9405-2.ch007

[41] C. R. Syaakirah, L. Syifa, and I. Muda, "Digital forensic investigation in cybercrime cases: Case studies and recommendations", *Multidisciplinary Journal of Engineering and Technology*, Vol. 2, No. 1, 2025, pp. 9-15. doi: 10.61784/mjet3018

[42] M. R. Shamota, "Artificial intelligence cybercrime and need for regulation", in: *The Interdisciplinary Nexus: Law, Humanities, and Management,* 2025, p. 20. Available in: https://shorturl.at/hxnWe (29.08.2025).

[43] Y. Shamoo, "The role of explainable AI (XAI) in forensic investigations", in: *Advances in Digital Crime, Forensics, and Cyber Terrorism*. Hershey: IGI Global, 2025b, pp. 31-62. doi: 10.4018/979-8-3373-0857-9.ch002