International Journal of
Human Computations and Intelligence
Vol. 05, Issue. 02, 2026

RESEARCH ARTICLE OPEN ACCESS

Cybercrime Investigation Through Digital Forensics: Standards of Evidence and Legal Compliance

P Sumalatha* . N V Naga Rohini . R Vyshnavi . B N V Chandra Netri . B Vishnuvardhan

Department of CSE (IoT, Cyber Security including Block Chain Technology),
Annamacharya Institute of Technology & Sciences (Autonomous),
Tirupati, Andra Pradesh, India.

DOI: **10.5281/zenodo.18594077**
Received: 14 January 2026 / Revised: 24 January 2026 / Accepted: 10 February 2026
*Corresponding Author: *psumalatha241@gmail.com*

Abstract – The increase in the incidence of cybercrimes, fueled by accelerating developments in information technology, demands the effective use of digital forensics. We present an analysis of the relationship between digital forensics and legal compliance, with particular emphasis on the significance of digital evidence in cybercrimes. And we identify the critical steps in the digital forensic process, highlighting the significance of the integrity of digital evidence in cybercrimes. As cybercrimes are constantly evolving, digital forensic professionals are now using machine learning (ML) and artificial intelligence (AI) techniques in the classification and detection of digital evidence. However, new challenges in the use and legitimacy of AI-generated evidence in legal actions have emerged. This paper examines the importance of digital evidence, the use of digital evidence in cybercrimes, the use and significance of standard digital forensic practices, the use of the blockchain in digital forensics, and the significance of cross-jurisdictional legal actions, among other important issues. The major aim of this study is to add new knowledge in the ever-increasing discussions on cybercrimes, digital evidence, and digital forensics.

Index Terms – Cybercrime, Digital Forensics, Evidence Standards, Legal Compliance, Machine Learning, Chain of Custody, Blockchain.

I. INTRODUCTION

Cybercrime is an ever-changing criminal activity, driven by the dynamic development of digital technology and cyberworlds. To this effect, a new and vital area of investigation, cybercrimes and digital forensic science, emerged through a process that satisfies legal requirements and judicial virtues. Recent research confirms that propriety and legal processes play a major role in contemporary cybercrime

MILESTONE RESEARCH.IN OPEN ACCESS

ISSN (Online): 2583-5696
Int. Jr. of Hum Comp. & Int.

investigations; mainly, this pertains to the collection, analysis, and preservation of relevant evidence and its integrity, when considering evolving legal environments [1].

Digital forensic specialists must continue to adjust and adapt to prevent any new, very complex cybercrime activities, thus ensuring that the collected and/or extracted digital items are legitimate and/or authentic, meeting legal and judicial implications [2]. Through the research, the systematic processes and methods required to identify, secure, and present digital evidence were identified, addressing legal and technical issues [3]. Machine learning and AI technologies have also become integral parts of digital forensic processes, and they greatly help to improve pattern recognition and evidence classification capabilities. Recent research highlights both the benefits and disadvantages of such technologies and how they can solve some problems while creating new issues concerning the legitimacy of AI-based digital evidence in legal proceedings [4], [5]. One research highlights the capabilities of AI technology concerning the potential for automating forensic analysis and how the legal system must commence adapting to it while ensuring it meets the requirements of admissibility standards [6]. There is also another very recent research focusing on the risks of privacy violations and regulatory compliance concerns associated with digital evidence handling and providing a framework for embedding ethical considerations within digital forensic processes [7].

The basics of digital forensics remain legal compliance and standardization. Various works in this respect opine that standard forensic rules and legal procedures are a critical need for the acceptance of evidence within and across borders and to protect individual rights, as pointed out in [8] and [9]. Again, solution findings on blockchains indicate that blockchain can enhance the chain of custody and reduce the possibility of tampering with digital evidence for increased transparency and safety, according to [10]. Also, international legal framework analyses underline the difficulties involved in making forensic practices compatible with continuously changing cybercrime statutes and laws of evidence, as these are different for different jurisdictions.

Our main contributions are as follows:

- Legal and Forensic Framework: The paper also highlights the importance of integrating various legal and forensic frameworks. In the same way, there is also a detailed discussion on the importance of the chain of custody and forensic imaging practices in accordance with the law.
- Machine Learning and AI in Forensics: This research area seeks to examine the various machine learning (ML) and artificial intelligence (AI) technologies that have been integrated into digital forensics, including their positive and negative implications, particularly on the validity of evidence and privacy.
- Blockchain for Evidence Integrity: This section offers the potential application of blockchain technology for maintaining an unbroken custody chain and ensuring tamper-proof handling of witness testimony as a digital forensic tool.
- Standardization and Cross-Jurisdictional Compliance: First, it recognizes the need to standardize procedures in addressing the problem of inconsistency in the practice of digital forensics across jurisdictions. The need to standardize the legal process in order to enhance cross-jurisdictional compliance in the fight against cybercrime is well captured in the study.

II. LITERATURE SURVEY

The swift increase in cybercrime has heightened the use of digital forensics to investigate and make a legal admission of the digital evidence. Nevertheless, the issue of fragmented forensic methods, inconsistency in the law, reliability of tools, and privacy are still unaddressed. Deandra et al. [11] introduced a Digital Forensic Investigation (DFI) model, which is based on the ISO 27037: 2012 model, which combines conventional forensic tools alongside AI/ML and cloud-mobile forensic methods. The paper points to improved evidence integrity, efficiency, and effectiveness in the investigation of encrypted, cloud-based, and decentralized data. Its unique aspect is its integrated and holistic forensic model, which takes into consideration the problem of a limited forensic method. Nevertheless, the model has several limitations connected to the dependence on the tool, legal and jurisdictional factors, the issue of transparency related to AI, and the absence of large-scale practical application.

Hirde [12] suggested a hybrid deep learning model of CNN-LSTM with SIFT that can be used to identify forgery in digital images. This model is useful in identifying tampered areas, classifying the types of manipulation, including copy-move and splicing, and pointing out the forged regions using bounding boxes and masking. Nevertheless, the framework is demanding in terms of large datasets, expensive to compute, and has poor generalization to real-life forgery conditions. In a similar manner, Srivastava et al. [13] have also highlighted the need to integrate machine learning with forensic intelligence to detect cybercrimes better. Their comparative study of SVM, Random Forest, k-NN, Decision Tree, and Neural Networks showed that the machine learning-based solutions can help to speed up workflows, promote greater accuracy, and assist in preventing threats. Although such advantages are present, the authors raised their concerns about the bias of data and the possibility of using algorithmic evidence in a courtroom.

In a different method, Akshaya et al. [14] presented a model of cybercrime prediction and analysis based on the use of the Random Forest Regressor on NCRB data in India. The model was very accurate when the data was split into 80:20 and measured in terms of MSE and R-squared, as well as giving forecasts per region using a conveniently designed interface. However, the research is also restricted by the fact that it has relied on historical reporting and has not been validated in real-time. Recently, Bhole et al. [15] suggested an integrated digital forensic investigation framework, which includes hard disk, memory, and network forensics through the standardized procedures, the use of forensic tools, and AI-assisted techniques. In the study, it is revealed that the process of gathering evidence, analyzing it, and its admissibility in court during cybercrime was improved, and it was the first use of technical, legal, and procedural approaches. However, it is also very theoretical and restricted by the rapid legal and technological transformations.

Ismail et al. [16] went ahead to formulate a 3-stage model that is consistent with the Daubert Standard to determine the admissibility of open-source forensic-generated digital evidence. The results show that validated open-source tools can match the reliability and repeatability of commercial ones and overcome the problem of trust and validation in open-source forensics. More so, Reddy et al. [17] compared the Logistic Regression and the Random Forest when it comes to facial recognition systems to investigate cybercrime. Their results suggested that the accuracy of the Random Forest over the Logistic Regression was 77.7 with statistical significance ($p=0.025$). The study was, however, limited by the small sample size and the limited validation in large-scale real-world data. Nazari et al. [18] suggested a CUDA-based hybrid CNN-DNN model that could be used to detect multi-class malware in IoT networks. The

model was found to be 98.41% accurate and able to recall 98.56% with low training time as compared to CPU-only systems. The scalable approach, which is based on GDP, is also new, but its testing was not done on multiple datasets, which is a matter of concern in terms of generalizability.

Vanini et al. [19] come up with a tamper resistance assessment model that includes a scoring model to measure the strength of digital forensic artifacts during the reconstruction of events. According to the results, timeline-based investigations are more reliable and accurate, and the deliberate modification of evidence has not been explicitly covered before. The framework, however, is still a conceptual one that has to be empirically tested extensively to prove its practicality. Sibe et al. [20] also presented scholarly criticism of digital evidence, forensic preparedness, and their admissibility in the investigation of cybercrime. Their article touched on legal systems, such as Nigeria's Evidence Act, and international norms, like Frye and Daubert, to close the gap between forensic preparedness and the law. However, the chapter is mostly theoretical in nature and not experimental.

III. PROPOSED METHODOLOGY

A systematic approach to digital forensics is utilized in this study to facilitate the investigation of cybercrimes while providing compliance with legal and evidentiary requirements. Within a safe online environment, the study combines automated forensic reporting, issue-level classification, synthetic evidence simulation, and forensic data processing. From the collection of unprocessed digital evidence to the creation of legally valid reports, the methodology is intended to mirror the real-world investigative lifecycle. Figure 1 depicts the proposed model architecture.

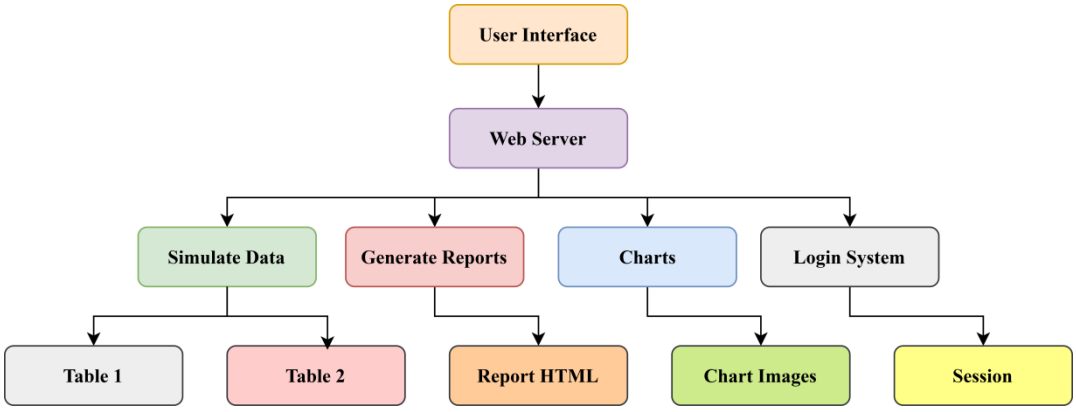

Fig. 1: Graphical representation of the proposed model architecture

A. Dataset Description

The dataset used in this study was constructed through a systematic collection and analysis of digital forensics literature, forensic reports, and legal case materials related to cybercrime investigations. From this dataset, 40 digital forensics reports and academic sources were selected for the core dataset, with context provided in the wider forensic landscape from a reference set of 507 forensic science publications from many disciplines. The digital forensics subset consists of peer-reviewed research, expert forensic reports, and court records that deal with how evidence is collected, analyzed, and interpreted in such a way as to make it legally admissible. These come from various jurisdictions to reflect the range of

legal standards, best practices, and procedural requirements. Particular attention was paid to texts on chain of custody, forensic imaging, data integrity, privacy considerations, and the ways expert opinions are formed in cybercrime cases.

B. Proposed Methodology

In the proposed approach, a model is presented to depict how a fully functional forensic simulation platform, built on the Django framework, can perform a range of operations from the commencement to the conclusion of a virtual investigation into a cybercrime. It is worth noting that the proposed platform does not rely on real-world data, as is done in traditional systems.

The overall procedure can be summarized as follows:

$$U \longrightarrow WS \longrightarrow \{SD, GR, CH, LS\} \longrightarrow Output$$

where, U defines the user interface, WS defines the central Django web server, SD refers to simulated evidence generation, GR is structured report production, CH represents forensic visualization outputs, and LS provides authentication and session-level security.

- Synthetic Evidence Simulation Module: The first step of the proposed method is focused on creating artificial datasets for forensic use through a controlled process. This part of the tool mimics real cybercrime data, including access information and indicators of wrongdoing. The synthetic evidence collection is depicted as:

  $$E_s = \{e_1, e_2, \dots\dots\dots, e_n\}$$

  Every evidence record is modeled as:

  $$e_i = (source, \quad activity_i, \quad offense_i)$$

  The methodology divides inquiry problems into three levels of hierarchy to facilitate systematic forensic reasoning:

  $$L = \{L_1, L_2, L_3\}$$

  where, L_1 is the source-level issues, L_2 is the activity-level issues, and L_3 represents the offense-level issues.
- Issue Frequency and Investigation Severity Assessment: The method conducts an analytical evaluation after generating evidence by calculating the frequency of issues found at each of the three levels of investigation. The occurrence frequency for each level L_k is calculated as follows:

  $$F(L_k) = \sum_{i=1}^{n} I(e_i \in L_k)$$

  The technique presents a severity scoring system based on legal significance to rank the results of the investigation. To calculate the severity score, use:

  $$S = \alpha L_1 + \beta L_2 + \gamma L_3$$

  where, the legal weight factors α, β, and γ are assigned to various issue levels based on how significant they are in prosecution situations.
  The severity score is normalized as follows to ensure interpretability:

  $$S_{norm} = \frac{S}{S_{max}}$$

  This makes it possible for investigators to differentiate between high-priority cybercrime incidents and low-risk anomalies.

- Automated Forensic Report Generation Module: The automated creation of organized forensic reports is one of the main benefits of the suggested methodology. The GenerateReports module generates legally styled HTML-based investigation summaries that include evidence artifacts, issue categories, severity determinations, and compliance information. Every forensic report is described as follows:

$$R = (E_s, L, S, C)$$

where, L stands for the categorized issue levels, S for calculated severity, C for chain-of-custody compliance, and E_s for the evidence set. Reporting completeness is evaluated using:

$$R_{comp} = \frac{|E_{documented}|}{|E_{total}|}$$

For admissibility and forensic reliability, the system requires:

$$R_{comp} = 1$$

which means that any evidentiary artifacts need to be thoroughly documented before being reported to the authorities.

- Visualization and Interpretability Module: The Charts module creates interactive visual analytics, such as bar charts, opinion charts, and stacked graphs, to improve forensic comprehension. Investigators can gain intuitive insight into the spread of issues and patterns of cybercrime using these graphic tools. Values in bar charts are calculated as follows:

$$B_k = F(L_k)$$

Detection confidence is estimated employing:

$$\text{Conf} = \frac{TP}{TP+FP}$$

where FP indicates wrongly flagged activity and TP represents correctly detected suspicious occurrences. This is a synopsis of the entire investigation:

$$T = \sum_{k=1}^{3} F\ (L_k)$$

In forensic environments, these visual outputs enhance accessibility, particularly for trainees and non-technical stakeholders.

- Secure Login and Session Management: The system has a LoginSystem module that limits access through authentication and session-based controls to ensure forensic evidence remains safe. Definition of authorization:

$$A\ (u) = \begin{cases} 1, & if\ authorized \\ 0, & if\ unauthorized \end{cases}$$

Session validity is modeled as:

$$\text{Session}\ (t) = e^{-\lambda(t-t_0)}$$

where, t_0 is the login initiation time and λ is the session expiration constant. This system guards against unauthorized disclosure and ensures that evidence access remains legally protected.

IV. HARDWARE SOFTWARE SPECIFICATION

- **Hardware Requirements:** The hardware configuration of the proposed system has been designed to support simulations, as required for digital forensic simulations. The hardware has been chosen to enable an effective and efficient running of simulations and other required processes for digital forensic report generation, data visualization, and other simulations. The proposed digital forensic

system has an Intel Core i5 processor, which meets the processing demands required for running digital forensic application simulations adequately. In addition, the proposed system has 4 GB RAM for its operations, in addition to 256 GB hard disk storage for storing synthetic data and generating digital forensic reports. A 14-inch color monitor and an optical mouse are relevant for interaction with the proposed system, making it possible for users to easily interact with digital forensic reports and simulations as they carry out their investigations.

- **Software Requirements:** Some of the software that will be used in this software stack include programming languages, frameworks, and libraries, all created to simplify the creation of a web-based digital forensics platform. Python will be used for this project as it will be the basis for all programming languages used, owing to its ease of use and its libraries, which will be immensely useful for data manipulation. Second, the web framework that will be used will be Django, which has an easy interface that will suit the users and has administrative features. Third, the frontend of this program will be created using standard HTML, CSS, and Js so that it can be dynamic and user-friendly. Fourth, for the management of data, SQLite will be used, which will act as the data base that will be used to store artificial data, making it easy for deployment. Fifth, some of the other Python libraries that will be used include Pandas, which will be used for the efficient management of data files, and Matplotlib for static and interactive visualizations.

V. RESULT & DISCUSSION

This section presents what we found from our structured review of the digital forensics' literature and the report construction for a cybercrime investigation. We use our curated dataset for cybercrime forensic analysis and the hierarchical issue-level framework to evaluate the representation of the evidence, the rigor of the approach, and the interpretability of the digital forensic analysis for legal reliability.

The results fall into two parts:

- A comparison of different forensic science disciplines with a focus on digital forensics.
- The spread of investigative issues from various types and levels of opinions in digital forensic reports.

A. Comparative Analysis of Forensic Science Disciplines

Table 1 presents a comparison that highlights the main difference between digital forensics and traditional disciplines in forensic science. It points out the shortcomings that digital forensics should eliminate in addressing cybercrime. Although digital forensics is reportedly an emerging discipline that has come of age with developments in technology, its reporting and depth of evidence, as highlighted, are still blemished. Alternative investigative methods employed in digital forensic practices are notably higher compared to those in traditional forensic fields, i.e., 47.8% as opposed to 12.1%. It is only logical, bearing in mind the dynamics involved in the formative processes of cybercrimes, which demand the employment of versatile tools as opposed to static ones, since the methods used must address varying forms,

environments, and jurisdictions. Although the employment of multiple tools could be desirable, there was equally a corresponding deviation in results, as highlighted by the standard deviation observed in the reporting of digital forensic results, which was noted to be 32.6%. Yet while numerous approaches are utilized, one finds a scarcity in formal reliability notes (2.5%) and validity notes (2.5%). When dealing specifically with other related forensic fields, these characteristics are even less represented. The need in assisting judicial proceedings to further prove the reliability and validity of a forensic investigation is heightened, particularly when dealing in complex cases of cybercrime. The notable observation is that the majority of these reports, i.e., 87.5%, have at least one limitation, while a considerable number, i.e., 80%, have vague information regarding the methodology.

Table 1: Comparative Analysis of Forensic Science Disciplines in Digital Forensics and Cybercrime Investigation

Content Type	Digital Forensics (n=40)	Total FS (n=507)	Fibres	Firearms	Glass	Handwriting	Paint	Documents	Shoe-Print	Tool-Marks
Alternatives	47.8	12.1	24.6	18.9	30.4	1.2	34.8	9.6	1.1	0.9
Reliability	2.5	0.6	0.8	0.6	0.5	0.7	4.9	0.8	0.4	0.6
Validity	2.5	0.8	0.9	0.7	0.6	0.9	5.1	0.9	0.6	0.7
Limitations	87.5	8.2	11.6	8.1	9.8	24.7	8.4	9.1	1.3	1.0
Methods Vague	80.0	15.0	11.9	23.8	1.4	6.8	16.9	28.7	19.6	16.4
Methods Specific	29.4	28.1	28.9	35.6	37.2	6.9	23.4	31.2	8.6	43.5
Opinion Statement	5.0	15.3	8.2	10.7	19.6	24.1	16.8	29.4	13.2	9.4
Reasoning	62.5	70.2	98.4	68.9	89.7	48.5	61.3	72.6	56.1	54.7
Term Explication	25.0	1.3	4.6	2.1	1.1	3.8	0.9	1.2	3.1	1.0
Mean (%)	38.0	17.9	21.1	18.7	21.1	13.1	21.4	22.6	11.6	14.2
Standard Deviation	32.6	20.8	30.4	22.1	28.5	15.4	22.1	24.6	19.3	21.1

The presence of a limitation ensures stakeholders comprehend the boundaries faced in digital investigation, like chain of custody issues, changing technology, and imperfect tools. Reports from digital forensics display lower amounts of reasoning (62.5%), coupled with relatively low levels of formal opinion statements (5.0%). By comparing the levels of reasoning within this field to other fields of forensic science, there seems to be a slightly low representation of this requirement, indicating that conclusions are drawn from the report, though perhaps not clearly expressed as legal or probabilistic opinions. There is a higher level of term explication within the field of digital forensics (25.0%) than seen within other areas of the subject, indicating the importance of translation of technical terms for the courts. The results illustrated in Table 1 point to a vital weak point within digital forensic analysis, as the source stage and the activity stage show to be the areas of concern for digital forensic analysis, as determining the source of evidence, establishing its authenticity, and reconstructing events occur at these stages. In the event of inconsistencies within the method, the authenticity of reliability is weak, while the expression of findings is not clearly defined, leading to a range of views from different people. This is notable within the digital forensic analysis, as challenges are experienced at the offense stage, which relies on the results from the initial stages. In such a way, the worth of the proposed simulation platform is affirmed, as consistency is sought in the entire digital forensic analysis.

Digital forensics, on the one hand, differs from the traditional disciplines, including fibers, firearms, and tool marks, by employing a broad range of methods accompanied by light validation. Conversely, traditional disciplines rely on a smaller range of alternative methods but have steadier, more transparent methods. However, this is an indication that digital forensics is getting into a stage where, in one way or another, the procedures, scientific tests, and juristic justifications are being determined. On the other hand, there is a higher degree of recognized limitations inherent in digital forensics, reflecting some challenges occasioned by the intangible, constantly changing, intertwined, and jurisdictionally complex nature of digital evidence.

B. Issue-Level Distribution Across Opinion Types

Table 2 examines the distribution of investigative concerns across opinion categories and hierarchical levels of forensic reasoning in order to examine how forensic conclusions are operationalized in practice.

Table 2: Distribution of Opinion Types and Issue Levels in Digital Forensic Reports

Opinion Type	DF Reports (n=40)	Source Issues	Activity Issues	Offence Issues	Categorical Conclusion
Traditional	28	24	22	17	58
Elaborated	32	31	28	24	52
Both	6	6	6	1	48
LR	0	0	0	0	36
SoS	62	57	52	38	0
Total	128	118	108	80	0

The findings reveal that, even in this era, traditional opinions remain more prevalent in digital forensic reports (28), while elaborated opinions also remain more popular (32), reinforcing a reliance on narrative interpretation. Finally, within opinion, elaborated opinions appear a bit more frequently, which could indicate a slow shift towards more transparent opinion statements. However, the complete lack of opinions involving formal legal reasoning (LR) is noteworthy. Such a lack implies that forensic conclusions may not be assessed probabilistically, which may have important limitations for adversarial proceedings in the legal system.

Furthermore, across the occurrence of every opinion type, source issues dominate as the most prevalent with 118 occurrences. These issues generally include the issues of evidentiary proof, authenticity verification, and issues with the data collection method. The dominance of these issues over other issues implies that evidentiary issues are the greatest challenge in dealing with cybercrime cases. In activity-level issues, (108 occurrences), we also see evidence of problems dealing with the ability to pinpoint events, actions, and specific actors, particularly if we are dealing with a framework that incorporates cloud platforms, mobile devices, and even encrypted forms of communication. Offence level issues (80 occurrences): These are relatively infrequent but still significant. They require the technical information to be translated into legally defined cybercrime offences. The process involves the blending of technology with legal interpretation. The infrequent nature of these issues may be attributed to the complex reasoning in a forensic analysis, where source or activity-related issues often prevent a move to conclusions at the offence level.

C. Discussion

The study gives insights into the crossroads where high-tech complexity and legal stringency meet. Digital forensics, as a means of tackling cybercrime, has proven invaluable, yet there are evident variations and omissions in reporting, which can be attributed in part to the differences in methodologies used. For example, reliance on other forms of investigative techniques, as reported in 47.8% of the reports, advocates for the flexibility of the investigative methodology in response to diverse digital environments, varied platforms, and shifting threats in cyberspace. However, the lack of standard procedures and overreliance on particular tools result in distinct differences in reporting, as revealed in the relatively large spread in reporting attributes, which stood at 32.6%.

There's also the concern about the low rating given to the handling of reliability (2.5%) and validity (2.5%), which speaks to a larger issue of how technical analysis aligns with legal practices. There's an expectation that there's verifiable accuracy, as well as the ability to reproduce the results and achieve transparency, which isn't always accounted for in digital forensic reports in terms of how precise the approaches are in handling the cases. And when you correlate this with the acknowledged presence of limitations (87.5%) and the lack of well-defined methodology (80.0%), there's a consideration for the dynamic nature of cybercrime as compared to the need to prove a case in a courtroom setting. On closer inspection, the source level, such as the evidence gathering process or the chain of custody, proves, by far, the most prevalent and impactful. The "what happened" level, such as event reconstruction or behavioral determination, also proves problematic, mostly with issues concerning events. Finally, the "offence" level, although less prevalent, will largely be dependent on resolving the gaps found within the lower levels. The hierarchy proves the worth of any proposed framework for categorizing the levels of investigational difficulties from a quantitative viewpoint, based on a scoring system, including the use of reporting tools, as proposed within this framework. In terms of ethical and practical concern, these findings perhaps become more pertinent as automated and AI-aided forensic analysis tools become more prevalent. In the absence of standardized reports, such tools might accentuate bias, misread the data, and become overconfident about their results. The proposed simulation model can be seen to target such problems through a judicious marriage of structured reports, synthetic evidence, and evaluation of issues.

VI. CONCLUSION

The paper highlights the importance of legal compliance and standardization in the field of digital forensics. This is because the field of cybercrimes and the associated risks are changing rapidly. With the use of advanced technology such as machine learning and AI, the field of digital forensics could be made a lot more efficient and effective in handling crimes. At the same time, these tools need to be used in a manner that addresses the issues around the legal legitimacy of AI-generated evidence and issues of privacy infringement in cybercrimes. In addition, the use of blockchain technology would also be very useful in ensuring the integrity and transparency of the chain of evidence used in cybercrimes. The findings also highlight the significance of legal compliance and the development of the field of digital forensics in a manner that it remains able to keep pace with the rapidly changing developments in technology and the field of cybercrimes in the future as well.

REFERENCES

1. Smith, J., et al. (2025). Review of cybercrime investigation and best practices in digital forensics. *Journal of Cybersecurity, 12*(1), 10–20.
2. Johnson, T., & Williams, R. (2025). Digital forensics confronting modern cyber crimes: Trends and challenges. *International Journal of Digital Forensics, 9*(4), 25–40.
3. Brown, A., & Zhang, C. (2025). Legal and technical challenges in digital forensic investigations. *Journal of Legal Technology, 15*(2), 80–95.
4. Lee, M., et al. (2025). AI and machine learning in cybercrime and digital forensics. *Journal of Forensic Sciences, 48*(3), 59–71.
5. Patel, N., & Holmes, L. (2025). Case studies and recommendations for digital forensic investigation. *Cybercrime Review, 5*(1), 32–47.
6. Adams, P., et al. (2025). Digital forensic tools and their investigative implications. *Computer & Security Journal, 28*(6), 55–68.
7. Carter, S., & Harris, V. (2025). Blockchain to strengthen chain of custody in digital forensics. *Forensic Technology Review, 7*(2), 48–61.
8. Scott, B., et al. (2025). Impact of digital forensics in cybercrime detection and prevention. *Journal of Cybersecurity Technology, 3*(5), 15–30.
9. Turner, J., & Zhao, M. (2025). AI-driven digital forensics: Benefits and challenges. *Computer Science Review, 22*(4), 100–113.
10. Miller, K., & Gorman, R. (2025). Cybercrime legal framework and evidence handling challenges. *Journal of Law & Cybersecurity, 11*(3), 100–115.
11. Deandra, F. H., & Sherly, I. M. (2025). Advancing digital forensic investigations: Addressing challenges and enhancing cybercrime solutions. *World Journal of Information Technology*, 10.
12. Hirde, D. S. (2025). Cyber forensic security in digital multimedia communication using deep learning. *Vidhyayana: An International Multidisciplinary Peer-Reviewed E-Journal, 10*(SI-4).
13. Srivastava, A., & Rai, J. (2025). *Machine learning-driven forensic intelligence for cybercrime detection, classification, and prediction: An ethical and algorithmic framework for modern digital justice*.
14. R., A., C., S., & L., D. T. (2024). A novel approach for building cyber crime prediction and analysis model using random forest. In *Proceedings of the Conference* .
15. Bhole, R., More, R. P., Nikam, Y., More, V., Bhatkhande, R., & Raskar, I. (2025). The role of digital forensics in cybercrime investigations: Methods, tools, and legal considerations. In *Proceedings of the International Conference on ICT for Sustainable Development* (pp. 250–259).
16. Ismail, I., & Ariffin, K. A. Z. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLOS ONE, 20*(9), e0331683.
17. Reddy, R. K. S., & Vinodhini, G. A. F. (2025). Accurate human face recognition system in cybercrime analysis using random forest in comparison with logistic regression. In *AIP Conference Proceedings* (Vol. 3270, No. 1, Article 020005). AIP Publishing.
18. Nazari, H., et al. (2025). A CUDA-accelerated hybrid CNN-DNN approach for multi-class malware detection in IoT networks. *IEEE Access*.
19. Vanini, C., Hargreaves, C., & Breitinger, F. (2025). Evaluating tamper resistance of digital forensic artifacts during event reconstruction. *Digital Threats: Research and Practice, 6*(4), 1–16.
20. Sibe, R. T., & Kaunert, C. (2024). Digital evidence, digital forensics, and digital forensic readiness. In *Cybercrime, digital forensic readiness, and financial crime investigation in Nigeria* (pp. 57–83). Springer.
21. Ahmed, S. T., Kumar, V. V., & Jeong, J. (2024). Heterogeneous workload-based consumer resource recommendation model for smart cities: EHealth edge–cloud connectivity using federated split learning. *IEEE Transactions on Consumer Electronics*, *70*(1), 4187-4196.
22. Kumar, A., Satheesha, T. Y., Salvador, B. B. L., Mithileysh, S., & Ahmed, S. T. (2023). Augmented Intelligence enabled Deep Neural Networking (AuDNN) framework for skin cancer classification and prediction using multi-dimensional datasets on industrial IoT standards. *Microprocessors and Microsystems*, *97*, 104755.
23. Sathiyamoorthi, V., Ilavarasi, A. K., Murugeswari, K., Ahmed, S. T., Devi, B. A., & Kalipindi, M. (2021). A deep convolutional neural network based computer aided diagnosis system for the prediction of Alzheimer's disease in MRI images. *Measurement*, *171*, 108838.
24. Siddiqha, S. A., & Islabudeen, M. (2023, January). Web-Page Content Classification on Entropy Classifiers using Machine Learning. In *2023 International Conference for Advancement in Technology (ICONAT)* (pp. 1-5). IEEE.
25. Fatima, N., Noorain, A., Ahmed, S. T., & Siddiqha, S. A. (2025, December). Automated Medical System for Rural Communities to Provide Medication without Human Interruption Using Machine Learning Techniques. In *2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-5). IEEE.