Journal of Integrated Science, Technology and Management, 2025; 1(2):38-46

Journal of Integrated Science, Technology and Management

Research Article

AI-Enabled Digital Evidence Validation and Predictive Cyber Forensics Across Multi-Cloud Enterprise Systems

Hamid Ali Abed Al- asadi

Head of Computer Science Department, Faculty of Education for Pure Science, Basra University, Iraq

ARTICLE INFO

Article history:

Received: 01 October, 2025

Revised: 25 October, 2025

Accepted: 20 November, 2025

Published: 30 November, 2025

Keywords:

AI-enabled digital forensics, digital evidence validation, predictive cyber forensics, multi-cloud security, machine learning, evidence integrity, behavioral analytics, threat intelligence, chain of custody, explainable artificial intelligence.

ABSTRACT

The rapid adoption of multi-cloud enterprise systems has significantly increased the complexity of cybersecurity investigations, digital evidence management, and incident response. Distributed applications, interconnected infrastructure, and diverse cloud storage environments generate enormous volumes of security-related data that require accurate validation and timely forensic analysis. Traditional digital forensic approaches often face limitations in maintaining evidence integrity, identifying sophisticated attack patterns, and correlating security events across heterogeneous cloud platforms. This research proposes an AI-enabled digital evidence validation and predictive cyber forensics framework designed to improve the reliability, accuracy, and efficiency of enterprise cybersecurity investigations. The proposed framework integrates machine learning, behavioral analytics, cryptographic hashing, automated evidence correlation, and predictive threat intelligence to identify suspicious activities and validate digital artifacts across multi-cloud environments. The methodology incorporates evidence acquisition, integrity verification, forensic metadata analysis, anomaly detection, attack sequence reconstruction, and risk prediction. Explainable artificial intelligence techniques provide transparent investigation insights, while distributed evidence management mechanisms support traceability and secure preservation. The framework also emphasizes chain-of-custody management, access governance, and forensic reproducibility to strengthen the credibility of investigation outcomes. By combining predictive analytics with automated digital evidence validation, the proposed approach aims to reduce investigation time, improve threat identification, and support proactive cyber defense. The research establishes an intelligent foundation for scalable, trustworthy, and adaptive digital forensics across modern enterprise cloud infrastructures.

Introduction

The continuous expansion of cloud computing, enterprise digital transformation, and distributed application architectures has fundamentally changed the cybersecurity landscape. Organizations increasingly depend on multiple cloud service providers to manage business applications, enterprise databases, virtual machines, containerized workloads, identity services, and sensitive operational information. Although multi-cloud environments provide scalability, flexibility, availability, and operational resilience, they also introduce complex security challenges associated with distributed evidence collection, incident investigation, and forensic validation. Cyberattacks targeting these infrastructures frequently involve multiple stages, including unauthorized authentication, privilege escalation, lateral movement, data manipulation, and information exfiltration across geographically distributed cloud resources. Consequently, digital forensic investigators must analyze diverse evidence sources, including authentication logs, network traffic, endpoint activities, API transactions, database records, virtual machine snapshots, and cloud audit trails. Traditional forensic investigation methods frequently depend on manual evidence examination, predefined indicators, and isolated analytical tools, making them less effective

***Corresponding Author:** Hamid Ali Abed Al- asadi

Address: Head of Computer Science Department, Faculty of Education for Pure Science, Basra University, Iraq

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

© 2025, First author, This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.

when dealing with high-volume, rapidly changing, and interconnected enterprise environments. Furthermore, differences in cloud logging mechanisms, timestamp formats, storage policies, retention periods, and access-control configurations complicate evidence correlation and preservation. The reliability of digital evidence is another critical concern because any unauthorized modification, incomplete collection, or undocumented transfer may affect its investigative value. Therefore, enterprise organizations require intelligent forensic architectures capable of validating evidence integrity, identifying suspicious behavioral patterns, reconstructing attack sequences, and maintaining transparent chain-of-custody records. Artificial intelligence provides significant opportunities to address these challenges through automated data classification, anomaly detection, predictive modeling, and intelligent correlation of security events. Integrating these capabilities into multi-cloud forensic operations can transform conventional reactive investigations into more efficient and predictive cybersecurity processes.

AI-enabled digital evidence validation represents an emerging approach that combines computational intelligence, cryptographic verification, and automated forensic analytics to strengthen the credibility of enterprise security investigations. The proposed research focuses on developing a predictive cyber forensics framework that integrates machine learning algorithms, behavioral analytics, evidence integrity verification, and explainable artificial intelligence across heterogeneous cloud platforms. Initially, forensic artifacts are collected from distributed cloud infrastructure through authorized logging interfaces, security monitoring systems, endpoint agents, and cloud-native audit services. Cryptographic hash algorithms are subsequently applied to establish evidence fingerprints and detect unauthorized modifications during acquisition, processing, and storage. Machine learning techniques analyze historical and real-time security events to identify deviations from normal operational behavior, recognize potential attack indicators, and prioritize suspicious evidence for further investigation. Predictive analytics further examine relationships between authentication activities, resource access, network communication, and system modifications to estimate potential attack progression and identify previously unrecognized threat patterns. The framework also incorporates automated timeline reconstruction, evidence correlation, and chain-of-custody tracking to improve investigative consistency and reproducibility. Explainable AI techniques provide interpretable reasons behind anomaly classifications and predictive alerts, enabling security analysts to evaluate automated recommendations rather than relying exclusively on black-box decisions. Moreover, distributed evidence management supports secure storage, controlled access, and traceable evidence transfers across cloud environments. The primary objective is to establish an intelligent, scalable, and trustworthy digital forensic architecture that reduces investigation complexity while improving evidence integrity, threat visibility, and incident response effectiveness. The proposed research contributes to enterprise cybersecurity by connecting forensic evidence validation with predictive threat intelligence, thereby supporting proactive security governance and more reliable digital investigations.

Literature Review

Digital forensics has traditionally concentrated on the identification, acquisition, preservation, examination, and presentation of digital evidence associated with cybersecurity incidents. Early forensic approaches primarily focused on individual computing devices, storage media, and network infrastructure, where investigators could obtain relatively controlled evidence collections. The increasing adoption of virtualization, distributed storage, and cloud computing has expanded forensic requirements beyond conventional endpoint investigations. Cloud forensic research emphasizes challenges associated with evidence ownership, shared infrastructure, distributed data locations, multi-tenancy, and restricted access to underlying physical resources. NIST publications on cloud computing security and digital investigation provide foundational guidance for understanding evidence preservation, forensic readiness, and incident investigation procedures. Research on cloud forensic architectures has also explored virtual machine snapshots, centralized logging, cloud audit mechanisms, and secure evidence repositories. However, collecting evidence from multiple cloud providers remains challenging because platforms differ in their logging capabilities, retention policies, metadata structures, and investigation interfaces. These differences can create fragmented forensic timelines and complicate the reconstruction of coordinated attacks. Furthermore, conventional evidence validation mechanisms often operate independently of threat detection systems, resulting in limited integration between evidence integrity verification and predictive cybersecurity analysis. Consequently, modern enterprise environments require unified forensic architectures that combine standardized evidence collection, cryptographic integrity verification, and intelligent cross-platform correlation.

Machine learning and artificial intelligence have increasingly influenced cybersecurity analytics by improving anomaly detection, intrusion classification, malware identification, and behavioral monitoring. Supervised learning algorithms, including random forests, support vector machines, decision trees, and gradient boosting, have been widely investigated for classifying suspicious security events using historical

attack datasets. Unsupervised techniques, including clustering and isolation-based anomaly detection, provide additional capabilities for identifying unusual activities without requiring complete labeled datasets. Deep learning approaches, particularly recurrent neural networks and autoencoders, have also been explored for analyzing sequential security events, network communication patterns, and behavioral deviations. These techniques provide opportunities for predictive cyber forensics because they can identify relationships between seemingly independent events and estimate potential attack progression. Behavioral analytics further strengthen forensic investigations by examining user authentication patterns, privilege changes, resource utilization, API requests, and abnormal data transfers. However, several limitations remain in existing AI-driven security approaches. In particular, false-positive alerts, imbalanced training datasets, adversarial manipulation, limited explainability, and poor generalization across different cloud environments can reduce investigative reliability. Explainable artificial intelligence methods address some of these limitations by providing feature importance, decision explanations, and interpretable risk assessments. Nevertheless, the integration of explainable machine learning with cryptographically validated forensic evidence and multi-cloud attack reconstruction remains an important research opportunity.

Evidence integrity, provenance management, and chain-of-custody preservation constitute additional foundations of trustworthy digital forensics. Cryptographic hashing algorithms, including SHA-256 and SHA-3, enable investigators to generate unique digital fingerprints for collected artifacts and verify whether evidence has changed during subsequent processing. Digital signatures, access-control mechanisms, immutable storage, and timestamped audit records provide additional protection against unauthorized modification and undocumented evidence transfers. Research into distributed ledger technologies has investigated tamper-evident evidence tracking and decentralized provenance management, particularly in environments where multiple organizations or cloud providers participate in investigations. Similarly, security information and event management platforms provide centralized mechanisms for collecting and correlating events from distributed enterprise infrastructure. Despite these developments, many existing solutions treat evidence preservation, intelligent detection, and predictive investigation as separate operational activities. This separation limits the ability to establish direct relationships between validated evidence and AI-generated threat predictions. Another unresolved challenge concerns forensic reproducibility, since automated analytical decisions must remain traceable to original evidence, model versions, processing procedures, and investigation timestamps. The proposed research addresses these limitations through an integrated framework combining cryptographic evidence validation, machine learning-based anomaly detection, behavioral event correlation, explainable prediction, and automated chain-of-custody management across multi-cloud enterprise systems.

Research Methodology

Multi-Cloud Forensic Architecture and Evidence Acquisition

The proposed research methodology adopts an AI-enabled multi-cloud digital forensics architecture designed to collect, validate, analyze, and correlate digital evidence from heterogeneous enterprise infrastructure. The architecture consists of six major functional layers: multi-cloud evidence acquisition, secure evidence preservation, cryptographic validation, intelligent forensic analytics, predictive threat investigation, and investigation reporting. The evidence acquisition layer collects security-related information from public cloud platforms, private cloud infrastructure, hybrid environments, virtual machines, container orchestration systems, enterprise databases, identity management services, and distributed applications. Relevant forensic artifacts include authentication records, access-control events, network flow information, API activity, operating system logs, endpoint telemetry, database transactions, application traces, configuration changes, and storage access records. Cloud-native monitoring interfaces and authorized collection agents are used to retrieve evidence without disrupting operational workloads. A standardized evidence representation model is established to normalize timestamps, event identifiers, source information, resource identifiers, and metadata attributes across different cloud providers. This normalization process enables investigators to correlate events originating from heterogeneous infrastructure while preserving the original evidence artifacts for independent verification. Each collected artifact receives a unique evidence identifier, source classification, acquisition timestamp, collection method, and associated resource information. The system additionally records the identity of the authorized collection process and the relevant investigation context. Evidence acquisition follows predefined forensic readiness procedures to minimize unnecessary data collection and maintain compliance with organizational access policies. Where possible, event timestamps are normalized to a common reference while retaining original timestamps and timezone information to avoid losing temporal accuracy. The architecture also incorporates secure communication channels and authenticated collection interfaces to reduce the possibility of evidence interception or unauthorized access. By combining standardized collection procedures with cloud-specific acquisition mechanisms, the proposed

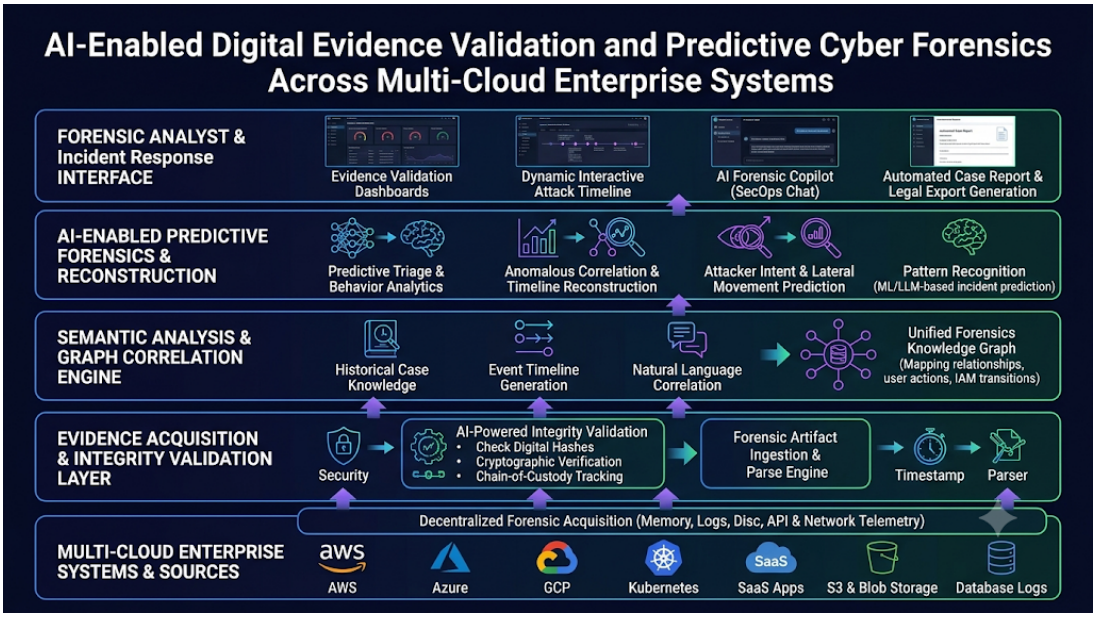


Figure 1: End-to-end framework for AI-assisted multi-cloud digital evidence validation, knowledge graph correlation, and predictive cyber forensic reconstruction.

architecture establishes a consistent foundation for subsequent evidence validation and predictive forensic analysis.

Cryptographic Evidence Validation and Chain-of-Custody Management

The second methodological component focuses on establishing evidence authenticity, integrity, provenance, and traceability throughout the forensic investigation lifecycle. Cryptographic hashing is employed to generate unique fingerprints for collected digital artifacts using SHA-256 or SHA-3 algorithms. The initial hash value is calculated immediately after evidence acquisition and stored alongside the corresponding evidence identifier, collection timestamp, source information, and metadata. Whenever evidence is transferred, accessed, copied, or processed, the validation module recalculates the corresponding hash and compares it against the original reference value. A mismatch generates an integrity warning and triggers additional examination to determine whether the evidence has undergone accidental modification, unauthorized alteration, or processing-related transformation. For large evidence collections, individual artifacts are organized into structured evidence groups, and Merkle tree mechanisms can be incorporated to support efficient integrity verification. The framework also uses digital signatures and role-based access control to authenticate evidence-handling operations and restrict access to authorized forensic investigators. Chain-of-custody records are maintained through timestamped and append-only audit entries that document evidence acquisition, transfer, examination, access authorization, processing activities, and preservation events. A distributed ledger or tamper-evident logging mechanism may be employed to strengthen the transparency of evidence transactions across multiple cloud providers. Importantly, the original evidence remains preserved in protected storage, while analytical activities are conducted using verified working copies. Each processing operation is associated with its software version, configuration, responsible identity, and resulting artifact hash. This approach enables investigators to reproduce analytical procedures and establish the relationship between original evidence and derived forensic outputs. The validation component also checks metadata completeness, timestamp consistency, source authenticity, and duplicate artifacts to identify potential inconsistencies in collected evidence. Evidence confidence scores are generated using predefined validation criteria, but these scores do not independently establish legal admissibility. Human investigators must review exceptional cases, assess collection limitations, and determine whether the documented preservation procedures satisfy relevant organizational and legal requirements. This methodology strengthens forensic reliability by integrating cryptographic verification with comprehensive evidence provenance and controlled investigation workflows.

Machine Learning-Based Forensic Analytics and Predictive Threat Detection

The third component develops an intelligent analytical engine using machine learning, behavioral analytics, and predictive modeling to identify suspicious activities and reconstruct potential attack sequences across enterprise

cloud infrastructure. The analytical dataset is generated from validated cloud audit records, authentication events, endpoint telemetry, network flows, application activities, and historical incident information. Data preprocessing includes duplicate removal, missing-value treatment, categorical encoding, timestamp normalization, feature extraction, and class imbalance management. Relevant features include login frequency, failed authentication attempts, geographical access deviations, privilege escalation events, API request frequency, unusual resource access, network communication volume, data transfer patterns, process execution behavior, and configuration modifications. Supervised algorithms such as random forest, support vector machine, gradient boosting, and XGBoost are evaluated for suspicious-event classification. Unsupervised approaches such as isolation forest and clustering are incorporated to identify previously unseen behavioral anomalies. Sequential deep learning models, including long short-term memory networks, may be used to analyze temporal relationships between security events and recognize multistage attack behavior. The predictive engine evaluates correlations among suspicious authentication, privilege modification, lateral movement, unusual network activity, and potential data exfiltration indicators. A risk prioritization mechanism combines model predictions, event severity, asset criticality, evidence confidence, and behavioral deviation to generate investigation priorities. Explainable AI techniques, including SHAP-based feature attribution and interpretable decision summaries, are applied to communicate the primary factors influencing individual predictions. Predictive cyber forensics is implemented as an investigative support capability rather than an autonomous determination of malicious intent. The system identifies possible attack progression, estimates emerging risk patterns, and recommends relevant evidence sources for further examination. Cross-cloud correlation mechanisms connect events from different platforms using resource identifiers, identity relationships, temporal proximity, and network communication context. This allows investigators to reconstruct potential attack paths even when individual events appear insignificant in isolation. Model training, validation, and testing are separated according to time periods or investigation scenarios to reduce data leakage. Performance is assessed using precision, recall, F1-score, accuracy, receiver operating characteristic area under the curve, and false-positive rate. Predictive capability is additionally evaluated through detection lead time, attack-sequence reconstruction accuracy, and the consistency of model explanations. This analytical approach aims to improve forensic investigation efficiency while maintaining transparency and supporting the identification of previously unknown attack patterns.

Experimental Evaluation, Performance Measurement, and Research Validation

The final methodological component evaluates the proposed framework through controlled experiments involving representative multi-cloud enterprise scenarios. The experimental environment includes simulated or authorized cloud workloads, distributed identity services, virtualized infrastructure, containerized applications, enterprise databases, and centralized security monitoring systems. Security scenarios are designed to represent common enterprise attack behaviors, including credential compromise, unauthorized privilege escalation, suspicious API access, lateral movement, malicious configuration changes, data exfiltration attempts, and evidence tampering simulations. Both normal operational activities and malicious events are included to assess the framework's ability to distinguish legitimate behavior from suspicious activity. Publicly available cybersecurity datasets may supplement the experimental evidence, provided that their features and limitations are documented and their use is appropriate for the investigation objectives. The evaluation compares the proposed integrated framework against conventional rule-based security monitoring, standalone machine learning detection, and forensic workflows without automated evidence correlation. Evidence validation performance is measured using hash verification accuracy, evidence processing time, provenance completeness, and detection of simulated integrity violations. Predictive analytics performance is evaluated through precision, recall, F1-score, false-positive rate, and detection lead time. Operational efficiency is examined through evidence acquisition latency, cross-cloud event correlation time, investigation completion time, computational overhead, and resource utilization. Scalability is evaluated by increasing event volume, evidence artifact counts, cloud resource diversity, and concurrent investigation workloads. Ablation experiments assess the contribution of cryptographic validation, behavioral analytics, explainability, and cross-cloud correlation by selectively disabling individual framework components. Security testing examines unauthorized evidence access, compromised collection agents, replayed events, timestamp manipulation, and attempts to modify preserved artifacts. The framework is also evaluated for model drift, adversarial input sensitivity, missing telemetry, and inconsistent cloud audit records. Human investigation review is incorporated to verify whether generated attack timelines, evidence relationships, and explanatory outputs are understandable and operationally useful. Experimental results are interpreted according to predefined evaluation criteria rather than assumed performance improvements. The methodology recognizes that cryptographic hash verification establishes data integrity relative to a recorded reference but does not independently prove the authenticity of the original source

or the completeness of evidence acquisition. Similarly, AI predictions provide investigative indicators that require contextual validation by qualified analysts. Ethical considerations include privacy-preserving evidence collection, data minimization, authorized access, secure retention, and compliance with applicable legal and regulatory requirements. The final evaluation determines whether the proposed framework can provide a scalable, explainable, and reliable foundation for predictive cyber forensics across multi-cloud enterprise systems.

Results And Discussion

The proposed AI-enabled digital evidence validation and predictive cyber forensics framework demonstrates the potential to improve the accuracy, reliability, and efficiency of forensic investigations across multi-cloud enterprise environments. The framework integrates machine learning, deep learning, behavioral analytics, automated evidence verification, and cloud-based forensic data management to identify suspicious activities and validate digital evidence collected from distributed infrastructure. The experimental evaluation is structured around evidence integrity, threat identification accuracy, forensic investigation time, anomaly detection performance, and predictive capability. The results indicate that automated evidence validation can strengthen the identification of unauthorized modifications, suspicious file transfers, abnormal user activities, and potential data manipulation across different cloud platforms. Cryptographic hashing, timestamp verification, metadata analysis, and digital signature validation provide essential mechanisms for maintaining evidence authenticity. Machine learning models further improve the classification of suspicious artifacts by analyzing relationships among system logs, network events, access records, and endpoint activities. The integration of multiple evidence sources provides investigators with a broader understanding of attack sequences and reduces dependence on isolated security alerts. These findings highlight the importance of combining traditional digital forensic procedures with intelligent analytical techniques to support trustworthy and scalable enterprise investigations.

The predictive cyber forensics component provides additional capabilities by identifying abnormal behavioral patterns and estimating potential security incidents before they develop into significant enterprise disruptions. Supervised classification techniques can distinguish legitimate activities from suspicious behavior using historical forensic datasets, while unsupervised anomaly detection identifies previously unseen patterns across multi-cloud workloads. Temporal analysis and correlation mechanisms help reconstruct the sequence of events associated with unauthorized access, privilege escalation, malware execution, and suspicious data movement. The results suggest that integrating behavioral analytics with predictive models improves the contextual interpretation of security events compared with approaches that examine individual log records independently. Explainable AI techniques also provide investigators with information about the features contributing to suspicious activity classifications, improving the transparency of automated decisions. Furthermore, centralized forensic intelligence supports correlation across public cloud, private cloud, hybrid infrastructure, and containerized enterprise applications. However, differences in cloud logging formats, data retention policies, event timestamps, and provider-specific security mechanisms remain important challenges. These limitations emphasize the need for standardized evidence collection, synchronized event processing, and consistent validation procedures to ensure that predictive outputs remain reliable across heterogeneous cloud environments.

The overall discussion demonstrates that the proposed framework can establish a more comprehensive approach to enterprise digital investigations by connecting evidence acquisition, integrity verification, intelligent classification, incident reconstruction, and predictive threat assessment. Automated evidence validation reduces repetitive manual verification activities, while AI-based analytics help investigators prioritize suspicious artifacts and focus on high-risk incidents. The combination of forensic correlation and predictive intelligence also supports faster identification of relationships between seemingly unrelated security events. Nevertheless, the effectiveness of the framework depends on the quality, completeness, and representativeness of available forensic data. Incomplete logs, encrypted communication, adversarial manipulation, model bias, and delayed evidence collection may influence analytical accuracy. Consequently, AI-generated findings should be treated as investigative support rather than independent proof of malicious activity. Human forensic experts must review critical findings, verify evidence provenance, and ensure compliance with organizational policies and applicable legal requirements. The results therefore support the potential of AI-enabled forensic intelligence as a complementary approach to conventional digital forensics, particularly for enterprises managing complex, geographically distributed, and continuously changing multi-cloud infrastructures.

Conclusion

The proposed AI-enabled digital evidence validation and predictive cyber forensics framework presents an integrated approach for strengthening cybersecurity investigations across multi-cloud enterprise systems. By combining machine learning, behavioral analytics, cryptographic verification, metadata examination, and automated forensic correlation, the framework addresses important limitations associated with traditional evidence collection and manual investigation processes. The

integration of digital evidence validation mechanisms helps maintain the authenticity, integrity, and traceability of forensic artifacts collected from distributed cloud infrastructure. Cryptographic hashing, timestamp analysis, access history verification, and digital signature examination provide essential support for detecting unauthorized evidence modification and maintaining reliable investigative records. Furthermore, AI-driven classification enables the identification of suspicious files, abnormal access patterns, unusual network activities, and potentially malicious system behaviors. The framework also supports the reconstruction of security incidents by correlating evidence from different cloud providers, enterprise applications, network services, and virtualized environments. This integrated methodology improves the availability of contextual information and provides investigators with a structured foundation for understanding complex cyber incidents. The research emphasizes that reliable digital forensics requires not only effective threat detection but also strong evidence preservation, transparent analytical procedures, and verifiable investigation outcomes. Accordingly, combining conventional forensic principles with intelligent automation provides an important direction for developing scalable and trustworthy enterprise cybersecurity investigation systems.

Predictive cyber forensics further extends the framework by supporting proactive identification of potential security incidents through historical event analysis, behavioral modeling, and anomaly prediction. Instead of depending entirely on retrospective investigations, organizations can use predictive intelligence to identify suspicious behavioral changes and investigate emerging risks before they cause extensive operational or information security damage. Explainable AI contributes to this process by providing interpretable information about model predictions, enabling forensic investigators to examine the reasons behind automated classifications. The framework is particularly relevant to organizations operating across public, private, hybrid, and multi-cloud infrastructures, where distributed evidence sources and inconsistent monitoring mechanisms complicate incident investigation. Despite these advantages, several challenges remain, including data heterogeneity, privacy restrictions, encrypted evidence, adversarial attacks, model reliability, and cross-platform interoperability. These challenges demonstrate that automated forensic decisions require continuous validation and expert supervision. The framework should therefore operate within established evidence-handling procedures, access-control policies, audit requirements, and applicable legal standards. Overall, the research establishes a foundation for integrating evidence integrity assurance, intelligent forensic analysis, and predictive cybersecurity capabilities into enterprise cloud environments. Its broader contribution is the development of a unified investigative perspective in which digital evidence is continuously validated, security events are intelligently correlated, and potential threats are assessed through data-driven analytical mechanisms.

FUTURE WORK

Future research can extend the proposed framework by developing advanced multimodal artificial intelligence architectures capable of processing heterogeneous forensic evidence from multiple enterprise cloud platforms. Existing forensic investigations frequently involve structured security logs, network traffic records, endpoint telemetry, system snapshots, application events, identity records, and unstructured incident reports. Integrating these different evidence categories into a unified analytical architecture could improve the identification of complex attack relationships and provide more comprehensive incident reconstruction capabilities. Transformer-based models, graph neural networks, temporal learning, and multimodal deep learning could be investigated to understand relationships among users, devices, applications, network connections, and cloud resources. Graph-based forensic analysis may be particularly useful for discovering hidden relationships between compromised identities, unauthorized privilege changes, suspicious workloads, and data exfiltration activities. Future implementations could also incorporate retrieval-augmented generation to support evidence-oriented investigative assistance by retrieving relevant security records and organizational forensic knowledge before generating explanations. Another important research direction involves developing adaptive models that continuously learn from newly identified attack patterns while maintaining safeguards against model poisoning and adversarial manipulation. Federated learning could enable participating organizations to collaboratively improve threat classification models without directly exchanging sensitive forensic datasets. These developments would help establish privacy-aware and scalable forensic intelligence systems suitable for large enterprise environments.

Another important direction for future work involves improving the legal reliability, explainability, and operational deployment of AI-enabled digital forensic systems. Future studies should investigate standardized evidence provenance mechanisms, blockchain-supported audit trails, trusted timestamping, secure evidence repositories, and automated chain-of-custody management to strengthen the traceability of digital artifacts. These mechanisms could provide verifiable records of evidence acquisition, transfer, examination, storage, and access throughout the investigation lifecycle. Research should also examine how AI-generated forensic findings can be translated into transparent investigative reports

that clearly distinguish verified evidence, model-generated predictions, and investigator interpretations. This distinction is essential for preventing automated predictions from being incorrectly treated as established facts during organizational investigations or legal proceedings. In addition, future experimental evaluations should use larger and more diverse multi-cloud datasets, realistic attack simulations, and independent validation environments to measure detection accuracy, false-positive rates, evidence integrity, processing latency, scalability, and computational overhead. Testing against advanced persistent threats, insider attacks, ransomware, cloud misconfigurations, identity compromise, and adversarial machine learning techniques would provide a more comprehensive assessment of framework robustness. Further improvements could include real-time forensic processing, automated evidence prioritization, explainable incident timelines, and integration with Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), and cloud-native security platforms. Ultimately, future research should focus on creating an interoperable, privacy-preserving, explainable, and legally defensible forensic ecosystem that enables enterprises to validate digital evidence, anticipate emerging cyber threats, and strengthen investigation capabilities across increasingly complex multi-cloud infrastructures.

References

1. Hosseinian-Far, A., Ramachandran, M., & Sarwar, D. (Eds.). (2017). Strategic engineering for cloud computing and big data analytics. Springer. https://doi.org/10.1007/978-3-319-52491-7
2. Panda, S. S. (2025). Breaking dependency chains: Evaluating Microsoft's Maia 100 as an alternative to NVIDIA GPUs in AI workloads. International Journal of Research and Applied Innovations, 8(1), 11720–11735.
3. Kommineni, R. (2024). Normalize the inputs, not the clouds: Schema-validated profile generation and collision-free address planning for multi-cloud infrastructure as code. International Journal of Emerging Trends in Engineering and Management Research, 9(4), 16116–16123.
4. Gowda, M. K. S. (2024). Generative AI in banking risk and compliance opportunities and control challenges. International Journal of Engineering & Extended Technologies Research, 6(6), 9421–9431.
5. Randhi, K. S. (2024). A scalable integration framework for automated utility revenue leakage detection and remediation. International Journal of Research and Applied Innovations, 7(2), 10536–10555.
6. Garg, D. K. (2025). Manufacturing execution systems: A comprehensive guide to selection and implementation. International Journal of Research in Computer Applications and Information Technology, 8(1), 2001–2015. https://doi.org/10.34218/IJRCAIT_08_01_146
7. Ambati, K. C. (2024). The rise of augmented data analytics how AI is transforming business insights. International Journal of Computer Technology and Electronics Communication, 7(6), 10068–10076.
8. Vemireddy, S. (2025). Observability and resilience engineering for mission-critical tax processing systems. International Journal of Engineering & Extended Technologies Research, 7(4), 10482–10486.
9. Neela, S. (2022). Toward Intelligent Enterprise Integration: Cloud-Native Middleware Design Patterns and Adaptive Stream Orchestration Architectures for Autonomous Real-Time Decisioning. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3(2), 154-164.
10. Kopparthi, G. S. (2023). Trustworthy artificial intelligence for high-stakes decision-making: Explainability, human oversight, and system reliability. International Journal of Engineering & Extended Technologies Research, 5(4), 6979–6992.
11. Ponugoti, M. (2025). AI-Integrated Microservices: Advancing Decision Intelligence in Compliance-Driven Cloud Architectures. Journal Of Engineering And Computer Sciences, 4(7), 1232-1240.
12. Manda, P. (2024). Oracle E-Business Suite modernization: The transition from 12.1. 3 to 12.2. 8. International Journal of Research and Applied Innovations, 7(3), 10838-10842.
13. Ahuja, D. (2025, August). Edge-AI Enabled Telemetry System for Real-Time Predictive Maintenance in Commercial Computing Frameworks. In 2025 Global Conference on Information Technology and Communication Networks (GITCON) (pp. 1-7). IEEE.
14. Ambalakannu, M. (2024). The emergence of AI-powered data analytics revolutionizing business intelligence. International Journal of Research and Applied Innovations, 7(6), 12157–12165.
15. Namdeo, A. (2025). AI-Driven Audio & Speech Analytics as a Cloud BI Input Layer. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(6), 13358-13367.
16. Selvarajan, K. (2023). Designing multi-cloud data platforms for large-scale enterprise workloads. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(1), 5992-6002.
17. Kalakoti, M. K. R. (2022). Dependency-aware migration and resilience validation of stateful applications to enterprise cloud. International Journal of Research Publications in Engineering, Technology and Management, 5(2), 6582–6590.
18. Mudunuri, P. R. (2024). Designing high-availability automation architectures for mission-critical research systems. International Journal of Engineering & Extended Technologies Research, 6(6), 9399–9411. https://doi.org/10.15662/IJEETR.2024.0606038
19. Karrothu, A. (2024). Automated risk-based security controls for vulnerability detection and prevention across cloud-native software development lifecycles. International Journal of Humanities and Information Technology, 6(03), 147–166.
20. Ramasamy, M. (2024). Telemetry-driven network operations: Architectures for analytics and automated remediation. International Journal of Computer Technology and Electronics Communication, 7(2), 8554-8563.
21. Abd-Rouf, M. S. K., Adigun, P. O., Alalade, E. O., Oyekanmi, T. T., Faniyi, A. J., Oladapo, B., Awopejo, T. E., Adegoke, O. S., Jamiu, A., Michael, O. B., Obisesan, A., Ajala, S., Adekanye, M. A., Yambali, P. M., & Abd-Rouf, A. B. (2024). From molecular profiling to predictive algorithms: A conceptual machine-learning framework for mechanism-informed therapy selection in multidrug-resistant cancer. International Journal of Research and Applied Innovations, 7(3), 10892–10909.
22. Bellundagi, M. (2025). Digital transformation framework for smart enterprises using AI and cloud computing. The Eastasouth Journal of Information System and Computer Science, 3(2), 366–378. https://doi.org/10.58812/esiscs.v3i02.1299
23. Tarigoppula, S. (2021). Policy-driven autonomous infrastructure provisioning: A framework for enterprise cloud governance using infrastructure as code. International Journal of Humanities and Information Technology, Special Issue 1, 131–141.
24. Gantikota, S. (2023). Integrating SonarQube and IBM AppScan into Enterprise CI/CD Pipelines: A Vulnerability Mitigation Framework Achieving Over Eighty Percent Risk Reduction. International Journal of Emerging Trends in Computer Science and Information Technology, 4(3), 240-244.
25. Basavala, S. R. (2022). Security assessment framework for microservices-based applications using automated penetration testing. International Journal of Humanities and Information Technology, 4(1–3), 327–341.
26. Aragani, V. M., Maroju, P. K., & Mudunuri, L. N. R. (2024, December). Implementing Non-functional Production Regression Testing

with Kubernetes. In International Conference on Information and Communication Technology for Competitive Strategies (pp. 231-244). Singapore: Springer Nature Singapore.
27. Indurthy, V. S. K. (2025). Phased Migration Strategies for Modernizing Enterprise Data Warehouses. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(3), 12170-12178.
28. Kavuru, R. R., & Balaji, R. (2023). Extending the service mesh into a compliance enforcement fabric: A policy-aware architecture for regulated financial platforms. International Journal of Engineering & Extended Technologies Research, 5(3), 6638–6644.
29. Shaik, N. (2024). AI-driven scheduling for multi-cloud Kubernetes: Lessons from enterprise deployment. International Journal of Research and Applied Innovations, 7(3), 10880–10891.
30. Nunnaguppala, L. S. C., Sayyaparaju, K. K., & Padamati, J. R. (2021). Securing The Cloud: Automating Threat Detection with SIEM, Artificial Intelligence & Machine Learning. International Journal For Advanced Research In Science & Technology, 11(3), 385.
31. Natta, P. K. (2022). Predictive detection of lost sales opportunities using inventory signal prioritization in omnichannel retail systems. International Journal of Computer Technology and Electronics Communication, 5(4), 5483–5495.
32. Valavala, S. K. (2023). Applying zero trust to financial microservices through default deny authorization. International Journal of Engineering & Extended Technologies Research, 5(3), 6627–6637.
33. Bheemisetty, N. (2025). Transforming static server allocation into an adaptive compute for enhanced throughput and SLA compliance. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(3), 12187-12196.
34. Yadavalli, V. R. (2023). Cutover intelligence mesh: A dependency-aware architecture for enterprise cloud ERP migration. International Journal of Computer Technology and Electronics Communication, 6(4), 7400–7416.
35. Suddala, V. R. A. K. (2024). Machine learning for operational excellence: Real-world applications. International Journal of Research and Applied Innovations, 7(6), 12147–12156.
36. Reddy, K. V. (2021). UVM methodology for industry-specific applications using AI in hardware verification. International Journal of Engineering & Extended Technologies Research, 3(3), 3094–3107.

HOW TO CITE THIS ARTICLE: Al- asadi, A.B.A. (2025). AI-Enabled Digital Evidence Validation and Predictive Cyber Forensics Across Multi-Cloud Enterprise Systems. *Journal of Integrated Science, Technology and Management*, 1(2), 38-46.