JISTecS: Journal of Information Systems, Technology and Security
ISSN 3125-1099 (online)
Vol. 1 Iss. 1 Pg. 1-19
https://ejournal.scmdigi.id/index.php/jistecs

Digital forensics in the era of cyber law: challenges of cloud computing and data privacy

Rostiana Utami*, Salma Julita
Universitas Mega Buana Palopo, Sulawesi Selatan, Indonesia
*Correspondence author: rostiana.utami@yahoo.com
DOI: https://doi.org/10.65881/jistecs.v1i1.49

ARTICLE INFO

History:
Received: 04-09-2026
Revised: 04-13-2026
Accepted: 04-14-2026
Published: 04-16-2026

Keywords:
digital forensics;
cyber law;
cloud computing;
data privacy;
digital investigations.

ABSTRACT

Purpose: to analyze the key challenges of digital forensics in the context of cloud computing and cyber law, identify the limitations of existing approaches, and propose an integrative framework to enhance the effectiveness of digital investigations while ensuring compliance with data protection principles.
Method: this study uses a qualitative descriptive approach based on a literature review, with thematic and normative analysis to examine technical and legal aspects of digital forensics in cloud environments.
Findings: digital forensics in cloud environments faces significant challenges, including limited access and control over data, architectural complexity, jurisdictional barriers, and conflicts with data protection regulations. These issues affect the integrity, authenticity, and availability of digital evidence, while existing forensic methods are often inadequate to address the dynamic and distributed nature of cloud systems.
Implications: the need for adaptive forensic methods, stronger collaboration with cloud service providers, and the development of integrated frameworks and international standards to ensure effective investigations while maintaining compliance with data protection principles.
Originality: providing an integrated analysis that bridges technical digital forensics challenges in cloud environments with cyber law and data protection frameworks, presenting a holistic approach that has been largely overlooked in prior research.

Introduction

The rapid development of information technology has driven digital transformation across various sectors, including law enforcement practices and the investigation of technology-based crimes (Mahmood et al., 2025). Digital forensics has emerged as a crucial discipline for identifying, collecting, analyzing, and presenting digital evidence in legal proceedings (Karagiannis & Vergidis, 2021). However, in the evolving era of cyber law, the landscape of digital forensics is undergoing significant

changes due to the adoption of cloud computing and the increasing emphasis on personal data protection (Malik et al., 2024). Cloud computing offers flexibility, scalability, and efficiency, but it also introduces new complexities in the acquisition and validation of digital evidence, as data is distributed across multiple jurisdictions and controlled by third parties (Karagiannis & Vergidis, 2021). Meanwhile, increasingly stringent data protection regulations create a dilemma between the needs of investigation and the protection of individual privacy rights (Kerber, 2022).

This situation gives rise to increasingly complex and multidimensional research problems. In the context of cloud computing, data is no longer stored centrally on a single physical device; rather, it is distributed across multiple servers that may be located in different geographic regions and managed by third-party service providers (Akhtar et al., 2021). This condition creates challenges in maintaining the integrity and authenticity of digital evidence, as the data acquisition process must rely on mechanisms that are not entirely under the control of investigators. Furthermore, the elastic and dynamic characteristics of cloud environments, such as auto-scaling, virtualization, and multi-tenancy, cause data to change rapidly or even be automatically deleted, thereby increasing the risk of losing critical digital traces that are essential to the investigative process.

On the other hand, cross-border jurisdictional barriers constitute a significant challenge, as data relevant to a particular case may be stored in multiple countries with differing legal systems and regulatory frameworks (Xia et al., 2024). This situation complicates the legal process of obtaining access to such data, particularly when it requires time-consuming international cooperation and complex procedural mechanisms. The problem is further exacerbated by the increasing use of end-to-end encryption and other security technologies, which, while essential for protecting user privacy, simultaneously limit the ability of law enforcement authorities to effectively access and analyze digital evidence.

Furthermore, there is a growing potential for conflict between law enforcement interests and personal data protection policies. Regulations such as data minimization principles and user consent requirements often limit investigators' ability to collect evidence, thereby creating ethical and legal dilemmas (Vlahou et al., 2021). In this context, traditional digital forensic practices that focus on the acquisition of physical devices, such as hard drives or local computers, are becoming increasingly less relevant. Distributed and service-based cloud environments demand more adaptive forensic methods, including remote acquisition techniques, log-based analysis, and collaboration with cloud service providers (Alashhab et al., 2022). Therefore, a new approach is required, one that not only addresses technical challenges but also aligns with legal frameworks and ethical principles, in order to ensure a balance between the effectiveness of investigations and the protection of individual privacy rights.

Numerous prior studies have examined the technical aspects of digital forensics in cloud environments, including data acquisition methods and techniques for analyzing digital evidence (Alshabibi et al., 2024; Karagiannis & Vergidis, 2021; Malik et al., 2024; Prakash et al., 2022). Other studies have also highlighted legal implications related to data protection and jurisdiction within the framework of cyber law (Andraško et al., 2021; Lim & Oh, 2025). However, most of this research remains partial in nature, with a fragmented focus that separates technical aspects from legal considerations, and has yet to comprehensively integrate the challenges of cloud computing with modern data protection frameworks. This research gap indicates the need for a more holistic approach to bridge the demands of digital forensic investigations with compliance to

privacy regulations. The novelty of this study lies in its holistic integration of technical, legal, and ethical dimensions into a unified framework for cloud-based digital forensics, while simultaneously taking into account the dimensions of cyber law and data protection.

The purpose of this research is to analyze the main challenges of digital forensics in the context of cloud computing and cyber law, to identify the limitations of existing approaches, and to formulate a strategy or framework that can improve the effectiveness of digital investigations without compromising data protection principles. This research is important because the increasing reliance on cloud services, along with the growing complexity of privacy regulations, demands adaptive and balanced solutions. Therefore, this study is expected to provide theoretical contributions to the development of a more comprehensive concept of digital forensics, as well as practical contributions in the form of recommendations for practitioners, law enforcement agencies, and policymakers in addressing the increasingly complex challenges of the digital era.

Method

The research method employed in this study is a qualitative approach with a descriptive-analytical research design, aimed at gaining an in-depth understanding of the challenges of digital forensics within the context of cloud computing and cyber law. This approach was selected because it is capable of providing a comprehensive overview of complex phenomena, particularly those involving technical, legal, and ethical aspects simultaneously. The study was conducted through a literature review by examining various relevant sources, including scientific journals, academic books, research reports, international standards, as well as regulations related to digital forensics, cloud computing, and personal data protection. The data collection technique was carried out by identifying, classifying, and analyzing literature relevant to the research topic. The data sources include reputable scientific publications, policy documents from international institutions, as well as legislative and regulatory frameworks related to cyber law and data privacy. To ensure the validity and reliability of the data, the researcher applied strict source selection criteria, such as the credibility of the publisher, the recency of the publication year, and the substantive relevance to the research focus.

The data were analyzed using qualitative analysis techniques with a thematic approach, in which the researcher identified patterns, key issues, and relationships among concepts emerging from the literature. Subsequently, a synthesis was conducted to integrate these findings into a holistic analytical framework, enabling the identification of research gaps and the formulation of relevant solutions or new approaches. In this process, the researcher also conducted a comparative analysis between traditional and modern digital forensic practices to assess their effectiveness in cloud environments. In addition, this study employed a normative approach in analyzing legal aspects by examining applicable regulations and data protection principles. This approach aimed to evaluate the alignment between digital forensic practices and existing legal frameworks, as well as to identify potential conflicts that may arise. By combining descriptive qualitative and normative approaches, this study is expected to produce a comprehensive analysis and provide practical recommendations for the advancement of digital forensics in the era of cloud computing and cyber law.

Results and discussion

The findings of this study indicate that digital transformation driven by the adoption of cloud computing has significantly reshaped digital forensic practices, both technically and legally (Karagiannis & Vergidis, 2021; Malik et al., 2024). Based on the literature review, it was found that the process of acquiring digital evidence in cloud environments faces limitations in direct access to physical infrastructure, resulting in investigators being highly dependent on cloud service providers (Alshabibi et al., 2024; Karagiannis & Vergidis, 2021; Malik et al., 2024). This dependency leads to reduced control over the evidence collection process and increases the risk to the integrity and authenticity of data. Moreover, variations in logging mechanisms and data storage across different service providers result in the absence of standardized procedures for obtaining and verifying digital evidence (David et al., 2021; Karagiannis & Vergidis, 2021; Singh et al., 2022).

This study also found that the inherent characteristics of cloud computing, such as virtualization and multi-tenancy, pose significant challenges in the process of identifying and isolating data relevant to a particular case (Hashim & Hussein, 2024; Narasayya & Chaudhuri, 2021). Data residing in shared environments may become intermingled with that of other users, thereby increasing the risk of privacy violations. Furthermore, the elastic nature of cloud computing causes data to change dynamically, complicating the process of reconstructing event chronology (timeline analysis) (Choudhary, 2025; Żurkowski & Zieliński, 2024). In some cases, the required data may no longer be available, as it may have been automatically deleted by the system.

From a legal perspective, the findings indicate a fundamental misalignment between the operational needs of digital forensics and the existing data protection regulatory framework. Data protection regulations generally emphasize principles such as purpose limitation, data minimization, and the requirement for obtaining data subject consent (Vlahou et al., 2021). In practice, these principles often restrict investigators' ability to access, collect, and process data necessary for evidentiary purposes. The data acquisition process must follow strict legal procedures, such as court orders or special authorizations, which can be time-consuming and potentially hinder rapid response in investigations of dynamic cyber incidents.

Furthermore, this study found that there is ambiguity in the interpretation of regulations regarding law enforcement access to data, particularly when such data is managed by third parties, such as cloud service providers (Tosza, 2021). In some cases, service providers tend to exercise caution or even refuse to grant data access, citing user privacy protection and compliance with local or international regulations (Issaoui et al., 2023). This creates legal uncertainty and prolongs the investigative process. Differences in jurisdiction between countries pose a significant challenge in the context of cross-border cloud computing (Bolatbekkyzy, 2024). Relevant data in a particular case may be stored on servers located in multiple countries, each governed by different legal systems. Requests for cross-border data generally must follow international cooperation mechanisms, such as mutual legal assistance, which are often complex, bureaucratic, and time-consuming. Regulatory misalignment between countries, including differences in data protection standards and legal procedures, further complicates this process (Lim & Oh, 2025; Yeung & Bygrave, 2022).

This study also indicates that delays in obtaining access to data can have a direct impact on the quality and availability of digital evidence (Stoykova, 2024). In dynamic cloud environments, data can change, move, or even be deleted within a short period, making delays in legal processes potentially result in the loss of crucial evidence

(Alshabibi et al., 2024; Karagiannis & Vergidis, 2021; Malik et al., 2024). This condition ultimately affects the effectiveness of law enforcement, both in terms of courtroom evidence and in efforts to comprehensively uncover criminal activity. Therefore, the findings underscore the need for regulatory harmonization and the development of legal mechanisms that are more adaptive to the characteristics of cloud technology and the requirements of modern digital forensics. The study also identifies that the increasing use of encryption technology presents an additional challenge for digital forensics (Malik et al., 2024; Ogunseyi & Adedayo, 2023). Encrypted data cannot be accessed without a valid key, thereby limiting investigators' ability to conduct analysis (Ogunseyi & Adedayo, 2023). Moreover, not all cloud service providers maintain transparent policies regarding data access for investigative purposes, which further contributes to legal uncertainty (Alshabibi et al., 2024; Malik et al., 2024).

Furthermore, the findings indicate that traditional digital forensic approaches, which focus on physical devices, are no longer sufficient to address the complexities of cloud environments (Alshabibi et al., 2024; Karagiannis & Vergidis, 2021; Malik et al., 2024; Prakash et al., 2022). New approaches are required, based on log analysis, network forensics, and collaboration with cloud service providers. The study also identifies the need for international standards and guidelines that can accommodate digital forensic practices in cloud environments, both from technical and legal perspectives (Karagiannis & Vergidis, 2021; Malik et al., 2024; Promise et al., 2024). Overall, the results reveal that the primary challenges of digital forensics in the era of cloud computing and cyber law include limited access to and control over data, the technical complexity of cloud environments, jurisdictional obstacles, conflicts with data protection regulations, and the limitations of traditional forensic methods. These findings highlight the need for the development of a more adaptive and integrated framework to enhance the effectiveness of digital forensics in the current digital era.

Technical challenges of acquiring and managing digital evidence in a cloud environment

The shift from conventional systems to cloud computing has brought fundamental changes to the process of acquiring and managing digital evidence, affecting not only investigative techniques but also the reliability and validity of forensic results (Alshabibi et al., 2024; Karagiannis & Vergidis, 2021; Malik et al., 2024; Prakash et al., 2022; Promise et al., 2024). In traditional environments, investigators have full control over physical devices, allowing processes such as imaging, cloning, and hashing to be performed directly according to strict procedural standards to ensure evidence integrity. However, in cloud environments, this control is entirely transferred to the service provider, meaning that investigators no longer have direct access to physical storage media. Consequently, the process of evidence acquisition must be conducted indirectly through the interfaces provided by the service provider.

This reliance on third parties introduces several serious implications. First, there is a risk to the transparency of the acquisition process, as investigators cannot directly verify how data is collected, filtered, or extracted by the service provider's system (Soylu et al., 2022). Second, the potential for data manipulation, whether intentional or unintentional, becomes more difficult to detect due to the lack of full visibility into the internal processes of the cloud system (Rizvi & Williams, 2024). Third, the chain of custody becomes more complex, involving multiple parties (multi-party custody), including cloud administrators, automated systems, and legal authorities (Park & Jeong, 2026). Under these conditions, detailed documentation and robust audit mechanisms

are essential. However, in practice, not all service providers offer sufficient logging and audit trails to meet forensic requirements.

In addition, technical challenges also arise from the heterogeneity of cloud systems themselves. Each cloud service provider has different architectures, storage policies, and logging mechanisms (Mamidala et al., 2023). These differences include log formats, data granularity, retention periods, and the accessibility of logs for users or third parties. As a result, investigators must perform complex data normalization processes before further analysis can be conducted. In some cases, the available logs are not sufficiently detailed to accurately reconstruct events, thereby reducing the forensic value of the data. Furthermore, evidence acquisition in cloud environments often involves "live forensics," or the collection of data directly from systems that are actively running (Alshabibi et al., 2024). This approach differs from traditional methods, which are typically static ("dead forensics"), and carries inherent risks of data alteration during the acquisition process. Improper procedures can compromise the integrity of evidence. Additionally, time synchronization across cloud systems presents a significant challenge, as discrepancies in timestamps can disrupt the reconstruction of event chronologies (Liu et al., 2025).

Another significant challenge is the limitation in conducting comprehensive data acquisition. In many cases, investigators can only obtain partial data in accordance with the permissions or policies of the service provider. This can result in the loss of context necessary for thorough analysis. For example, certain metadata or system activity logs may not be accessible to investigators, even though such information is crucial for reconstructing event sequences. Technical challenges in the acquisition and management of digital evidence in cloud environments are not only related to limited access but also encompass issues of transparency, standardization, data integrity, and operational complexity (Alshabibi et al., 2024; Karagiannis & Vergidis, 2021; Malik et al., 2024). These conditions necessitate the development of more adaptive forensic methods, the use of tools compatible with various cloud platforms, and enhanced collaboration between investigators and service providers to ensure that evidence collection processes remain forensically sound and legally accountable.

The complexity of cloud architecture: virtualization, multi-tenancy, and data elasticity

Cloud computing architecture presents far greater complexity compared to traditional systems, primarily due to its three main characteristics: virtualization, multi-tenancy, and data elasticity (Hashim & Hussein, 2024; Narasayya & Chaudhuri, 2021). These aspects not only change how data is stored and managed but also significantly impact the approach and effectiveness of digital forensic processes. Virtualization allows a single physical hardware host to run multiple virtual machines (VMs) simultaneously through a hypervisor (Pal et al., 2022). In the forensic context, this creates serious challenges because the relationship between data and its physical location becomes indirect (abstracted). Investigators cannot easily determine the actual physical location of data, as a VM can migrate from one host to another (live migration) without interrupting system operations. Moreover, digital artifacts exist not only at the operating system level but are also distributed across multiple layers, including the hypervisor, host OS, guest OS, and even containers. This situation demands more complex multi-layer analysis capabilities and a deep understanding of the cloud architecture in use. Without access to lower layers, such as the hypervisor, investigators risk losing critical context necessary to fully understand system activities (Lozano et al., 2023).

Multi-tenancy adds an additional layer of complexity, as a single cloud infrastructure is shared among multiple users (tenants) (Hashim & Hussein, 2024; Narasayya & Chaudhuri, 2021). In this scenario, data from different users is stored and processed within the same environment, although logically separated. A primary challenge in digital forensics is accurately isolating evidence without violating the privacy or integrity of other users' data (Horsman, 2022; Ogunseyi & Adedayo, 2023). Errors in the isolation process can lead to evidence contamination or even legal violations related to data protection (Gruber et al., 2023). Furthermore, the isolation mechanisms employed by cloud providers (e.g., sandboxing or containerization) are not always transparent to investigators, complicating the validation process to ensure that the data obtained truly originates from the relevant source. In certain situations, these access limitations can also hinder attribution efforts, making it difficult to determine who is responsible for specific digital activities.

Meanwhile, data elasticity in the cloud reflects the system's ability to automatically adjust resources and requirements, including data storage and processing (Choi et al., 2021; Narasayya & Chaudhuri, 2021). Data can be rapidly replicated across multiple locations, moved between servers, or automatically deleted through mechanisms such as auto-scaling, load balancing, and lifecycle management (Alharthi et al., 2024). From a forensic perspective, this dynamic behavior poses significant challenges in maintaining the consistency and continuity of digital evidence. Data targeted in an investigation can change within seconds, making it difficult to ensure that the analyzed data accurately represents the state at the time of the incident. Moreover, data replication across multiple locations can create both redundancy and inconsistency. Investigators may encounter multiple versions of the same data with differing timestamps or statuses, complicating the determination of the most authentic version. Elasticity also affects activity logs, as logs may be distributed across various system nodes and not always perfectly synchronized. This further complicates the reconstruction of event timelines, which is a critical element in digital forensics.

Furthermore, automatic deletion mechanisms in the cloud can result in the loss of evidence before it can be secured. Many service providers implement specific data retention policies, systematically deleting data that is no longer in use for efficiency purposes (Ashiq et al., 2022). If investigators do not act promptly or lack adequate access, critical evidence may be permanently lost. This necessitates a more proactive and real-time forensic approach, including the use of continuous monitoring and live data capture techniques. The complexity of cloud architecture not only adds technical challenges to digital forensics but also fundamentally alters the investigative paradigm (Alshabibi et al., 2024; Malik et al., 2024; Promise et al., 2024). Investigators are required to understand highly dynamic, distributed, and multi-layered environments and to develop methods capable of adapting to such changes. Conventional, static approaches are no longer sufficient, necessitating the integration of technology, enhancement of technical competencies, and closer collaboration with cloud service providers to ensure that forensic processes remain effective and legally accountable.

The mismatch between forensic needs and data protection regulations

This section highlights the tension that arises between the operational demands of digital forensics and the principles of personal data protection established by modern regulations. Data protection regulations, such as personal data protection laws in various countries or internal policies of cloud service providers, emphasize key principles including data minimization, purpose limitation, the data subject's right to

grant or withdraw consent, and the obligation to delete data after a specified period (Issaoui et al., 2023). The primary objective of these regulations is to safeguard individual privacy rights and prevent data misuse. However, in the context of digital forensics, these principles often present tangible obstacles to investigative processes.

In investigative practice, digital forensic investigators require access to various types of data, including activity logs, metadata, temporary files, and other system artifacts, to reconstruct event timelines and identify perpetrators (Suryal, 2024). Regulations that limit data collection or require explicit consent from data subjects can hinder evidence gathering, particularly when the data is sensitive or transient. For instance, data that is automatically deleted by the system or encrypted by default may be lost if legal processes or authorization procedures take a prolonged period. This creates a dilemma between law enforcement interests, obtaining complete and admissible evidence, and the obligation to respect individual privacy rights.

This misalignment is further exacerbated by the rapid pace of cloud computing technology. Dynamic, distributed, and elastic cloud infrastructures evolve far more quickly than regulatory frameworks can adapt. Many regulations were developed based on older technological models and are therefore insufficiently flexible to address emerging phenomena such as multi-tenancy, virtualization, auto-scaling, and end-to-end encryption. As a result, investigators often face situations where applicable legal procedures slow access to evidence or even limit their ability to obtain relevant evidence lawfully. Digital forensic practices in cloud environments frequently involve third parties, such as cloud service providers subject to local regulations in their respective countries (Karagiannis & Vergidis, 2021; Malik et al., 2024; Prakash et al., 2022). When data resides on servers across multiple jurisdictions, investigators must comply with a combination of local and international regulations, which often differ or even conflict. For example, data accessible to law enforcement in one country may be completely inaccessible in another due to stricter privacy regulations. This situation creates legal uncertainty, complicates cross-border law enforcement, and can result in delayed investigations or incomplete evidence.

The misalignment is also evident in the technological and compliance aspects. Regulations often fail to provide sufficient technical guidance to bridge the gap between data security and investigative needs (Ogbodo et al., 2025). For instance, strong encryption technology protects data privacy, but if regulators do not establish mechanisms for lawful investigative access, investigators may face deadlocks because the data becomes completely inaccessible. Similarly, regulations concerning logging and data retention policies are often not aligned with forensic analysis requirements, which demand complete historical evidence. The misalignment between forensic needs and data protection regulations creates multidimensional challenges, technical, legal, and operational (Katkuri, 2025). Addressing these challenges requires adaptive solutions, including the development of more flexible legal frameworks to support lawful access to digital evidence, the standardization of forensic procedures in cloud environments, and enhanced collaboration among regulators, law enforcement, and cloud service providers. A holistic approach of this kind is essential to ensure that digital forensic processes remain effective, responsive to technological developments, and respectful of individual privacy rights.

Regulatory ambiguity and uncertainty of data access by law enforcement

This study found that one of the significant challenges in digital forensics in the cloud era is regulatory ambiguity, which creates uncertainty regarding data access for

law enforcement authorities (Alshabibi et al., 2024; Karagiannis & Vergidis, 2021; Malik et al., 2024). Modern regulations often set imprecise limits on the authority and procedures for obtaining data from cloud service providers, particularly data stored on third-party or cross-jurisdictional servers (Eleanor, 2021). This lack of clarity encompasses various aspects, including whether law enforcement can access data directly, whether a court order is required, how data subject consent mechanisms are applied, and the legal responsibilities of service providers when data is granted or denied.

In practice, this ambiguity often leads cloud service providers to adopt a conservative approach. They frequently restrict investigator access to avoid potential legal violations or penalties for noncompliance with privacy regulations. For instance, providers may refuse access requests in the absence of clear legal authority or require investigators to undergo lengthy and complex legal procedures before data can be obtained. This creates the risk of investigative delays and even the loss of transient or volatile evidence. Legal uncertainty affects both parties. For law enforcement, regulatory ambiguity slows down investigations and raises the risk that obtained evidence may be deemed inadmissible in court because it was acquired unlawfully or without proper authorization. For cloud service providers, unclear regulations increase the risk of legal liability, as they must balance compliance with the law against cooperation with law enforcement. In some cases, this uncertainty leads providers to deny access entirely, causing investigations to stall or necessitating additional time-consuming legal efforts.

Regulatory ambiguity is further exacerbated by differing legal interpretations across jurisdictions. Cloud computing is inherently global, meaning that relevant data may be stored on servers located in countries with different legal systems (Ghaffar, 2024). Cross-border data requests, such as those conducted through mutual legal assistance or other forms of international cooperation, become complex, bureaucratic, and time-consuming (Bolatbekkyzy, 2024). The absence of clear international standards regarding law enforcement access to cloud data further compounds this uncertainty (Olorunlana, 2025). Additionally, the technical aspects of cloud computing introduce an extra layer of complexity. Data may be distributed across multiple physical locations, encrypted, or stored across several virtual machines. If regulations do not explicitly define law enforcement's rights to access encrypted or distributed data, service providers tend to withhold such data to avoid legal risks. In these cases, investigators face a dilemma between the need to obtain evidence promptly and existing legal constraints. Regulatory ambiguity thus generates legal uncertainty that hampers the effectiveness of digital forensics in the cloud era. This situation underscores the need for regulatory harmonization, clarification of law enforcement authority, and the development of clear data access guidelines for cloud service providers. Such measures would not only expedite investigative processes but also ensure that digital evidence is collected lawfully, admissible in court, and respects user privacy rights.

Cross-border jurisdictional challenges in cloud computing

Cloud computing is inherently global, and data distribution is multi-locational, meaning that a single cloud system can store user information on servers spread across multiple countries (Khayer et al., 2021). This characteristic poses significant legal jurisdiction challenges, as each country has its own legal system, regulations, and law enforcement procedures. These differences not only pertain to data access rights but also to privacy protection standards, law enforcement authority, and the responsibilities of cloud service providers. Consequently, cross-border digital forensic investigations are

far more complex than investigations conducted within a single jurisdiction. In the context of cross-border investigations, digital data collection typically must proceed through international cooperation mechanisms, such as Mutual Legal Assistance (MLA). This procedure involves an official request from one country to another to provide data or evidence relevant to a legal case. While this mechanism is designed to ensure legality and protect individual rights, in practice it often takes considerable time due to multiple administrative stages, legal reviews, and inter-agency communications. Such delays can have serious consequences, particularly when the required data is dynamic, such as system logs, transaction data, or ephemeral data that can be lost or altered quickly.

In addition to the lengthy procedural timelines, differences in data protection standards across countries pose an additional barrier. For instance, countries with stringent privacy regulations, such as the GDPR in Europe, restrict foreign law enforcement access to data or require the data subject's consent before data can be transferred. In contrast, other countries may have more lenient rules or different procedures regarding digital evidence collection. This regulatory misalignment creates legal uncertainty for investigators, who must navigate a complex combination of differing regulations, potentially hindering investigations and reducing the likelihood of obtaining complete evidence (Shandilya et al., 2024). This complexity is further compounded by the elastic and distributed nature of cloud computing. Data can be automatically replicated across multiple servers in various countries, migrated between locations, or deleted according to automated retention policies (Zeng et al., 2025). Under these conditions, determining the physical location of data relevant to a case becomes challenging. This difficulty is not merely technical but also legal, as jurisdictional access is determined based on the physical location of the server rather than the data owner's location. Lack of knowledge regarding data location may lead investigators to inadvertently violate local laws or fail to meet legal requirements for evidence acquisition.

Furthermore, cross-border data requests through Mutual Legal Assistance (MLA) or bilateral agreements often require additional legal verification from courts or relevant governmental authorities (Cochrane, 2022). These procedures tend to be rigid and bureaucratic, which can cause investigations that require rapid response, such as cyberattacks or transnational financial crimes, to lose critical momentum. In certain cases, data that is lost or altered during the legal request process can compromise the integrity of evidence, reduce the effectiveness of courtroom proof, and diminish the likelihood of successfully prosecuting offenders. The challenges of cross-jurisdictional issues in cloud computing underscore the need for more adaptive international cooperation mechanisms and the harmonization of global regulations regarding digital data access (Bolatbekkyzy, 2024). Such solutions should enable investigators to obtain legally admissible evidence promptly, without violating data subjects' privacy rights, while clarifying the responsibilities of cloud service providers across different jurisdictions. This approach would enhance the effectiveness of digital forensic investigations in the cloud era and reduce the risk of legal failures due to jurisdictional discrepancies.

Impact on the integrity, authenticity, and availability of digital evidence

The combination of various technical and legal challenges in cloud computing environments has a significant impact on the quality of digital evidence, particularly regarding integrity, authenticity, and availability (Alshabibi et al., 2024; Karagiannis & Vergidis, 2021; Promise et al., 2024). Maintaining the integrity of evidence becomes

difficult because investigators do not have full control over the processes of data acquisition and management. In cloud systems, data is not obtained directly from physical media but through interfaces controlled by the service provider. This situation introduces the possibility of data alteration due to automated processes such as replication, auto-scaling, or load balancing, which can occur without the investigator's knowledge. Furthermore, limited access to deeper system layers, such as the hypervisor or physical infrastructure, hampers comprehensive verification of data completeness. As a result, conventional methods, such as hashing, become more challenging to apply optimally, thereby increasing the risk of data inconsistency and weakening the assurance of digital evidence integrity.

On the other hand, the authenticity of digital evidence also faces significant challenges in multi-tenant cloud environments involving multiple parties (Hashim & Hussein, 2024). Evidence collection processes that rely on cloud service providers and automated systems create difficulties in ensuring that the data obtained genuinely originates from legitimate sources and is relevant to the case under investigation. The risk of misattribution is heightened, particularly when data resides in shared environments used by multiple users. Additionally, limited access to critical metadata, such as activity logs, user identities, and accurate timestamps, can hinder the verification of data provenance. This uncertainty also complicates the chain of custody, making it more difficult to track the evidence's lifecycle transparently and comprehensively. If the authenticity of the evidence cannot be firmly established, its validity in legal proceedings may be called into question.

Furthermore, the availability of digital evidence becomes a critical issue in dynamic and elastic cloud environments (Alshabibi et al., 2024; David et al., 2021; Karagiannis & Vergidis, 2021; Malik et al., 2024; Prakash et al., 2022). Data in the cloud can change, migrate, or even be automatically deleted within a short period, according to retention policies and system management protocols implemented by service providers. Delays in accessing data, whether due to complex legal procedures or cross-border jurisdictional barriers, can result in relevant evidence no longer being available when needed. This is particularly true for volatile data, such as activity logs or temporary data with limited retention periods. Moreover, the increasing use of encryption can also impede access to data, meaning that even when data is physically present, investigators cannot utilize it without the appropriate decryption keys. This situation creates a scenario where evidence exists technically but is practically inaccessible for investigative purposes.

The impact on the integrity, authenticity, and availability of digital evidence directly affects its probative value in legal proceedings (Alkhseilat et al., 2024; Moussa, 2021). Evidence whose integrity cannot be guaranteed, whose authenticity is in doubt, or that is not fully available may be rejected or deemed insufficiently probative in court. In this context, investigators face a greater evidentiary burden, as they must not only present the content of the evidence but also ensure that the entire process of acquisition and management complies with forensic standards and applicable legal requirements. Therefore, more adaptive and integrated mechanisms are necessary, such as the application of cryptographic techniques to maintain data integrity, transparent and standardized logging systems, and strengthened digital chain-of-custody documentation (Khan et al., 2023). Additionally, closer collaboration between law enforcement and cloud service providers is essential to ensure that digital evidence remains valid, authentic, and available in a timely manner to support law enforcement efforts in the digital era.

Encryption challenges and data access policies by service providers

The challenges posed by encryption and data access policies implemented by cloud service providers constitute a critical issue in modern digital forensic practice (Alshabibi et al., 2024; Karagiannis & Vergidis, 2021; Malik et al., 2024; Promise et al., 2024). The increasing use of encryption, including end-to-end encryption, data-at-rest encryption, and data-in-transit encryption is fundamentally designed to protect the confidentiality and integrity of data from unauthorized access (Jangam, 2023). However, in the context of forensic investigations, these mechanisms create significant obstacles for investigators. Encrypted data cannot be analyzed without the appropriate decryption keys, which, in many cases, are exclusively held by users or managed solely by the cloud service provider's system. This situation creates what is often referred to as "going dark," where data is technically available but inaccessible to law enforcement. Consequently, the processes of identifying, extracting, and analyzing digital evidence are hindered and may even fail entirely if no legal or technical mechanisms exist to obtain access to the encryption keys.

Furthermore, the implementation of advanced security technologies, such as zero-knowledge encryption, further complicates the situation, as cloud service providers themselves do not possess the ability to access or decrypt user data (Rekiel et al., 2025). In this scenario, even with a legal order, the provider cannot deliver data in a readable form. On one hand, this approach strengthens user privacy protection, but on the other hand, it creates a serious dilemma for law enforcement, particularly in cases involving cybercrime, terrorism, or organized crime, which heavily rely on digital evidence. Moreover, the use of techniques such as key rotation, ephemeral keys, and forward secrecy adds further complexity, as encryption keys may change periodically or not be stored long-term, thereby reducing the likelihood that investigators can gain access to historical data.

In addition to the technical challenges posed by encryption, the data access policies implemented by cloud service providers also complicate the digital forensic process (Alshabibi et al., 2024; Karagiannis & Vergidis, 2021; Malik et al., 2024). Each provider maintains internal policies for responding to law enforcement data requests, typically influenced by local regulations, commitments to user privacy, and potential legal risks. In many cases, these policies are neither fully transparent nor readily accessible to the public, leaving investigators without certainty regarding procedures, requirements, or limitations for obtaining data. This lack of transparency can lead to inconsistencies in the investigative process, where similar data requests may yield different responses depending on the cloud service provider involved.

Cloud service providers tend to adopt a conservative approach in granting data access to avoid potential violations of data protection regulations (Issaoui et al., 2023). They often require complete legal documentation, such as court orders or formal requests through international cooperation mechanisms, before granting access to user data. While these procedures are essential for ensuring legality and protecting individual rights, they are often time-consuming. In the context of dynamic cloud environments, such delays can have critical consequences, as the required data may have changed, been relocated, or deleted before investigators are able to obtain it. Furthermore, there are differences in the types of data that can be accessed. Some service providers only make limited data available, such as metadata or basic account information, while more sensitive data,such as the content of communications or encrypted files, cannot be accessed without user consent or additional legal mechanisms. This creates limitations for forensic analysis, as investigators are unable to

obtain a comprehensive view of the digital activities under investigation. In some cases, service providers also enforce strict data retention policies, meaning certain data is only stored for a limited period and cannot be recovered once deleted.

The combination of encryption challenges and inconsistent data access policies creates significant uncertainty in the digital forensic process (Ogunseyi & Adedayo, 2023). Investigators face not only technical obstacles in accessing data but also the complexity of navigating policy frameworks that are often opaque (Zibani et al., 2026). As a result, the effectiveness of investigations may decrease, case processing times may be prolonged, and the risk of evidence loss increases. Therefore, a more integrated approach is required, including the development of legal frameworks that clarify access to encrypted data, increased transparency in cloud service providers' policies, and strengthened collaboration between the public and private sectors. Such measures can help achieve a more optimal balance between privacy protection and law enforcement needs in an increasingly complex digital era.

The need for method transformation and development of new frameworks

The increasing complexity of cloud computing environments necessitates a fundamental transformation in digital forensic methods, encompassing technical, procedural, and conceptual aspects (Alshabibi et al., 2024; Malik et al., 2024; Promise et al., 2024). Traditional forensic approaches that focus on the acquisition of physical devices, such as hard drives or local computers, are no longer adequate for addressing the distributed, dynamic, and service-based nature of cloud systems (Alashhab et al., 2022). In such environments, data is not tied to a single physical location but is instead spread across multiple virtual servers that can migrate automatically. Therefore, more adaptive and contextual forensic methods are required, including log-based forensics, network forensics, and remote acquisition techniques that allow investigators to obtain data without direct access to physical devices. These approaches also need to be supported by real-time analysis capabilities and continuous monitoring, given the highly dynamic nature of cloud data and its susceptibility to rapid changes.

In addition to transforming technical methods, a paradigm shift in the investigative process is also required, moving from a reactive approach to a more proactive and collaborative one (Huang, 2023). In the context of cloud computing, investigators can no longer operate independently; they must establish close collaboration with cloud service providers, who control the infrastructure and data. This collaboration encompasses various aspects, such as providing lawful access to data, ensuring transparency in logging mechanisms, and offering technical support during the acquisition and analysis of evidence. Without effective cooperation, investigators face significant limitations in obtaining relevant and valid evidence. Therefore, a clear collaborative framework is necessary, including operational agreements, communication protocols, and audit mechanisms that ensure accountability for both parties.

This study emphasizes the importance of developing a digital forensic framework specifically designed for cloud environments. Such a framework must be capable of integrating technical, legal, and ethical aspects in a balanced manner. From a technical perspective, the framework should encompass standardized procedures for data acquisition, log management, time synchronization, and verification of the integrity and authenticity of evidence. From a legal standpoint, it must align with data protection regulations and cross-jurisdictional requirements, ensuring that the evidence collection process remains legally valid. Ethically, the framework should guarantee that

investigative procedures do not violate user privacy or principles of personal data protection. This holistic approach is essential to ensure that digital forensics can operate effectively without compromising legal compliance or ethical standards.

The need for international standardization has become increasingly urgent in addressing the challenges posed by the globalization of cloud computing (Wang et al., 2024). Currently, there is no comprehensive global standard that governs digital forensic practices in cloud environments, from either a technical or procedural perspective (Karagiannis & Vergidis, 2021; Malik et al., 2024; Promise et al., 2024). As a result, significant differences exist in the methods, tools, and procedures employed by various countries or organizations, which can hinder cross-jurisdictional collaboration and reduce the consistency of investigative outcomes. The development of international standards is expected to provide a common reference for the collection, analysis, and presentation of digital evidence, thereby enhancing interoperability and the reliability of forensic results. Such standardization can also help strengthen the legitimacy of digital evidence in court, as the procedures used would be widely recognized.

Moreover, the transformation of digital forensic methods must be supported by the development of both human and technological capacities. Investigators need to possess a broader set of competencies, not only in traditional forensics but also in cloud architecture, cybersecurity, big data analytics, and an understanding of international regulations. The use of advanced forensic tools that are compatible with diverse cloud platforms is also essential to enhance the efficiency and accuracy of analyses. Thus, this transformation is not merely technical but also encompasses the enhancement of institutional and professional capabilities. The need for methodological transformation and the development of new frameworks in digital forensics is a response to the fundamental changes brought about by cloud computing. An adaptive, collaborative, and standardized approach is key to ensuring that investigative processes remain effective, legally sound, and capable of addressing the increasingly complex challenges of the digital era. With a comprehensive framework in place, digital forensics is expected to continue evolving as a relevant and reliable discipline that supports law enforcement in the future.

Conclusions

The adoption of cloud computing has brought fundamental changes to digital forensic practices, both technically and legally. The main findings indicate that limited direct access to physical infrastructure, dependence on cloud service providers, and the complexity of architectures such as virtualization, multi-tenancy, and data elasticity pose significant challenges in the acquisition and analysis of digital evidence. Furthermore, cross-border jurisdictional barriers, regulatory ambiguities, and the misalignment between forensic requirements and data protection principles further complicate the investigative process. The increasing use of strong encryption also highlights limitations in data access, directly impacting investigative effectiveness. From these various challenges, this study finds that the quality of digital evidence in cloud environments is highly vulnerable with respect to integrity, authenticity, and availability. Digital evidence becomes more difficult to verify, at risk of being incomplete, or even entirely inaccessible. This situation has direct implications for evidentiary strength in legal proceedings, where the validity of evidence may be questioned. Therefore, a transformation toward more adaptive digital forensic methods is required, including the use of log-based analysis, network forensics, and remote acquisition

techniques, which are capable of accommodating the dynamic and distributed characteristics of cloud environments.

This study provides a more holistic approach by integrating the technical aspects of digital forensics with data protection legal frameworks into a comprehensive analysis. It also offers a conceptual understanding of the importance of developing a cloud-based digital forensic framework that balances technical, legal, and ethical considerations. Furthermore, the study emphasizes the significance of collaboration between law enforcement and cloud service providers, as well as the urgency of international standardization to enhance the consistency and effectiveness of cross-jurisdictional digital forensic practices. However, this study has several limitations. The approach employed is qualitative and literature-based, and therefore lacks empirical data or direct case studies in the field. Additionally, the study has not practically tested the effectiveness of the proposed methods or frameworks in real investigative scenarios. Another limitation lies in the scope of the analysis, which remains general and does not specifically examine implementation on particular cloud platforms or compare practices across different service providers.

Based on these limitations, future research is recommended to develop empirical studies through real-case analysis or simulations of digital forensic investigations in cloud environments. Subsequent studies could also focus on testing and validating the proposed frameworks, as well as developing more applicable technical models. Additionally, more specific research is needed regarding the policies and practices of various cloud service providers to understand the differences in implementation in the field. Future research could also explore the integration of new technologies, such as artificial intelligence and automation, to support more efficient digital forensic processes that are responsive to the dynamic nature of cloud environments.

References

Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A., & Praveen, S. (2021). A Comprehensive Overview of Privacy and Data Security for Cloud Storage. *International Journal of Scientific Research in Science, Engineering and Technology*, 113–152. https://doi.org/10.32628/IJSRSET21852

Alashhab, Z. R., Anbar, M., Singh, M. M., Hasbullah, I. H., Jain, P., & Al-Amiedy, T. A. (2022). Distributed Denial of Service Attacks against Cloud Computing Environment: Survey, Issues, Challenges and Coherent Taxonomy. *Applied Sciences*, *12*(23), 12441. https://doi.org/10.3390/app122312441

Alharthi, S., Alshamsi, A., Alseiari, A., & Alwarafy, A. (2024). Auto-Scaling Techniques in Cloud Computing: Issues and Research Directions. *Sensors*, *24*(17), 5551. https://doi.org/10.3390/s24175551

Alkhseilat, A., Billeh, T. Al, Albazi, M., & Ali, N. Al. (2024). The authenticity of digital evidence in criminal courts: a comparative study. *International Journal of Electronic Security and Digital Forensics*, *16*(6), 720–738. https://doi.org/10.1504/IJESDF.2024.142010

Alshabibi, M. M., Dookhi, A. K. B., & Rahman, M. M. H. (2024). Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review. *Computers*, *13*(8), 213. https://doi.org/10.3390/computers13080213

Andraško, J., Mesarčík, M., & Hamuľák, O. (2021). The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework. *AI & SOCIETY*, *36*(2), 623–636. https://doi.org/10.1007/s00146-020-01125-5

Ashiq, M., Usmani, M. H., & Naeem, M. (2022). A systematic literature review on research data management practices and services. *Global Knowledge, Memory and Communication*, *71*(8/9), 649–671. https://doi.org/10.1108/GKMC-07-2020-0103

Bolatbekkyzy, G. (2024). Legal Issues of Cross-Border Data Transfer in the Era of Digital Government. *Journal of Digital Technologies and Law*, *2*(2), 286–307. https://doi.org/10.21202/jdtl.2024.15

Choi, J., Cho, M., & Kim, J.-S. (2021). Employing Vertical Elasticity for Efficient Big Data Processing in Container-Based Cloud Environments. *Applied Sciences*, *11*(13), 6200. https://doi.org/10.3390/app11136200

Choudhary, S. K. (2025). Implementing Event-Driven Architecture For Real-Time Data Integration In Cloud Environments. *International Journal Of Computer Engineering And Technology*, *16*(1), 1535–1552. https://doi.org/10.34218/IJCET_16_01_113

Cochrane, T. (2022). The Presumption Against Extraterritoriality, Mutual Legal Assistance, and the Future of Law Enforcement Cross-Border Evidence Collection. *The Modern Law Review*, *85*(2), 526–538. https://doi.org/10.1111/1468-2230.12675

David, K. A., Al-Hadhrami, T., Alazab, M., Shah, N., & Shalaginov, A. (2021). BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem. *Future Generation Computer Systems*, *122*, 1–13. https://doi.org/10.1016/j.future.2021.03.001

Eleanor, H. (2021). Modernizing Data Security: Best Practices for Compliance with U.S. and International Privacy Regulations. *International Journal of Trend in Scientific Research and Development*, *5*(4), 1881–1894. https://www.ijtsrd.com/computer-science/computer-security/43672/modernizing-data-security-best-practices-for-compliance-with-us-and-international-privacy-regulations/eleanor-hughes

Ghaffar, H.-A. N. A. Al. (2024). Government Cloud Computing and National Security. *Review of Economics and Political Science*, *9*(2), 116–133. https://doi.org/10.1108/REPS-09-2019-0125

Gruber, J., Hargreaves, C. J., & Freiling, F. C. (2023). Contamination of digital evidence: Understanding an underexposed risk. *Forensic Science International: Digital Investigation*, *44*, 301501. https://doi.org/10.1016/j.fsidi.2023.301501

Hashim, W., & Hussein, N. A.-H. K. (2024). Securing Cloud Computing Environments: An Analysis of Multi-Tenancy Vulnerabilities and Countermeasures. *SHIFRA*, *2024*, 8–16. https://doi.org/10.70470/SHIFRA/2024/002

Horsman, G. (2022). Defining principles for preserving privacy in digital forensic examinations. *Forensic Science International: Digital Investigation*, *40*, 301350. https://doi.org/10.1016/j.fsidi.2022.301350

Huang, J. (2023). Digital engineering transformation with trustworthy AI towards industry 4.0: emerging paradigm shifts. *Journal of Integrated Design and Process Science*, *26*(3–4), 267–290. https://doi.org/10.3233/JID-229010

Issaoui, A., Örtensjö, J., & Islam, M. S. (2023). Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance. *Future Business Journal*, *9*(1), 107. https://doi.org/10.1186/s43093-023-00285-2

Jangam, S. K. (2023). Importance of Encrypting Data in Transit and at Rest Using TLS and Other Security Protocols and API Security Best Practices. *International Journal of AI, BigData, Computational and Management Studies*, *4*(3), 82–91.

https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I3P109

Karagiannis, C., & Vergidis, K. (2021). Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information*, *12*(5), 181. https://doi.org/10.3390/info12050181

Katkuri, S. (2025). Securing the Digital Frontier: Legal Analysis of Cybersecurity, Data Privacy and Cyber Forensics in India. *Indian Journal of Public Administration*, *71*(1), 75–91. https://doi.org/10.1177/00195561241284886

Kerber, W. (2022). Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law. *The Antitrust Bulletin*, *67*(2), 280–301. https://doi.org/10.1177/0003603X221084145

Khan, A. A., Shaikh, A. A., & Laghari, A. A. (2023). IoT with Multimedia Investigation: A Secure Process of Digital Forensics Chain-of-Custody using Blockchain Hyperledger Sawtooth. *Arabian Journal for Science and Engineering*, *48*(8), 10173–10188. https://doi.org/10.1007/s13369-022-07555-1

Khayer, A., Jahan, N., Hossain, M. N., & Hossain, M. Y. (2021). The adoption of cloud computing in small and medium enterprises: a developing country perspective. *VINE Journal of Information and Knowledge Management Systems*, *51*(1), 64–91. https://doi.org/10.1108/VJIKMS-05-2019-0064

Lim, S., & Oh, J. (2025). Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. *IET Information Security*, *2025*(1). https://doi.org/10.1049/ise2/5536763

Liu, Y., Sun, B., Wu, Y., Zhang, Y., Yang, J., Wang, W., Thotakura, N. L., Liu, Q., & Liu, Y. (2025). Time Synchronization Techniques in the Modern Smart Grid: A Comprehensive Survey. *Energies*, *18*(5), 1163. https://doi.org/10.3390/en18051163

Lozano, S., Lugo, T., & Carretero, J. (2023). A Comprehensive Survey on the Use of Hypervisors in Safety-Critical Systems. *IEEE Access*, *11*, 36244–36263. https://doi.org/10.1109/ACCESS.2023.3264825

Mahmood, T., Rasool, F. G., & Samee, H. (2025). Technological Innovations in Criminal Justice: The Role of Cybersecurity in Crime Detection, Investigation and Prevention. *Journal of Asian Development Studies*, *14*(1), 1579–1593. https://doi.org/10.62345/jads.2025.14.1.125

Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. *Sensors*, *24*(2), 433. https://doi.org/10.3390/s24020433

Mamidala, J. V., Attipalli, A., Enokkaren, S. J., Bitkuri, V., Kendyala, R., & Kurma, J. (2023). A Survey on Hybrid and Multi-Cloud Environments: Integration Strategies, Challenges, and Future Directions. *International Journal of Humanities and Information Technology*, *5*(02), 53–66. https://doi.org/10.21590/ijhit.05.02.08

Moussa, A. F. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, *11*(1), 20. https://doi.org/10.1186/s41935-021-00234-6

Narasayya, V., & Chaudhuri, S. (2021). Cloud Data Services: Workloads, Architectures and Multi-Tenancy. *Foundations and Trends in Databases*, *10*(1), 1–107. https://doi.org/10.1561/1900000060

Ogbodo, D. C., Awan, I.-U., Cullen, A., & Zahrah, F. (2025). From Regulation to Reality: A Framework to Bridge the Gap in Digital Health Data Protection. *Electronics*, *14*(13), 2629. https://doi.org/10.3390/electronics14132629

Ogunseyi, T. B., & Adedayo, O. M. (2023). Cryptographic Techniques for Data Privacy in

Digital Forensics. *IEEE Access*, *11*, 142392–142410. https://doi.org/10.1109/ACCESS.2023.3343360

Olorunlana, T. J. (2025). Securing the Global Cloud: Addressing Data Sovereignty, Cross-Border Compliance, and Emerging Threats in a Decentralized World. *International Journal of Science, Architecture, Technology and Environment*, 1394–1407. https://doi.org/10.63680/ijsate0525102.117

Pal, S., Le, D., & Pattnaik, P. K. (2022). Virtualization Environment in Cloud Computing. In *Cloud Computing Solutions* (pp. 57–76). Wiley. https://doi.org/10.1002/9781119682318.ch4

Park, Y., & Jeong, D. (2026). A blockchain-based digital evidence management system: Integrating forensic procedures and multi-party authorization. *Information Processing & Management*, *63*(5), 104654. https://doi.org/10.1016/j.ipm.2026.104654

Prakash, V., Williams, A., Garg, L., Barik, P., & Dhanaraj, R. K. (2022). Cloud-Based Framework for Performing Digital Forensic Investigations. *International Journal of Wireless Information Networks*, *29*(4), 419–441. https://doi.org/10.1007/s10776-022-00560-z

Promise, E. E., Idahosa, S., Asante, G., & Okungbowa, A. (2024). Digital Forensic Investigation Standards in Cloud Computing. *Universal Journal of Computer Sciences and Communications*, *3*(1), 23–45. https://doi.org/10.31586/ujcsc.2024.923

Rekiel, A. S., Kanciak, K., & Kelner, J. M. (2025). Zero-Knowledge Proof in 5G and Beyond Technologies: State of the Arts, Practical Aspects, Applications, Security Issues, Open Challenges, and Future Trends. *IEEE Access*, *13*, 138352–138380. https://doi.org/10.1109/ACCESS.2025.3596122

Rizvi, S., & Williams, I. (2024). Analyzing transparency and malicious insiders prevention for cloud computing environment. *Computers & Security*, *137*, 103622. https://doi.org/10.1016/j.cose.2023.103622

Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Navigating the Regulatory Landscape. In *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy* (pp. 127–240). https://doi.org/10.1007/978-3-031-53290-0_3

Singh, A., Ikuesan, R. A., & Venter, H. (2022). Secure Storage Model for Digital Forensic Readiness. *IEEE Access*, *10*, 19469–19480. https://doi.org/10.1109/ACCESS.2022.3151403

Soylu, A., Corcho, Ó., Elvesæter, B., Badenes-Olmedo, C., Yedro-Martínez, F., Kovacic, M., Posinkovic, M., Medvešček, M., Makgill, I., Taggart, C., Simperl, E., Lech, T. C., & Roman, D. (2022). Data Quality Barriers for Transparency in Public Procurement. *Information*, *13*(2), 99. https://doi.org/10.3390/info13020099

Stoykova, R. (Adi). (2024). A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings. *Computer Law & Security Review*, *55*, 106040. https://doi.org/10.1016/j.clsr.2024.106040

Suryal, A. (2024). RETRACTED: Leveraging metadata in social media forensic investigations: Unravelling digital clues- A survey study. *Forensic Science International: Digital Investigation*, *50*, 301798. https://doi.org/10.1016/j.fsidi.2024.301798

Tosza, S. (2021). Internet service providers as law enforcers and adjudicators. A public role of private actors. *Computer Law & Security Review*, *43*, 105614. https://doi.org/10.1016/j.clsr.2021.105614

Vlahou, A., Hallinan, D., Apweiler, R., Argiles, A., Beige, J., Benigni, A., Bischoff, R., Black, P.

C., Boehm, F., Céraline, J., Chrousos, G. P., Delles, C., Evenepoel, P., Fridolin, I., Glorieux, G., van Gool, A. J., Heidegger, I., Ioannidis, J. P. A., Jankowski, J., … Vanholder, R. (2021). Data Sharing Under the General Data Protection Regulation. *Hypertension*, *77*(4), 1029–1035. https://doi.org/10.1161/HYPERTENSIONAHA.120.16340

Wang, S., Jiang, X., & Khaskheli, M. B. (2024). The Role of Technology in the Digital Economy's Sustainable Development of Hainan Free Trade Port and Genetic Testing: Cloud Computing and Digital Law. *Sustainability*, *16*(14), 6025. https://doi.org/10.3390/su16146025

Xia, L., Cao, Z., & Zhao, Y. (2024). Paradigm Transformation of Global Health Data Regulation: Challenges in Governance and Human Rights Protection of Cross-Border Data Flows. *Risk Management and Healthcare Policy*, *17*, 3291–3304. https://doi.org/10.2147/RMHP.S450082

Yeung, K., & Bygrave, L. A. (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*, *16*(1), 137–155. https://doi.org/10.1111/rego.12401

Zeng, W., Yan, W., Simpson, E., & Molina–Jimenez, C. (2025). Quantitative Risk Assessment for Cloud-Based Software Migration Processes. *Concurrency and Computation: Practice and Experience*, *37*(6–8). https://doi.org/10.1002/cpe.70009

Zibani, P., Rajkoomar, M., Naicker, N., & Marimuthu, F. (2026). Navigating research data management challenges in an academic landscape: a framework for a university of technology research repository context. *Digital Library Perspectives*, *42*(1), 5–31. https://doi.org/10.1108/DLP-08-2024-0127

Żurkowski, B., & Zieliński, K. (2024). Root Cause Analysis for Cloud-Native Applications. *IEEE Transactions on Cloud Computing*, *12*(1), 232–250. https://doi.org/10.1109/TCC.2024.3358823