computers

MDPI

Review

Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review

Munirah Maher Alshabibi *, Alanood Khaled Bu dookhi and M. M. Hafizur Rahman

Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia; 224108486@student.kfu.edu.sa (A.K.B.d.); mhrahman@kfu.edu.sa (M.M.H.R.)

* Correspondence: 222453716@student.kfu.edu.sa

Abstract: Cloud computing technology delivers services, resources, and computer systems over the internet, enabling the easy modification of resources. Each field has its challenges, and the challenges of data transfer in the cloud pose unique obstacles for forensic analysts, making it necessary for them to investigate and adjust the evolving landscape of cloud computing. This is where cloud forensics emerges as a critical component. Cloud forensics, a specialized field within digital forensics, focuses on uncovering evidence of exploitation, conducting thorough investigations, and presenting findings to law enforcement for legal action against perpetrators. This paper examines the primary challenges encountered in cloud forensics, reviews the relevant literature, and analyzes the strategies implemented to address these obstacles.

Keywords: cloud forensics; cloud security; digital investigation; investigating cloud-based data

Citation: Alshabibi, M.M.; Bu dookhi, A.K.; Hafizur Rahman, M.M. Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review. *Computers* **2024**, *13*, 213. https://doi.org/10.3390/computers13080213

Academic Editor: Lilatul Ferdouse

Received: 21 July 2024
Revised: 18 August 2024
Accepted: 20 August 2024
Published: 22 August 2024

1. Introduction

In recent years, there has been a significant increase in the daily use of the virtual realm, providing convenient access to individuals from all walks of life. Cloud computing has emerged as a contemporary and widely adopted approach for delivering computer resources, including servers, networks, storage, applications, and services, in a flexible and fast manner [1]. It is widely recognized as a fundamental strategy for the successful implementation of computer systems and other integrated methodologies [2,3]. Among the various technological advancements, one of the most crucial services is the opportunity it offers people to securely store their information in remote locations and retrieve it as needed. Cloud computing has a distinctive aspect of storage, allowing the storage and management of data on remote servers that can be accessed via the internet. This enables users to easily access and utilize the stored data, thus reaping their benefits [4]. While cloud computing architecture provides flexibility, it also presents potential advantages for criminal activities, posing challenges for forensic investigators. Investigators utilize computer forensics as a tool to pinpoint the source of an attack. On the other hand, digital forensics is a scientific field that involves the gathering, retrieval, and assessment of digital data with the goals of preventing fraud, collecting digital evidence, preserving it for investigations, and even recovering accidentally erased data [5].

The investigation of digital evidence in the cloud is known as cloud forensics and involves a wide range of searching and investigation due to the increasing reliance on the cloud. The challenges in cloud investigation are multifaceted, as the dynamic nature of the cloud environment makes the collection and preservation of evidence difficult [6]. Moreover, having multiple types of cloud deployment models (private, public, and hybrid) and multiple types of service models (infrastructure as a service, platform as a service, and software as a service) requires different investigation strategies for each one [6]. Furthermore, the privacy aspects of the cloud add layers of complexity to the investigation [7]. The

absence of tools and procedures to assist in cloud investigation further complicates this process [8].

The significance of digital forensics lies in various aspects of cybercrime. In incident response and cloud analysis, it plays a critical role in identifying the source of breaches during incidents, enabling organizations to implement mitigation strategies to reduce risks [9]. Moreover, digital forensics is essential for compliance with legal requirements, ensuring the safety, security, and privacy of digital evidence [6]. It also safeguards data integrity and privacy in cloud environments managed by third-party service providers [10]. In addition, digital forensics offers tools and methods to track malicious activities in the cloud [11]. In the realm of cybercrime, analyzing and preserving data is of utmost importance.

The objective of our research is to identify and document the obstacles encountered in cloud forensics, as well as the strategies employed to address these obstacles. This research contributes to the existing literature by conducting a comprehensive review of recent publications focusing on cloud computing forensics. We specifically examined the challenges encountered in this field and the critical data involved. Furthermore, we analyzed the approaches employed to address these challenges. Finally, we compared our findings with other studies that shared a similar research objective.

Finding solutions for these and other challenges is important to improve the methodologies used in forensics, make investigations effective despite the privacy constraints of clouds, and maintain the integrity of the investigation process.

2. Background

Computer forensics is considered a vital component of digital forensics and a crucial aspect in handling computer-related evidence. It involves the investigation of digital storage media. Simply put, it encompasses the extraction, analysis, and presentation of forensic evidence from digital storage media, with the aim of preserving and retrieving it as needed.

Investigations into cloud-based data face numerous challenges, with security being paramount among them. Balancing the need for protection against unauthorized access with the constraints imposed by cloud service providers on accounts and privacy presents a formidable task. Unauthorized access poses a significant threat, while provider-imposed security measures can limit investigative efforts. Finding the right balance between security and accessibility is crucial for successful investigations into cloud-based data. Computer system requirements increase in tandem with technological advancements, and cloud services can enhance operational agility, reduce expenses, and maximize resource utilization. We also observe the use of digital forensics in cloud computing to verify activities and files in cloud environments. This means that digital analysis techniques can be used to monitor data access, detect unauthorized activities, and provide digital evidence for investigations.

The relationship between digital forensics and cloud computing is close in several aspects, such as data being stored in the cloud instead of traditional local systems, allowing remote access and analysis by digital forensics operations without the need for a local data presence. Cloud computing stores, processes, and accesses data on demand over the internet. It offers scalability, flexibility, cost-efficiency, and accessibility from anywhere with an internet connection. Cloud computing has become an influential force within the ever-changing information technology world, transforming how businesses handle data processing, storage, and service delivery. The transition from conventional physical infrastructure to cloud-based ones presents exceptional opportunities for efficiency, scalability, and flexibility.

Cloud forensics is a specialized field of digital forensics focused on investigating and analyzing digital evidence in cloud environments. As data increasingly reside in remote cloud servers, forensic practitioners face new challenges in acquiring, preserving, and analyzing evidence stored in the cloud. Cloud forensics applies traditional forensic techniques to cloud environments, addressing various issues such as data integrity, privacy, jurisdictional challenges, and the dynamic nature of cloud services. The connection between

cloud computing and digital forensics has given rise to the field of cloud forensics, which focuses on improving tools, techniques, and methodologies to investigate cybercrime, data breaches, and other security incidents in cloud environments. Digital forensics, in this context, involves searching for and auditing crimes and errors using the servers and devices provided by the cloud. In [7], they illustrate the preparedness of forensic tools through the execution of a strategy aimed at reconfiguring data collection systems utilizing log tools and monitoring. This initiative involved the development of incident response protocols tailored to each service model, resulting in a decrease in response time and an enhancement in investigation accuracy. Therefore, forensics is capable of analyzing electronic crimes and uncovering their causes and details.

Researchers and practitioners in this field are working towards enhancing the forensic readiness of cloud services. They aim to ensure the admissibility of digital evidence in court, and address the unique challenges posed by cloud storage and computing models. Overall, the background of cloud computing and cloud forensics highlights the need for robust security measures, forensic capabilities, and legal frameworks to effectively investigate and mitigate cyber threats in cloud environments [12].

In summary, cloud forensics bridges the gap between digital investigations and cloud-based environments, enabling efficient analysis even without a local data presence. As cloud adoption continues to grow, understanding and advancing cloud forensics practices are essential for cybersecurity professionals and investigators alike. This paper focuses on the following important objectives of cloud forensic analysis:

- Detecting cloud crimes related to data and activities conducted through cloud services, such as security breaches, electronic fraud, data theft, and espionage.
- Providing legal evidence that can be used in courts to help solve crimes.
- Maintaining cloud stability by identifying weaknesses in the cloud infrastructure to prevent future attacks.
- Supporting international legal investigations by analyzing cloud user data and tracking illicit activities online.

Systematic literature review (SLR) is essential for exploring and summarizing existing research. Conducting an SLR in cloud forensics helps researchers gain a comprehensive understanding of the existing literature, challenges, and solutions related to cloud forensics. We conducted an SLR on our topic to identify gaps in current and previous research, identifying key issues, and suggesting future research directions that relate to cloud forensics investigations.

2.1. Overview of Cloud Computing

Cloud computing offers businesses unprecedented levels of adaptability, scalability, and efficiency. It represents a paradigm shift in the provision and utilization of computer services. A comprehensive review of cloud computing's definition and prominent features is presented here, as it is considered one of the most significant and powerful innovations in the modern world.

Cloud computing is similar in structure to a strong building base, with its cornerstone being computer resources. It provides precise services including storage, processing, and networking, without being restricted to full ownership of the infrastructure. In addition, cloud computing efficiently and quickly provides access to resources, adding further importance to its value. For example, in terms of storage services, many sectors are shifting towards cloud computing for file storage due to its lower costs. One of the most prominent examples is the e-learning sector, whose owners and founders required massive resources at staggering costs.

Cloud computing has transformed the IT industry by offering scalability, flexibility, cost-efficiency, and accessibility to a wide range of computing resources. It has enabled organizations to innovate, streamline operations, and adapt to changing business needs more effectively. Cloud computing provides a powerful and versatile platform for individuals

and businesses to leverage computing resources, store data, run applications, and drive digital transformation in a dynamic and interconnected world.

2.1.1. Cloud Deployment Models

Today's digital world is undergoing a major transformation that renders storage problems negligible in the face of cloud computing. Storage servers are revolutionizing organizational perspectives by shifting from traditional storage to cloud storage. This cost efficiency is achieved through factors such as economies of scale, shared resources, and optimized infrastructure management practices, making cloud storage a cost-effective choice for organizations.

Cloud computing offers multiple deployment models, as previously discussed in the introduction, specifically [13,14]:

- Public Cloud: This is considered the most common of the deployment models because it is accessible to the general public, as its name implies, and available to everyone. In other words, companies lease resources to users based on their needs only, on a pay-as-you-go principle. Some offer free services but with limitations. There is a demand for them because they do not require maintenance or hardware changes on the part of the client [15].
- Private Cloud: We are not differentiating in the cloud infrastructure as all models are similar, and the technical structure of the private cloud is similar to the public cloud. However, the main difference lies in cloud ownership as it falls under the control of the company owner only. Maintenance and setup are carried out in a dedicated location belonging to the owning company. However, it is considered better in terms of security as it achieves high-level access authorization management. Only authorized personnel designated by the company are allowed access to the stored resources [16].
- Hybrid Cloud: This is considered a blend of the benefits of both public and private clouds, with high-quality management and protection policies applied. It provides a fundamental level of security and substantial resources. The hybrid cloud operates on the principle of segmentation, where there is a portion for protecting sensitive information from loss or damage and another portion for public deployment and general use. This cloud is typically owned by the company owner who leases it [16].

Table 1 presents various cloud deployment models, each outlined with its features and drawbacks to provide a comprehensive understanding of the characteristics and considerations associated with each model. Understanding the characteristics of each deployment model can assist in making informed decisions based on specific requirements, such as security, scalability, cost-effectiveness, and data management needs.

Table 1. Cloud deployment models.

Cloud Deployment Models	Features	Drawbacks
Public Cloud	• Easy-to-set-up infrastructure, making the user experience and maintenance very simple. • Service pricing is very reasonable as it offers pay-as-you-go payment. • The client can increase usage according to the resources needed, as they are not bound by any plan.	• Since some of the plans offered are free, the public cloud suffers from weak security. • It lacks the required level of efficient cloud resources. • It can only be used by small businesses such as offices, very small companies, and the like.
Private Cloud	• High level of security in this model. • Provides a broad infrastructure capable of serving the needs of large enterprises. • Can provide the appropriate volume and protection for any sensitive and critical information.	• High cost. • Requires complex hardware, servers, and maintenance.

Table 1. *Cont.*

Cloud Deployment Models	Features	Drawbacks
Hybrid Cloud	• High level of security for public cloud storage and greater availability of resources than with public cloud. • Reasonable cost for small business owners who possess precise and sensitive information.	• Difficulty in partitioning information.

2.1.2. Cloud Service Models

Many services provided by the cloud cannot be encompassed under a single title. However, we will classify the service models offered by the cloud, including all cloud services, as outlined below [17].

Software as a Service (SaaS): This falls under the core models of cloud service lists. It involves the provision of resources and basic infrastructure applications over the internet. Users do not need to download or install software on their system, but instead subscribe to it as a monthly paid plan. In this type of service, the software is hosted online and used by clients—for example, services such as email. The key strengths of this service include the following:

- Ease of access and use by customers.
- Automatic updates are performed by the service provider.
- Customers are not restricted to a specific type of device to access the service.
- Cost savings for the client, as they pay a monthly subscription instead of purchasing the service.

Platform as a Service (PaaS): This represents the development environment needed by developers, hosted on the cloud and provided as a service. This eliminates the need for developers to manage infrastructure, allowing them to concentrate solely on the development process. The model of cloud services we are discussing has a distinctive set of strengths that sets it apart. These strengths include the following:

- It is highly suitable for developers as it promotes a collaborative environment among them.
- It relieves developers from the burden of updates by means of an automatic system and software updates.
- It offers responsiveness and seamless integration with other cloud services.
- It allows resource consumption to be tailored to the specific needs of each client or developer.

Infrastructure as a Service (IaaS): This is considered one of the most important service models as it provides resources such as hardware. There are several advantages that highlight the strength of this model of cloud service, including the following:

- Scalable Resource Provisioning: Instead of purchasing resources, this model offers resource expansion based on the company's needs. Resources are provided as a service in exchange for a monthly subscription.
- High-Level Security and Data Protection: This enhances client information and data with a high level of security and protection.
- Deployment Flexibility: This type of cloud service makes it possible to deploy in the region desired by the client, as providers typically own data centers in various regions.

2.2. Digital Forensics

Digital forensics, also known as computer forensics or cyber forensics, is a specialized branch of forensic science that involves the identification, preservation, analysis, and presentation of digital evidence stored on electronic devices and systems. The primary

goal of digital forensics is to uncover and investigate cybercrime, security incidents, and other illicit activities by examining digital artifacts such as files, emails, logs, metadata, and network traffic. Digital forensic investigators use a variety of tools and techniques to extract and analyze data from computers, mobile devices, servers, and other digital storage media. They follow strict procedures to ensure the integrity and authenticity of the evidence collected, adhering to legal and ethical standards to maintain the chain of custody and ensure that the evidence is admissible in court. Moreover, digital forensics plays a critical role in criminal investigations, cybersecurity incidents, civil litigation, and corporate security matters. By applying forensic principles and methodologies to digital evidence, investigators can reconstruct events, identify perpetrators, uncover motives, and provide crucial information for legal proceedings. In an increasingly digital world, digital forensics has become essential for combating cybercrime, protecting sensitive information, and upholding the rule of law in the digital domain. It is the process of uncovering and interpreting electronic data to be used as evidence in criminal investigations, civil litigation, or cybersecurity incidents [18].

In short, it can be explained as the process of searching and examining digital data to uncover evidence and activities indicative of electronic crime, investigating them, and taking necessary actions. Investigators utilize various tools to gather sufficient evidence. Digital forensic investigation examines digital records relying on various digital tools that can assist in uncovering digital crimes, which may include fraud, forgery, hacking, or electronic espionage. It encompasses a variety of software and techniques designed to collect, analyze, and uncover digital evidence.

Table 2 presents various digital forensic investigation tools used by forensic investigators and highlights their specific functions and applications. These tools play a critical role in uncovering and investigating cybercrime by examining digital artifacts such as files, emails, logs, metadata, and network traffic.

Table 2. Digital forensic investigation tools.

Tool	Description
Data Recovery Software	Used to retrieve deleted or lost data from digital devices such as computers and smartphones.
Digital Analysis Software	Utilized for analyzing various forms of digital data, including images, videos, and text files.
Network Extraction and Analysis Tools	Employed to analyze network traffic and extract data related to network communications and online activities.
Encryption and Decryption Software	Utilized for analyzing encrypted data and decrypting it to extract analyzable information.
Image and Video Recovery Tools	Assist in recovering deleted or hidden images and video clips from digital devices.
Smart Analysis and Pattern Recognition Software	Used for intelligent data analysis and detecting unusual patterns and trends that may indicate illicit activities.

2.3. Cloud Forensic Analysis Assists in Conducting Cloud Forensic Investigations

Cloud forensic analysis plays a crucial role in cloud forensic investigations by providing tools and methodologies to collect, preserve, and analyze digital evidence stored in cloud environments [6]. This assists investigators in uncovering evidence related to potential crimes such as data breaches or electronic fraud. For example, consider a case where a company suspects a data breach in their cloud storage system. By conducting cloud forensic analysis, investigators can gather information from the cloud service provider, audit activities within the cloud, obtain evidence related to unauthorized access, analyze the collected data to identify suspects, and ultimately investigate the breach. This process

helps in determining the cause of the breach, identifying the extent of the damage, and gathering evidence that can be used in legal proceedings.

A case study illustrating the importance of cloud forensic analysis is the Dropbox data breach incident. In this case, unauthorized access to Dropbox accounts resulted in the exposure of sensitive data. Through cloud forensic analysis, investigators were able to trace the unauthorized access, identify the vulnerabilities in the cloud storage system, and gather evidence to track down the perpetrators. This highlights how cloud forensic analysis can assist in investigating and resolving security incidents in cloud environments. Cloud forensic analysis is essential for ensuring the reliability and admissibility of digital evidence in legal proceedings, strengthening cybersecurity measures, and holding those involved in illegal activities in cloud services to account [6].

Cloud forensics is highly valuable as a technique for investigating data stored in the cloud, due to various factors such as data collection and preservation. Cloud forensic tools and methodologies enable investigators to collect digital evidence and preserve it in cloud environments. Cloud service providers typically generate comprehensive logs and metadata about user activities and interactions with cloud services. In addition, cloud forensics tools uncover digital artifacts left in cloud environments. Despite compliance with legal and regulatory requirements, including rules regarding data privacy, evidence handling, and chain of custody, cloud forensic analysis assists in cloud forensic investigations by providing tools and methodologies to collect, preserve, and analyze digital evidence stored in cloud environments [6].

2.4. Cloud Forensics

Cloud computing is a technology that enables users to access and utilize computing resources over the internet on a pay-as-you-go basis. Instead of owning physical servers or infrastructure, users can leverage cloud services provided by third-party providers to store data, run applications, and access various IT resources. Cloud forensics is like being a detective in the digital world, but specifically focusing on investigating and analyzing evidence stored in cloud services such as Google Drive or Dropbox. As an increasing number of people use the cloud to store their data, there is a need for experts who can navigate the challenges of conducting investigations into these online environments. Cloud forensics uses special techniques to collect, protect, and examine digital evidence from cloud platforms. They face issues such as dealing with data spread across different servers, sharing space with other users, and not having direct access to physical storage devices. In addition, they must consider legal and jurisdictional factors, since data stored in the cloud may be subject to different privacy laws based on its location [19].

Cloud forensics is a part of digital forensic investigations that revolves around collecting and analyzing evidence in a cloud computing environment. This involves gathering data from cloud service providers, analyzing activities and communications, and extracting evidence relevant to potential crimes, such as data breaches or electronic fraud. The challenges in cloud forensics include privacy and security issues, in addition to the complexity of data structures and activities in the cloud environment. Investigators or analysts typically follow several steps:

- Gathering information from cloud service providers.
- Auditing activities that occurred within the cloud.
- Obtaining evidence related to unauthorized access or any breaches.
- Analyzing all the aforementioned points to identify suspects.
- Investigating and obtaining the outcome.

The main goal of cloud forensics is to ensure that the digital evidence collected from cloud services is reliable, genuine, and can be used in legal proceedings. By creating specific methods, tools, and best practices for cloud investigations, experts can uncover evidence of cybercrime, security breaches, and other illegal activities that involve cloud services. Cloud forensics is essential for strengthening cybersecurity, supporting legal cases, and holding those who engage in wrongdoing online to account. It requires individuals with a

well-developed ability to focus and understand all the signals associated with suspicious activity. They must have fundamental analysis skills to comprehend the flow of activities and accurately identify evidence, as digital crimes occur with a high level of sophistication and expertise [19].

2.4.1. The Impact on Forensic Strategies

The accountability associated with accessing and controlling data based on cloud deployment models and service models is evident and has a significant influence on forensic strategies, making it an important aspect. Every model presents distinct challenges and opportunities for forensic implementation.

- **Impact of the Cloud Deployment Models.**
  Utilization of the public cloud involves the sharing of resources among numerous tenants, creating challenges in effectively segregating forensics data without impacting others. It is important to include forensic strategies to separate each tenant accurately. The legal agreement with cloud service providers plays a crucial role in ensuring access to forensics data [20].
  The private cloud offers a high level of control and customization, but this comes at a significant cost and results in management complexity. The organization must ensure robust security measures and implement effective forensic strategies. These strategies should have the most control over the infrastructure to enforce various policies. Consequently, the organization can develop and deploy specialized tools and protocols within the private cloud for forensic purposes [21].
  Integrating both private and public cloud services into the hybrid cloud may lead to challenges in conducting forensic investigations due to varying levels of control over data and infrastructure. Investigators must navigate through different policies and forensic tools utilized across the data sources [20].
  The community cloud facilitates data sharing between organizations with similar interests and simplifies forensic efforts through standardized policies and procedures. The nature of the infrastructure presents similar challenges to those encountered in public cloud environments when separating data [20].
- **Impact of Service Models.**
  Investigators in the IaaS models have access to resources at a lower level, such as virtual machines and storage systems. This simplifies detailed forensic analysis, but requires a deep understanding of the virtual environment and the ability to manage and analyze a vast amount of data [20].
  In the PaaS models, most of the infrastructure is abstracted, making it difficult to access primary data for forensic purposes. Investigators must collaborate closely with cloud service providers to obtain the required logs and other evidence, potentially causing delays in the investigation [20].
  The SaaS model presents a significant challenge for the forensic field, with a high level of obfuscation and limited visibility into the infrastructure. Service providers control access to forensic data, leading to legal procedures to obtain the necessary evidence [20].

2.4.2. Challenges in Cloud Forensics

Cloud forensics faces challenges due to the complexity and changing nature of cloud computing. Data are shared, stored virtually, and spread out, making it difficult for investigators to find and protect evidence. They cannot physically touch storage devices, and data from many users can get mixed up, making it challenging to keep evidence safe and reliable. Privacy and legal issues also pose challenges, as data in the cloud may be subject to different rules about privacy and protection. This complicates following the correct laws and ensuring that evidence can be used in legal cases. Moreover, as cloud technology advances, investigators must continuously learn about new tools and methods to effectively collect and analyze evidence. Traditional forensic methods may not work

well in cloud environments due to the vast amount of data, requiring investigators to find improved ways to deal with data in the cloud. Cloud forensic examination is complex and requires a high level of analytical ability and precision, depending on the case [19].

Table 3 presents the challenges in cloud forensics, involving the investigation of digital evidence stored in cloud computing environments. These challenges arise due to the complex and dynamic nature of cloud computing, making it difficult for investigators to collect, preserve, and analyze evidence effectively. Addressing these challenges can enhance investigators' skills in conducting effective investigations in cloud computing environments.

Table 3. Challenges in cloud forensics.

Characteristics of Cloud	Forensics Challenge
Scalability	Ensuring data integrity and maintaining chain of custody during dynamic resource scaling.
Accessibility	Investigating unauthorized access and data breaches across remote locations with different access levels.
Shared Resources	Managing data combination challenges and isolating digital evidence within a shared infrastructure.
Virtualization	Addressing forensic analysis problem in virtualized systems and abstracted hardware environments.
Data Distribution	Handling the challenges associated with legal jurisdictions and data locations in cloud storage systems spread across multiple geographic regions.

Legal, technical, time, and administrative challenges can make the investigation process difficult, requiring special skills from investigators to ensure the protection of the collected information and evidence.

Preserving data on the cloud is a challenging requirements when it comes to data gathering and maintenance. The ability to delete and modify data on the cloud poses a significant challenge in ensuring their preservation. A notable example is the United States case against the Microsoft Corporation relating to data stored on a server in Ireland. This case highlights the challenges of preserving data and dealing with jurisdictional issues, as well as the rapid removal of data in the cloud environment [22].

In cloud environments, multiple tenants utilize the same physical resources, presenting various challenges in maintaining data separation. For example, investigations of data breaches by Dykstra and Sherman (2013) revealed that data from different users were stored on shared cloud servers. In such cases, forensic experts must exercise caution to meticulously separate the data in order to prevent any cross-contamination [23].

2.5. Need for Cloud Forensics

2.5.1. Cases Requiring Cloud Analysis

When an organization plans to incorporate cloud computing into its technological strategy, conducting cloud analysis before launching into cloud operations is essential. In addition, IT service professionals who require cloud services must undergo analysis to select the best options based on various constraints in their work. Cloud service providers themselves require cloud analysis to ensure that data and applications transferred to the cloud comply with cloud regulatory laws. Furthermore, cloud analysis involves a thorough cost analysis of cloud computing usage. This helps in assessing potential risks associated with relying on cloud computing, enabling cloud service providers to develop effective management strategies. In essence, cloud analysis is crucial whenever cloud technology is utilized, to ensure the success of its implementation [24].

2.5.2. The Need for Cloud Forensic Investigation Arises from Several Factors

The increasing adoption of cloud services by organizations and individuals has led to the complexity of digital crimes, necessitating continuous cloud analysis. This is due to the evolving techniques used in digital crimes, which now include exploiting vulnerabilities in cloud infrastructure, making it a crucial factor in the increased demand for cloud analysis. Furthermore, safeguarding data and preserving their integrity are essential factors, requiring criminal investigations to determine the cause and extent of breaches when they occur. On the other hand, cloud forensic investigation is at the core of probing internet crimes, where data stored in the cloud are used as digital evidence. In summary, with the growing use of cloud computing and the ongoing need to protect data, cloud forensic investigation becomes imperative [25].

2.6. Cloud Security Concerns

Cloud security concerns include worries about data protection and privacy. With the increasing use of cloud services by many, data have become more vulnerable. Cloud users fear a lack of availability of cloud-provided services. Moreover, legislation and regulations regarding privacy and security have not compelled everyone to comply yet, necessitating the presence of policies that enforce compliance. One of the most pressing concerns for cloud users is cyber breaches and attacks. Cloud security challenges require the implementation of effective measures and policies to protect data and systems hosted in the cloud environment, ensuring a secure cloud experience for the customer. This includes encryption implementation, access controls, and raising awareness among users about potential security risks to make it possible for swift action to be taken with any threat [26].

2.7. Process of Cloud Forensics

Cloud forensic investigation focuses primarily on collecting and analyzing evidence within the cloud computing environment. It follows several basic steps, starting with the identification of the investigation's objectives and understanding the cause of a security incident. Digital evidence is then gathered from various sources within the cloud environment, such as activity logs, communication records, and other relevant data. The next step involves analyzing the collected evidence to identify suspicious activities and pinpoint weaknesses in the security system. Finally, the investigation concludes with the preparation of technical reports outlining the findings. All results are documented to ensure transparency [27].

2.8. Valuable Practical and Innovative Perspectives of Cloud Forensics

Certain technical reports authored by industry experts can offer valuable practical and innovative perspectives on the field of cloud forensics. For instance, the Azure Security and Compliance Blueprint by Microsoft provides detailed guidance on conducting forensics and incident response within Microsoft Azure, covering aspects such as data collection, log analysis, and cloud monitoring [28].

The Amazon Web Services (AWS) report provides a detailed guide on security practices for analyzing cloud forensics. It explores the tools and methodologies utilized for the collection and examination of digital evidence within the AWS infrastructure. Stressing the importance of evidence security, the report underscores the need to uphold a chain of custody in cloud environments [29].

In addition, the European Union Agency for Cybersecurity (ENISA) has released a comprehensive report that examines the benefits and potential risks associated with cloud computing, with a specific emphasis on information security and cloud forensics. The report also offers suggestions for incorporating proactive forensic measures within cloud settings [30].

Finally, the reports provided by industry leaders offer valuable insights and innovative approaches in cloud forensics. With their extensive experience in infrastructure management and digital evidence handling, these experts contribute to the advancement

of the field. By keeping updated on the latest methodologies and tools through these reports, investigators and researchers in cloud forensics are better equipped to address the challenges they may encounter.

2.9. Discussion

This section discusses the impact of cloud forensic investigation on enhancing cloud security. Cloud forensic investigation is a powerful tool that can be relied upon for this purpose. By analyzing unauthorized activities and identifying vulnerabilities in security systems, protection is strengthened and security risks are reduced.

The capability of identifying and addressing security incidents has increased the number of cloud service users, due to their growing confidence in cloud computing environments. Moreover, cloud forensic investigations can reduce losses resulting from attacks by identifying risks and how to address them, thereby minimizing the magnitude of these losses. In fact, the increase in response accuracy and security awareness depends on cloud forensic investigation.

3. Methodology

Systematic literature review is a crucial research method used to thoroughly explore previous research and studies on a particular topic. Its main goal is to provide a complete collection of relevant papers in that field. It is an effective way to bring together past findings and fill any gaps in our knowledge. With the increasing amount of research and scientific papers, there is an increasing need for a dependable and robust study that summarizes previous work and integrates these findings to address identified gaps. In our research paper, we used the PRISMA 2020 flow diagram designed for new systematic reviews (see Figure 1) to visually represent how many records were included or excluded during the process of selecting studies. PRISMA provides an organized methodology to ensure applicability and accuracy in implementing the SLR.

The specified source type for the review was "Scientific Journal or Conference Paper". During the identification phase, the search process was conducted across multiple databases, including IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. We used multiple search terms to encompass our range: "Cloud forensics" OR "digital forensics", "cloud security", "digital investigation" OR "cloud investigation", "investigating cloud-based data", and "challenges in cloud forensics" AND "issues". A total of 500 papers were initially identified from various databases. After removing 100 duplicates, 400 unique studies remained. Subsequently, during the title and abstract screening stage, 300 papers that did not fully meet the criteria were excluded. Finally, after a thorough evaluation of the full text of the remaining studies, 100 studies were considered for inclusion. Of these, 80 studies were further excluded, resulting in a final selection of 20 studies. Also, we initially explored the other methods identified and collected 50 studies from websites. The websites display references below the studies, allowing for scientific and follow-up citations. After conducting in-depth research, 80 studies were excluded from the examination and review process. These studies were deleted due to their lack of relevance to our paper's topic or because our request caused them to be inappropriate. Additionally, some papers were unable to be extracted and others were not written in English. This selection process is visually represented in Figure 1.

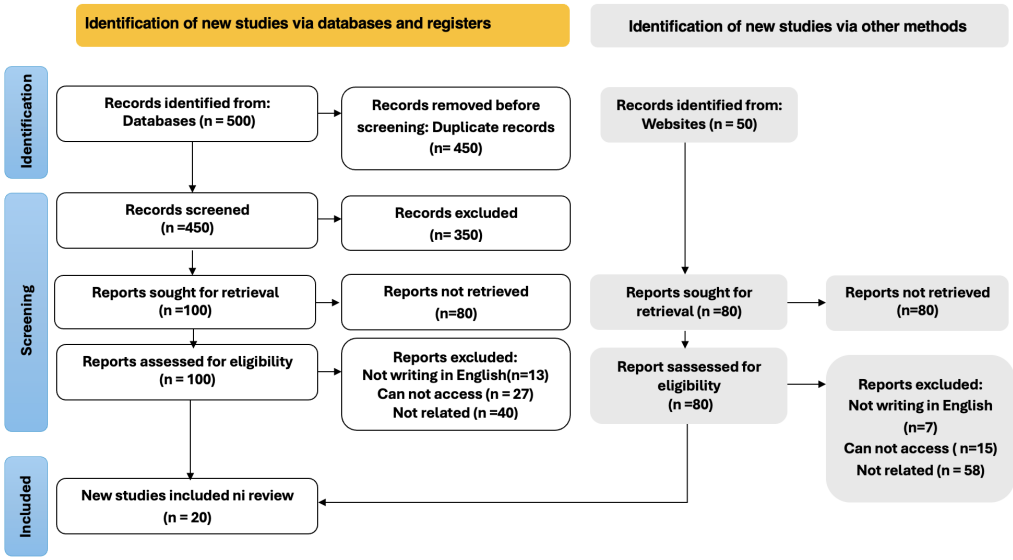

Figure 1. Selection of papers for review using PRISMA model.

4. Related Works

This section presents an overview of recent studies and research in the field. Selecting the best research efforts and analyzing them to highlight the most crucial information is a laborious task. In this analysis, we present the challenges together with the appropriate techniques to address them.

Purnaye et al. [31] established a comprehensive framework for collecting the necessary data to support reliable cloud forensics and introduced a new classification system for this field. In addition, their work contributed to bridging the existing research gap regarding the application of machine learning in cloud forensics analysis and event detection. Moreover, they proposed the development of a practical framework based on this classification system. The primary objective of this entire endeavor was to investigate cloud forensics, address associated challenges, and advance the field of evidence and analysis. The study's findings highlight the utilization of machine learning to identify research gaps, the introduction of an innovative technique that considers forensic challenges, the exploration of blockchain as a valuable resource for evidence, and the recognition of the importance of reliable evidence and analysis.

Mohammed et al. [32] conducted an analysis of the challenges encountered by cloud computing. The researchers focused on the vulnerabilities within the cloud environment that can be exploited for cybercrime. The primary objective of this research was to provide a comprehensive understanding of digital forensics. In addition, the authors proposed various models and tools that assist in the examination and retrieval of digital evidence obtained from compromised systems.

Malik et al. [25] enhanced the understanding of challenges related to data storage in a cloud environment and proposed improvements. Their study also highlights potential research opportunities to advance our knowledge of cloud data protection and storage complexity. In addition, their research addresses the strategic development challenges in cloud computing and provides a thorough analysis to address the complexities inherent in the evolution of cloud computing. The findings of this study contribute to enhancing the defense of digital evidence in the cloud through improved evidence collection and analysis, secure data transfer, and enhanced data security and integrity.

Karagiannis et al. [4] thoroughly examined the challenges associated with concealing crime in cloud computing. These challenges encompass both practical and legal aspects. The authors identify these challenges, retrieving digital evidence stored on cloud servers and carrying out a methodical analysis. Moreover, they propose the concept of power dis-

posal as an interdisciplinary approach that involves collaboration between organizational, legal, and technological perspectives with global implications.

Yassin et al. [33] provided a comprehensive examination of the challenges encountered during the investigation of cloud computing practices. Moreover, they focused on the specific complexities associated with managing digital evidence stored on cloud servers. The authors highlight the significance of enhancing security measures and bolstering confidence in threat investigations within the cloud environment. This is achieved through a thorough analysis of the threats and the proposed introduction of innovative approaches.

Fernando [34] conducted a study focused on assessing the effectiveness of forensics technologies in cybercrime investigations. The study explored the utilization of advanced technologies, such as machine learning and deep learning algorithms, to improve the precision of forensic tools, address the obstacles encountered by investigation tools when handling data, and underscore the necessity for detection mechanisms.

Pandi et al. [35] explored the vulnerabilities and potential risks associated with forensic issues in a distributed cloud system, with a view to providing recommendations for mitigating these challenges. The authors explored the challenges posed by cybercrime in the context of cloud computing, such as data tampering, email attacks, and denial of service attacks across wide geographical areas. In addition, they leveraged cloud computing technologies to address the scarcity of literature on the subject. Their study examined the primary obstacles encountered in cloud forensics and proposed a framework for preserving the integrity and confidentiality of logs.

The primary objective of the research by CHOI [36] was to explore the challenges faced by forensic experts in safeguarding organizations against criminal activities and to propose strategies to address these challenges. Moreover, it emphasized the importance of digital forensic methodologies in investigating and preventing criminal behavior. The study made several recommendations, such as leveraging cloud computing for centralized data storage and backup solutions, establishing legal frameworks for the handling and presentation of digital evidence in legal proceedings, and adopting advanced detection techniques to enhance the link between digital investigations and crime analysis. The ultimate goal of these proposed solutions is to enhance the capabilities of digital forensics teams in identifying organizational misconduct and ensuring the admissibility of collected evidence in court.

Sharma et al. [37] presented a new approach to digital forensics in the context of the traceable cloud. The main objective of their study was to promptly identify and retrieve unique evidence related to malicious activities, with a specific emphasis on cloud-based mobile applications. They proposed a system that aims to enhance the ability to track the cloud within the vast cloud storage infrastructure. The ultimate goal of this approach is to enhance cloud-based digital forensics and facilitate the investigation of cybercrime involving mobile applications, particularly those operating in cloud environments.

Vaidya et al. [38] conducted a study that explored the potential opportunities and challenges of cloud forensics within the cloud computing landscape. The introduction of the "Forensic Cloud" concept in this research enables investigators to streamline the investigative process within a cloud-based environment, ultimately enhancing and streamlining the cloud forensics investigation approach.

Abiodun et al. [39] conducted a thorough analysis of data provenance in cloud forensic investigations. Their research focused on investigating methods to track the source, history, and authentication of data in cloud computing settings for forensic use. It also addressed the obstacles related to data provenance in cloud forensics and explored potential solutions such as best practices, technologies, and methodologies to improve the efficiency of data acquisition in cloud forensic investigations.

Deebak et al. [40] concentrated primarily on the creation of a secure authentication framework for the Internet of Things (IoT) and cloud-based forensics, utilizing thin smartcards. However, they also emphasized the authentication of cloud-based data for forensic purposes. By improving user authentication procedures within cloud environments, their

research makes a valuable contribution to enhancing the overall security position of cloud-based data.

Sonia Akter et al. [41] conducted a study centering on the examination of cloud-based data in the context of forensic investigation in cloud computing environments. Their research not only examined the challenges faced during forensic analysis of cloud-stored data but also proposed solutions to overcome these challenges. Furthermore, the study emphasized the importance of comprehending the distinct attributes of cloud data, such as decentralized storage, encryption, and reliance on cloud service providers.

Ahmed [42] focused primarily on the examination of the obstacles associated with cloud-based data in the field of cloud forensics. The author's research explored the unique challenges confronted by forensic investigators when confronted with data stored on cloud servers. These challenges encompass issues related to data acquisition, preservation, and analysis. Moreover, the study highlighted that cloud environments present distinctive challenges due to various factors, including data storage across multiple geographic locations, the utilization of shared servers by multiple users, encryption, and security measures, as well as the dynamic nature of cloud computing.

Hassan Kaleem [43] analyzed the obstacles encountered by forensic examiners in gathering evidence against cybercriminals operating in cloud environments, while also ensuring the preservation and protection of data integrity and security. Moreover, this study examined various concerns, such as data privacy, data integrity, data ownership, and the preservation of digital evidence within cloud infrastructures. In addition, it highlighted the potential of blockchain technology as a reliable and transparent approach for tracking and validating digital evidence within cloud environments.

Alouffi et al. [44] investigated and analyzed digital data stored in cloud environments. They conducted an SLR to explore the latest cloud forensic frameworks, tools, and challenges in the field of cloud forensics, and made recommendations to overcome these challenges.

Ahmed Ali et al. [45] attempted to identify and resolve the obstacles encountered in cloud forensics, specifically in the investigation of cloud data. They emphasized the challenges faced by investigators due to the special features of cloud computing. These features include its distributed architecture, data volatility, encryption, and reliance on cloud service providers (CSPs). In addition, their study offered a clear understanding of the effective execution of forensic investigations within cloud environments.

Prakash et al. [46] examined the effects of cloud computing on computer forensics. They focused on the challenges encountered by digital forensics in handling data stored in cloud environments and suggested possible solutions to deal with these challenges. Furthermore, their study aimed to enhance digital forensic practices within the environment of cloud and edge computing.

Hemdan et al. [47] introduced a cloud forensics investigation model (CFIM) designed to assist in the examination of cybercrime within cloud computing settings. The model addresses the challenges faced by digital investigators in handling data stored in the cloud, such as reconstructing historical events, and recognizing, gathering, safeguarding, analyzing, interpreting, and documenting digital proof. The innovative system suggested in their study takes snapshots of virtual machine conditions for forensic scrutiny, improving the efficiency of forensic investigations in cloud environments by emphasizing a method that is both forensically sound and prompt in investigating cloud-stored data.

Joshi et al. [48] explored the environment of cloud forensics, and their examination of cloud-based data focused on secure logging systems. The authors highlighted the significance of safeguarding the confidentiality and privacy of cloud users by employing searchable encryption methods to safeguard sensitive information stored in cloud logs. Furthermore, the paper concentrated on the vulnerabilities and challenges associated with examining cloud-based data and ensuring the integrity of forensic investigations.

Literature Reviews

The latest research and studies related to our SLR are encompassed within this section. In order to construct a theoretical framework, it is imperative to thoroughly examine each study, pinpoint the key themes, and extract the primary conclusions, obstacles faced, and the corresponding strategies utilized to address these challenges. This information is presented in the tables below.

Table 4 presents a summary of various literature reviews related to the field of digital forensics and its specific focus on cloud computing environments. These literature reviews offer insights into the challenges, methodologies, tools, and solutions relevant to conducting forensic investigations in cloud-based systems.

By synthesizing and analyzing the literature reviews presented in Table 4, researchers can gain a valuable understanding of the current research landscape, emerging trends, and unresolved issues in digital forensics within cloud computing environments.

Table 4. Literature reviews.

Ref.	Techniques	Challenges	Main Finding
[31]	• Machine learning. • Cloud forensics taxonomy. • Digital forensics tools. • Network forensics. • Log analysis.	• Identification of evidence. • Architectural support. • Trust and provenance. • Data privacy and security. • Scalability.	• Determine the primary obstacles in cloud forensics and investigate the methods employed to overcome them.
[32]	• Some techniques used by attackers to conceal or obscure. • A range of instruments for gathering and evaluating evidence. • Methods for reporting and analyzing evidence in the context of digital forensics.	• Technological challenges. • Legal challenges. • Resource challenges. • The ease with which evidence may be committed and erased in cloud systems, as well as the identification of breach indications and unusual network activity, pose challenges for cloud forensics.	• The value of digital forensics in recovering digital evidence from corrupted devices, examining it, and presenting it in court.
[25]	• A comprehensive review of publications in the domain of digital forensics for clouds. • Analyzing the financial implications of data breaches. • Analyzing the differences between traditional digital forensics and forensic procedures tailored to the cloud.	• Applying the encryption methods. • Handling the difficulties associated with decentralized data management. • Guaranteeing the secure transfer and storage of data.	• Emphasized the significance of comprehending and overcoming the data-related obstacles, especially those posed by the cloud environment. Also emphasized the differences between the process of digital forensics that is unique to cloud computing and the face of traditional digital forensics.

Table 4. *Cont.*

Ref.	Techniques	Challenges	Main Finding
[34]	• Algorithms for deep learning and machine learning • Mechanisms for real-time intrusion detection. • Selecting features and identifying data. • Real-time acquisitions in mobile devices and network systems. • Patterns and data sets for training.	• Accuracy. • Data extraction capacity. • Responsiveness. • Encryption. • Compatibility issues. • Outdated data sets. • Real-time intrusion detection. • Technology variations.	• Identify problems with cyber forensics and provide an overview of obstacles in the technique.
[35]	• System of identity protection. • Accessible forensic software. • Development of a framework to improve forensic expertise. • Mitigation technique to improve the forensics process.	• Inadequate equipment in the given situation. • Absence of analysis and collection of evidence. • Anti-forensic equipment. • Integrity. • Multi-tenants. • Privacy. • Volatile data. • Encryption.	• Determine the dangers, vulnerabilities, security concerns, and forensics issues that affect the dispersed cloud infrastructure and take steps to address them.
[36]	• Anti-forensic methods include using contemporary encryption software among other things. • Laws and rules create a legal framework that will offer instructions on how to gather and present digital evidence in court. • Data collecting includes creating software to protect data while it is being collected and preserving the integrity of digital evidence, among other things. • Changes in technology include adopting new tools and software, providing training on them, and using updated tools and software to improve data interpretation and analysis in digital forensic investigations.	• Technical problems include encryption software impeding the availability of criminal evidence, among other things. • Legal issues include the absence of rules and regulations governing the presenting of evidence in courts and other settings. • Resource problems include the need for specialists in digital forensics and specific tools for data analysis, among other things.	• The difficulties and fixes discovered in the organization's defense against crimes.

Table 4. *Cont.*

Ref.	Techniques	Challenges	Main Finding
[37]	• Synchronization of time. • Analysis both within and between applications. • Reduction and extraction of data. • Live forensics on memory.	• Abuse of social media platforms. • Cloud traceability. • Synchronization of time. • Gather and examine the information.	• Devise a new method of mobility cloud forensics focused on synchronizing the time and process of digital forensics.
[38]	• Improve forensic instruments.	• Storage system authority. • Setting with multiple tenants. • Restoring deleted information. • Gathering of evidence. • In cloud systems, it might be difficult to connect a single data file to a certain suspect.	• The cloud presents particular difficulties for digital forensic investigators, who must also comprehend the cloud's forensic component in order to address criminal matters.
[39]	• Implementation of policies and standards to ensure the confidentiality of data provenance. • Developing methods to track the origin of data objects. • Exploring approaches to extract provenance information from data themselves.	• Ensuring the confidentiality of data provenance while maintaining security and privacy. • Ensuring data accountability and integrity. • Handling the extraction of provenance from incomplete or partially available information.	• Recognize the challenges in data sourcing for cloud forensic investigations, and emphasize the importance of addressing these challenges to ensure the integrity of digital evidence.
[40]	• Smartcard-based authentication. • Establishing secure session keys between devices to facilitate secure communication and data access.	• Security concerns: ensuring robust security measures in cloud-based IoT applications. • Balancing security requirements with the need for efficient authentication processes. • Resistance to attacks. • Maintaining user anonymity while ensuring proper authentication and authorization processes. • Managing session keys securely. • Optimizing the performance of authentication processes.	• Development of a novel lightweight authentication solution tailored for cloud-based forensics in intelligent data computing environments.

Table 4. *Cont.*

Ref.	Techniques	Challenges	Main Finding
[41]	• Identification techniques. • Preservation techniques. • Collection techniques. • Examination and analysis methods. • Presentation and reporting strategies.	• Log format unification. • The presence of servers with different log formats in different geographic locations operating under different time zones. • Real-time investigation limitations. • Data integrity and evidence preservation. • Lack of terms and conditions in SLA. • Forensics skills gap. • Coordination in cross-national data access. • Dependency on cloud service providers (CSPs). • Data integrity risks with CSP agreements.	• Explores the threats and attacks that cloud environments may face. Discusses different approaches and frameworks that can be employed in cloud forensics to address the practical challenges and limitations encountered during forensic investigations in cloud computing environments.
[42]	• Data acquisition tools: researchers have developed tools and techniques for acquiring data from cloud servers, including methods for extracting data from cloud storage providers such as Dropbox and Google Drive.	• Data acquisition challenges. • Data preservation complexity. • Encryption and security measures. • Lack of control over cloud infrastructure. • Dynamic nature of cloud computing. • Standardization and collaboration. • Legal and regulatory issues.	• This paper highlights the critical nature of digital and cloud forensics in modern investigations, the challenges faced in these fields, and the necessity for ongoing research, standardization, collaboration, and specialized tools to enhance the effectiveness of forensic investigations in digital and cloud environments.
[33]	• Gain access to the cloud environment's logs. • Module for trust platform (TPM). • Make use of the remote control log server. • Snapshots of virtual machines (VMs). • Intrusion system detection. • Isolate the devices in the virtual computer.	• The challenges in obtaining the available evidence. • The customer's knowledge and the lack of control over the cloud system. • Legal concerns about global cloud computing. • Problems with the data safe. • Restricted authority over access. • Duplication of data and encryption.	• There are several obstacles to overcome when researching the investigation and forensics of cloud computing.

Table 4. *Cont.*

Ref.	Techniques	Challenges	Main Finding
[43]	• Digital forensics methodologies: the study explores the methodologies used in digital and cloud forensics, emphasizing the importance of systematic approaches for collecting, preserving, extracting, and presenting digital evidence in cloud environments. These methodologies provide a structured framework for conducting forensic investigations in the cloud.	• Data privacy concerns: Cloud environments raise significant data privacy issues due to the distributed nature of data storage and the potential for unauthorized access. Ensuring the privacy of sensitive information during forensic investigations poses a challenge for investigators.	• Identification of challenges: the study identifies various challenges faced by forensic investigators when dealing with cloud-based data, including issues related to data privacy, data integrity, data ownership complexities, and the preservation and analysis of digital evidence in cloud environments.
[44]	• Intrusion detection systems (IDSs): the study discusses the use of IDSs as a solution to security threats in cloud computing environments, emphasizing the importance of detecting and preventing unauthorized access and malicious activities.	• Challenges in forensic data collection and edge computing environments, including risks such as forensic data removal or log leakage.	• Identification of security threats such as data tampering, data leakage, data intrusion, and data storage challenges in cloud computing environments. Recognition of the importance of intrusion detection systems (IDSs) in providing security solutions for cloud-based data.
[45]	• Log-based techniques to trace intruders and identify malicious activity in cloud environments. • Forensic frameworks for cloud computing to support evidence collection, analysis, and investigation processes.	• Distributed architecture: the complex and distributed nature of cloud environments poses a challenge for forensic investigators in tracing and correlating data across heterogeneous cloud structures.	• Identification of challenges: the paper identifies various challenges faced by forensic investigators in cloud environments, such as the distributed architecture, data volatility, encryption, and dependency on cloud service providers (CSPs).
[46]	• Distributed nature and remote storage: techniques for establishing location and data identification as part of the investigation process in cloud environments, despite challenges in identifying cloud suspects and preserving evidence.	• Lack of international collaboration and jurisdictional issues: challenges arise due to the complexities of international collaboration and jurisdictional issues, impacting the timely arrest and detention of witnesses and suspects residing abroad.	• Identification of the impact of cloud and edge computing on computer forensics, highlighting the challenges faced by digital forensic practitioners in dealing with data stored in cloud environments.

Table 4. *Cont.*

Ref.	Techniques	Challenges	Main Finding
[47]	• Cloud forensics investigation model (CFIM): The paper introduces the CFIM as a technique to support the investigation of cybercrime in cloud computing environments. This model involves periodically capturing snapshots of virtual machine states for forensic analysis, enhancing the ability to reconstruct past events and extract digital evidence in the cloud.	• Complexity of cloud systems: the virtualized, distributed, and dynamic nature of cloud systems poses challenges for forensic investigators in reconstructing past events and collecting digital evidence.	• Introduction of a cloud forensics investigation model (CFIM) designed to support the investigation of cybercrime in cloud computing environments.
[48]	• Secure logging system: The paper proposes a secure logging system that encrypts sensitive information in cloud logs using encryption techniques such as AES and MD5. By encrypting user data, including IP addresses, MAC addresses, and email addresses, the system aims to enhance the security of cloud-based data and protect against unauthorized access.	• Security vulnerabilities: Cloud environments are susceptible to security breaches and attacks, making it challenging to ensure the confidentiality and integrity of user data stored in the cloud. The paper emphasizes the need for robust security measures to protect sensitive information and prevent unauthorized access.	• Proposal of a secure logging system: the paper proposes a secure logging system that focuses on encrypting sensitive information in cloud logs, such as IP addresses, MAC addresses, and email addresses, to enhance the security of user data stored in the cloud.
[4]	• A thorough examination of the legal implications of cloud forensics, with an emphasis on gathering and managing digital evidence in the cloud.	• Territoriality. • Possession. • Confiscation procedure.	• Select the main three legal challenges.

5. Findings and Insights

In the realm of cybercrime investigation, digital forensics plays a crucial role in the identification, preservation, and examination of digital evidence. Nevertheless, conducting digital forensic analysis on cloud data presents unique challenges that must be overcome to guarantee the efficiency of investigations and the successful prosecution of cybercrime. The obstacles encountered in cloud-based digital forensics investigations are numerous, and this section examines the specific challenges outlined above. All the information mentioned in this section is derived from our thorough analysis and extensive collection of challenges and technologies that were discussed in Section 4. We have gained a comprehensive understanding through the careful examination and evaluation of sources.

5.1. Challenges in Cloud Forensics

The papers that were analyzed encompassed a wide range of challenges, including privacy concerns, encryption methods, legal reporting and transferring procedures, ensuring confidentiality and integrity, and resistance to attacks, as well as the gathering and examination of information, among many others. Drawing from the previous section, the challenges confronting digital forensics in cloud computing can be categorized into various types.

- **Technical Issues**
  Cloud computing presents various technical challenges when it comes to preserving digital evidence, one of which involves safeguarding the evidence against any unauthorized modifications.
- **Legal Issues**
  The issue at hand pertains to privacy, which poses a significant obstacle for investigators. Consequently, investigators must meticulously and lawfully store the data they have collected.
- **Resource Issues**
  Conducting investigations in a cloud environment presents a range of challenges for investigators, including limitations that impact various aspects of digital forensics.

The most important challenges that were identified and extracted from the articles are analyzed and categorized into their types in Table 5.

Table 5. Challenges for each type

Technical Challenges	Resource Challenges	Legal Challenges
• Identification/gathering of evidence. • Architectural support. • Data privacy and security. • Scalability. • Protecting evidence. • Anti-forensic techniques. • Anti-forensic equipment. • Automated tools. • Handle large amounts of data. • Applying the encryption methods. • Handling the difficulties associated with decentralized data management. • Guaranteeing the secure transfer and storage of data. • Customer's knowledge and lack of control over the cloud system. • Restricted authority over access. • Duplication of data. • Accuracy. • Data extraction. • Capacity. • Responsiveness. • Compatibility issues. • Outdated data sets. • Real-time intrusion detection. • Technology variations. • Inadequate equipment in the given situation. • Absence of analysis and collection of evidence. • Integrity.	• Scalability. • Investigating large amounts of data. • Data integrity. • Considering only recent and relevant information. • Handling the difficulties associated with decentralized data management. • Guaranteeing the secure transfer and storage of data. • Challenges in obtaining the available evidence. • Customer's knowledge and lack of control over the cloud system. • Legal concerns about global cloud computing. • Data extraction. • Capacity. • Responsiveness. • Compatibility issues. • Outdated data sets. • Real-time intrusion detection. • Technology variations. • Inadequate equipment in the given situation. • Absence of analysis and collection of evidence. • Need for specialists in digital forensics. • Specific tools for data analysis. • Synchronization of time.	• Architectural support. • Data privacy and security. • Ensuring that information is stored legally. • Applying the encryption methods. • Guaranteeing the secure transfer and storage of data. • Territoriality. • Possession. • Confiscation procedure. • Legal concerns about global cloud computing. • Restricted authority over access. • Duplication of data. • Anti-forensic equipment. • Integrity. • Multi-tenants. • Volatile data. • The absence of rules and regulations governing the presenting of evidence. • Abuse of social media platforms. • Cloud traceability. • Gather and examine the information. • Storage system authority. • Restoring deleted information. • Gathering of evidence. • Difficult to connect a single data file to a certain suspect. • Confidentiality. • Accountability.

Table 5. *Cont.*

Technical Challenges	Resource Challenges	Legal Challenges
• Multi-tenants. • Privacy. • Volatile data. • Encryption software. • Abuse of social media platforms. • Cloud traceability. • Synchronization of time. • Gather and examine the information/data collected. • Storage system authority. • Restoring deleted information. • Difficult to connect a single data file to a certain suspect. • Confidentiality. • Accountability. • Extraction of provenance information. • Resistance to attacks. • Maintaining user. • Managing session keys securely. • Optimizing the performance of authentication processes. • Log format unification. • The presence of servers with different log formats in different geographic locations operating under different time zones. • Real-time investigation limitations. • Evidence preservation. • Forensics skills gap. • Data acquisition challenges. • Data preservation complexity. • Security measures. • Lack of control over cloud infrastructure. • Dynamic nature of cloud computing. • Standardization and collaboration. • Development of specialized tools and techniques. • Edge computing environments. • Forensic data removal or log leakage. • Suspicious intrusion detection systems (IDSs). • Distributed architecture. • Lack of forensic services. • Evidentiary considerations. • Identifying cloud suspects. • Complexity of cloud systems. • Data provenance and evidence segregation. • Crime scene reconstruction. • Snapshot preservation. • Security vulnerabilities. • Insider attacks. • Forensic analysis in cloud environments.	• Gather and examine the information/data collected. • Gathering of evidence. • Extraction of provenance information. • Real-time investigation limitations. • Forensics skills gap. • Coordination in cross-national data access. • Dependency on cloud service providers (CSPs). • Data acquisition challenges. • Data preservation complexity. • Lack of control over cloud infrastructure. • Dynamic nature of cloud computing. • Standardization and collaboration. • Legal and regulatory issues. • Development of specialized tools and techniques. • Fostering collaboration among stakeholders. • Data ownership complexities. • Multi-jurisdictional distribution. • Edge computing environments. • Suspicious intrusion detection systems (IDSs). • Distributed architecture. • Data volatility. • Handling big data. • Time and cost constraints. • Lack of forensic services. • Inadequate equipment in the given situation. • Lack of international collaboration and jurisdictional issues. • Legal barriers. • Complexity of cloud systems. • Snapshot preservation. • Forensic analysis in cloud environments. • Compliance and legal issues.	• Evidence preservation. • Lack of terms and conditions in SLA. • Coordination in cross-national data access. • Dependency on cloud service providers (CSPs). • Security measures. • Lack of control over cloud infrastructure. • Dynamic nature of cloud computing. • Standardization and collaboration. • Legal and regulatory issues. • Data ownership complexities. • Multi-jurisdictional distribution. • Forensic data removal or log leakage. • Suspicious intrusion detection systems (IDSs). • Lack of international collaboration and jurisdictional issues. • Evidentiary considerations. • Legal barriers. • Identifying cloud suspects. • Data provenance and evidence segregation. • Crime scene reconstruction. • Security vulnerabilities. • Insider attacks. • Forensic analysis in cloud environments. • Compliance and legal issues.

This structured approach enables a more targeted and effective strategy for overcoming the diverse obstacles faced in digital forensic investigations.

The articles we analyzed revealed that certain challenges are frequently discussed. Data privacy and security are prominent challenges, falling under both legal and technical categories, and they were mentioned multiple times in separate articles. Similarly, the challenge of applying encryption methods is also categorized under technical and legal challenges, appearing in nearly seven separate articles.

When it comes to the resource field, we found that the challenge of gathering and examining information/data collection is the most frequently mentioned challenge in the analyzed articles. It is important to note that our analysis focused solely on recent articles discussing the challenges in digital forensics. Other challenges are presented in Table 5.

As presented in Figure 2, the percentage of technical challenges (42%) is greater than any other type, followed by resource challenges (30%), and lastly legal challenges (28%). It is also important to note that some types of challenges can fall under multiple categories. For example, integrity is both a legal and a technical challenge, as presented in Table 5.

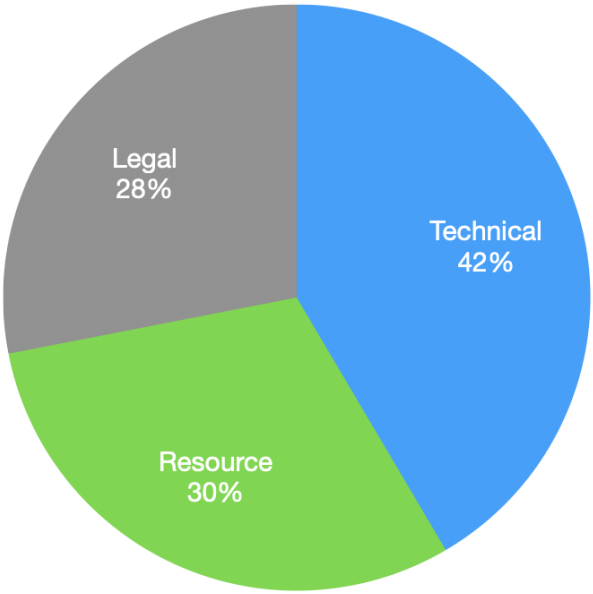

Figure 2. Percentage of each type.

Figure 3 presents some challenges in each type of problem that are repeated through the analyzing process in each article. In addition, it was through this analyzing process that the solution or the techniques used to solve the challenges faced by the investigators emerged, as demonstrated in the above section. This part of the work adds more value to our survey.

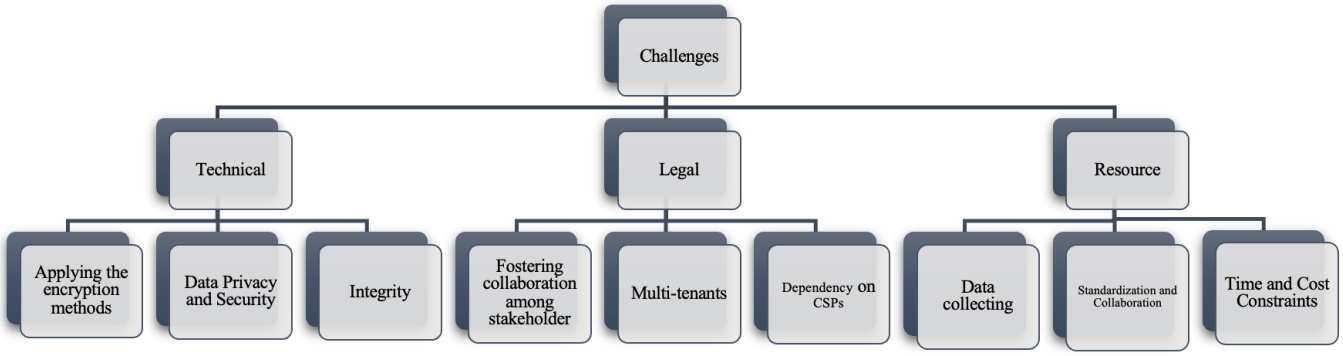

Figure 3. Various challenges for each type.

5.2. Techniques That Are Used to Solve the Challenges

After analyzing the selected articles, we identified various techniques to address the challenges encountered in the forensic process.

Table 6 presents the potential security solution for each challenge that can be overcome or addressed using certain security techniques.

Table 6. Potential security solution for each challenge.

Challenge	Type	Potential Security Solution
Identification/gathering of evidence	Technical	Implement advanced data collection tools and techniques for efficient evidence gathering.
Architectural support	Technical	Develop forensic tools that are compatible with various cloud architectures.
Data privacy and security	Technical	Utilize strong encryption methods and access controls to protect data integrity and confidentiality.
Protecting evidence	Technical	Establish secure storage mechanisms and access controls to prevent tampering with evidence.
Customer's knowledge and lack of control	Resource	Provide training and education to users to enhance their understanding of cloud security best practices.
Restricted authority over access	Resource	Implement role-based access controls and privilege management to restrict unauthorized access.
Accuracy	Resource	Implement data validation and integrity checks to ensure the accuracy of forensic findings.
Duplication of data	Resource	Establish data deduplication processes to eliminate redundant data and improve storage efficiency.
Absence of analysis and collection of evidence	Legal	Establish clear legal procedures for evidence collection and analysis in cloud environments.
Integrity	Legal	Ensure data integrity throughout the forensic investigation process to maintain the credibility of evidence.
Multi-tenants	Legal	Develop protocols for handling data from multiple tenants in shared cloud environments to prevent data leakage.
Privacy	Legal	Implement privacy-enhancing technologies and policies to protect sensitive information during investigations.

Many strategies are employed to mitigate the obstacles in cloud forensics, including updating forensic tools, training personnel, utilizing trusted platform models, implementing the cloud forensics investigation model (CFIM), enhancing authentication methods, and establishing secure logging systems, among others. However, the most crucial and commonly utilized techniques in this domain include machine learning, analyzing evidence, generating reports, collecting data for examination, detecting intrusions, utilizing forensic software, and employing log-based techniques.

The most commonly used techniques to address the challenges identified and analyzed in this paper are presented in Figure 4. Based on our analysis, it can be inferred that the majority of strategies employed to address the obstacles encountered in the field of forensics pertaining to cloud computing focus primarily on the collection and administration of evidence, constituting approximately 21% of the total of 37 techniques extracted from previous research.

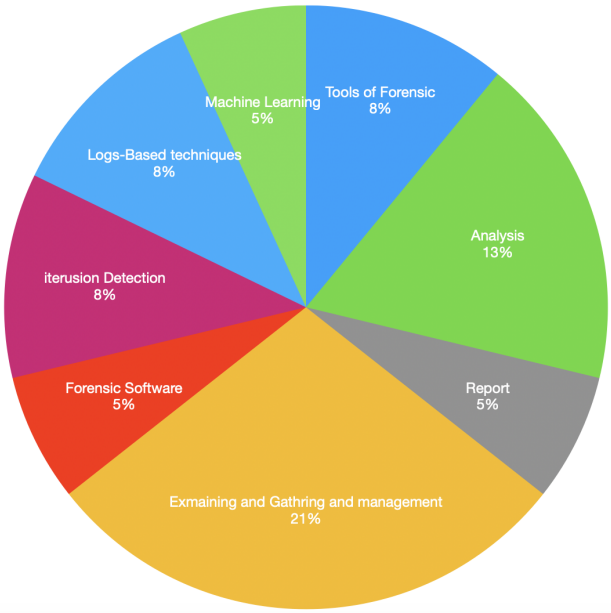

Figure 4. Most commonly used techniques.

6. Comparison of Systematic Literature Review with Another Paper

This section presents a comparison between our SLR and the SLR presented in [49], focusing on the aims of the SLRs, the methodologies used, the extraction of information, and the conclusions derived from each SLR.

First, ref. [49] provides a comprehensive survey to identify the latest tools, technologies, and challenges in digital forensics. That study focuses on identifying the challenges and future directions in computer forensics. By contrast, our SLR concentrates on identifying the challenges and corresponding technologies used to address each challenge, thereby assisting readers and researchers in finding and simplifying possible solutions. Moreover, our SLR is specifically focused on cloud computing, whereas [49] addresses the broader field of digital forensics.

The methodology in [49] involves selecting the most important and recent digital forensics concepts from existing research and comparing the characteristics of various tools. It also identifies current challenges and future research directions in digital forensics. Furthermore, it presents a model for recognizing tools, which assists researchers in deciding which tools to use in specific situations. Our SLR, on the other hand, is focused on cloud computing and includes a general overview of cloud computing along with the concept of digital forensics, specifically in the context of cloud computing. We discuss the challenges faced by investigators in cloud forensics, categorizing them by type (resource, technical, or legal), and present the techniques used to address these challenges.

As far as challenges are concerned, ref. [49] emphasizes the resource challenges faced by researchers in digital forensics and provides a model that optimizes tools for these challenges. Our SLR categorizes each challenge by type and includes techniques or solutions from recent publications to address each challenge.

While [49] highlights resource-type challenges and presents a model with the characteristics of each tool, our paper classifies each challenge by type and mentions the techniques and tools used to solve these challenges.

7. Conclusions

This article emphasizes the significance of keeping abreast of the latest trends and advancements in digital forensics within cloud computing. As technology progresses swiftly, it is essential for investigators to adapt and improve their skills to effectively address the intricacies of cloud-based investigations. The implementation of the PRISMA methodology in conducting the literature review enhances the research's credibility and applicability.

By presenting a thorough overview of the challenges and solutions in this domain, this study serves as a valuable resource for both experienced professionals and newcomers in the digital forensics field. It provides insights into the optimal practices and strategies that can be utilized to overcome obstacles and ensure successful investigations in the cloud computing landscape.

This study classifies the challenges of cloud forensics into technical, legal, and resource-based categories, offering techniques and tools as solutions to address these challenges.

In conclusion, this document serves as a comprehensive manual for individuals seeking to deepen their knowledge of digital forensics in the realm of cloud computing. It lays out a roadmap for navigating the complexities of this rapidly evolving field and equips readers with the necessary knowledge and tools to effectively deal with challenges and achieve successful outcomes in their investigations. In order to advance the field of cloud forensics, it is imperative to focus on the development of tools and methods, as well as improving their interoperability. In addition, it is crucial to enhance the preparedness of cloud forensics for future challenges.

8. Future Works

There are several areas that future research on cloud forensics could focus on in order to address emerging issues and advance knowledge in this field. Some potential avenues for future research include the following:

- Addressing security vulnerabilities: Given the constantly evolving nature of cybersecurity threats, future research could concentrate on identifying and mitigating security vulnerabilities in cloud environments. This could involve developing strategies to detect and prevent insider attacks, data breaches, and other security incidents that may impact forensic investigations.
- Improving forensic analysis techniques: Research efforts could be directed towards enhancing forensic analysis techniques to overcome the unique challenges posed by cloud environments. This could involve exploring advanced methods for data recovery, memory forensics, and network traffic analysis techniques that are specifically optimized for cloud-based data.
- Promoting collaboration and knowledge sharing: Encouraging collaboration and knowledge sharing among researchers, practitioners, law enforcement agencies, and cloud service providers is crucial for advancing the field of cloud forensics. Future research could explore mechanisms for facilitating collaboration, such as establishing interdisciplinary research networks, organizing workshops and conferences, and creating repositories of best practices and case studies.

In addition, we recommend utilizing actionable solutions to the challenges identified in cloud forensics, such as the following:

- Implement comprehensive logging and monitoring: It is important to verify that all cloud services have been set up to produce comprehensive logs and to consistently review and analyze these logs.
- Data preservation and collection: Create uniform protocols for safeguarding and gathering digital evidence within cloud settings to guarantee the reliability and acceptability of information.
- Ensure forensic readiness: Get ready for possible forensic investigations by integrating forensic readiness into the corporate culture and cloud deployment plan.

In conclusion, future research on cloud forensics should prioritize interdisciplinary collaboration, technological innovation, and a proactive approach to addressing emerging challenges. This will help advance the field and enhance the effectiveness of digital forensic investigations in cloud-based data environments.

Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. KFU241499].

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. KFU241499]. The authors would like to thank the anonymous reviewers for their insightful scholastic comments and suggestions, which improved the quality and clarity of the paper.

Conflicts of Interest: The authors declare no conflicts of interest.The funders had no role in the design of the study; in the collection, analyses, or interpretation of data.

References

1. Mell, P.; Grance, T. *The NIST Definition of Cloud Computing*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011; pp. 800–1457. [CrossRef]
2. Bhardwaj, A.K.; Garg, L.; Garg, A.; Gajpa, Y. E-Learning during COVID-19 Outbreak: Cloud Computing Adoption in Indian Public Universities. *Comput. Mater. Contin.* **2021**, *66*, 2471–2492. [CrossRef]
3. Njenga, K.; Garg, L.; Bhardwaj, A.K.; Prakash, V.; Bawa, S. The cloud computing adoption in higher learning institutions in Kenya: Hindering factors and recommendations for the way forward. *Telemat. Inform.* **2019**, *38*, 225–246. [CrossRef]
4. Karagiannis, C.; Vergidis, K. Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information* **2021**, *12*, 181. [CrossRef]
5. Ali, K.M. Digital Forensics Best Practices and Managerial Implications. In Proceedings of the 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks, Phuket, Thailand, 24–26 July 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 196–199. [CrossRef]
6. Ruan, K.; Carthy, J.; Kechadi, T.; Baggili, I. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digit. Investig.* **2013**, *10*, 34–43. [CrossRef]
7. Simou, S.; Kalloniatis, C.; Gritzalis, S.; Mouratidis, H. A survey on cloud forensics challenges and solutions. *Secur. Commun. Netw.* **2016**, *9*, 6285–6314. [CrossRef]
8. Martini, B.; Choo, K.K.R. Cloud storage forensics: OwnCloud as a case study. *Digit. Investig.* **2013**, *10*, 287–299. [CrossRef]
9. Taylor, M.; Haggerty, J.; Gresty, D.; Lamb, D. Forensic investigation of cloud computing systems. *Netw. Secur.* **2011**, *2011*, 4–10. [CrossRef]
10. Marty, R. Cloud application logging for forensics. In *ACM Symposium on Applied Computing, Proceedings of the SAC'11: The 2011 ACM Symposium on Applied Computing, TaiChung, Taiwan, 21–24 March 2011*; Association for Computing Machinery: New York, NY, USA, 2011; pp. 178–184. [CrossRef]
11. Dykstra, J.; Sherman, A.T. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. *Digit. Investig.* **2013**, *10*, S87–S95. [CrossRef]
12. Vadetay Saraswathi Bai, T.S. A Systematic Literature Review on Cloud Forensics in Cloud Environment. *Int. J. Intell. Syst. Appl. Eng.* **2023**, *11*, 565–578.
13. Ruan, K.; Baggili, I.; Prof, J.; Carthy, P.; Kechadi, T. Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. *Researchate* **2011** . Available online: https://www.researchgate.net/publication/228419717_Survey_on_cloud_forensics_and_critical_criteria_for_cloud_forensic_capability_A_preliminary_analysis (accessed on 11 July 2024).
14. Casino, F.; Dasaklis, T.K.; Spathoulas, G.P.; Anagnostopoulos, M.; Ghosal, A.; Borocz, I.; Solanas, A.; Conti, M.; Patsakis, C. Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews. *IEEE Access* **2022**, *10*, 25464–25493. [CrossRef]
15. Bamiah, M.; Brohi, S. Exploring the Cloud Deployment and Service Delivery Models. *Int. J. Res. Rev. Inf. Sci.* **2011**, *3*, 2046–6439. Available online: https://www.researchgate.net/publication/257995661_Exploring_the_Cloud_Deployment_and_Service_Delivery_Models (accessed on 3 July 2024).
16. Gill, S.S.; Wu, H.; Patros, P.; Ottaviani, C.; Arora, P.; Pujol, V.C.; Haunschild, D.; Parlikad, A.K.; Cetinkaya, O.; Lutfiyya, H.; et al. Modern computing: Vision and challenges. *Telemat. Inform. Rep.* **2024**, *13*, 100116. [CrossRef]
17. Alqahtany, S.; Clarke, N.; Furnell, S.; Reich, C. Cloud Forensics: A Review of Challenges, Solutions and Open Problems. In Proceedings of the 2015 International Conference on Cloud Computing (ICCC), Riyadh, Saudi Arabia, 26–29 April 2015; pp. 1–9.
18. Sandhu, A.K. Big Data with Cloud Computing: Discussions and Challenges. *Big Data Min. Anal.* **2022**, *5*, 32–40. [CrossRef]

19. Almulla, S.; Iraqi, Y.; Jones, A. Cloud forensics: A research perspective. In Proceedings of the 2013 9th International Conference on Innovations in Information Technology (IIT), Al Ain, United Arab Emirates, 17–19 March 2013; pp. 66–71. [CrossRef]
20. Alazab, A.; Khraisat, A.; Singh, S. *A Review on the Internet of Things (IoT) Forensics: Challenges, Techniques, and Evaluation of Digital Forensic Tools*; Intechopen: London, UK, 2023. [CrossRef]
21. Abdulsalam, Y.S.; Hedabou, M. Security and Privacy in Cloud Computing: Technical Review. *Future Internet* **2022**, *14*, 11. [CrossRef]
22. Microsoft. Microsoft Corp. v. United States. *Supremecourt* **2018**. Available online: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf (accessed on 11 July 2024).
23. Dykstra, J.; Sherman, A.T. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digit. Investig.* **2012**, *9*, S90–S98. [CrossRef]
24. Farina, J.; Scanlon, M.; Le-Khac, N.A.; Kechadi, M.T. Overview of the Forensic Investigation of Cloud Services. In Proceedings of the 2015 10th International Conference on Availability, Reliability and Security, Toulouse, France, 24–27 August 2015; pp. 556–565. [CrossRef]
25. Malik, A.; Park, T.J.; Ishtiaq, H.; Ryou, J.C.; Kim, K.I. Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. *Sensors* **2024**, *24*, 433. [CrossRef] [PubMed]
26. Chinedu, P.; Nwankwo, W.; Daniel; Shaba, M.; Momoh, M. Cloud Security Concerns: Assessing the Fears of Service Adoption. *Arch. Sci. Technol.* **2020**, *1*, 164–174. Available online: https://www.researchgate.net/publication/349607793_Cloud_Security_Concerns_Assessing_the_Fears_of_Service_Adoption (accessed on 13 July 2024).
27. Ruan, K.; Carthy, J.; Kechadi, T.; Crosbie, M. Cloud forensics: An overview. *ResearchGate* **2011**. Available online: https://www.researchgate.net/publication/229021339_Cloud_forensics_An_overview (accessed on 11 July 2024).
28. Microsoft. Governance, Security, and Compliance in Azure. *Cloud Adoption Framework* **2024**. Available online: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/govern-org-compliance?tabs=AzureSecurityCenter (accessed on 25 July 2024).
29. AWS. AWS Security Best Practices. *AWS Whitepaper* **2016**. Available online: https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/welcome.html (accessed on 25 July 2024).
30. Catteddu, D. Cloud Computing: Benefits, Risks and Recommendations for Information Security. In *Web Application Security: Iberic Web Application Security Conference, IBWAS*; Springer: Berlin/Heidelberg, Germany, 2010; Volume 72, pp. 93–113. [CrossRef]
31. Purnaye, P.; Kulkarni, V. A Comprehensive Study of Cloud Forensics. *Arch. Comput. Methods Eng.* **2021**, *29*, 33–46. [CrossRef]
32. Mohammmed, S.; Sridevi, R. A Survey on Digital Forensics Phases, Tools and Challenges. In Proceedings of the Third International Conference on Computational Intelligence and Informatics: ICCII 2018, Hyderabad, India, 28–29 December 2018; Volume 1090, pp. 237–248. Available online: https://api.semanticscholar.org/CorpusID:215834965 (accessed on 24 July 2024).
33. Yassin, W.M.; Abdollah, M.F.; Ahmad, R.; Yunos, Z.; Ariffin, A.F.M. Cloud Forensic Challenges and Recommendations: A Review. *OIC-CERT J. Cyber Secur.* **2020**, *2*. Available online: https://api.semanticscholar.org/CorpusID:216175392 (accessed on 9 July 2024).
34. Fernando, V. Cyber Forensics Tools: A Review on Mechanism and Emerging Challenges. In Proceedings of the 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 19–21 April 2021; pp. 1–7. [CrossRef]
35. Pandi (Jain), G.S.; Shah, S.; Wandra, K. Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation. *Procedia Comput. Sci.* **2020**, *167*, 163–173. [CrossRef]
36. CHOI, D.H. Digital forensic: Challenges and solution in the protection of corporate crime. *J. Ind. Distrib. Bus.* **2021**, *12*, 47–55. [CrossRef]
37. Sharma, P.; Arora, D.; Sakthivel, T. Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications. *Procedia Comput. Sci.* **2020**, *167*, 907–917. https://api.semanticscholar.org/CorpusID:219139378. [CrossRef]
38. Vaidya, N. Cloud Forensics: Trends and Challenges. *Int. J. Eng. Res. Technol.* **2020**, *9*. Available online: https://www.ijert.org/research/cloud-forensics-trends-and-challenges-IJERTV9IS090415.pdf (accessed on 20 June 2024).
39. Isaac Abiodun, O.; Alawida, M.; Esther Omolara, A.; Alabdulatif, A. Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 10217–10245. [CrossRef]
40. Deebak, B.; AL-Turjman, F. Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing. *Future Gener. Comput. Syst.* **2021**, *116*, 406–425. [CrossRef]
41. Sharma, P.; Goel, S. A Practical Guide on Security and Privacy in Cyber-Physical Systems: Foundations, Applications and Limitations. *World Sci. Ser. Digit. Forensics Cybersecur.* **2023**, *3*, 264. [CrossRef]
42. Alenezi, A.M. Digital and Cloud Forensic Challenges. *arXiv* **2023**, arXiv:2305.03059.
43. Kaleem, H.; Ahmed, I. Cloud Forensics: Challenges and Solutions (Blockchain Based Solutions). *Innov. Comput. Rev.* **2021**, *1*, 1–26. [CrossRef]
44. Alouffi, B.; Hassnain, M.; Alharbi, A.; Alosaimi, W.; Alyami, H.; Ayaz, M. A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access* **2021**, *9*, 57792–57807. [CrossRef]
45. Ali, S.A.; Memon, S.; Sahito, F. Challenges and Solutions in Cloud Forensics. In Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing, Barcelona, Spain, 3–5 August 2018; pp. 6–10. [CrossRef]

46. Prakash, V.; Williams, A.; Garg, L.; Savaglio, C.; Bawa, S. Cloud and Edge Computing-Based Computer Forensics: Challenges and Open Problems. *Electronics* **2021**, *10*, 1229. [CrossRef]
47. Hemdan, E.E.D.; Manjaiah, D. An efficient digital forensic model for cybercrimes investigation in cloud computing. Multimedia Tools and Applications. In *Multimedia Tools and Applications, Proceedings of the ICCBDC'18: 2018 2nd International Conference on Cloud and Big Data Computing, Barcelona, Spain, 3–5 August 2018*; Association for Computing Machinery: New York, NY, USA, 2018; Volume 80, pp. 14255–14282. [CrossRef]
48. Joshi, S.N.; Chillarge, G.R. Secure Log Scheme for Cloud Forensics. In Proceedings of the 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 7–9 October 2020; pp. 188–193. [CrossRef]
49. Javed, A.R.; Ahmed, W.; Alazab, M.; Jalil, Z.; Kifayat, K.; Gadekallu, T.R. A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. *IEEE Access* **2022**, *10*, 11065–11089. [CrossRef]