Scientific Publications

Universal Journal of Computer Sciences and Communications, 2024, 3, 923
www.scipublications.org/journal/index.php/ujcsc
DOI: 10.31586/ujcsc.2024.923

Article

Digital Forensic Investigation Standards in Cloud Computing

Ehigiator Egho-Promise [1,*], Sunday Idahosa [2], George Asante [3], Augusta Okungbowa [4]

[1] Department of ICT, City of Oxford College & University Centre, UK

[2] Value Chain Advisor, Pro-poor Growth and Employment Promotion in Nigeria Programme (SEDIN), Nigeria

[3] Department of IT Education, Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development, Ghana

[4] Computer Science, Shaka Polytechnic, Benin City, Nigeria

*Correspondence: Ehigiator Egho-Promise (eghopromise@yahoo.com)

Abstract: Digital forensics in cloud computing environments presents significant challenges due to the distributed nature of data storage, diverse security practices employed by service providers, and jurisdictional complexities. This study aims to develop a comprehensive framework and improved methodologies tailored for conducting digital forensic investigations in cloud settings. A pragmatic research philosophy integrating positivist and interpretivist paradigms guides an exploratory sequential mixed methods design. Qualitative methods, including case studies, expert interviews, and document analysis were used to explore key variables and themes. Findings inform hypotheses and survey instrument development for the subsequent quantitative phase involving structured surveys with digital forensics professionals, cloud providers, and law enforcement agencies, across the globe. The multi-method approach employs purposive and stratified random sampling techniques, targeting a sample of 100-150 participants, across the globe, for qualitative components and 300-500 for quantitative surveys. Qualitative data went through thematic and content analysis, while quantitative data were analysed using descriptive and inferential statistical methods facilitated by software such as SPSS and R. An integrated mixed methods analysis synthesizes and triangulates findings, enhancing validity, reliability, and comprehensiveness. Strict ethical protocols safeguard participant confidentiality and data privacy throughout the research process. This robust methodology contributed to the development of improved frameworks, guidelines, and best practices for digital forensics investigations in cloud computing, addressing legal and jurisdictional complexities in this rapidly evolving domain.

Keywords: Cloud Computing, Digital Forensics, Forensic Investigation Standards, Cloud Forensics, Cybercrime Investigation, Data Acquisition

How to cite this paper:
Egho-Promise, E., Idahosa, S., Asante, G., & Okungbowa, A. (2024). Digital Forensic Investigation Standards in Cloud Computing. *Universal Journal of Computer Sciences and Communications, 3*(1), 23–45. Retrieved from https://www.scipublications.com/journal/index.php/ujcsc/article/view/923

Received: March 2, 2024
Revised: April 8, 2024
Accepted: April 28, 2024
Published: April 29, 2024

1. Introduction

In recent times, there has been a strong and growing move to cloud computing all over the world. This is demonstrated in many businesses all over the world. Changes like this are driven by the promise of better size control, money saving and accessibility that online platforms offer compared to old self-owned systems. As firms use cloud services to save data, carry out actions with it and run programs, the large volumes of valuable online items in these computer-like spaces have grown a lot [1].

The appeal of cloud computing stems from its ability to provide on-demand access to computing resources without the need for physical infrastructure. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) have become integral components of IT strategies, enabling organizations to rapidly adapt their operations to meet evolving business needs [2]. This shift towards cloud computing is

being embraced by businesses of all sizes, from small enterprises to large corporations, seeking to optimize their IT resource utilization and enhance operational agility [3]. Even though cloud computing has a lot of benefits, there are number of challenges that are associated with its use. These include data loss, cyber-attacks, heterogeneity of resources and complexity of investigating security incidents. With incidence response, having knowledge of what happened and by whom can be a challenge due to the distributed and shared nature of cloud services.

The primary objective of this research is to contribute to the development of improved methodologies and standardized frameworks for digital forensic investigations in cloud computing environments. By addressing the gaps and challenges identified in this domain, the findings aim to guide digital forensic practitioners, policymakers, and cloud service users in effectively navigating the complexities associated with cloud-based investigations. Ultimately, this study seeks to facilitate the establishment of a comprehensive and legally admissible approach for conducting digital forensic examinations in cloud computing settings.

The widespread adoption of cloud computing has introduced new challenges for digital forensics. The very characteristics that make cloud computing attractive, such as resource sharing and distributed data storage, pose significant obstacles when conducting forensic investigations. Digital forensics, which involves the identification, acquisition, and analysis of digital evidence related to cybercrime or other illicit activities, is a critical process [4].

In the realm of cloud storage, digital forensics assumes paramount importance. The dynamic and distributed nature of cloud environments necessitates the development of standardized methodologies and best practices to address security incidents and potential legal violations effectively [5]. A comprehensive understanding of cloud forensics is crucial to ensure the admissibility of evidence in legal proceedings. As businesses increasingly entrust vital data to cloud services, digital forensics has become an indispensable tool for detecting and mitigating cybercrime threats, safeguarding against vulnerabilities, and ensuring the integrity of cloud operations [6].

This study explores the challenges and opportunities associated with digital forensics in cloud computing environments, with a particular emphasis on the acquisition, preservation, and analysis of digital evidence from cloud-based systems. Through a comprehensive review of literature and industry practices, the research identifies areas where existing guidelines and frameworks may be inadequate or require refinement. The study employs a multi-faceted approach, incorporating case studies, surveys, expert interviews with digital forensic practitioners and cloud service providers, as well as consultations with law enforcement agencies [4]. Additionally, an evaluation of existing standards and guidelines, such as ISO/IEC 27037, 27041, and the NIST SP 800 series, is conducted to assess their applicability and effectiveness in cloud computing contexts. The overarching goal is to develop a robust framework that prioritizes data confidentiality and integrity while ensuring the admissibility and reliability of collected evidence [2].

1.1. Problem statement

The increase in using cloud computing has introduced new challenges for digital forensic investigations. The distributed and shared nature of cloud environments poses significant obstacles, as traditional forensic methods designed for localized systems are ill-suited for the remote and virtualized infrastructure of cloud computing. Acquiring and preserving digital evidence from geographically dispersed locations becomes increasingly complex, as data is stored across multiple servers and shared resources, complicating the process of data extraction and analysis [5].

Furthermore, the lack of standardized policies and diverse security practices adopted by various cloud service providers exacerbates the difficulties faced by investigators. Ensuring the consistency and legal admissibility of forensic techniques across different

cloud platforms is a significant concern [6]. The global reach of cloud computing further compounds these challenges, giving rise to jurisdictional and legal complexities regarding data ownership, cross-border data transfer, and the applicability of laws in different regions. The intricate distribution of data storage across international boundaries poses additional hurdles in resolving cases seamlessly [4].

These challenges underscore the pressing need for a comprehensive framework and improved methodologies tailored specifically for digital forensic investigations in cloud computing environments. [4] emphasized the necessity for a holistic approach that ensures the effectiveness, reliability, and legal admissibility of digital forensic investigations in cloud computing settings, irrespective of geographic boundaries.

The absence of consistent standards and diverse security practices employed by cloud service providers hinder investigators' ability to conduct forensic examinations effectively and consistently across different cloud platforms [6]. Moreover, the global nature of cloud computing introduces jurisdictional complexities related to data ownership, cross-border data transfer, and the applicability of laws across various regions. The intricate distribution of data storage across international boundaries further complicates the resolution of cases, necessitating a comprehensive framework and enhanced methodologies specifically designed for conducting digital forensic investigations in cloud computing environments. In summary, the main challenges of a cloud computing environment that calls for a standardized framework for forensics investigation include:

1. Distributed and shared nature of cloud environment
2. Geographically dispersed locations
3. Lack of standardized policies
4. Diverse security practices
5. Jurisdictional and legal complexities
6. Cross-border data transfer
7. Applicability of laws in different regions.

1.2. Aims and Objective of the Research

The main aim of this research is to develop a comprehensive, standardized framework and improved methodology for conducting digital forensics investigations in a cloud environment. Specifically, the research seeks to:

1. Determine the unravelling challenges in digital forensics investigation in the cloud environment, and how distributed data storage, diverse security practices and jurisdictional complexities affect cloud investigation.
2. Conduct an in-depth assessment of current standards and guidelines to discern their effectiveness and relevance in diverse scenarios.
3. Explore new ways or better rules for cloud digital forensics investigation.

1.3. Significance of the study

The adoption of cloud computing has fundamentally transformed the way data is stored and processed, necessitating a thorough examination of the unique issues that arise during digital forensic investigations in online environments [1].

Firstly, the study aims to explore the fundamental challenges posed by the dynamic and shared nature of cloud computing. Traditional forensic techniques, designed for localized environments, encounter significant obstacles when applied to distributed networks and remote systems. The movement and sharing of digital data across multiple servers and geographic locations render the acquisition, collection, and preservation of evidence exceedingly complex [5].

Furthermore, the lack of standardized policies and diverse security practices employed by various cloud service providers hinder the efforts of forensic investigators. Ensuring the consistency, reliability, and legal admissibility of forensic methodologies across different cloud platforms is a daunting task. The research seeks to evaluate the efficacy of existing guidelines and standards, such as ISO/IEC 27037, 27041, and the NIST SP 800 series, in facilitating digital forensic operations within cloud computing environments [3].

Moreover, the global adoption of cloud computing services has given rise to legal complexities regarding data ownership and jurisdictional boundaries. The study addresses the intricate legal landscape and its implications for digital forensic investigations. It recognizes the need for a comprehensive examination of the applicable laws and regulations across different regions, as well as the varying data handling practices employed by computing infrastructure worldwide [1].

By addressing these critical challenges, the research aims to establish a robust framework and set of best practices tailored specifically for conducting digital forensic investigations in cloud computing environments, ensuring the integrity, admissibility, and cross-jurisdictional applicability of the evidence obtained. This research will serve as a guideline for security agencies and digital forensics experts in conducting forensics investigations in a cloud environment.

2. Literature review

2.1. Cloud Computing and Digital Forensics

2.1.1. Exploring the existing literature on the intersection of cloud computing and digital forensics

As per [7], with our world becoming more digitalized and technology influencing nearly every part of our lives, it is regrettable to say that cybercrime is on the rise. As criminals use the digital system's weaknesses to carry out illegal operations, there is an urgent need for a specialized area that can look into, evaluate, and uncover digital proof. Digital forensics is the name given to this field. Digital forensics is the term that is used for a collection of methods, instruments, and procedures used in legal or investigation processes to preserve, examine, and present digital evidence [8]. Digital forensics is sometimes referred to as computer forensics or cyber forensics. It entails gathering, analysing, and interpreting data from a variety of digital sources, including computers, mobile devices, networks, and digital storage media, using scientific and investigative techniques. The importance of digital forensics cannot be underrated. [9] research study claimed that it is essential to the fight against all forms of cybercrime, from financial fraud and hacking to cyberterrorism and theft of intellectual property.

However, experts in digital forensics use cutting-edge technology and specialized knowledge to try and solve the riddles of digital systems by finding crucial hints that may help identify and bring charges against hackers. The recovery of lost or damaged data, network traffic analysis, system log inspection, and encryption and decryption are just a few examples that fall under the broad umbrella of digital forensics. As per [10] strict standards and regulations are followed in the digital forensic process to uphold the chain of custody and guarantee that the evidence is unadulterated and trustworthy throughout the inquiry.

The research study by [11] showed that one of the most advanced knowledge domains in the modern world is cloud computing technology. On the other hand, as cloud computing has grown quickly, so has cybercrime. This model offers a wealth of information on the investigative process framework, all of which is very helpful in investigating if the currently used framework or approach is efficient in finding manual proof that requires human intervention at every level. However, the research study by [12]

proposed that the duties and obligations of cloud providers and customers are not well defined in the context of cloud forensic investigation. Nevertheless, since consumers are in charge of gathering and examining data from the cloud services, thus they should choose for forensic reasons, to locate, rank, and collect data from the cloud components. Additionally, [13] proposed that organizations have worked very hard lately to move their infrastructure to the cloud. For malicious actors, this makes the cloud a highly desirable target. To verify or refute the theory, digital forensics—a scientific method—must be applied while analyzing a corrupted cloud instance. Even though cloud forensics has a lot of advantages, [14] pinpointed that cloud forensics faces various challenges. Cloud services usually utilize shared things and can spread information across numerous servers. Cloud information is continuously changing, which makes it hard for digital forensics investigators to catch and keep proof before somebody changes or eliminates data portions.

2.2. Identifying key challenges and opportunities.

The well-known advantages of cloud computing include resource and cost-sharing, dispersed and lean processing, and quicker technology integration. However, there are several issues with cloud computing, which include the following:

2.2.1. Key Challenges

2.2.1.1. Data privacy challenges

According to [15], several users share the same resources and infrastructure while using cloud computing. One of the biggest challenges that investigators face in digital forensics is guaranteeing data privacy. They have to negotiate shared environments, which are complicated places where several users' data coexist on the same physical infrastructure. However, during digital forensic investigations, encryption, access restrictions, and secure data segregation are used to safeguard the privacy of individual users' data. To cope with data privacy challenges, [16] proposed that a multi-tenancy method must be used. Multi-tenancy is defined as hosting data from several users or organizations on the same physical infrastructure [17]. It makes it more difficult to isolate and separate tenant data during forensic examinations. Specialists need to make ways and arrangements so they can precisely connect explicit activities or realities with given individuals. This ensures things are accused properly, and stops any altering of proofs.

2.2.1.2. Jurisdictional and legal challenges

[18] demonstrated that cloud computing crosses national boundaries, making it difficult to investigate online crime due to disputes over who is in charge. It is essential to manage different legitimate guidelines, regulations and world arrangements while taking a gander at wrongdoings in Personal Computers that incorporate numerous regions. Specialists and police need to collaborate with gatherings and legitimate specialists [19]. They assist with settling conflicts about who has expertise in various regions and ensure proof that can be utilized in a court. As a result, it is stated that they must adhere to various rules. These incorporate guidelines for various enterprises and regulations about protection and guarding information. Additionally, experts must adhere to rules when conducting computer investigations, this ensures that they get and keep verification appropriately as per regulations set up. In court, the proof should be allowable and strong. This depends on observing guidelines of regulation.

2.2.1.3. Challenges related to resource allocation

[20] proposed that for the best utilization of assets, cloud computing frameworks need to utilize techniques with adaptable allotment and tasks. Since it changes, watching and estimating how assets are shared or moved during digitalized examinations may be hard. In any case, analysts need to foster designs for following and re-establishing the

circulation of assets. This makes exact checking done in a cloud environment where activities are continuing as of now. Additionally, investigators must use tactics including real-time resource allocation monitoring, gathering pertinent logs and information, and utilizing forensic analysis tools that are made especially for cloud systems to tackle resource allocation problems [21]. These techniques aid in rebuilding the distribution and use of resources by giving a thorough grasp of all the events and actions that are pertinent to the inquiry.

2.2.2. Key opportunities

2.2.2.1. Advanced Forensic Devices and Methods

According to [22], crime-solving tools and procedures are considered crucial in tackling the problems related to cloud environments. However, better approaches for checking recollections and organizations in a cloud environment are considered better devices and methods for acquiring the best digital proof.

2.2.2.2. AI and Automation

According to [23], the enormous amount of information made in cloud settings needs mechanization for computerized forensic steps. Big data can be studied quickly as a result of machine learning. Machine learning helps assistants spot designs, odd things, and conceivable security issues.

2.2.2.3 Upgraded Incident Response Planning

The research study by [24] claimed that better problem resolution can easily be achieved by making use of the cloud's capacity for expansion and adaptation. This requires the use of robust recording systems, real-time monitoring, and automated responses to cloud-specific issues.

2.3. Standards and Guidelines

2.3.1. Reviewing established digital forensic standards and guidelines

2.3.1.1. ISO/IEC 27037:2012

The International Electrotechnical Commission (IEC), an international not-for-profit organization, and the International Organisation for Standardisation (ISO), an international non-governmental organization, to harmonize practices between nations, produce and publish international standards. International guidelines for the identification, collection, acquisition, and preservation of digital evidence were released in 2012 by the International Electrotechnical Commission (IEC) and the International Organisation for Standardisation (ISO) as part of the ISO/IEC 27037 guidelines. ISO/IEC 27037:2012 is the one that provides guidelines for particular digital evidence-handling tasks, such as identifying, gathering, acquiring, and preserving potentially useful digital evidence [25]. It helps organizations with their disciplinary procedures and facilitates the transmission of potentially relevant digital evidence between jurisdictions. It also gives individuals assistance regarding typical circumstances faced throughout the digital evidence handling process.

2.3.1.2. ISO/IEC 27041:2015

As per [25], additional guidelines on the digital forensics process have been published by the ISO/IEC. These cover the following topics: the validity and reliability of digital forensic tools and methods (ISO/IEC 27041:2015, Guidance on assuring suitability and adequacy of incident investigative methods) and the phases of the process that involve examination (or analysis) and interpretation. The promotion of best practices in forensic acquisition and examination of digital evidence is the primary goal of the ISO27041:2015 digital forensics standards [26]. It is hoped that standardization will lead

to the adoption of similar approaches internationally, making it easier to compare, combine, and contrast the results of such investigations even when performed by different people or organizations and possibly across various jurisdictions. As a result, individual investigators, organizations, and jurisdictions may retain certain methods, processes, and controls well.

2.3.1.3. US National Institute of Standards and Technology

Digital forensics tools, including database, cloud, drone, and vehicle forensics tools, are available in a searchable database maintained by the US National Institute of Standards and Technology. The utilization of digital forensics technologies and their preferences vary throughout national law enforcement organizations. According to [27], an important but little-studied subfield of digital forensics is smart vehicle forensics. The need to develop smart vehicle forensics procedures, standards, and instruments that could facilitate a forensically sound digital investigation of vehicles has increased due to the widespread use of smart cars with internet-enabled features and the development of autonomous vehicles [28]. When investigating crimes involving smart or autonomous vehicles (e.g., hacking) or other crimes where the information gathered from these vehicles could be used as evidence of a crime, these vehicles can provide a wealth of information (e.g., places travelled and frequented, home and work address, numbers dialled, phone calls received, etc.).

2.4. NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response

This guide offers broad suggestions for carrying out the forensic procedure. Additionally, it provides comprehensive guidance on how to apply the analytic method to the four main types of data sources—applications, operating systems, files, and network traffic [29]. In addition to providing methods for gathering, examining, and analyzing data from each category, the standard concentrates on elucidating the fundamental elements and traits of data sources within each category. Additionally, the guide offers suggestions on how to combine various data sources to enhance comprehension of an event.

3. Materials and Methods

This study employed mixed methodology and strategies. The section below discusses the research philosophy, approach, design, method and strategy used in conducting the research. Data collection methods used such as case studies, surveys and interviews were also discussed. Ethical considerations and participants' confidentiality were also considered. Best standards and practices were proposed. And how these standards and practices could be implemented and validated were also discussed.

3.1. Research Philosophy

This study adopts a pragmatic research philosophy that combines elements of both positivism and interpretivism. The positivist aspect ensures objectivity through the analysis of quantitative data and factual information. Simultaneously, the interpretivist perspective allows for deeper insights into the complex phenomena of digital forensics in cloud computing environments. This pluralistic philosophical stance leverages the strengths of multiple paradigms, fostering a more comprehensive and robust understanding of the research problem.

3.2. Research Approach

The study employs an integrated methodology that blends quantitative and qualitative approaches through mixed methods research. This multi-strategy design enables triangulation of findings from diverse data sources, enhancing the validity and reliability of the results. The quantitative component provides statistical rigour and

generalizability, while the qualitative aspect offers rich contextual insights into the practical challenges and nuances inherent in cloud forensics.

3.3. Research Design

An exploratory sequential mixed methods design is adopted, involving an initial qualitative phase followed by a quantitative phase. The qualitative exploration aims to identify key variables, themes and constructs through case studies, interviews, and document analysis. These findings inform the development of hypotheses and the design of survey instruments for the subsequent quantitative phase. This iterative process ensures a comprehensive examination of the research problem and facilitates the integration of multiple perspectives.

3.4. Research Method

This study uses many different methods to look at rules for digital investigations in cloud computing. Using both main and additional information sources, the study makes unbiased decisions about the data happening. The way they do it involves getting information by using different scientific methods like surveys, talking to people and studying cases. [30] explains this process well. This all-round method makes sure we look at the topic from lots of different ways, getting understanding in many forms. The study uses main and second-hand sources along with different ways to learn. It wants to give a strong look at how digital investigations work in cloud computing, which can change quickly. For this study, a multi-method research approach was used. Primary and secondary sources of data were used to study phenomena and draw objective conclusions to analyse Digital forensic investigation standards in cloud computing. It involves collecting data from scientific methods such as (surveys and interviews, case studies and document analysis) [30].

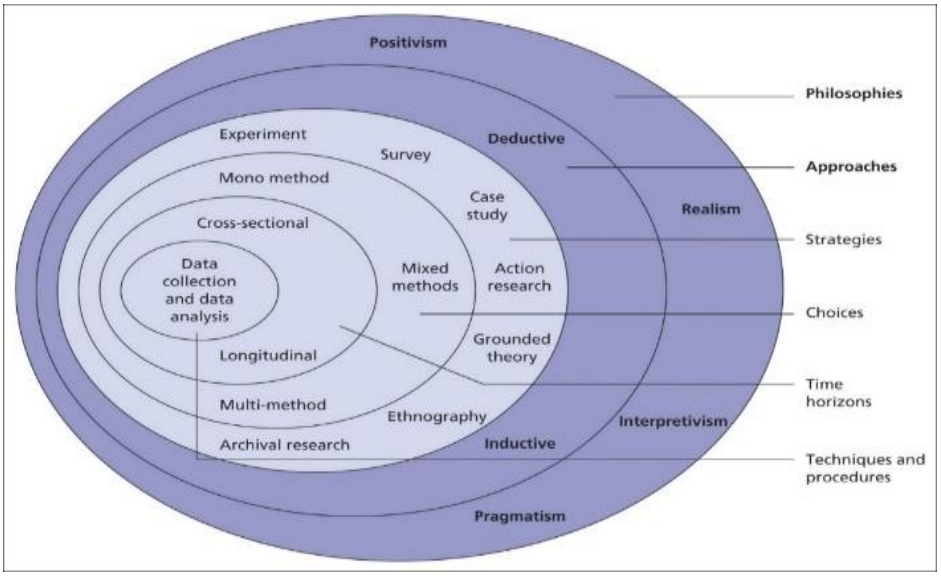

Figure 1. Research Onion

3.5. Research Strategy

The ways of collecting market data can be split into two types: qualitative and quantitative. Knowing the difference is important for making good decisions, according to [31]. The first research approach used is a mix of methods, including surveys, talks with people and document study. This big plan combines different ways of studying to get an understanding from many points of view. The study uses both qualitative and quantitative methods to make the market information more in-depth and detailed. Using

many ways helps to understand everything well. It makes smart conclusions from survey results, talk answers, observation of studies and looking at documents all mixed. It is a possible technique for collecting market data and being aware of the distinctions between the two assisted in arriving at more well-informed conclusions [31]. The first kind of study to be carried out is multimethod research, from surveys and interviews, case studies and document analysis assembled from the results of studies that have been carried out.

3.6. Data Collection Method

To fully reach the goals of research, it is suggested that we use different ways to collect data.

3.6.1. Case Studies Analysis

We closely looked at real-life examples of internet searches in cloud places. These examples provide helpful tips about the issues faced, methods used and outcomes achieved in real situations [32]. The study closely looked at real-life examples of computer investigations happening in the cloud. Looking at these real-life examples helps a lot to understand the problems faced, ways used and results achieved in proper situations [32]. By intently looking at these circumstances, the review learns a painstakingly definite comprehension of how troublesome and complex it is to do computerised examinations in cloud places. This way allows researchers to utilise genuine circumstances to improve their comprehension and help with making a more extensive view of how computerised criminological techniques are utilised for changing cloud conditions.

3.6.2. Survey and Interviews

The review addresses advanced hints specialists, cloud administration staff and cops. It utilises a method for getting various perspectives. By talking and associating with the people who utilise advanced examinations in distributed computing, the review tries to think about different perspectives. This enjoyable method helps us understand issues and good opportunities in the fast-changing world of digital crime for cloud Storage [33]. These talks give important details, making the study complete and more understandable. The researchers talked to and asked questions of the experts in digital forensics, people from companies that supply cloud services. This also includes workers from police stations. This way makes sure the researchers get different viewpoints on problems, chances and top methods in the area of digital forensics for cloud computing [34].

3.6.3. Document Analysis

The researchers carefully studied the current rules and advice for digital forensics. This means looking closely at old rules like ISO/IEC 27037 and 27041, and NIST SP 800 series documents. The researchers wanted to find the good parts but also places where they can be better or need fixing. This complete way of gathering information tries to find the same results from different places. It helped make a strong basis for what researchers learn by adding lots of viewpoints to their study [30].

3.7. Sample Size and Sampling Technique

The study employs a combination of purposive and stratified random sampling techniques. Purposive sampling was used to identify and recruit participants, across the globe, who have relevant expertise and experience in digital forensics, cloud computing, and related legal domains. Stratified random sampling ensures representation from various sectors, organization sizes, and geographic regions, enhancing the generalizability of the findings.

The target sample size is approximately 100-150 participants for the qualitative phase (interviews and case studies) and 300-500 respondents for the quantitative survey phase.

Sample sizes were determined based on data saturation principles for the qualitative component and statistical power analysis for the quantitative component.

3.8. Data Analysis

Qualitative data from case studies, interviews, and document analysis were analysed using thematic analysis and content analysis techniques. This process involves identifying recurring patterns, themes, and constructs related to challenges, methodologies, legal considerations, and best practices in cloud forensics.

Quantitative data from surveys were analysed using descriptive and inferential statistical methods, facilitated by software such as SPSS or R. Techniques include regression analysis, factor analysis, structural equation modelling, and other appropriate methods based on the nature of the data and research hypotheses.

The study employed an integrated mixed methods analysis approach, synthesizing and triangulating findings from both qualitative and quantitative components. This integration enhances the validity, reliability, and comprehensiveness of the research conclusions.

3.9. Ethical Considerations and Participant Confidentiality

Strict ethical protocols were followed to ensure the protection of participant confidentiality and data privacy. Informed consent was obtained from all participants, highlighting the voluntary nature of participation and the right to withdraw at any stage without consequences. Anonymization and data encryption techniques were employed to safeguard sensitive information and maintain participant anonymity.

The study adhered to established ethical guidelines and principles, such as those outlined by relevant professional organizations and institutional review boards. Ethical clearance was obtained before commencing data collection, and ongoing ethical oversight was maintained throughout the research process.

This comprehensive research methodology, combining multiple methods, data sources, and analytical techniques, ensures a robust and rigorous investigation of digital forensic investigation standards in cloud computing environments. The findings contributed to the development of improved frameworks, guidelines, and best practices while addressing legal and jurisdictional complexities in this rapidly evolving domain.

3.10. challenges in cloud forensics

3.10.1. Data Privacy and Jurisdiction

One of the most significant issues in cloud forensics is gathering data, maintaining privacy and dealing with legal boundaries. In the cloud, storing and processing data is one of the most critical tasks, and knowing which rules are needed is important. Determining the problems with cloud services needs to follow many sets of rules [35]. There was a time when various complicated situations arose due to different laws for storing things secretly in other areas. Cloud services that work anywhere make it hard to get and keep proof, and there are different rules about maintaining private data and limits on moving data between countries involved. A detective working in the digital world needs to effectively work on complicated legal situations and ensure their proof can be used in court.

3.10.2. Challenges Related to Cross-Border Data Issues and Legal Jurisdiction

One of the most critical situations is that cloud forensics deals with data from different countries and legal controls. However, Cloud computing often uses and moves data across other areas. This makes it hard for digital investigators to follow legal rules. Data protection law is one big problem, with conflicting regulations in different countries [36]. Every area might have rules about getting, dealing with and keeping digital proof. Thus, the critical job of a detective is to go through this law land to make sure they follow

many different and often disagreeing rules. General Data Protection Regulation (GDPR) in Europe puts strict rules on keeping data safe and private. Other areas might have various regulations [35]. In the end, problems with data sharing across borders and legal authority for cloud forensics need a smart way to handle it. Investigators need to know a lot about international laws, be good at working with paperwork stuff, and work well with people in different places. This helps make sure digital searches in the cloud are legal and successful.

3.10.3. Ephemeral Nature of Cloud Data

The short-lived nature of cloud data causes a big problem in digital investigations. Most of the time, cloud environments use changing storage. They often update or remove data in their regular work. This makes it hard for detectives to maintain and get information because the data could change or be deleted quickly [1]. Old ways of solving crimes that are made for still places need to be more in the moving and changing world of cloud computing. People who look into crimes have to deal with constantly changing cloud data. This means they need special skills and tools to keep and save proof immediately, ensuring it is safe and true while investigating.

3.10.4. Difficulties in Preserving and Collecting Volatile Cloud Data

Keeping and saving fast cloud data is hard in computer forensics because it is always changing and short-lived in cloud places. Volatility means that information can change quickly, making it hard for researchers to understand what is happening at a certain time [37]. The problems in this process are very big in cloud computing places where data is always changing and moving. One big problem is that updating cloud data happens in real-time. Cloud platforms often use spread-out and growing designs. They put data on many servers and places. This spreading out makes it hard to keep the data safe because changes can happen simultaneously in different parts. Old-style ways of staying place can need help keeping up with all the changes happening fast in the cloud.

Moreover, cloud technology's diffuse and shared setup makes it harder to find and separate important data for investigative work. In a place where many people use the same stuff, the detective has to figure out how to tell good from bad actions [38]. Using resources together can mix up data, making it hard to know which person or group did what. Cloud service providers often use fancy virtualisation technology and shared resources. They give out these resources based on need, and it is even harder for an investigator to save changing information because they have to deal with layers of abstract data created by virtualisation. This makes it difficult to get a full and correct picture of the system state.

3.10.5. Multi-Tenancy and Shared Resources

Digital forensic investigations get more complex when dealing with multi-tenancy and shared resources in cloud computing, and challenges potentially make things harder to solve. In a spot where many folks use the same items, it takes work on particular activities and tying them with one person or group is tough. This usual method can make it difficult to find likely bad actions and stop digital proof. Understanding safety issues must solve the issue of sharing resources and deciding who did what [39]. This happens because what one person does can change how safe and easy it is for others to get resources. Solving these issues requires creating detective methods to unravel joint resources' intricacies, ensuring a full and accurate investigation process.

3.10.6. Challenges Associated with Shared Resources and Multi-Tenancy

Difficulties with shared items and numerous users in cloud computing make digital forensic investigation tough. This makes it hard to find, split up and study digital evidence. Many users or tenants share the same physical resources and systems in a cloud

environment. This is called multi-tenancy. This common way creates issues that harm the strength of online search inquiries [40]. A major issue is figuring out and showing who did something in a shared place. When many people use the same servers, storage, and network, it is hard to judge good user actions from bad ones. Looking into things carefully is needed to show a clear link between certain people and digital hints tied to an event about safety. Not having enough room might make it hard for the detective to find out where bad things began. It can also make it harder to get solid evidence. A different issue in shared cloud areas is getting resources mixed up [41]. When resources are shared based on need, jobs and information from other users may be stored together on the same machinery. When data is mixed, it can lead to unintentional leaks or contamination. This makes it tougher to discover and safeguard computer information— people who look into crime need to use special methods for looking at things that many people share.

3.11. Proposed standards and best practice

3.11.1. Proposed Modifications or Additions to Existing Standards for Cloud Forensics

The special problems that come with cloud environments are always changing and shared by many people [35]. Modifying existing standards will help with the special problems caused by cloud environments' fast-changing and shared parts. With the ISO/IEC 27037, which provides rules for digital proof, changes must be made to include thoughts about multi-tenancy, mixing resources and shared things. The rule could be improved by adding clear ways to find, keep safe, and get proof in places where many people use the same stuff [1]. Furthermore, clear rules for handling data across borders, legal jurisdiction troubles and working with cloud service providers should be included. Similarly, NIST Publication 800-53, which is about security rules, should change cloud-related security rules directly. These controls should discuss separating resources, dividing data, and responding to incidents in a way that suits the cloud world [39]. This helps the detective correctly determine who did what in those shared areas.

Moreover, the rule could be improved by highlighting how cloud data can vanish quickly. This would show the importance of getting quick, real-time evidence to keep and grab changing information. In addition, these standards could be improved by including rules about openness and checking for cloud service providers. This means making logging habits the same and ensuring that people looking into crimes can get full and time-stamped logs for investigations. Basic changes should focus on providing cloud service providers with records about how resources are used, what users do, and setting changes. This will help with investigations more easily. The rules might also be for the growth and use of standardised tools for digital proofs in the cloud [37]. This would ensure they work and are the same on different cloud servers. This might mean setting rules for data in evidence items and logs to improve how various systems work together. It also makes checking simpler for detectives. Updates to these stands need to keep happening with the help of people who work on rules, crime experts and companies that provide cloud services. This is because cloud technology constantly changes, and we must deal with new problems [40]. By adding these new rules and improvements to current standards, we will make them stronger and easier to use for cloud forensics. This reliable structure will help investigators in this ever-changing field.

3.11.2. Developing a Set of Best Practices for Digital Forensic Investigations in the Cloud

Potential practices should focus on the need for cloud-friendly forensic tools to manage the spread-out and virtual aspects of cloud resources. This helps gather correct evidence without affecting the quality of your data. Investigators need to take a more active approach. Tools should be designed for use in the cloud. These tools should be made to work with the changing, spread out and computerised parts of cloud resources.

This includes tools for catching changing information quickly, ensuring evidence is safe and stays the same, and ensuring it works with different cloud systems. Add ways to watch and find things on their own in the best ways. This will help us quickly spot abnormal things and possible security problems [41]. Because cloud places change a lot, constant watching helps us answer quickly to new dangers. This makes it harder for bad actions to stay hidden. Best practices should suggest ways to deal with multi-tenancy issues and keep data apart effectively. Investigators must ensure that looking into one tenant's evidence does not accidentally affect or harm another tenant's data. This means putting barriers to access, coding security measures, and correctly separating data in cloud systems [42]. Other ways should promote making and using quick-answer forensic technology questions to handle the fleeting nature of data in the cloud. These ways should have quick analysis and use high-tech forensics to get data as it happens. This ensures that important proof gets noticed because cloud resources can change quickly. Practices about the law should be important, stressing that it follows local and world data protection rules. Simple rules for dealing with data problems between countries, setting limits on who is in charge and knowing what agreements are with cloud service providers help protect evidence in court. Training and skill growth for forensic investigators make up the last important part of best practices. Investigators need to know about new technologies, cloud designs and changing dangers. It helps them work well in an ever-changing cloud world and involves always learning to use the latest forensic tools and techniques specifically for the cloud.

3.12. Implementation and validation

3.12.1. Prototypes and Tools

Making models or tools from suggested rules for digital evidence investigation in cloud computing means creating easy-to-use answers that match what is already set. Here are two examples such as Cloud Forensic Readiness Assessment Tool, and Cloud Incident Response Platform (CIRP).

Cloud Forensic Readiness Assessment Tool is used to assess the forensic readiness of cloud environments based on ISO/IEC 27041:2015 and NIST SP 800-53 rules. This tool can test how ready a group is for computer evidence investigations in the cloud. It spots parts that need fixing and keeps things right with rules from industry standards [43]. The Cloud Incident Response Platform (CIRP) tool puts together tips from NIST SP 800-61 Rev.2 and CSA Cloud Forensics Incident Response Guide to make a full system for handling incidents in cloud areas. CIRP assists in quickly spotting incidents, collecting evidence automatically and keeping data safe in the cloud [44].

These models help develop the cloud's digital forensic skills, pushing for usual methods and business rules. They take care of the changing issues of distributed computing, ensuring that advanced measurable examinations function admirably and keep guidelines in this new, and innovative world [45].

3.12.2. Prototyping Conformance with Proposed Standards

Creating examples that fit new rules is very crucial to ensure we follow the given regulations and requirements. One such prototype is the "Standardised Digital Evidence Collection Module" designed under ISO/IEC 27037: 2012 [46]. This part helps to find, collect and keep digital proof safe. It maintains quality throughout this process. The example works with tools we use right now to solve crimes. It provides a basic way for detectives to work together easily [47].

Also, a "Check Compliance Tool" fits with NIST SP 800-53. This allows companies to check and make sure they stick with security and privacy rules in their cloud systems. This device checks if things follow the rules [48]. It shows where they are and gives suggestions for improving it, making everything more secure in the end. These examples

not only help to apply suggested rules but also make digital crime checks easier and more similar. They aid businesses in reviewing and improving the regulations they must abide by. This creates a good system for digital investigation in the fast-changing world of cloud computing [49].

3.12.3. Tooling Support for Implementation of Proposed Standards

Creating tools that aid in using new rules is crucial for ensuring many people use them and can easily fit with good practices. One such tool is the "Standard Compliance Validator," designed to align with ISO/IEC 27041: 2015 [50]. This tool compares cloud computing services with the standard's rules. It gives a complete report on what they need to fix. These steps should be followed. It helps businesses create good safety rules for their cloud areas [51].

The "Automated Controls Enforcer" is built based on NIST SP 800-53. This helps companies automatically enforce safety and private rules. This tool makes sure rules are always followed by watching and changing them as needed. It reduces the chances of breaking those rules and also makes cloud systems more secure overall [52]. By providing useful methods linked with suggested rules, these answers help businesses put in and keep safe cloud storage. The tooling support not only helps make it easier to follow rules but also adds power and reliable performance in cloud systems when dealing with online safety issues that change often [53].

3.12.4. Validation through Simulations

It is important to check out whether new standards work or not using tests or experiments. This assists us to see how well they could be used in the real world and what influence they may have. One way is to make a fake cloud setting that represents usual situations found in real uses [44]. For instance, in the context of ISO/IEC 27037: In 2012, can do a controlled experiment that imitates cyber-incidents in cloud settings. This simulation would check how well we can find, get and keep digital evidence following the rules in these standards. The results of the test, like how well and fast evidence is found, can then be compared to what was expected in the standard [47].

In the same way, for NIST SP 800-53 a controlled test might concentrate on responding to incidents in a cloud area. Acting out different safety problems, such as data leaks or stopped services, would let experts check how well the security rules suggested by the guide work. We can measure and compare things like how fast responses come, how well computer systems bounce back after a problem and the quality of data against what these standards aim to achieve [45]. By doing these tests or controlled experiments, groups can get useful information about the good and bad points of suggested rules. This real-world testing assists make the standards better by using them in practice. It makes sure they work well at improving safety and investigative abilities for cloud computing environments [47].

3.12.5. Simulation-based Assessment of Proposed Standards

Checking a model-based test of proposed rules is very important for looking at how much they work in real-life situations. For instance, in simulating ISO/IEC 27037: In 2012, an experiment was run where they could copy a digital forensics situation in the Cloud. This means making situations like losing data or allowing someone to enter without permission happen [43]. We then look at how good the rules are for finding and keeping evidence when we are in changing cloud places. In the same way, when talking about NIST SP 800-53, a simulation might be set up by making security problems happen in a cloud system. This lets us fully check the safety controls they suggest. We can measure how well these controls find, answer to and get back from different online threats [47]. The method that uses simulation assists in testing how well the standards work in different cloud computing situations. It gives us a clear understanding of whether these

rules are useful and effective or not. Things like how fast responses are, the correctness of getting proofs and the time systems take to get better can be measured [47]. This makes a company's use of practical data for making their plans with computer tools more effective. This step-by-step process of testing and checking makes sure that suggested rules line up with the changing side of cloud computing. It gives a strong plan to handle growing threats online in a pretend but real-world way [45].

3.12.6. Controlled Experiments for Empirical Validation of Standards

Making careful tests to prove if rules work is a very important step in making sure they are useful. For example, in validating ISO/IEC 27037: In 2012, a controlled experiment could make a pretence of cloud area for changing or messing up digital proof on purpose [45]. This allows us to measure how well the rules in this standard for finding, getting and keeping evidence work under real-life situations. It gives numbers on just how right these forensic tasks are done quickly. NIST SP 800-53 can use controlled experiments to mimic security problems in a cloud setup [44]. This lets us test how well its advised safety measures work against those issues. We can measure things like how accurate a system is in finding problems, the time it takes to deal with incidents and how well we get back up after attacks. These are used as real-world tests of whether this standard makes cloud environments safer [45].

These tests give real information about the good and bad points of these rules. They help companies to improve how they put them into action. The information obtained from careful experiments gives proof for smart choices [47]. This makes sure that rules are not only good in theory but also work well and strong when put into use in cloud computing situations. This process of trying out and checking makes standards better over time. It assists them in staying flexible as the changing world of internet safety in cloud areas develops [43].

4. Results and Discussion

4.1. Case Studies

It is a well-evident fact that there is an increasing trend of digital forensic investigation in cloud computing. This could be attributed to the rapid adoption of cloud services. This section exclusively outlines a few real-world case studies to highlight associated challenges and complexities. The study argues about the Capital One Data Breach in 2019, Uber Data Breach in 2016, and Home Depot Data Breach in 2014. These case studies have been exclusively considered due to their wider service provisions and handling of cloud security.

4.1.1. Capital One Data Breach

The data breach that occurred at Capital One in 2019 involved a former employee of Amazon Web Services (AWS) who took advantage of a web application firewall that had been improperly set to obtain access to customer information that was stored in AWS S3 buckets. Forensic investigators needed to wade through cloud logs, access restrictions, and settings to get an understanding of the scope of the breach and the data that was exposed. The investigation consisted of tracking the activity of the attacker throughout the cloud infrastructure, analysing logs, and determining the vulnerabilities that were exploited.

4.1.2. Uber Data Breach

Hackers gained access to Uber's GitHub repository, where they uncovered credentials that gave them access to the AWS environment used by the firm. Personal information belonging to 57 million Uber drivers and users was exposed as a result of this attack. To assess the extent of the data that was exposed, forensic investigators were

required to trace down the illegal access that occurred inside the cloud infrastructure. This example brought to light the need to implement more stringent mechanisms for credential management and access control.

4.1.3. The Home Depot Data Breach

The credit card information of about 56 million consumers was compromised as a result of this hack. Attackers were able to acquire access to Home Depot's network by using the credentials of a third-party vendor. This gave them the ability to move laterally around the network and compromise data. The investigators were confronted with the task of tracking the actions of the attackers inside the cloud infrastructure to determine the original access point and the scope of the data that was compromised.

These case studies underscore the difficulties that are intrinsic to forensic investigations conducted in the cloud, such as the intricacy of cloud infrastructures, models of shared responsibility, the requirement to navigate through numerous service providers, and the criticality of dependable recording and monitoring systems. Digital forensic specialists are required to modify their approaches to efficiently gather and assess evidence in cloud environments, taking into account the fluid and decentralized characteristics of cloud systems.

4.2. Survey Data Analysis

To acquire the desired research, aim and objectives, the study developed a survey questionnaire from 15 respondents. The questionnaire included different aspects of digital forensic investigation in the context of cloud computing. The questionnaire has been distributed into demographic information, challenges, evaluating existing standards and guidelines, and proposing enhancements or new standards for cloud forensics.

4.2.1. Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.509	0.547	6

The reliability statistics of the questionnaire has been assessed with the help of Cronbach's alpha which is low (0.509). However, an increase in the sample would further increase the internal consistency of the survey questionnaire.

4.2.2. Description of Demographic Details

Table 1. Demographic Summary of Respondents

Variable	Frequency	Percentage
Gender		
Female	7	46.7
Male	8	53.3
Age		
25-34	4	26.7
35-44	5	33.3
35-45	1	6.7
45-54	1	6.7
45-55	2	13.3
55 and above	2	13.3
Educational Background		
Bachelor	3	20.0
Master	7	46.7
PH. D	5	33.3

Occupation		
Academic/Researcher	2	13.3
Digital Forensic Analyst	5	33.3
IT Professional	3	20.0
Security Specialist	5	33.3
Years of Experience in Digital Forensics		
1 to 3 years	2	13.3
4 to 6 years	5	33.3
7 to 10 years	3	20.0
8 to 10 years	2	13.3
More than 10 years	3	20.0
1 to 3 years	2	13.3

The demographic details of the respondents have been explained in Table 1. According to the table, 53.3% of the respondents were male and 13.3% were related to the age group of 45-55 years. 46.7% had degree of Masters and 33.3% were digital forensic analysts. Referring to the experience, 33.3% of the respondents had experience of 4 to 6 years.

4.2.3. Identifying Challenges in Conducting Digital Forensics in Cloud Computing

Table 2. Responses of Respondents Regarding Challenges

	Response	**Frequency**	**Percentage**
Lack of Physical Access to Servers	Strongly agree	15	100.0
Dynamic and Elastic Nature of Cloud Environments	Strongly agree	15	100.0
Multi-Tenancy and Shared Resources	Agree	7	46.7
	Strongly agree	8	53.3
Encryption of Data in the Cloud	Strongly agree	15	100.0
Legal and Jurisdictional Issues	Strongly agree	15	100.0

Table 2 provides a summary of the responses regarding the challenges in conducting a digital forensic investigation. The table indicates that all respondents strongly agreed that lack of physical access, the dynamic and elastic nature of cloud environments, encryption of data in the cloud, and legal and jurisdictional issues are major concerns of respondents. Whereas 53.3 shared that they strongly agree about the multi-tenancy and shared resources. Whereas 46.7% opted "agree" as their option.

4.2.4. Perception-Based Assessment

Table 3. Perception-Based Assessment

	Response	Frequency	Percent
"How satisfied are you with the clarity and effectiveness of existing standards and guidelines for digital forensics in cloud computing?"	Very Satisfied	15	100.0
"How confident are you in your organization's ability to overcome challenges in digital forensics within cloud computing environments?"	Very Confident	15	100.0
"ISO/IEC 27037 (Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence)"	Strongly agree	15	100.0
"NIST SP 800-61 (Computer Security Incident Handling Guide)"	Strongly agree	15	100.0
"Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)"	Strongly agree	15	100.0
"To what extent do you agree with the need for the development of new or enhanced standards for cloud forensics?"	Strongly agree	15	100.0

"How satisfied are you with the applicability of existing standards and guidelines for digital forensics in cloud computing to your organization's needs?"	Very Satisfied	15	100.0
"On a scale of 1 to 5, how effectively do you believe your organization implements existing standards and guidelines for digital forensics in cloud computing?"	Highly Effective	15	100.0
"To what extent do you feel that the current standards for cloud forensics adequately address emerging technologies and trends?"	Highly Effective	15	100.0
Proposing Enhancements or New Standards for Cloud Forensics			
How necessary do you believe it is to establish standardized processes for cross-cloud forensics?"	Highly necessary	15	100.0
"To what extent do you agree that industry collaboration is essential in developing new standards for cloud forensics?"	Strongly Agree	15	100.0
"How satisfied are you with the level of industry collaboration in shaping standards for cloud forensics?"	Very satisfied	15	100.0
"To what extent do you agree that a unified framework for cloud forensics should encompass both legal and technical aspects?"	Strongly Agree	15	100.0
"How confident are you in the potential success of new or enhanced standards for cloud forensics in addressing future challenges?"	Very Confident	15	100.0

The survey results on digital forensics in cloud computing are shown in Table 3. All 15 participants gave consistent answers to the different questions, with 100% of them agreeing with the study's findings. Remarkably, all respondents (100%) expressed "Very Satisfied" feelings on the efficacy and rationality of the current rules and guidelines on digital forensics in cloud computing as predicted by [53]. Comparably, everyone expressed great confidence in their ability to overcome obstacles in cloud settings; 100% of participants said they were "Very Confident," demonstrating unanimity. The support for certain standards, such ISO/IEC 27037, NIST SP 800-61, and the Cloud Security Alliance's Cloud Controls Matrix, was uniform, as 100% of respondents said that they "Strongly Agree" with these standards. This finding is aligned with the study of [54] who affirmed the use of these standards in cloud computing. Furthermore, all participants strongly agreed that new or improved standards for cloud forensics should be developed [55], and they were also satisfied with the usefulness and efficacy of the standards that are now in place. Additionally, all participants (100%) stressed the need for industry cooperation in defining new standards, the requirement of established protocols for cross-cloud forensics, and the significance of a unified framework that encompasses both legal and technological components. Finally, expressing 100% agreement once again, all respondents said they were "Very Confident" about the possible success of new or improved standards in solving upcoming difficulties. As shown by the unanimity percentages across all poll parameters, the overwhelming agreement in these replies demonstrates a strong favourable emotion toward current standards and a common desire for additional developments in cloud forensics.

4.3. Results of the Interview

The study also incorporated interview sessions with 15 respondents to perform a more comprehensive assessment in the context of expert opinion. Therefore, different questions related to forensic investigation and cloud computing while outlining challenges, and enhancement of new standards. In response to 11 questions, the study developed the following themes using thematic analysis.

4.3.1. Theme 1: Jurisdictional Data Privacy and Challenges

The discussion with respondents indicated that they often experienced difficulty while dealing with jurisdiction for data privacy. For instance, Respondent 1 emphasised the significance of data residency and jurisdictional issues, highlighting the need to collaborate with cloud service providers and comply with interoperability standards. Respondent 2 reiterated similar concerns while pointing out data dispersion across many sites, isolation hazards, and cross-border data transfers [56].

4.3.2. Theme 2: Virtualisation and Shared Resources

The other discussed challenge was virtualisation and shared resources highlighted by Respondents 5 and 6. The respondents indicated issues associated with encryption, the dynamic nature of virtual environments, and shared and multi-tenant systems. The discussion highlighted the importance of working with cloud service providers and suggested policies like transparency reports and forensic methods that protect privacy [57].

4.3.3. Theme 3: Lack of Physical Control over Infrastructure

Respondents also explained that there is a dearth of control over physical infrastructure. The experts have to cope with the changing IP addresses, delimited access, and exertion in conversing the chain of custody in a virtual setting. Additionally, Respondent 9 spoke about difficulties including the inability to access physical memory and live snapshot problems. These difficulties were thought to have consequences for gathering and storing evidence in a cloud computing setting [58].

4.3.4. Theme 4: Standards and Guidelines

Current standards and guidelines were cited by respondents. Several responders brought up ISO/IEC standards like 27037, 27041, and 27043. Respondent 1 referenced ISO/IEC 27037:2012, which highlights the protocols for identifying, gathering, obtaining, and preserving electronic evidence. Respondent 2 notably mentioned ISO/IEC 27041:2015 and argued for agile standards development, which NIST principles were also commended for.

4.3.5. Theme 5: Collaboration with Cloud Service Provider

Respondent 5 urged community engagement and emphasized the value of collaboration. Concerning vendor-specific formats and tools, respondent number eight emphasized the need for incident response certification and training programs. Overall, a major priority was ensuring that cloud service provider rules adhered to industry standards, with a focus on openness, participation, and respect for established guidelines.

4.3.6. Need for New Standards

Several respondents said that new standards were required, ones that were specific to the difficulties that cloud-based digital forensics presents. The proposals made by Respondents 10 and 13, which called for industry forums for cooperation, legal harmonization, and standards related to the cloud, were very clear examples of this. There have been requests for standards that can adjust to new difficulties in the cloud computing environment due to the dynamic nature of laws and technology.

4.3.7. Recommendations

Throughout all of the comments, suggestions for cooperation appeared often. Standardized logging and auditing were highlighted by Respondent 7 as crucial elements of productive teamwork. Respondent 9 suggested criteria for education and training as well as privacy by design. Law enforcement organisations and forensic investigators were included in the collaborative element, which also called for frequent industry events, training initiatives, and worldwide cooperation in addition to cloud service providers.

Respondents offered a variety of other perspectives and suggestions, ranging from moral norms and transparency to continuity requirements. Attention was called to the areas of emerging technologies, global data dissemination, and legislative harmonization. It was advised that incident response and threat intelligence be integrated with ongoing standards review and upgrades to ensure efficacy in the changing area of cloud-based digital forensics.

5. Conclusions

5.1. Summary of Findings

The study outlined the recent advancement in the domain of digital forensic investigation standards in cloud computing. For this purpose, a comprehensive data analysis strategy was adopted through examining real-world case studies, survey data and interview sessions. The case study analysis shed light on different hurdles faced by organisations in cloud forensics highlighting the need to employ credible monitoring and record set-ups. Meanwhile, the case study analysis suggested developing shared models of accountability to cope with the issues due to the dearth of cloud infrastructure. Additionally, survey data from 15 respondents explained respondents' demographic information and helped to identify the prominent challenges faced during digital forensic investigations. On the whole, the findings of the survey suggested that respondents always had to deal with numerous challenges while conducting forensic investigations. These tentatively include multi-tenancy [39, 40, 41], lack of physical access to servers, dynamic cloud settings, data encryption, and legal/jurisdictional concerns. Furthermore, the participants conveyed serenity with the current norms and protocols, including ISO/IEC 27037, NIST SP 800-61, and the Cloud Security Alliance's Cloud Controls Matrix [54]. Lastly, the interview session with respondents further clarified the validation of results from case studies and surveys. The respondents indicated various related factors that created problems in conducting a successful assessment of cloud computing. In this regard, regulatory data privacy [56], virtualization and shared resources [57], loss of physical control over infrastructure [58], following rules and regulations, and the significance of working with cloud service providers stand out. Meanwhile, these interview sessions were effective in collecting valuable recommendations from respondents to enhance the current standards and jurisdiction related to forensic investigation. Respondents stressed the need for industry cooperation, awareness and education, enhancement in training standards, design privacy, and better service provisions for data logging and auditing.

The results show that experts in digital forensics agree on the difficulties and prerequisites for conducting efficient investigations in cloud computing, opening the door for further developments in standards and procedures in this developing sector.

5.2. Implications of the Research

The study has noteworthy implications for academics, practitioners, and legislators. The research highlights the prerequisite for experts to work together with cloud service providers and adapt their investigative practices given the details of cloud settings. The results may be used by policymakers to amend rules, with a particular emphasis on harmonising laws and standardising practices. Scholars are urged to explore particular issues found in cloud-based digital forensics, make contributions to creative approaches, and confirm the study's conclusions with more empirical research. To put it briefly, the study contributes to focused inquiry for researchers in the dynamic area of cloud-based digital forensics, regulatory updates for legislators, and practical adaptations for practitioners.

Author Contributions: Ehigiator Egho-Promise: Conceptualization, writing-original draft preparation, methodology, data collection and analysis.

Sunday Idahosa: Conceptualization, methodology, writing-review.

George Asante: methodology, Formal Analysis, Writing – original draft preparation, review and editing.

Augusta Okungbowa: methodology, data validation, writing- review and editing.

References

[1] Alex, M. E., & Kishore, R. (2017). Forensics framework for cloud computing. Computers & Electrical Engineering, 60, 193-205. (https://doi.org/10.1016/j.compeleceng.2017.02.006).

[2] Kishore, R. (2017). Forensics framework for cloud computing. Computers & Electrical Engineering, 60, 193-205. (https://doi.org/10.1016/j.compeleceng.2017.02.006).

[3] Badger, M. L., Grance, T., Patt-Corner, R., & Voas, J. M. (2012). Cloud computing synopsis and recommendations. National Institute of Standards & Technology. (https://doi.org/10.6028/NIST.SP.800-146).

[4] Birk, D., & Wegener, C. (2011, May). Technical issues of forensic investigations in cloud computing environments. In 2011 Sixth IEEE international workshop on systematic approaches to digital forensic engineering (pp. 1-10). (IEEE. 10.1109/SADFE.2011.17).

[5] Wegener, C. (2011, May). Technical issues of forensic investigations in cloud computing environments. In 2011 Sixth IEEE international workshop on systematic approaches to digital forensic engineering (pp. 1-10). (IEEE. 10.1109/SADFE.2011.17).

[6] Chen, G., Du, Y., Qin, P., & Du, J. (2012, September). Suggestions to digital forensics in Cloud computing ERA. In 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content (pp. 540-544). (IEEE. 10.1109/ICNIDC.2012.6418812).

[7] Grinin, L., Grinin, A., & Malkov, S. (2023). Sociopolitical Transformations: A Difficult Path to Cybernetic Society. In Reconsidering the Limits to Growth: A Report to the Russian Association of the Club of Rome (pp. 169-189). Cham: Springer International Publishing. (10.1007/978-3-031-34999-7_10)

[8] Brunty, J. (2023). Validation of forensic tools and methods: A primer for the digital forensics' examiner. Wiley Interdisciplinary Reviews: Forensic Science, 5(2), e1474. (https://doi.org/10.1002/wfs2.1474)

[9] Phillips, A., Ojelade, I., Taiwo, E., Obunadike, C., & Oloyede. (2023) K. CYBER-SECURITY TACTICS IN MITIGATING CYBER-CRIMES: AReview AND PROPOSAL. (10.5121/ijcis.2023.13201)

[10] USMAN, O. J., YUNUSA, E., & Gomment, T. I. (2023). CRIMINAL PROFILING AND THE CHALLENGES OF CRIMINAL INVESTIGATION IN NIGERIA POLICE FORCE KOGI STATE COMMAND. GPH-International Journal of Social Science and Humanities Research, 6(10), 31-65. (https://doi.org/10.5281/zenodo.10007913)

[11] Hamzah, M., Islam, M. M., Hassan, S., Akhtar, M. N., Ferdous, M. J., Jasser, M. B., & Mohamed, A. W. (2023). Distributed Control of Cyber-Physical System on Various Domains: A Critical Review. Systems, 11(4), 208. (https://doi.org/10.3390/systems11040208)

[12] Khan, A. A., Shaikh, A. A., Laghari, A. A., & Rind, M. M. (2023). Cloud forensics and digital ledger investigation: a new era of forensics investigation. International Journal of Electronic Security and Digital Forensics, 15(1), 1-23. (https://doi.org/10.1504/IJESDF.2023.127745)

[13] Islam, R., Patamsetti, V., Gadhi, A., Gondu, R. M., Bandaru, C. M., Kesani, S. C., & Abiona, O. (2023). The Future of Cloud Computing: Benefits and Challenges. International Journal of Communications, Network and System Sciences, 16(4), 53-65. (10.4236/ijcns.2023.164004)

[14] Iqbal, F., Jaffri, A., Khalid, Z., MacDermott, A., Ali, Q. E., & Hung, P. C. (2023). Forensic investigation of small-scale digital devices: a futuristic view. Frontiers in Communications and Networks, 4, 1212743. (https://doi.org/10.3389/frcmn.2023.1212743)

[15] Tusa, F., & Clayman, S. (2023). End-to-end slices to orchestrate resources and services in the cloud-to-edge continuum. Future Generation Computer Systems, 141, 473-488. (https://doi.org/10.1016/j.future.2022.11.026).

[16] Sharma, A., & Kaur, P. (2023). A Survey of Distributed Data Storage in the Cloud for Multitenant Applications. International Journal of Performability Engineering, 19(3). (10.23940/ijpe.23.03.p4.184192)

[17] Olabanji, D., Fitch, T., & Matthew, O. (2023). Multi-tenancy in Cloud-native Architecture: A Systematic Mapping Study. WSEAS Transactions on Computers, 22, 25-43. (10.37394/23205.2023.22.4)

[18] Zhang, H., & Gong, X. (2023). The research on an electronic evidence forensic system for cross-border cybercrime. The International Journal of Evidence & Proof, 13657127231187059. (https://doi.org/10.1177/13657127231187059)

[19] Cohen, G., & Cohen, N. (2023). Understanding street-level bureaucrats' informal collaboration: Evidence from police officers across the jurisdictional divide. Public Management Review, 25(2), 224-242. (https://doi.org/10.1080/14719037.2021.1963824)

[20] Alhaidari, F., Rahman, A., & Zagrouba, R. (2023). Cloud of Things: architecture, applications and challenges. Journal of Ambient Intelligence and Humanized Computing, 14(5), 5957-5975. (10.1007/s12652-020-02448-3)

[21] Rani, D. R., Sultana, S. N., & Sravani, P. L. (2016). Challenges of digital forensics in cloud computing environment. Indian Journal of Science and Technology, 9(17), 1-7. (10.17485/ijst/2016/v9i17/93051).

[22] Spyropoulos, A. Z., Bratsas, C., Makris, G. C., Garoufallou, E., & Tsiantos, V. (2023). Interoperability-Enhanced Knowledge Management in Law Enforcement: An Integrated Data-Driven Forensic Ontological Approach to Crime Scene Analysis. Information, 14(11), 607. (10.3390/info14110607)
[23] Rizvi, A., & Srivastava, N. (2023). Exploring the Potentials of Robotic Process Automation: A Review. Journal of Informatics Electrical and Electronics Engineering (JIEEE), 4(2), 1-12. (https://doi.org/10.54060/jieee.2023.100)
[24] Wang, B., Zhang, Z., Song, Y., Chen, M., & Chu, Y. (2023). Application of Quantum Particle Swarm Optimization for task scheduling in Device-Edge-Cloud Cooperative Computing. Engineering Applications of Artificial Intelligence, 126, 107020. (https://doi.org/10.1016/j.engappai.2023.107020)
[25] Shin, S. M., Hong, J. W., & Kim, G. B. (2023). Study on the standard components of digital forensics laboratory. Journal of Forensic Sciences. (https://doi.org/10.1111/1556-4029.15254)
[26] Gostojić, M. M., & Vuković, Ž. (2023). A knowledge-based system for supporting the soundness of digital forensic investigations. Forensic Science International: Digital Investigation, 46, 301601. (https://doi.org/10.1016/j.fsidi.2023.301601)
[27] Li, J., Song, Z., Zhang, Z., Li, Y., & Cao, C. (2023). In-Vehicle Digital Forensics for Connected and Automated Vehicles With Public Auditing. IEEE Internet of Things Journal. (10.1109/JIOT.2023.3310578)
[28] Tageldin, L., & Venter, H. S. (2023). Machine Learning Forensics: State of the Art in the Use of Machine Learning Techniques for Digital Forensic Investigations within Smart Environments. (10.20944/preprints202306. 1660.v1)
[29] Sheeraz, M., Paracha, M. A., Haque, M. U., Durad, M. H., Mohsin, S. M., Band, S. S., & Mosavi, A. (2023). Effective Security Monitoring Using Efficient SIEM Architecture. Hum.-Centric Comput. Inf. Sci, 13, 1-18.
[30] Mik-Meyer, N., (2020). Multimethod qualitative research. Qualitative research, pp.357-374.
[31] Ruggiano, N. & Perry, T.E., (2019). Conducting secondary analysis of qualitative data: Should we, can we, and how? Qualitative Social Work, 18(1), pp.81-97. (https://journals.sagepub.com/doi/full/10.1177/1473325017700701).
[32] Davidson, E., Edwards, R., Jamieson, L. & Weller, S., (2019). Big data, qualitative style: a breadth-and-depth method for working with large amounts of secondary qualitative data. Quality and quantity, 53(1), pp.363-376. (https://link.springer.com/article/10.1007/s11135-018-0757-y)
[33] Hughes, K., Frank, V.A., Herold, M.D. & Houborg, E., (2021). Data reuse across international contexts? Reflections on new methods for International Qualitative Secondary Analysis. Qualitative Research, p.14687941211052278. (https://journals.sagepub.com/doi/pdf/10.1177/14687941211052278)
[34] Dufour, I.F. & Richard, M.C., (2019). Theorizing from secondary qualitative data: A comparison of two data analysis methods. Cogent Education, 6(1), p.1690265. (https://www.tandfonline.com/doi/full/10.1080/2331186X.2019.1690265).
[35] Alenezi, A., Atlam, H.F. & Wills, G.B. (2019). Experts reviews of a cloud forensic readiness framework for organizations. Journal of Cloud Computing, 8(1). doi:https://doi.org/10.1186/s13677-019-0133-z.
[36] Simou, S., Kalloniatis, C., Gritzalis, S. & Katos, V. (2018). A framework for designing cloud forensic-enabled services (CFeS). Requirements Engineering, 24(3), pp.403–430. doi:https://doi.org/10.1007/s00766-018-0289-y.
[37] Ali, S.A., Memon, S. & Sahito, F. (2018). Challenges & Solutions in Cloud Forensics. Proceedings of the 2018 2nd International Conference on Cloud & Big Data Computing - ICCBDC'18. doi:https://doi.org/10.1145/3264560.3264565.
[38] Purnaye, P. & Kulkarni, V. (2021). A Comprehensive Study of Cloud Forensics. Archives of Computational Methods in Engineering. doi:https://doi.org/10.1007/s11831-021-09575-w.
[39] Pichan, A., Lazarescu, M. & Soh, S.T. (2018). Towards a practical cloud forensics logging framework. Journal of Information Security & Applications, [online] 42, pp.18–28. doi:https://doi.org/10.1016/j.jisa.2018.07.008.
[40] Chen, L., Takabi, H. & Le-Khac, N.-A. (2019). Security, Privacy, & Digital Forensics in the Cloud. [online] Google Books. John Wiley & Sons. Available at: https://books.google.com/books?hl=en&lr=&id=R5VPCwAAQBAJ&oi=fnd&pg=PA1&dq=Digital+Forensic+Investigation+St&ards+in+Cloud+Computing&ots=1Sg8THXVW2&sig=_cS4djdrPosLZC7T8RO9po3x9Qc [Accessed 30 Dec. 2023].
[41] Choi, D.-H. (2021). Digital Forensic: Challenges & Solution in the Protection of Corporate Crime. The Journal of Industrial Distribution & Business, [online] 12(6), pp.47–55. doi:https://doi.org/10.13106/jidb.2021.vol12.no6.47.
[42] Karie, Nickson.M., Keb&e, V.R., Venter, H.S. & Choo, K.-K.R. (2019). On the importance of st&ardising the process of generating digital forensic reports. Forensic Science International: Reports, 1, p.100008. doi:https://doi.org/10.1016/j.fsir.2019.100008.
[43] Chukwu, E., & Garg, L. (2020). A systematic review of blockchain in healthcare: frameworks, prototypes, & implementations. Ieee Access, 8, 21196-21214. (https://doi.org/10.1109/ACCESS.2020.2969881).
[44] Coito, T., Martins, M. S., Viegas, J. L., Firme, B., Figueiredo, J., Vieira, S. M., & Sousa, J. M. (2020). A middleware platform for intelligent automation: An industrial prototype implementation. Computers in industry, 123, 103329. (https://doi.org/10.1016/j.compind.2020.103329).
[45] Kai, D., Goldstein, G. P., Morgunov, A., Nangalia, V., & Rotkirch, A. (2020). Universal masking is urgent in the COVID-19 p&emic: SEIR & agent based models, empirical validation, policy recommendations. (arXiv preprint arXiv:2004.13553).
[46] Kamel, E., & Memari, A. M. (2019). Review of BIM's application in energy simulation: Tools, issues, & solutions. Automation in construction, 97, 164-180. (https://doi.org/10.1016/j.autcon.2018.11.008).
[47] Kikusato, H., Orihara, D., Hashimoto, J., Takamatsu, T., Oozeki, T., Matsuura, T., & Miyazaki, T. (2022). Performance analysis of grid-forming inverters in existing conformance testing. Energy Reports, 8, 73-83. (https://doi.org/10.1016/j.egyr.2022.10.106)

[48] Liu, C., Vengayil, H., Lu, Y., & Xu, X. (2019). A cyber-physical machine tools platform using OPC UA & MTConnect. Journal of Manufacturing Systems, 51, 61-74. (https://doi.org/10.1016/j.jmsy.2019.04.006).
[49] Peng, Z., Huang, M., Zhong, Y., Chen, L., & Liu, G. (2020). A new method for interoperability & conformance checking of product manufacturing information. Computers & Electrical Engineering, 85, 106650. (https://doi.org/10.1016/j.compeleceng.2020.106650).
[50] Reeves, J. J., Holl&sworth, H. M., Torriani, F. J., Taplitz, R., Abeles, S., Tai-Seale, M., & Longhurst, C. A. (2020). Rapid response to COVID-19: health informatics support for outbreak management in an academic health system. Journal of the American Medical Informatics Association, 27(6), 853-859. (https://doi.org/10.1093/jamia/ocaa037).
[51] Schandelmaier, S., Briel, M., Varadhan, R., Schmid, C. H., Devasenapathy, N., Hayward, R. A., & Guyatt, G. H. (2020). Development of the Instrument to assess the Credibility of Effect Modification Analyses (ICEMAN) in r&omized controlled trials & meta-analyses. Cmaj, 192(32), E901-E906. (https://doi.org/10.1503/cmaj.200077).
[52] Schlüter, F., Hetterscheid, E., & Henke, M. (2019). A simulation-based evaluation approach for digitalization scenarios in smart supply chain risk management. Journal of Industrial Engineering & Management Science, 2019(1), 179-206. (https://doi.org/10.1016/j.simpat.2019.03.004).
[53] Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., & Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Generation Computer Systems, 92, 265-275.
[54] Henriques, J., Caldeira, F., Cruz, T., & Simões, P. (2024). A Survey on Forensics and Compliance Auditing for Critical Infrastructure Protection. IEEE Access.
[55] Roussev, V., Ahmed, I., Barreto, A., McCulley, S., & Shanmughan, V. (2016). Cloud forensics–Tool development studies & future outlook. Digital investigation, 18, 79-95.
[56] Celeste, E., & Fabbrini, F. (2020). Competing jurisdictions: Data privacy across the borders. Data Privacy and Trust in Cloud Computing, 43-58.
[57] Brandao, P. R. (2019). Forensics and digital criminal investigation challenges in cloud computing and virtualization. American Journal of Networks and Communications, 8(1), 23-31.
[58] Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2020). Cyber-physical systems forensics: Today and tomorrow. Journal of Sensor and Actuator Networks, 9(3), 37.