Cloud Digital Forensics

Subjects: Others

Contributor: Annas Wasim Malik, David Samuel Bhatti, Tae-Jin Park, Hafiz Usama Ishtiaq, Jae-Cheol Ryou, Ki-Il Kim

Cloud computing technology is rapidly becoming ubiquitous and indispensable. Despite the multiple advantages the cloud offers, organizations remain cautious about migrating their data and applications to the cloud due to fears of data breaches and security compromises.

Keywords: cloud computing ; data loss ; cloud digital forensic ; security breaches

1. Introduction

Cloud computing is a framework that permits pervasive, user-oriented, and on-demand admittance to a shared pool of configurable computing assets over the cloud (internet) without direct active management by the user [1]. The primary benefits of cloud computing are not only limited to reduction in time and costs but also agility and scalability. The idea of cloud computing was originally linked to the concepts of distributed parallel computing, utility computing, and autonomic computing. Cloud computing has different models based on deployment and service delivery. Based on cloud deployment, there are four models: public cloud, private cloud, hybrid cloud, and community cloud while based on service delivery; models could be categorized as SaaS (Software as a service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service), as shown in **Figure 1** [2]. Some leading corporations, including Amazon, Google, IBM, Microsoft, Dell Technologies, Hewlett Packard Enterprise, Cisco Systems, and Oracle, have invested in cloud computing and are offering individuals and businesses a range of cloud-based solutions. In the past few years, interest in adopting the cloud computing paradigm has increased not only in the IT industry but also in other sectors like banking, finance, education, health, utility, telecom, etc. According to a study in 2020, the presence of cloud-based applications or computing infrastructure in organizations had increased to 81% from 73% in 2018 [3]. It was forecasted that global end-user investments in public cloud services would grow in 2021 to USD 304.9 billion, up from USD 257.5 billion in 2020 [4]. The ability to use on-demand, adaptable cloud models for achieving cost-effectiveness and business continuity is motivating organizations to rapidly accelerate their digital business transformation plans. Cloud computing is envisioned as a potential future of computing, and there is no doubt that cloud tools and solutions are here to stay. Cloud computing is arguably the most significant technological advancement of the 21st century. However, as cloud computing gains more recognition worldwide, concerns are also being raised about the data security and privacy issues introduced through the adoption of this modern computing paradigm. Data security and privacy have consistently been primary issues in Information Technology. The concerns regarding data security and privacy become particularly serious in the cloud computing environment because data are scattered across various locations on different machines and storage devices, including personal computers, servers, and various mobile devices. Handling data security and privacy in cloud computing is more complex than in conventional information systems. While cloud services are helping remote workers effectively collaborate as part of a team, they are also opening new opportunities for cyber-criminals to conduct cyber frauds. According to a recent study, 92% of the participating organizations still report a cloud security readiness gap, and they are not comfortable with the security consequences of moving their workloads to the cloud environment [5]. According to IBM's data breach report, the global average total cost of a data breach in the year 2020 was USD 3.86 million with the healthcare sector alone incurring the highest industry cost of USD 7.13 million [6].

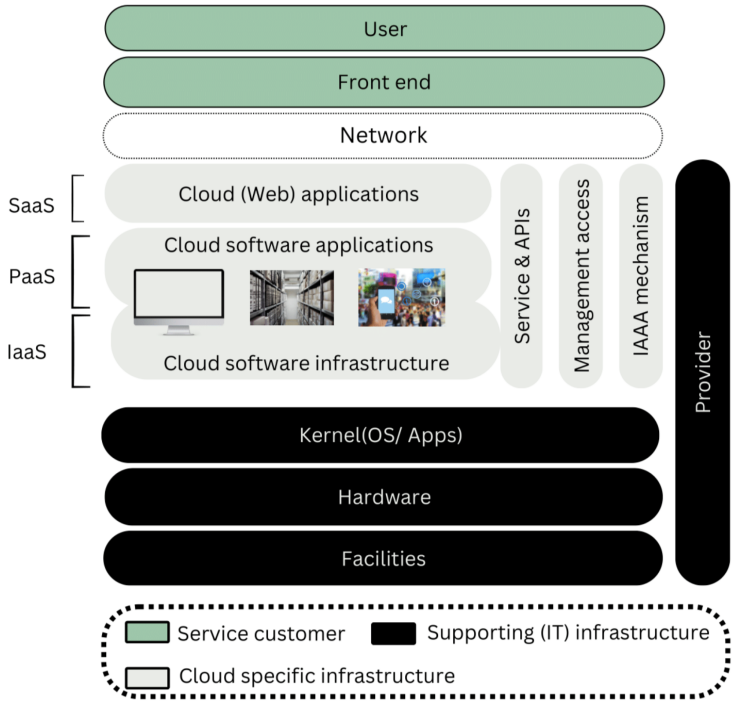

Figure 1. Models of cloud services.

In the rapidly evolving digital landscape, data breaches have become a significant concern for organizations across various industries. When a data breach occurs, highly sensitive and confidential information can be compromised, leading to severe repercussions for the affected organization [7]. The aftermath of such incidents can include financial losses, damage to the organization's reputation, erosion of customer trust, and potential legal consequences. The increasing frequency of data breaches has raised pertinent questions about the security of data stored in cloud computing environments. While cloud computing offers numerous advantages, including flexibility, scalability, and cost-effectiveness, it also introduces inherent security risks [8]. The shared nature of cloud infrastructure and the remote storage of data necessitate a meticulous examination of cloud security practices. Addressing intricate challenges, cloud forensics emerges as a specialized subset of digital forensics, focusing on investigating and mitigating security incidents intrinsic to cloud environments [9][10]. This involves identifying vulnerabilities and attack vectors to facilitate proactive security measures, while also contributing to evidence preservation, incident response planning, regulatory compliance, and the refinement of security strategies. The iterative process sharpens security measures, reinforces employee training, and offers insights for legal remedies and third-party risk management, thus nurturing a resilient and secure digital landscape. Expertise in both digital forensics and cloud technologies is pivotal for this distinctive approach [11]. Proficient practitioners in cloud forensics meticulously gather and maintain evidence in accordance with forensic norms, preserving its integrity and authenticity for potential legal proceedings. The five key phases of digital forensics, which include identification, preservation, collection, analysis, and reporting [12].

The prevalence and impact of data breaches underscore the criticality of cloud security. While cloud security encompasses measures to protect data and systems from unauthorized access and breaches, it is essential to differentiate cloud forensics within the broader scope of digital forensics. Carrier's work [13] on file system forensic analysis highlights the distinction between general data security practices and forensic investigations tailored for legal evidentiary standards. Cloud forensics, as a specialized domain within digital forensics, plays a pivotal role beyond data security. It involves investigating incidents, preserving evidence in a manner suitable for court admissibility, identifying vulnerabilities, and facilitating data recovery. Understanding this distinction is crucial, as expert cloud forensics practices are not solely focused on data protection but also on collecting evidence that meets legal criteria. These practices are vital for safeguarding sensitive data, upholding trust in the digital ecosystem, and mitigating the potential fallout of data breaches in cloud computing environments. Cloud forensics analyzes logs, access controls, and user activities to identify vulnerabilities in cloud infrastructure that lead to data breaches [14]. It helps organizations enhance security and recover compromised or deleted data in complex environments [15]. However, experts face technological and legal challenges in cross-border data governance, necessitating collaboration with cloud service providers. Cloud forensics is crucial in investigating incidents, preserving evidence, mitigating fallout, safeguarding sensitive data, and upholding trust in the digital ecosystem [14][15].

2. Cloud Digital Forensics

Cloud digital forensics is a specialized field that tackles cybercrime investigations in cloud environments, navigating multi-jurisdictional scenarios and evidence preservation protocols [16]. Its complexity is further exacerbated by the concept of multi-tenancy, and the evolving techniques and methodologies employed by cloud forensic experts [17][18].

2.1. The Cloud Digital Forensic Process Model

The National Institute of Standards and Technology (NIST) defines digital forensics as a meticulous process that encompasses the recovery, preservation, and analysis of digital data with meaningful applications in criminal investigations and prosecutions [19]. This process is equally applicable to cloud digital forensics, which involves addressing the unique challenges posed by cloud environments. The investigation journey in cloud forensics can be distilled into four pivotal stages [20], each contributing to the comprehensive understanding of a digital incident, as outlined below and depicted in **Figure 2**. The forensic process consists of the following steps:

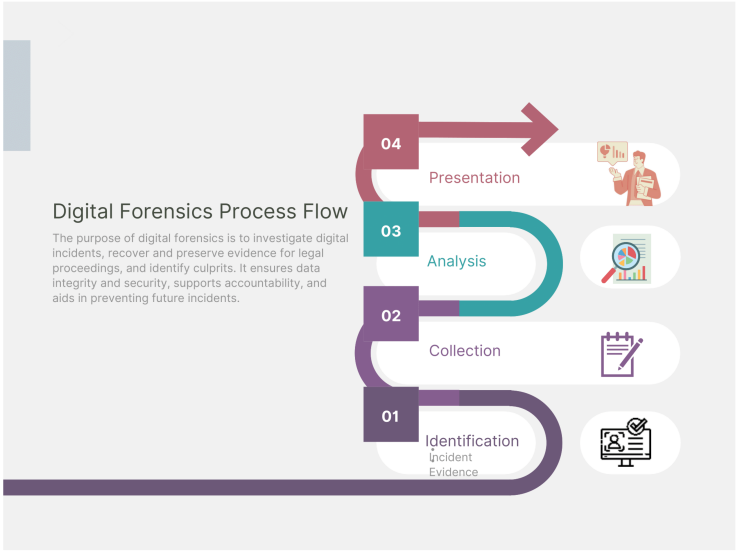

Figure 2. The cloud digital forensics process.

- Identification: Cloud forensics involves identifying and locating relevant cloud-based systems and applications, examining the service provider, services, and data types. Detecting crimes in the cloud is more challenging than traditional forensics, often starting with unauthorized resource usage complaints. New methods are needed to efficiently use existing tools and isolate cloud evidence.

- Preservation: The preservation stage is crucial for safeguarding digital evidence's integrity, ensuring its legal use. It involves systematic data capture, secure storage, and documentation, acting as a digital custodian.

- Examination and analysis: The analysis phase in cloud forensics involves using tools and methodologies to examine digital evidence, uncovering insights through log files, network activity patterns, metadata decoding, and data recovery. This phase requires technical prowess and a discerning eye.

- Presentation: Cloud forensics aims to present investigative findings in a clear, concise manner, leveraging information as credible evidence in legal proceedings. This involves creating comprehensive reports, using visual aids, and offering expert testimony.

Cloud forensic procedures must adapt to diverse service delivery and deployment models, ensuring the integrity of collected evidence [21]. Rapid evolution of cloud environments necessitates timely capture and retention of evidence to prevent gaps in the evidential trail. Validation of cloud-based evidence in legal proceedings is essential, and techniques like hash codes, digital signatures, and encryption enhance confidence in the veracity of evidence. The robustness of evidence credibility is based on its secure preservation [22].

2.2. Cloud Digital Forensics Tools and Technologies

In the realm of cloud digital forensics, the availability of specialized tools plays a pivotal role in facilitating investigations within cloud computing environments. **Table 1** delineates their key functionalities and significance in uncovering digital evidence.

Table 1. Summary of digital forensic tools and their features.

Category	Tools	Features
Cloud digital forensic tools	Magnet AXIOM cloud	Comprehensive cloud data collection and analysis
	Cellebrite UFED cloud analyzer	Acquisition and analysis of data from cloud accounts
	Mandiant CloudLens	Visibility into cloud environments for security
	Volatility Framework	Memory forensics framework for virtual machines
	AccessData cloud extractor	Collection and preservation of digital evidence
	Oxygen forensic cloud extractor	Supports over 20 cloud services for forensics
Offline digital forensic tools	Autopsy	Open-source digital forensics platform
	BlackBag BlackLight	Analysis of data from devices and cloud services
	X-Ways Forensics	Examination of evidence from cloud storage, email, etc.
	Azure Security Center	Threat protection in Azure and hybrid environments
	AWS CloudTrail	API call logs in AWS accounts for forensic analysis
	EnCase Forensic	Comprehensive forensic software for evidence
	AccessData Forensic Toolkit (FTK)	Tool for collecting, analyzing, and examining data
	Forensic Falcon	Hardware-based solution for offline and live forensics
	Paladin Forensic Suite	Live forensic system bootable from a USB drive
	Digital Evidence and Forensics Toolkit (DEFT)	Linux distribution for digital forensics
	Bulk Extractor	Command-line tool for scanning disk images
	Digital forensics framework (DFF)	Open-source digital forensics platform that provides a modular and extensible framework for conducting forensic investigations.

1. Magnet AXIOM cloud: This tool offers comprehensive cloud data collection and analysis capabilities [23]. It supports various cloud services like AWS, Azure, and Google Cloud, allowing users to recover, examine, and preserve cloud-based evidence.

2. Cellebrite UFED cloud analyzer: The UFED cloud analyzer enables the acquisition and analysis of data from cloud accounts, including social media, email, and storage services [24]. It supports a wide range of cloud providers and helps in uncovering digital evidence.

3. Mandiant CloudLens: This tool by Mandiant, a FireEye company, provides visibility into cloud environments for security purposes [25]. It helps in detecting and investigating threats by monitoring cloud activities and analyzing logs.

4. Volatility framework: Although not exclusively for the cloud, Volatility is a popular open-source memory forensics framework [26]. It is used to analyze memory dumps of virtual machines, including those in cloud environments, to identify signs of compromise.

5. AccessData cloud extractor: This tool facilitates the collection and preservation of digital evidence from cloud storage services, social media platforms, and webmail providers [27]. It assists in building a comprehensive picture of a user's online activities.

6. AccessData cloud extractor: This tool facilitates the collection and preservation of digital evidence from cloud storage services, social media platforms, and webmail providers [27]. It assists in creating a comprehensive forensic copy of a user's online activities.

7. Oxygen forensic cloud extractor: Oxygen forensic cloud extractor [28] supports over 20 cloud services, enabling investigators to gather data from cloud storage, social media, and email accounts for digital forensics purposes.

8. Autopsy: While not exclusively designed for cloud forensics [29], Autopsy is an open-source digital forensics platform that allows examiners to analyze evidence from various sources, including cloud storage services.

9. BlackBag BlackLight: BlackLight [30] is a digital forensics solution that supports the analysis of data from both traditional devices and cloud services. It aids in extracting and interpreting data from cloud accounts.

10. X-Ways Forensics: X-Ways Forensics is a versatile digital forensics tool that supports the examination of evidence from cloud storage services, email accounts, and other sources [31].

11. Azure Security Center: Microsoft's Azure Security Center [32] provides a cloud-native solution for threat protection across Azure and hybrid environments. It helps in detecting and responding to threats in cloud infrastructure.

12. AWS CloudTrail: Amazon Web Services CloudTrail [33] logs all API calls made on an AWS account, allowing for detailed forensic analysis and audit trail creation.

Some other offline digital forensic tools are [34]:

1. EnCase Forensic: EnCase is a widely used forensic software that provides comprehensive capabilities for acquiring, analyzing, and reporting digital evidence from various devices and file systems.

2. AccessData forensic toolkit (FTK): FTK is a powerful forensic tool that allows investigators to collect, analyze, and examine data from computers and mobile devices. It includes advanced searching and analysis features.

3. Forensic Falcon: This hardware-based solution offers both offline and live forensic capabilities, allowing investigators to analyze and image digital media in the field.

4. Paladin Forensic Suite: Paladin is a live forensic system that can be booted from a USB drive. It includes a variety of open-source forensic tools and utilities for evidence collection and analysis.

5. DEFT (Digital Evidence and Forensics Toolkit): DEFT is a Linux distribution specifically designed for digital forensics and incident response. It includes a collection of pre-installed forensic tools and utilities.

6. Bulk Extractor: Bulk Extractor is a command-line tool designed to quickly and efficiently scan disk images for specific types of information, such as email addresses, credit card numbers, and URLs.

7. Digital Forensics Framework (DFF): DFF is an open-source digital forensics platform that provides a modular and extensible framework for conducting forensic investigations.

References

1. Mell, P.; Grance, T. The NIST Definition of Cloud Computing; Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011. Available online: https://csrc.nist.gov/pubs/sp/800/145/final (accessed on 1 November 2023).
2. Badger, M.L.; Grance, T.; Patt-Corner, R.; Voas, J.M. Cloud Computing Synopsis and Recommendations; National Institute of Standards & Technology: Gaithersburg, MD, USA, 2012.
3. International Data Group. 2020 Cloud Computing Study. 2020. Available online: https://www.idg.com/tools-for-marketers/2020-cloud-computing-study/ (accessed on 1 November 2023).
4. Costello, K.; Rimol, M. Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021. Gartner. 2020. Available online: https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021 (accessed on 1 November 2023).
5. Davidson, M.A. Oracle and KPMG Cloud Threat Report 2020. 2020. Available online: https://www.oracle.com/security/cloud-threat-report/ (accessed on 1 November 2023).
6. IBM. Cost of a Data Breach Report 2020. 2020. Available online: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (accessed on 1 November 2023).

7. Barona, R.; Anita, E.M. A survey on data breach challenges in cloud computing security: Issues and threats. In Proceedings of the 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Kollam, India, 20–21 April 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–8.
8. Carroll, M.; Van Der Merwe, A.; Kotze, P. Secure cloud computing: Benefits, risks and controls. In Proceedings of the 2011 Information Security for South Africa, Johannesburg, South Africa, 15–17 August 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 1–9.
9. Sun, H.; He, R.; Zhang, Y.; Wang, R.; Ip, W.H.; Yung, K.L. eTPM: A Trusted Cloud Platform Enclave TPM Scheme Based on Intel SGX Technology. Sensors 2018, 18, 3807.
10. Khanafseh, M.; Qatawneh, M.; Almobaideen, W. A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics. Int. J. Adv. Comput. Sci. Appl. 2019, 10, 202706103.
11. Khodayarseresht, E.; Majumdar, S. Digital forensics for emerging technologies: Present and future. In Innovations in Digital Forensics; World Scientific: Singapore, 2023; pp. 1–11.
12. Abdalla, S.; Hazem, S.; Hashem, S. Guideline model for digital forensic investigation. In Proceedings of the Conference on Digital Forensics, Security and Law, Alexandria, VA, USA, 18–20 April 2007.
13. Carrier, B. File System Forensic Analysis; Addison-Wesley Professional: Boston, MA, USA, 2005.
14. Raghavendra, S.; Srividya, P.; Mohseni, M.; Bhaskar, S.C.V.; Chaudhury, S.; Sankaran, K.S.; Singh, B.K. Critical Retrospection of Security Implication in Cloud Computing and Its Forensic Applications. Secur. Commun. Netw. 2022, 2022, 1791491.
15. Surange, G.; Khatri, P. IoT forensics: A review on current trends, approaches and foreseen challenges. In Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 17–19 March 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 909–913.
16. Malik, A.W.; Abid, A.; Farooq, S.; Abid, I.; Nawaz, N.A.; Ishaq, K. Cyber threats: Taxonomy, impact, policies, and way forward. KSII Trans. Internet Inf. Syst. 2022, 16, 2425–2458.
17. Alex, M.E.; Kishore, R. Forensics framework for cloud computing. Comput. Electr. Eng. 2017, 60, 193–205.
18. Prakash, V.; Williams, A.; Garg, L.; Barik, P.; Dhanaraj, R.K. Cloud-Based Framework for Performing Digital Forensic Investigations. Int. J. Wirel. Inf. Netw. 2022, 29, 419–441.
19. Materese, R. Digital Evidence. 2021. Available online: https://www.nist.gov/digital-evidence (accessed on 1 November 2023).
20. Rani, D.R.; Sultana, S.N.; Sravani, P.L. Challenges of digital forensics in cloud computing environment. Indian J. Sci. Technol. 2016, 9, 1–7.
21. Zawoad, S.; Hasan, R.; Skjellum, A. OCF: An open cloud forensics model for reliable digital forensics. In Proceedings of the 2015 IEEE 8th International Conference on Cloud Computing, New York, NY, USA, 27 June–2 July 2015; pp. 437–444.
22. Liao, Y.C.; Langweg, H. Evidential Reasoning for Forensic Readiness. J. Digit. Forensics, Secur. Law 2016, 11, 2.
23. Moreb, M. Cloud Computing Forensics: Dropbox Case Study. In Practical Forensic Analysis of Artifacts on iOS and Android Devices: Investigating Complex Mobile Devices; Springer: Berlin/Heidelberg, Germany, 2022; pp. 329–369.
24. Akinbi, A.; Berry, T. Forensic investigation of google assistant. SN Comput. Sci. 2020, 1, 272.
25. Davenport, T.H.; Miller, S.M. Mandiant: AI Support for Cyberthreat Attribution. In Working with AI: Real Stories of Human-Machine Collaboration; MIT Press: Cambridge, MA, USA, 2022; pp. 75–81.
26. Volatility Foundation. Volatility Framework. Available online: https://www.volatilityfoundation.org/ (accessed on 1 November 2023).
27. AccessData. AccessData Cloud Extractor. Available online: https://www.carahsoft.com/accessdata (accessed on 1 November 2023).
28. Oxygen Forensics. Oxygen Forensic Cloud Extractor. Available online: https://oxygenforensics.com/en/resources/oxygen-forensic-cloud-extractor/ (accessed on 1 November 2023).
29. Basis Technology. Autopsy. Available online: https://www.autopsy.com/ (accessed on 1 November 2023).
30. BlackBag Technologies. BlackLight. Available online: https://www.blacklightsoftware.com/ (accessed on 1 November 2023).
31. X-Ways Software Technology AG. X-Ways Forensics. Available online: https://www.x-ways.net/forensics/ (accessed on 1 November 2023).

32. TechTarget Azure Security Center. Available online: https://www.techtarget.com/searchcloudcomputing/definition/Microsoft-Azure-Security-Center (accessed on 1 November 2023).
33. Amazon Web Services. AWS CloudTrail. Available online: https://aws.amazon.com/cloudtrail/ (accessed on 1 November 2023).
34. Yassin, W.; Abdollah, M.F.; Ahmad, R.; Yunos, Z.; Ariffin, A. Cloud forensic challenges and recommendations: A review. OIC-CERT J. Cyber Secur. 2020, 2, 19–29.