# Challenges of Trustworthy of Digital Evidence and Its Chain of Custody on Cloud Computing Environment: A Systematic Review

Lucien Rocha Lucien[a]
*CESAR, Recife Center for Advanced Studies and Systems, Apolo Street, Recife, Brazil*

Keywords: Digital Forensics, Trustworthy, Digital Evidence, Chain of Custody, Cloud Computing.

Abstract: For reliable digital evidence to be admitted in a court of law, it is important to apply scientifically proven digital forensic investigation techniques to corroborate a suspected security incident. Mainly, traditional digital forensics techniques focus on computer desktops and servers. However, recent advances in usage of cloud computing environments increased the need for the application of digital forensic investigation techniques to their infrastructure, that has some particularities, such as multi-jurisdictions storage, improper handling by third parties, high level of volatility, etc. In this paper, we perform a systematic review about the challenges of thustworthy of digital evidence and its chain of custody (CoC) on cloud computing environment. The literature search yielded 32 articles that met the study criteria. It resulted in mapping the main challenges found in the literature when applying existing approaches to increase the admissibility in courts of digital evidence collected on cloud computing environment. Furthermore, this work aims to update the systematic research regarding this subject covering the period of 2020 to 2023.

## 1 INTRODUCTION

In the last decade, cloud computing and storage has become the solution many companies and users seek to solve their problems. Cloud computer solutions offer an attractive economic benefit at a low cost, with a pay as you go model, and the flexibility of having a highly scalable server infrastructure; furthermore, it prevents companies from having to invest and maintain their services owever. However, the use of these technologies has increased potential threats and criminal activity, while making it hard for a forensic investigator and law enforcement to track and prosecute. Futhermore, criminal activity in the cloud can often leave little evidence (Yankson and Davis, 2019).

It is increasingly common that digital evidence relevant to a criminal case is not located in the State in which a crime was committed, and is dispersed in the cloud, thus becoming accessible only through the intervention of the service provider, services that perform storage (Daniele, 2019).

The challenge of obtaining digital information as evidence has become more complex with time, and investigators must ensure the integrity of digital evidence so that it may be used in court. The admissibility of digital evidence can be threatened in several ways, including improper handling, virus infection, deliberate tampering, or even by faulty hardware that compromises its integrity (Granja and Rafael, 2017).

The preservation of digital evidence involves three main factors: i) maintaining the reliability of the data, ii) ensuring the uses of the evidence, and iii) maintaining the security of the evidence . Care must be taken to ensure that the digital evidence is consistent with the data collected from a crime scene and during investigations (Rasjid et al, 2019).

Increased adoption of the cloud also brought more adversaries to the cloud. Forensics in a cloud environment is not the same as traditional forensics, because of the distinct nature of the cloud (Purnaye and Kulkami, 2022).

The study contained herein is an effort present a systematic literature review regarding the challenges gathering, handling and secure store digital evidence in cloud computing environment aiming admissibility of its digital evidence in court.

This article is organized as follows: in Section 2, basic concepts related to Theoretical Background in

[a] https://orcid.org/0000-0002-3123-2256

Lucien, L.
Challenges of Trustworthy of Digital Evidence and Its Chain of Custody on Cloud Computing Environment: A Systematic Review.
DOI: 10.5220/0012702800003690

In *Proceedings of the 26th International Conference on Enterprise Information Systems (ICEIS 2024) - Volume 2*, pages 240-246
ISBN: 978-989-758-692-7; ISSN: 2184-4992

cloud forensics and their issues regarding common standards and frameworks commonly used by law enforcements agents (LEA). In Section 3, the methods, processes, and the protocol used in the systematic review will be described. In Section 4 and 5, the results related to the conducted research will be detailed. Finally, in the last session, some conclusions and future works will be portrayed.

## 2 BACKGROUND

The cloud computing paradigm presents many benefits both to the organisations and individuals. One of such advantages relates to the manner in which data is managed by the cloud infrastructure. For instance, data is spread between various data centres to improve performance and facilitate load-balancing, scalability, and deduplication features. Because of this, data requires an efficient indexing so that retrieval and optimisation performance can take place to evade duplication that often contributes to the expansion of storage needs.

However, despite its many benefits, cloud computing poses significant challenges to the Law Enforcement Agents (LEA) and Digital Forensics Experts (DFE) from a forensic perspective. These include, but are not limited to, issues associated with the absence of standardisation amongst different CSPs, varying levels of data security and their Service Level Agreements, multiple ownerships, tenancies, and jurisdictions (Almulla et al, 2013). Moreover, the distributed nature of cloud computing services presents a variety of challenges to LEAs as data often resides in a number of different jurisdictions. In contrast with traditional Digital Forensic in which data is held on a single device, within cloud environments data is often spread over multiple different nodes.

As a result, LEAs need to rely on local laws to be able to conduct digital evidence acquisition ( Morioka and Sharbaf, 2015).Therefore, the discrepancy in the legal systems of different jurisdictions combined with the lack of cooperation between CSPs also poses significant challenges from a DF perspective (Montasari and Hill, 2019).

National Institute of Standards and Technology (NIST) recognizing the issue, has formed a cloud forensic working group. The group has published the working draft "NIST Cloud Computing Forensic Science Challenges," which identifies and classifies cloud forensic challenges (Yankson and Davis, 2019), but due to technology disruption, there are still difficulties in defining a standard framework to meet all scenarios (Rasjid et al, 2019).

In this sense, the lack of regulation of a unified standard to serve cloud service providers, led the European Union to initiate efforts to define minimum standards of compliance with providers of cloud computing services, with the aim of creating mechanisms to support the investigative process on this environment (Daniele, 2019).

## 3 APPLIED PROTOCOL

Based upon the guidelines for the development of systematic reviews in software engineering described by Kitchenham (2007) and the analysis of the review model by Dyba and Dingsøyr (2008), a new methodology for revision was created. Our review methodology is composed of six steps: (1) development of the protocol, (2) identification of inclusion and exclusion criteria, (3) search for relevant studies, (4) critical assessment, (5) extraction of data, and (6) synthesis.

The steps applied to the study contained herein are presented below: The primary objective of this review is to answer the following questions:

RQ1: What are the challenges surrounding the chain of custody of digital evidence in a cloud computing environment?

RQ2: What solutions are being proposed to tackle this problem by researchers?

### 3.1 Search Strategies

In this systematic review, the selection of studies is guided by specific criteria intended to cover various perspectives related to digital evidence and cloud forensic's chain of custody. The criteria include the last 5 years papers about the subject in four major reference bases: IEEE Explore, ACM Digital Library, Science Direct and Scopus, these bases were chosen because they concentrate the main research carried out in this segment.

For this purpose, the following keywords were chosen: "forensic", "cloud computing" and "evidence" to perform the string search on the reference bases, after search string normalization, considering the cut-off date on September, 22th 2023:

> IEEE: ("All Metadata":forensic) AND ("All Metadata":cloud computing) AND ("All Metadata":evidence) Filters Applied: 2019 - 2023

SD: ("All Metadata":forensic) AND ("All Metadata":cloud computing) AND ("All Metadata":evidence) AND Year:2019-2023

ACM: "query": { AllField:(forensic) AND AllField:(evidence) AND AllField:(cloud computing) } "filter": { E-Publication Date: Past 5 years, ACM Content: DL }
SCOPUS: ALL ( cloud AND computing+evidence+forensic ) AND PUBYEAR > 2018 AND PUBYEAR < 2024

Table 1: Amount of Studies Found on each Database.

| Database | Amount of Studies |
|---|---|
| **IEEE Explore** | 64 |
| **Science Direct Elsevier** | 9 |
| **ACM Digital Library** | 1.114 |
| **Scopus** | 3.175 |
| **TOTAL** | 4.362 |

## 3.2 Inclusion and Exclusion Criteria

Furthermore, in order to obtain the state of the art in research, the following criteria were considered for the selection of articles:

| Inclusion | Exclusion |
|---|---|
| • Law Enforcement<br>• Chain of Custody<br>• Eletronic Evidence<br>• Framework<br>• Admissibility<br>• Method<br>• Focus in IT<br>• Review, Conference Paper and Journals<br>• Data forensics | • Hardware<br>• Internet of Things<br>• Mobile/Apps forensics<br>• Digital Forensic Readiness<br>• Forensic Tool<br>• Anti Forensics<br>• Attacks<br>• Education<br>• Network Forensics<br>• Media forensics<br>• Facial forensics<br>• Books/Chapter<br>• Artificial Inteligence |

The justification for the chosen criteria is because the digital forensics segment is very broad and encompasses other market niches outside the area of cloud computing. For example, books were excluded to the scope of the search due to the state of the art on the subject against the book publication schedule.

## 3.3 Study Selection Process

After the initial search in the databases indicated above, filtering by titles was carried out, based on the inclusion and exclusion criteria. The chosen articles were imported into the Zotero reference control tool and duplicates articles were eliminated. Next, after analysing the Abstract and titles, the third and final filtering of articles was carried out.

| Database | Filtered by Title | Filtered by Abstract | Read Selection |
|---|---|---|---|
| **IEEE Explore** | 18 | 13 | 9 |
| **Science Direct Elsevier** | 0 | 0 | 0 |
| **ACM Digital Library** | 17 | 3 | 2 |
| **Scopus** | 116 | 51 | 22 |
| **TOTAL** | | | 33 |

Then, after deduplication process, the total amount of articles selected were 32.

## 3.4 Quality Assessment

In this stage, the studies underwent a critical evaluation and were analysed in full, rather than just their titles or abstracts. Subsequently, the final studies that were not aligned with the proposal of the systematic review were eliminated, resulting in the final set of works.

To assist in quality assessment, seven questions based on Kitchenham (2007) and Dyba and Dingsøyr (2008) were used. These questions helped to evaluate the applicability, quality, accuracy and reliability of the work. The questions were:

- Q1: Does the study present the research methodology used?
- Q2: Does the study answer the research questions?
- Q3: Does the study present aspects related to challenges, opportunities or next steps in the topic?
- Q4: Is the study reproducible (research basis)?

# 4 RESULTS

As was described in the previous section, each of the primary studies was assessed according to four quality criteria that relate to rigor and credibility as well as to relevance.

If considered as a whole, these four criteria provide a trustworthiness measure to the conclusions that a particular study can bring to the review. The classification for each of the criteria used a scale of positives (1 - yes) and negatives (0 - no) and is presented in Table 2.

Table 2: Quality Criteria Analysis.

| # | Study | Q1 | Q2 | Q3 | Q4 |
|---|---|---|---|---|---|
| **1** | Purnaye and Kulkarni, 2022 | 0 | 1 | 1 | 0 |
| **2** | Liu et al, 2021 | 0 | 0 | 1 | 0 |
| **3** | Simou et al, 2019 | 0 | 0 | 1 | 0 |
| **4** | Kumari and Mohapatra, 2022 | 0 | 1 | 1 | 0 |

Table 2: Quality Criteria Analysis (cont.).

| # | Study | Q1 | Q2 | Q3 | Q4 |
|---|---|---|---|---|---|
| 5 | Ali et al, 2023 | 1 | 0 | 0 | 0 |
| 6 | Sree and Raja, 2022 | 0 | 1 | 0 | 0 |
| 7 | Apirajitha and Remuka, 2021 | 0 | 0 | 1 | 0 |
| 8 | Bai and Sudha, 2023 | 0 | 1 | 1 | 0 |
| 9 | Manral et al, 2019 | 0 | 1 | 1 | 0 |
| 10 | Yankson and Davis, 2019 | 0 | 1 | 1 | 0 |
| 11 | Verma et al, 2023 | 0 | 0 | 1 | 0 |
| 12 | Yan et al, 2020 | 0 | 1 | 0 | 0 |
| 13 | Li et al, 2021 | 0 | 1 | 0 | 0 |
| 14 | Huang et al, 2023 | 0 | 1 | 1 | 0 |
| 15 | Khan et al, 2023 | 0 | 0 | 0 | 0 |
| 16 | Dhake et al,2022 | 0 | 1 | 1 | 0 |
| 17 | Prakash et al, 2022 | 0 | 1 | 1 | 0 |
| 18 | Alruwaili, 2021 | 0 | 1 | 0 | 0 |
| 19 | Tiwari et al, 2021 | 0 | 0 | 0 | 0 |
| 20 | Syed and Anu, 2021 | 1 | 1 | 1 | 0 |
| 21 | Daniele, 2019 | 0 | 1 | 1 | 0 |
| 22 | Al-Dhaqm et al, 2021 | 1 | 1 | 1 | 1 |
| 23 | Ewald, 2019 | 0 | 1 | 1 | 0 |
| 24 | Chauhan and Basal, 2021 | 0 | 1 | 1 | 0 |
| 25 | Srivastava and Choudhary, 2021 | 0 | 1 | 1 | 0 |
| 26 | Sampana, 2019 | 1 | 1 | 1 | 0 |
| 27 | Agbedanu et al, 2019 | 0 | 1 | 1 | 0 |
| 28 | Rasjid et al, 2019 | 0 | 1 | 1 | 0 |
| 29 | Ramadhani and Mulyati, 2019 | 0 | 0 | 1 | 0 |
| 30 | Montasari and Hill, 2019 | 0 | 1 | 1 | 0 |
| 31 | Petroni et al, 2019 | 0 | 0 | 0 | 0 |
| 32 | Hettige and Fernando, 2022 | 0 | 1 | 1 | 0 |

Most of the 31 studies analysed provided information in the context of this research and contributed in some way to the preparation of this paper. As seen in the above table, only Petroni et al (2019), Tiwari et al (2021) and Khan et al (2023) doesn't apply the quality criteria, otherwise, only Al-Dhaqm et al (2021) fully answered and attend all the quality criteria, followed by Syed and Anu(2021) and Sampana(2019).

## 5 DISCUSSIONS

After the analysis and data extraction, steps performed on the primary works, it was possible to identify some aspects relating our research questions, as followed:

**RQ1: What are the Challenges Surrounding the Chain of Custody of Digital (CoC) Evidence in a Cloud Computing Environment?**

Data in the cloud are often physically distributed among different servers and data centers. Hence the evidence might be distributed among thousands of servers, data is inherently volatile, it's almost impossible to physically access the hardware and acquire the evidence due to third parties' restrictions, so, investigators will have to depend on the CSP for evidence gathering, and it would affect the existing chain-of-custody rules. Investigators will not have the power to verify the CSP's process used for the evidence acquisition. Evidence from multiple time zones will contain different timestamps (Hettige and Fernando, 2022).

Hettige and Fernando (2022) also noticed that cloud computing environments has some particularities regarding the traditional forensics (such as: geo location, timezone, multi-jurisdiction, etc), so the researches had said that traditional digital forensic models and techniques might not be highly suited for usage in cloud computing environments, those information were supported by others autors cited by them (e.g: Dykstra and Sherman, 2011; Reilly et al., 2011; Grispos et al., 2012; Martini and Choo, 2012; Zawoad and Hasan, 2012).

Rasjid et al(2019) also provide an important analysis regarding the digital preservation models vs. digital evidence admissibility policy compliance, as well, the literature review carried out by Agbedanu et al (2019), Sree and Raja(2022), Bai and Sudha (2023).

Li et al (2021) also maps that the challenges in cloud forensics surrounding the CoC are loss of control, lack of transparency from the CSPs, jurisdictional issues, inability to turn off all servers, multi-tenancy, lack of clear security assurance and lack of sophisticated tools.

On this subject (Purnaye, 2021) makes a relevant contribution regarding the Comprehensive Study of Cloud Forensics mapping the future directions about the subject, as illustrated in figure 1.

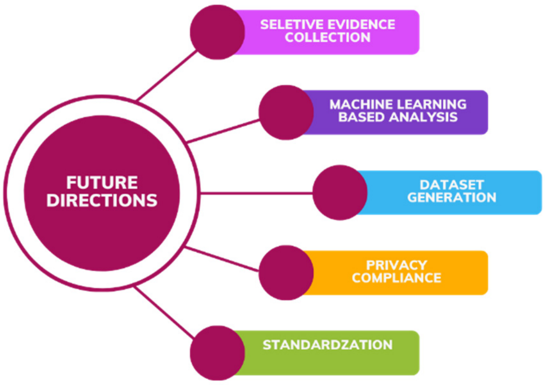

Figure 1: Future Directions on Cloud forensics.

Other relevant information collected by Purnaye (2021) evolves the directions of the studies regarding the subject up to 2019, as represented by figure 2.

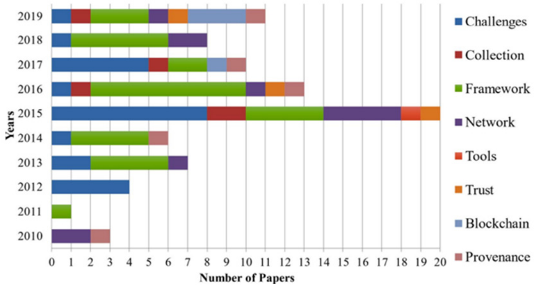

Figure 2: What the researchers written about cloud forensics (Purnaye, 2021).

**RQ2: What Solutions are Being Proposed to Tackle this Problem by Researchers?**

Al-Dhaqm et al(2021) clarify the various methodologies and stipulated guidelines in the subdomains of digital forensics to articulate the convergent and divergent (where applicable) towards a unified generally acceptable guideline for cloud environments, as well as, Ewald (2019), Daniele (2019) and Syed and Anu(2021), among which stands out the ISO 27037:2013, NIST guidelines and the new Europe Union regulation that create a channel of direct cooperation between the judicial authorities interested in acquiring the evidence and the providers on the EU.

Rasjid et al (2019), Agbedanu et al (2019) and Prakash et al (2022) had performed surveys and a taxonomy model to evaluate cloud computing security and related legal issue. The authors of the studies proposed new frameworks and new issues to evaluate during forensics in cloud environment.

Kumari and Mohapatra (2022) and Simou et al(2019) proposed a novel framework and Agbedanu et al (2019) performed a literature analysis about the subject up to 2018.

The solutions to tackle the issue were surrounded by established an uniform standard, define an international court to due the multi-jurisdiction issues, CSP's forensic readiness (Yankson and Davis, 2019).

## 6 CONCLUSION

The main objective of this paper was to conduct an updated search and analysis into the challenges regarding performing digital forensics on cloud environment focused on chain of custody and patterns/standards that could be applied on courts.

To that goal a systematic review was conducted, briefly analysing 4.362 papers and deep analysing 32 papers in order to discuss topics not only related with cloud but also how the academy is dealing with the major issues regarding digital evidence for judicial accreditation.

During the analysis phases it was clear that cloud is of highly importance to the technology community and that there are areas of research to address technology to enforce digital laws, privacy, and security. The complexity of these subject requires continued research and deeper analysis to develop effective strategies to mitigate the security risks and establish standards and patterns that fits the laws and tools issues.

The research demonstrated that India and China have the largest number of studies on this subject, beyond that this work updated the systematic review on cloud forensics in time lapse 2021 – 2023, enforcing the need for standardizations and valuation criteria for use by LEA during the forensic on these environments.

As future works, it is intended to conduct further studies related to digital evident on cloud environment and how CSP's and countries legislations are working to address these issues.

## REFERENCES

Agbedanu, P. R., Wang, P., Nortey, R. N., Odartey, L. K., 2019. Forensics in the Cloud: A Literature Analysis and Classification, in: 2019 5th International Conference on Big Data Computing and Communications (BIGCOM). pp. 124–132. https://doi.org/10.1109/BIGCOM.2019.00027

Almulla, S., Iraqi, Y., & Jones, A. (2013). Cloud forensics: A research perspective. In 9th International Conference on Innovations in Information Technology (IIT) (pp. 66–71).

Al-Dhaqm, A., Ikuesan, R.A., Kebande, V.R., Razak, S.A., Grispos, G., Choo, K.-K.R., Al-Rimy, B.A.S., Alsewari, A.A., 2021. Digital Forensics Subdomains: The State of the Art and Future Directions. IEEE Access 9, 152476–152502. https://doi.org/10.1109/ACCESS.2021.3124262

Ali, M., Ismail, A., Elgohary, H., Darwish, S., Mesbah, S., 2022. A Procedure for Tracing Chain of Custody in Digital Image Forensics: A Paradigm Based on Grey Hash and Blockchain. Symmetry 14. https://doi.org/10.3390/sym14020334

Alruwaili, F.F., 2021. Custodyblock: A distributed chain of custody evidence framework. Information 12, 1–12. https://doi.org/10.3390/info12020088

Aparecido Petroni, B.C., Gonçalves, R.F., Sérgio de Arruda Ignácio, P., Reis, J.Z., Dolce Uzum Martins, G.J., 2020.

Smart contracts applied to a functional architecture for storage and maintenance of digital chain of custody using blockchain. For. Sci. Int: Dig. Investigation 34. https://doi.org/10.1016/j.fsidi.2020.300985

Apirajitha, P., Renuka Devi, R., 2021. A Survey on Digital Forensics in Cloud Environment Using Blockchain Technology, in: Proc. Int. Conf. Comput. Commun. Technol., ICCCT. Presented at the Proceedings of the 2021 4th International Conf. on Computing and Communications Technologies, ICCCT 2021, Institute of Electrical and Electronics Engineers Inc., pp.160–163. https://doi.org/10.1109/ICCCT53315.2021.9711768

Bai, V.S., Sudha, T., 2023. A Systematic Literature Review on Cloud Forensics in Cloud Environment. Internat. J. Intel. Syst. Appl. Eng. 11, 565–578.

Chauhan, P., Bansal, P., 2021. Enhancing Trust and Immutability in Cloud Forensics, in: Tuba M., Akashe S., Joshi A. (Eds.), Adv. Intell. Sys. Comput. Presented at the Advances in Intelligent Systems and Computing, Springer Science and Business Media Deutschland GmbH, pp. 771–778. https://doi.org/10.1007/978-981-15-8289-9_74

Daniele, M., 2019. Digital Evidence gathering from service providers: A worrying paradigm shift in international cooperation. Revista Brasileira Direito Proces. Penal 5, 1277–1296. https://doi.org/10.22197/rbdpp.v5i3.288

Dhake, B., Limaye, H., Motwani, D., 2022. Cloud Forensics: Threat Assessment and Proposed Mitigations, in: 2022 International Conference for Advancement in Technology (ICONAT). pp. 1–6. https://doi.org/10.1109/ICONAT53423.2022.9725922

Dykstra, Josiah & Sherman, A.T.. (2011). Understanding Issues in cloud forensics: Two hypothetical case studies. Journal of Network Forensics. 3. 19-31.

Dyba, T. and Dingsøyr, T.(2008).Empirical studies of agile software development: A systematic review.

Ewald, U., 2019. Digital Forensics vs. Due Process: Conflicting Standards or Complementary Approaches?, in: Proceedings of the Third Central European Cybersecurity Conference, CECC 2019. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3360664.3362697

Granja, F.T. M and Rafael, G.D. R. (2017) 'Model for digital evidence preservation in criminal research institutions – PREDECI', Int. J. Electronic Security and Digital Forensics, Vol. 9, No. 2, pp.150–166.

Grispos, G., Storer, T., & Glisson, W. (2012). Calm before the storm: The challenges of cloud computing in digital forensics. International Journal of Digital Crime and Forensics, 4(2), 28–48.

Hettige KHA and Fernando MSD (2022). A survey on issues in cloud forensics with an experiment on time consumption. International Journal of Advanced and Applied Sciences, 9(3): 19-30

Huang, L., Zhao, C., Chen, S., Zeng, L., 2023. Blockchain: a promising technology for judicial translation services in cases with foreign elements. Aslib J. Inf. Manage. https://doi.org/10.1108/AJIM-11-2022-0485

Khan, A.A., Laghari, A.A., Kumar, A., Shaikh, Z.A., Baig, U., Abro, A.A., 2023. Cloud forensics-enabled chain of custody: A novel and secure modular architecture using Blockchain Hyperledger Sawtooth. Int. J. Electron. Secur. Digit. Forensics 15, 413–423. https://doi.org/10.1504/IJESDF.2023.131959

Kitchenham, B. (2007). Guidelines for performing systematic literature reviews in software engineering.

Kumari, N., Mohapatra, A.K., 2022. A Novel Framework For Multi Source Based Cloud Forensic, in: 2022 6th International Conference on Computing Methodologies and Communication (ICCMC). pp. 1–7. https://doi.org/10.1109/ICCMC53470.2022.9753849

Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., Buyya, R., 2021. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. J. Cloud Comput. 10. https://doi.org/10.1186/s13677-021-00247-5

Liu, G., He, J., Xuan, X., 2021. A Data Preservation Method Based on Blockchain and Multidimensional Hash for Digital Forensics. Complexity 2021. https://doi.org/10.1155/2021/5536326

Manral, B., Somani, G., Choo, K.-K.R., Conti, M., Gaur, M.S., 2019. A systematic survey on cloud forensics challenges, Solutions, and future directions. ACM Comput Surv 52. https://doi.org/10.1145/3361216

Martini, B., & Choo, K. K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 9(2), 71–80. doi: 10.1016/j.diin.2012.07.001

Montasari, R., Hill, R., 2019. Next-Generation Digital Forensics: Challenges and Future Paradigms, in: Proc. Int. Conf. Glob. Secur., Saf. Sustain., ICGS3. Presented at the Proceedings of 12th International Conference on Global Security, Safety and Sustainability, ICGS3 2019, Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICGS3.2019.8688020

Morioka, Emi & Sharbaf, Mehrdad. (2015). Cloud Computing: Digital Forensic Solutions. Proceedings - 12th International Conference on Information Technology: New Generations, ITNG 2015. 589-594. 10.1109/ITNG.2015.99.

Prakash, V., Williams, A., Garg, L., Barik, P., Dhanaraj, R.K., 2022. Cloud-Based Framework for Performing Digital Forensic Investigations. Int J Wireless Inf Networks 29, 419–441. https://doi.org/10.1007/s10776-022-00560-z

Purnaye, P., Kulkarni, V., 2022. A Comprehensive Study of Cloud Forensics. Arch. Comput. Methods Eng. 29, 33–46. https://doi.org/10.1007/s11831-021-09575-w

Ramadhani, E., Mulyati, S., 2020. Mapping the use of expert system as a form of cloud-based digital forensics development, in: J. Phys. Conf. Ser. Presented at the Journal of Physics: Conference Series, Institute of Physics Publishing. https://doi.org/10.1088/1742-6596/1567/3/032032

Rasjid, Z.E., Soewito, B., Witjaksono, G., Abdurahman, E., 2019. Framework for establishing confidence level of digital evidence admissibility. ICIC Express Lett. 13, 663–672. https://doi.org/10.24507/icicel.13.08.663

Reilly, D., Wren, C., & Berry, T. (2011). Cloud computing : Pros and cons for computer forensic investigations. International Journal Multimedia and Image Processing, 1(1), 26–34.

Sampana, S.S., 2019. FoRCE (Forensic Recovery of Cloud Evidence): A Digital Cloud Forensics Framework, in: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3). pp. 212–212. https://doi.org/10.1109/ICGS3.2019.8688215

Simou, S., Kalloniatis, C., Gritzalis, S., Katos, V., 2019. A framework for designing cloud forensic-enabled services (CFeS). Requir. Eng. 24, 403–430. https://doi.org/10.1007/s00766-018-0289-y

Sree, R.S., Raja, K., 2022. A Review on Forensic Investigation Analysis in Cloud Computing Environments, in: 2022 1st International Conf. on Computational Science and Technology (ICCST). pp. 1067–1074. https://doi.org/10.1109/ICCST55948.2022.10040384

Srivastava, P., Choudhary, A., 2021. Evolving evidence gathering process: Cloud forensics, in: Tiwari S., Ng A.K., Singh N., Suryani E., Mishra K.K. (Eds.), Lect. Notes Networks Syst. Presented at the Lecture Notes in Networks and Systems, Springer Science and Business Media Deutschland GmbH, pp. 227–243. https://doi.org/10.1007/978-981-15-8377-3_20

Syed, S., Anu, V., 2021. Digital Evidence Data Collection: Cloud Challenges, in: 2021 IEEE International Conference on Big Data (Big Data). pp. 6032–6034. https://doi.org/10.1109/BigData52589.2021.9672014

Tiwari, A., Mehrotra, V., Goel, S., Naman, K., Maurya, S., Agarwal, R., 2021. Developing Trends and Challenges of Digital Forensics, in: 2021 5th International Conference on Information Systems and Computer Networks (ISCON). pp. 1–5. https://doi.org/10.1109/ISCON52037.2021.9702301

Verma, S., Kumar, A., Pandey, S., Negi, P., 2023. Blockchain and Cloud Computing used in Preservation of Crime Scene Evidences, in: Proc. Int. Conf. Edge Comput. Appl., ICECAA. Presented at the Proceedings of the 2nd International Conf. on Edge Computing and Applications, ICECAA 2023, Institute of Electrical and Electronics Engineers Inc., pp. 7–11. https://doi.org/10.1109/ICECAA58104.2023.10212110

Yan, W., Shen, J., Cao, Z., Dong, X., 2020. Blockchain Based Digital Evidence Chain of Custody, in: Proceedings of the 2020 The 2nd International Conference on Blockchain Technology, ICBCT'20. Association for Computing Machinery, New York, NY, USA, pp. 19–23. https://doi.org/10.1145/3390566.3391690

Yankson, B., Davis, A., 2019. Analysis of the Current State of Cloud Forensics: The Evolving Nature of Digital Forensics, in: 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). pp. 1–8. https://doi.org/10.1109/AICCSA47632.2019.9035336

Zawoad, S., & Hasan, R. (2012). I have the proof: Providing proofs of past data possession in cloud forensics. 2012 International Conference on Cyber Security, (SocialInformatics), 75–82. doi: 10.1109/CyberSecurity.2012.