Cloud Forensics: Exploring the Challenges and Mapping Out Solutions for the Future.

[1]Pawan Mandal, [2]Isha Rajput

[1]Assistant Professor, Department of Forensic Science, RIMT University, Punjab

Abstract

With its multiple transformational effects on computing operations and myriad commercial and technological potential, cloud computing is a fast developing technology. However, appropriate forensic capabilities that could aid in the investigation of illegal activity in the cloud have not yet been established by cloud service providers and clients. The difficulty of seizing a suspect's computer and accessing their files without breaching the privacy of many other users is a result of the fact that storage systems are no longer local and that each cloud server now houses files from numerous users. Since a lack of digital investigation may increase hazards against cloud settings, cloud forensic investigations must be acknowledged for any occurrence that occurs in cloud services. The steps of identification, collection, inspection, analysis, and reporting are the focus of this study's evaluation of how to conduct forensic investigations on cloud computing in light of these challenges. Due to challenges with jurisdiction, data duplication, and multi-tenancy on the cloud platform, locating, identifying, and isolating the suspected or compromised targets is challenging. In contrast to earlier studies, this study distinguishes between the issues and potential solutions for non-cloud and cloud digital forensics by basing its analysis on the phases of traditional digital forensics. The study discusses the difficulties in cloud forensics and their remedies, and the presentation aids investigators in better understanding the issues in cloud systems.

Keywords: Cloud computing; Digital forensics; Multi-tenancy; Privacy; Security; Jurisdiction; Data duplication; Investigative phases.

1. Introduction

Cloud computing has become an essential technology in the modern digital world [1]. It has revolutionized the way organizations store, manage and process data [2]. Cloud computing provides various benefits such as scalability, cost savings, and flexibility [3]. However, along with these benefits, cloud computing also poses a significant challenge to digital forensics [4]. This challenge arises due to the fact that data in the cloud is stored remotely and is managed by a third party [5]. Therefore, investigating and analyzing data in the cloud requires specialized techniques and tools [6]. This is where the concept of cloud forensics comes into the picture [7]. Cloud forensics can be defined as the process of investigating and analyzing digital evidence in a cloud environment [8]. It involves the collection, preservation, and analysis of data that is stored, processed, or transmitted in a cloud computing environment [9]. Cloud forensics is a sub-discipline of digital forensics and is gaining importance due to the increasing use of cloud computing by organizations [10].

The cloud computing model consists of three service model- Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [11]. Each service model has different levels of control over the cloud environment, and therefore, requires different forensic techniques and tools [12]. In the SaaS model, the provider offers access to an application that runs on the cloud infrastructure [13]. The data is stored and managed by the provider, and the user accesses the application through a web browser [14]. In this model, the user has the least control over the cloud environment, and therefore, forensic investigations require the most specialized techniques and tools [15]. The investigator needs to obtain access to the cloud environment, analyze the data in transit, and collect the evidence from the provider's servers [16]. In the PaaS model, the provider offers a platform for developing, testing, and deploying applications [17]. The user has more control over the cloud environment than in the SaaS model, but the data is still managed by the provider [18]. Forensic investigations in the PaaS model require specialized tools to analyze the platform and the data stored on it [19]. In the IaaS model, the provider offers virtualized computing resources such as servers, storage, and network infrastructure [20]. The user has the most control over the cloud environment in this model, as they can install and manage the operating system and applications [21]. However, the data is still stored and managed by the provider [22]. Forensic investigations in the IaaS model require specialized tools to analyze the virtualized environment and the data stored on it [23].

The Investigation process in cloud forensics is similar to the investigation process in traditional digital forensics [24]. However, there are some additional challenges that need to be addressed in cloud forensics [25]. The first challenge is the location of data. In the cloud environment, data can be stored in different locations and can be accessed from multiple devices [26]. Therefore, investigators need to know where the data is stored and how it can be accessed [27]. The second challenge is the preservation of evidence. In the cloud environment, data can be easily modified, deleted, or moved [28]. Therefore, investigators need to take steps to ensure the integrity of the evidence [29]. The third challenge is the legal and regulatory requirements [30]. Investigators need to comply with the laws and regulations that govern the collection, preservation, and analysis of digital evidence [31].

There are several tools and techniques that can be used in cloud forensics. These include:

Cloud-specific forensic tools: These are specialized tools that are used for analyzing data in the cloud environment [32]. Examples of cloud-specific forensic tools include FTK Cloud and Magnet AXIOM Cloud [33].

Network forensic tools: These tools are used to analyze network traffic and identify suspicious activity [34]. Examples of network forensic tools include Wireshark and NetworkMiner [35].

2. Challenges in Cloud Forensics

With its ability to offer both organisations and people a flexible and adaptable infrastructure, cloud computing has become an essential component of today's technological landscape [36]. Thanks to cloud computing services like Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), users can now access and store data on remote servers [37]. But this development also creates new challenges for digital forensics investigators since cloud forensics requires obtaining, inspecting, and safeguarding digital evidence stored in cloud computing environments [38].

2.1 Challenges in Cloud Forensics:

I. Data Location:
Finding the location of data is one of the major issues in cloud forensics since cloud computing includes data being kept across various physical locations, making it difficult to identify the jurisdiction of data. [39]. For example, a cloud service provider may store data in servers located in multiple countries, making it difficult for digital investigators to determine where the data is being stored and which laws and regulations apply [40].

II. Data Ownership:
Another challenge is determining data ownership, as cloud service providers often store data for multiple users on the same servers [41]. This can lead to difficulties in determining who owns the data and the extent to which each user has access to the data [42]. Determining whether the cloud service provider has the authority to access the data is crucial since cloud service providers may also have access to user data [43].

III. Data Encryption:
Since cloud service providers frequently encrypt data to maintain its secrecy and security, data encryption presents additional hurdle in the field of cloud forensics [44]. Without the encryption keys, this encryption might make it challenging for digital investigators to access and analyse data [45]. Digital investigators could need to gain the encryption keys in order to access sensitive material, for instance, if an organisation utilises encryption to safeguard data stored in the cloud [46].

IV. Data Fragmentation:
Cloud service providers often store data in multiple locations, and this fragmentation of data can make it difficult to collect and analyze digital evidence [47]. For example, if data is stored in multiple cloud service providers, digital investigators may need to collect data from each provider to reconstruct the entire data set [48].

V. Dynamic Environments:
Data and applications are continually moving between servers and storage devices in cloud computing systems, which are extremely dynamic [49]. Because of this, gathering and preserving digital evidence may be challenging for digital investigators [50]. Digital investigators may not be able to recover deleted material from the cloud, for instance, as it may be permanently gone [51].

VI. Limited Visibility:
Cloud service providers often provide limited visibility into their infrastructure, making it challenging for digital investigators to determine how data is being stored and processed [52]. Additionally, cloud service providers may not provide access to log files or other relevant data, making it difficult for digital investigators to reconstruct the events leading up to a data breach [53].

VII. Legal Challenges:
Cloud computing involves storing data in multiple jurisdictions, making it challenging to determine the appropriate legal framework for digital investigations [54]. Additionally, cloud service providers may have different legal obligations in different jurisdictions, further complicating the legal landscape for digital investigators [55]. For example, if a cloud service provider stores data in a country with strict data protection laws, digital investigators may face legal challenges in accessing and analyzing the data [56].

2.2 Examples of Challenges in Cloud Forensics:

I. **Apple iCloud Data Breach:** In 2014, hackers accessed celebrity iCloud accounts and leaked private photos and videos [57]. The breach highlighted the challenges in cloud forensics, as the hackers accessed the data through a vulnerability in Apple's cloud computing infrastructure [58]. The breach also demonstrated the challenges in determining data ownership, as the leaked photos and videos were owned by the celebrities, but were stored on Apple's servers [59].

II. **Dropbox Data Breach:** In 2012, Dropbox suffered a data breach that compromised the login credentials of over 68 million users [60]. The breach demonstrated the challenges of data fragmentation, as the data was stored across multiple servers and was accessed by the hackers through a vulnerability in Dropbox's infrastructure [61]. The breach

also highlighted the challenge of data encryption, as the data was encrypted, making it difficult for digital investigators to determine the extent of the breach and the data that was compromised [62].

III. **AWS Data Breach:** Over 100 million customers' personal information was stolen by a data breach at Capital One in 2019 [63]. AWS server's misconfigured firewall was the cause of the breach, which highlights the difficulties of low visibility in cloud computing systems. [64]. The breach also demonstrated the challenge of legal frameworks, as Capital One had to navigate the legal landscape of multiple jurisdictions to determine the legal obligations and responsibilities of the various parties involved [65].

IV. **Cloud Storage Fraud:** Cloud storage fraud is another challenge in cloud forensics, where cybercriminals use fraudulent means to gain access to cloud storage accounts [66]. In 2020, a cybercriminal used phishing attacks to gain access to a cloud storage account belonging to a Canadian insurance company [67]. The attacker was able to steal sensitive data, including customer names, addresses, and credit card information, highlighting the challenge of data ownership and legal frameworks in cloud forensics [68].

V. **Amazon S3 Bucket Misconfiguration:** In 2017, a security researcher discovered that several companies had misconfigured their Amazon S3 buckets, allowing public access to sensitive data [69]. The misconfiguration demonstrated the challenges of data location and fragmentation, as the data was stored in multiple locations and was accessible by anyone with internet access [70]. The incident also highlighted the challenges of dynamic environments, as the misconfiguration occurred due to changes in the companies' cloud computing environments [71].

VI. **Microsoft Office 365 Data Breach:** In 2019, hackers were able to gain access to a number of Microsoft Office 365 accounts, compromising the personal data of over 300,000 users [72]. The breach demonstrated the challenges of dynamic environments in cloud forensics, as data and applications are constantly moving between servers and storage devices, making it difficult for digital investigators to identify the source of the breach [73].

3. Solutions and Developments

4.

As cloud computing continues to grow in popularity, new solutions and developments are emerging to address the challenges of cloud forensics [74]. These solutions and developments aim to provide digital investigators with better tools and techniques for collecting, analyzing, and preserving digital evidence in cloud computing environments [75].

Cloud-Specific Forensic Tools:

One of the most significant developments in cloud forensics is the emergence of cloud-specific forensic tools [76]. These tools are designed to address the unique challenges of cloud computing environments, such as data fragmentation, limited visibility, and dynamic environments [77]. Cloud-specific forensic tools can automate the collection and analysis of digital evidence, reducing the risk of human error and providing digital investigators with more accurate and reliable data [78]. Examples of cloud-specific forensic tools include Magnet AXIOM Cloud, Cellebrite UFED Cloud Analyzer, and Oxygen Forensic Cloud Extractor [79].

Digital Evidence Authentication:

Digital evidence authentication is another solution to the challenges of cloud forensics [80]. Digital evidence authenticationinvolves verifying the authenticity and integrity of digital evidence to ensure that it has not been tampered with or modified [81]. Digital evidence authentication can be challenging in cloud computing environments, as data is stored in multiple locations and is accessed by multiple users {82]. However, new developments in digital evidence authentication, such as blockchain technology, are emerging to address this challenge [83].

Cloud Service Level Agreements:

Cloud service level agreements (SLAs) are contractual agreements between cloud service providers and their customers that define the terms and conditions of the cloud computing services [84]. Cloud SLAs can include provisions for data ownership, data location, data access controls, and data encryption [85]. Cloud SLAs can also specify the responsibilities and obligations of the cloud service provider and the customer in the event of a security incident or breach [86]. Cloud SLAs can help to mitigate the challenges of data ownership, fragmentation, and limited visibility in cloud computing environments [87].

Cloud-Specific Forensic Certifications:

Cloud-specific forensic certifications, such as the Cloud Forensics and Incident Response certification offered by the International Association of Computer Investigative Specialists (IACIS), are emerging to address the need for specialized skills and knowledge in cloud forensics [88]. Cloud-specific forensic certifications can provide digital investigators with the knowledge and skills to navigate the challenges of cloud computing environments, including data location, ownership, and encryption [89].

Cloud-Specific Forensic Standards:

Cloud-specific forensic standards, such as the Cloud Forensics Framework developed by the National Institute of Standards and Technology (NIST), are emerging to provide digital investigators with a standardized approach to cloud forensics [90]. Cloud-

specific forensic standards can provide a common language and methodology for digital investigators, ensuring that digital evidence is collected and preserved in a consistent and reliable manner [91]. Cloud-specific forensic standards can also provide guidance on legal frameworks and regulations that apply to cloud computing [92].

5. Future Directions and Conclusion

Cloud forensics is a rapidly evolving field that is still in its early stages. The field poses many challenges, including the distributed nature of cloud computing environments, the dynamic nature of cloud resources, and the need for specialized tools and training. Despite these challenges, there are several existing research projects on cloud forensics that have made significant contributions to the field. These projects have focused on developing frameworks, tools, and training programs for cloud forensics investigators, as well as identifying the challenges associated with cloud forensics investigations. As cloud computing continues to become more prevalent, it is likely that cloud forensics will become an increasingly important field for digital investigators. Cloud computing has become an essential part of the modern IT infrastructure, offering on-demand access to computing resources, storage, and services over the internet. However, as more organizations move their data and applications to the cloud, there is a growing need for cloud forensic investigation to address the challenges of investigating and collecting digital evidence in cloud environments. In this article, we will discuss the future directions and conclusions of cloud forensic.

5.1 Future Directions:

a) *Standardization of Cloud Forensic Frameworks:* As cloud computing continues to grow, it is essential to develop standard forensic frameworks that are specific to cloud environments. Cloud forensic frameworks need to provide standard procedures, protocols, and techniques that can be applied to different cloud environments, such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

b) *Cloud Forensic Tool Development:* Cloud forensic tools need to be developed to extract, preserve, and analyze digital evidence in cloud environments. These tools should be specific to each cloud environment and should have the capability to analyze data at the network, operating system, and application levels. Moreover, the tools should be able to perform real-time analysis to detect and respond to security incidents in cloud environments.

c) *The incorporation of machine learning and artificial intelligence (AI) techniques:* The use of these approaches can aid in the discovery of pertinent digital evidence in cloud environments. The identification and categorization of digital evidence can be automated using these methods, which can drastically cut down on the time and effort needed to carry out a cloud forensic investigation.

d) *Cloud Forensic Training and Education:* There is a need for cloud forensic training and education to provide individuals with the necessary knowledge and skills to conduct forensic investigations in cloud environments. This training should focus on understanding cloud computing technologies, cloud forensic frameworks, cloud forensic tools, and best practices for conducting cloud forensic investigations.

e) *Collaboration and Cooperation:* Effective cloud forensic investigations require close coordination and cooperation between forensic investigators, cloud service providers, and law enforcement organisations. To carry out successful investigations, forensic investigators must collaborate closely with cloud service providers and law enforcement organisations. Cloud service providers must grant forensic investigators access to cloud infrastructure and data.

5.2 Conclusion:

Cloud computing has become a critical component of modern IT infrastructure, and its adoption is increasing rapidly. However, the growth of cloud computing has led to a significant increase in cybercrime and the need for cloud forensic investigation. Cloud forensic investigation is a complex process that requires specialized knowledge and skills. Therefore, it is essential to develop standard forensic frameworks, cloud forensic tools, and provide cloud forensic training and education to address the challenges of investigating and collecting digital evidence in cloud environments. The future of cloud forensic Investigation involves the incorporation of machine learning and artificial intelligence techniques, the development of cloud-specific forensic tools, and collaboration among cloud service providers, forensic investigators, and law enforcement agencies. These developments will help in the identification and classification of relevant digital evidence and reduce the time and effort required to conduct a cloud forensic investigation. In conclusion, cloud forensic investigation is an essential aspect of modern IT infrastructure, and the need for it is only going to increase in the future. Therefore, it is crucial to invest in research and development, standardization, training and education, and collaboration to ensure the effectiveness of cloud forensic investigation.

Reference

1. Yang, C., Huang, Q., Li, Z., Liu, K. and Hu, F., 2017. Big Data and cloud computing: innovation opportunities and challenges. International Journal of Digital Earth, 10(1), pp.13-53.
2. McAfee, A., Brynjolfsson, E., Davenport, T.H., Patil, D.J. and Barton, D., 2012. Big data: the management revolution. Harvard business review, 90(10), pp.60-68.
3. Al-Hujran, O., Al-Lozi, E.M., Al-Debei, M.M. and Maqableh, M., 2018. Challenges of cloud computing adoption from the TOE framework perspective. International Journal of E-Business Research (IJEBR), 14(3), pp.77-94.

4. Alghamdi, M.I., 2021. Digital forensics in cyber security—recent trends, threats, and opportunities. Cybersecurity Threats with New Perspectives.
5. Sharma, P.K., Kaushik, P.S., Agarwal, P., Jain, P., Agarwal, S. and Dixit, K., 2017, October. Issues and challenges of data security in a cloud computing environment. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 560-566). IEEE.
6. Fernando, V., 2021, April. Cyber forensics tools: A review on mechanism and emerging challenges. In 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-7). IEEE.
7. Roussev, V., Ahmed, I., Barreto, A., McCulley, S. and Shanmughan, V., 2016. Cloud forensics–Tool development studies & future outlook. Digital investigation, 18, pp.79-95.
8. Taylor, M., Haggerty, J., Gresty, D. and Hegarty, R., 2010. Digital evidence in cloud computing systems. Computer law & security review, 26(3), pp.304-308.
9. Taylor, M., Haggerty, J., Gresty, D. and Lamb, D., 2011. Forensic investigation of cloud computing systems. Network Security, 2011(3), pp.4-10.
10. Martini, B. and Choo, K.K.R., 2012. An integrated conceptual digital forensic framework for cloud computing. Digital investigation, 9(2), pp.71-80.
11. Raich, V., Sharma, P., Mewada, S. and Kumbhkar, M., 2013. Performance Improvement of Software as a Service and Platform as a Service in Cloud Computing Solution. ISROSET-International Journal of Scientific Research in Computer Science and Engineering, 1, pp.13-16.
12. Dykstra, J. and Sherman, A.T., 2012. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digital Investigation, 9, pp.S90-S98.
13. Viega, J., 2009. Cloud computing and the common man. Computer, 42(08), pp.106-108.
14. Jadeja, Y. and Modi, K., 2012, March. Cloud computing-concepts, architecture and challenges. In 2012 international conference on computing, electronics and electrical technologies (ICCEET) (pp. 877-880). IEEE.
15. Birk, D. and 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.
16. Choo, K.K.R., Esposito, C. and Castiglione, A., 2017. Evidence and forensics in the cloud: challenges and future research directions. IEEE Cloud Computing, 4(3), pp.14-19.
17. Soni, M., 2014. Cloud computing basics—platform as a service (PaaS). Linux Journal, 2014(238), p.4.
18. Popović, K. and Hocenski, Ž., 2010, May. Cloud computing security issues and challenges. In The 33rd international convention mipro (pp. 344-349). IEEE.
19. Guo, H., Jin, B. and Shang, T., 2012, August. Forensic investigations in cloud environments. In 2012 International Conference on Computer Science and Information Processing (CSIP) (pp. 248-251). IEEE.
20. Bhardwaj, S., Jain, L. and Jain, S., 2010. Cloud computing: A study of infrastructure as a service (IAAS). International Journal of engineering and information Technology, 2(1), pp.60-63.
21. Musse, H.M. and Alamro, L.A., 2016, July. Cloud computing: Architecture and operating system. In 2016 Global Summit on Computer & Information Technology (GSCIT) (pp. 3-8). IEEE.
22. Purcell, B.M., 2014. Big data using cloud computing. Journal of Technology Research, 5, p.1.
23. Hemdan, E.E.D. and Manjaiah, D.H., 2021. An efficient digital forensic model for cybercrimes investigation in cloud computing. Multimedia Tools and Applications, 80, pp.14255-14282.
24. Simou, S., Kalloniatis, C., Kavakli, E. and Gritzalis, S., 2014. Cloud forensics: identifying the major issues and challenges. In Advanced Information Systems Engineering: 26th International Conference, CAiSE 2014, Thessaloniki, Greece, June 16-20, 2014. Proceedings 26 (pp. 271-284). Springer International Publishing.
25. Alqahtany, S., Clarke, N., Furnell, S. and Reich, C., 2015, April. Cloud forensics: a review of challenges, solutions and open problems. In 2015 international conference on cloud computing (ICCC) (pp. 1-9). IEEE.
26. Stuedi, P., Mohomed, I. and Terry, D., 2010, June. Wherestore: Location-based data storage for mobile devices interacting with the cloud. In Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond (pp. 1-8).
27. Kagadis, G.C., Kloukinas, C., Moore, K., Philbin, J., Papadimitroulas, P., Alexakos, C., Nagy, P.G., Visvikis, D. and Hendee, W.R., 2013. Cloud computing in medical imaging. Medical physics, 40(7), p.070901.
28. Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), pp.9493-9532.
29. Zawoad, S., Dutta, A.K. and Hasan, R., 2013, May. SecLaaS: secure logging-as-a-service for cloud forensics. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security (pp. 219-230).
30. Zeni, N., Kiyavitskaya, N., Mich, L., Cordy, J.R. and Mylopoulos, J., 2015. GaiusT: supporting the extraction of rights and obligations for regulatory compliance. Requirements engineering, 20, pp.1-22.
31. Dehghantanha, A. and Franke, K., 2014, July. Privacy-respecting digital investigation. In 2014 Twelfth Annual International Conference on Privacy, Security and Trust (pp. 129-138). IEEE.
32. Bhagat, S.P. and Meshram, B.B., 2021. Digital Forensic Tools for Cloud Computing Environment. In ICT with Intelligent Applications: Proceedings of ICTIS 2021, Volume 1 (pp. 49-57). Singapore: Springer Singapore.
33. Badreldin, H., 2021. IPCFA: A Methodology for Acquiring Forensically-Sound Digital Evidence in the Realm of IaaS Public Cloud Deployments. Dakota State University.

34. Lubis, A. and Siahaan, A.P.U., 2016. Network forensic application in general cases. IOSR J. Comput. Eng, 18(6), pp.41-44.
35. Barik, K., Das, S., Konar, K., Banik, B.C. and Banerjee, A., 2021. Exploring user requirements of network forensic tools. Global Transitions Proceedings, 2(2), pp.350-354.
36. Ercan, T., 2010. Effective use of cloud computing in educational institutions. Procedia-Social and Behavioral Sciences, 2(2), pp.938-942.
37. Kumar, S. and Goudar, R.H., 2012. Cloud computing-research issues, challenges, architecture, platforms and applications: a survey. International Journal of Future Computer and Communication, 1(4), p.356.
38. Purnaye, P. and Kulkarni, V., 2022. A comprehensive study of cloud forensics. Archives of Computational Methods in Engineering, 29(1), pp.33-46.
39. Pichan, A., Lazarescu, M. and Soh, S.T., 2015. Cloud forensics: Technical challenges, solutions and comparative analysis. Digital investigation, 13, pp.38-57.
40. Hooper, C., Martini, B. and Choo, K.K.R., 2013. Cloud computing and its implications for cybercrime investigations in Australia. Computer Law & Security Review, 29(2), pp.152-163.
41. Yu, S., Wang, C., Ren, K. and Lou, W., 2010, March. Achieving secure, scalable, and fine-grained data access control in cloud computing. In 2010 Proceedings IEEE INFOCOM (pp. 1-9). Ieee.
42. Jordan, M.I. and Mitchell, T.M., 2015. Machine learning: Trends, perspectives, and prospects. Science, 349(6245), pp.255-260.
43. Takabi, H., Joshi, J.B. and Ahn, G.J., 2010. Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), pp.24-31.
44. Xue, K., Chen, W., Li, W., Hong, J. and Hong, P., 2018. Combining data owner-side and cloud-side access control for encrypted cloud storage. IEEE Transactions on Information Forensics and Security, 13(8), pp.2062-2074.
45. Hargreaves, C. and Chivers, H., 2008, March. Recovery of encryption keys from memory using a linear scan. In 2008 Third International Conference on Availability, Reliability and Security (pp. 1369-1376). IEEE.
46. Li, M., Yu, S., Zheng, Y., Ren, K. and Lou, W., 2012. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE transactions on parallel and distributed systems, 24(1), pp.131-143.
47. Caviglione, L., Wendzel, S. and Mazurczyk, W., 2017. The future of digital forensics: Challenges and the road ahead. IEEE Security & Privacy, 15(6), pp.12-17.
48. Ruan, K., Carthy, J., Kechadi, T. and Crosbie, M., 2011. Cloud forensics. In Advances in Digital Forensics VII: 7th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, January 31–February 2, 2011, Revised Selected Papers 7 (pp. 35-46). Springer Berlin Heidelberg.
49. Buyya, R., Ranjan, R. and Calheiros, R.N., 2009, June. Modeling and simulation of scalable Cloud computing environments and the CloudSim toolkit: Challenges and opportunities. In 2009 international conference on high performance computing & simulation (pp. 1-11). IEEE.
50. Karie, N.M. and Venter, H.S., 2015. Taxonomy of challenges for digital forensics. Journal of forensic sciences, 60(4), pp.885-893.
51. Odom, W., Sellen, A., Harper, R. and Thereska, E., 2012, May. Lost in translation: understanding the possession of digital things in the cloud. In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 781-790).
52. Padhy, R.P., Patra, M.R. and Satapathy, S.C., 2011. Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2), pp.136-146.
53. Pilli, E.S., Joshi, R.C. and Niyogi, R., 2010. Network forensic frameworks: Survey and research challenges. Digital investigation, 7(1-2), pp.14-27.
54. Daryabar, F., Dehghantanha, A., Udzir, N.I., bin Shamsuddin, S. and Norouzizadeh, F., 2013. A survey about impacts of cloud computing on digital forensics. International Journal of Cyber-Security and Digital Forensics, 2(2), pp.77-95.
55. Brown, A.J., Glisson, W.B., Andel, T.R. and Choo, K.K.R., 2018. Cloud forecasting: Legal visibility issues in saturated environments. Computer Law & Security Review, 34(6), pp.1278-1290.
56. Dove, E.S., Joly, Y., Tassé, A.M. and Knoppers, B.M., 2015. Genomic cloud computing: legal and ethical points to consider. European Journal of Human Genetics, 23(10), pp.1271-1278.
57. Patrick, S., 2022. More than a sex crime: a feminist political economy of the 2014 iCloud hack. Media, Culture & Society, 44(1), pp.39-55.
58. Singh, S., Jeong, Y.S. and Park, J.H., 2016. A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75, pp.200-222.
59. Filkins, B.L., Kim, J.Y., Roberts, B., Armstrong, W., Miller, M.A., Hultner, M.L., Castillo, A.P., Ducom, J.C., Topol, E.J. and Steinhubl, S.R., 2016. Privacy and security in the era of digital health: what should translational researchers know and do about it?. American journal of translational research, 8(3), p.1560.
60. Ahmed, M., Kambam, H.R., Liu, Y. and Uddin, M.N., 2020. Impact of human factors in cloud data breach. In Advances in Intelligent Systems and Interactive Applications: Proceedings of the 4th International Conference on Intelligent, Interactive Systems and Applications (IISA2019) 4 (pp. 568-577). Springer International Publishing.
61. Osaman, A.M.A. and Khalifa, T.E., 2019. A Survey Techniques to enhance confidentiality in cloud storage.
62. Cheng, L., Liu, F. and Yao, D., 2017. Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5), p.e1211.

63. Novaes Neto, N., Madnick, S., de Paula, M.G. and Malara Borges, N., 2020. A case study of the capital one data breach. Stuart E. and Moraes G. de Paula, Anchises and Malara Borges, Natasha, A Case Study of the Capital One Data Breach (January 1, 2020).
64. Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M.A. and Al-rimy, B.A.S., 2021. Secure cloud infrastructure: a survey on issues, current solutions, and open challenges. Applied Sciences, 11(19), p.9005.
65. Cho, G., 2014, June. Some legal concerns with the use of crowd-sourced Geospatial Information. In IOP conference series: earth and environmental science (Vol. 20, No. 1, p. 012040). IOP Publishing.
66. Khan, M.N.A. and Ullah, S., 2017. A log aggregation forensic analysis framework for cloud computing environments. Computer Fraud & Security, 2017(7), pp.11-16.
67. Syiemlieh, P., Khongsit, G.M., Sharma, U.M. and Sharma, B., 2015. Phishing-an analysis on the types, causes, preventive measuresand case studies in the current situation. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN, pp.2278-0661.
68. Bas, F.H., 2020. Insurance Fraud: The Case in Turkey. In Contemporary Issues in Audit Management and Forensic Accounting (Vol. 102, pp. 77-97). Emerald Publishing Limited.
69. Continella, A., Polino, M., Pogliani, M. and Zanero, S., 2018, December. There's a hole in that bucket! A large-scale analysis of misconfigured s3 buckets. In Proceedings of the 34th Annual Computer Security Applications Conference (pp. 702-711).
70. Baviskar, C.R., 2022. Cloud based automated encryption approach to prevent S3 bucket leakage using AWS Lambda (Doctoral dissertation, Dublin, National College of Ireland).
71. Saeed, I., Baras, S. and Hajjdiab, H., 2019, February. Security and privacy of AWS S3 and Azure Blob storage services. In 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS) (pp. 388-394). IEEE.
72. Chakkaravarthy, S.S., Sangeetha, D. and Vaidehi, V., 2019. A survey on malware analysis and mitigation techniques. Computer Science Review, 32, pp.1-23.
73. Gill, S.H., Razzaq, M.A., Ahmad, M., Almansour, F.M., Haq, I.U., Jhanjhi, N.Z., Alam, M.Z. and Masud, M., 2022. Security and privacy aspects of cloud computing: a smart campus case study. Intelligent Automation & Soft Computing, 31(1), pp.117-128.
74. Hosseinian-Far, A., Ramachandran, M. and Slack, C.L., 2018. Emerging trends in cloud computing, big data, fog computing, IoT and smart living. Technology for smart futures, pp.29-40.
75. Daryabar, F., Dehghantanha, A., Udzir, N.I., bin Shamsuddin, S. and Norouzizadeh, F., 2013. A survey about impacts of cloud computing on digital forensics. International Journal of Cyber-Security and Digital Forensics, 2(2), pp.77-95.
76. Manral, B., Somani, G., Choo, K.K.R., Conti, M. and Gaur, M.S., 2019. A systematic survey on cloud forensics challenges, solutions, and future directions. ACM Computing Surveys (CSUR), 52(6), pp.1-38.
77. Ali, M., Khan, S.U. and Vasilakos, A.V., 2015. Security in cloud computing: Opportunities and challenges. Information sciences, 305, pp.357-383.
78. Spiekermann, D., Eggendorfer, T. and Keller, J., 2015, July. Using network data to improve digital investigation in cloud computing environments. In 2015 International Conference on High Performance Computing & Simulation (HPCS) (pp. 98-105). IEEE.
79. Eppley, E., 2019. Critical Success Factors for Digital Forensic Investigations in Cloud Computing: An Exploratory Multiple-case Study (Doctoral dissertation, Capella University).
80. Damshenas, M., Dehghantanha, A., Mahmoud, R. and bin Shamsuddin, S., 2012, June. Forensics investigation challenges in cloud computing environments. In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 190-194). IEEE.
81. Wu, H. and Zheng, G., 2020. Electronic evidence in the blockchain era: New rules on authenticity and integrity. Computer Law & Security Review, 36, p.105401.
82. Reilly, D., Wren, C. and Berry, T., 2011. Cloud computing: Pros and cons for computer forensic investigations. International Journal Multimedia and Image Processing (IJMIP), 1(1), pp.26-34.
83. Ricci, J., Baggili, I. and Breitinger, F., 2019. Blockchain-based distributed cloud storage digital forensics: Where's the beef?. IEEE Security & Privacy, 17(1), pp.34-42.
84. Mirobi, G.J. and Arockiam, L., 2015, December. Service level agreement in cloud computing: An overview. In 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) (pp. 753-758). IEEE.
85. Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), pp.9493-9532.
86. Bernsmed, K., Jaatun, M.G., Meland, P.H. and Undheim, A., 2011, August. Security SLAs for federated cloud services. In 2011 Sixth International Conference on Availability, Reliability and Security (pp. 202-209). IEEE.
87. Padhy, R.P., Patra, M.R. and Satapathy, S.C., 2011. Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2), pp.136-146.
88. Kolochenko, I., 2022. Framework Proposal to Regulate Lawful Hacking by Police within Criminal Investigations (Doctoral dissertation, Capitol Technology University).
89. Herman, M., Herman, M., Iorga, M., Salim, A.M., Jackson, R.H., Hurst, M.R., Leo, R., Lee, R., Landreville, N.M., Mishra, A.K. and Wang, Y., 2020. Nist cloud computing forensic science challenges. US Department of Commerce, National Institute of Standards and Technology.

90. Moussa, A.N., Ithnin, N. and Zainal, A., 2018. CFaaS: bilaterally agreed evidence collection. Journal of Cloud Computing, 7(1), pp.1-19.
91. Baror, S.O., Venter, H.S. and Adeyemi, R., 2021. A natural human language framework for digital forensic readiness in the public cloud. Australian Journal of Forensic Sciences, 53(5), pp.566-591.
92. Ab Rahman, N.H., Glisson, W.B., Yang, Y. and Choo, K.K.R., 2016. Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Computing, 3(1), pp.50-59.