iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** I **Month of publication:** January 2024

DOI: https://doi.org/10.22214/ijraset.2024.58149

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

Preserving Digital Evidence in Real Time Cloud Environment for Integrity and Legal Admissibility

Joyce Chepkemoi Chepkwony[1], Dr. Andrew Kipkebut[2]
School of Science Engineering and Technology, Department of Computer science & Information Technology,Kabarak University, Private Bag 20157, Kabarak, Kenya

Abstract: ***The emergence of cloud computing has transformed the manner in which organizations handle their data and digital assets, delivering unmatched convenience and scalability. Though with this, it has also brought about new and unique challenges in preservation of digital evidence in ensuring integrity and admissibility in legal proceedings. To enhance the credibility of digital evidence, the study will review literature on specialized software tools and techniques that help in preserving evidence in its unaltered state for legal examination. The researcher will determine the effectiveness of cryptographic techniques in ensuring integrity of digital evidence that is stored in cloud environment. A comparative analysis will be done. The study will give an overview of different techniques and critical considerations that will facilitate the admissibility of digital evidence in legal proceedings. This will help in revealing the gaps in digital forensics in a Cloud Environment.***
Keywords: Digital forensic; Cloud Environment; Admissibility; Encryption; Digital Evidence.

I. INTRODUCTION

In today's world there is overreliance of digital evidence hence digital evidence plays a crucial role. It provides a non-biased record of events unlike human witnesses. It is often time stamped and therefore there is a clear picture of when particular data was created or modified. This enhances its authenticity in court. Digital forensics techniques can uncover hidden or deleted data, hence by providing valuable insights in courts. This includes recovering deleted files, examining metadata and identifying the source of electronic communications. According to [1], digital evidence transcends geographical boundaries, enabling investigations and legal proceedings to reach beyond local jurisdictions. Law enforcement agencies, legal professionals and regulatory bodies rely on digital evidence in investigating crimes, fraud, intellectual property theft, and other illicit activities [2]. Digital evidence can uncover motives and trace the movements of suspects. The review explores the challenges and solutions related to preserving digital evidence in a cloud environment. The study aims at addressing the importance of maintaining the integrity and legal admissibility of digital evidence in real-time scenarios. Digital forensic data is the information collected from digital devices during forensic investigations, such as disk images, RAM dumps, and digital artifacts [3].

II. LITERATURE REVIEW

Digital evidence refers to any information or data that is stored or transmitted in digital form and can be used in legal proceedings to support or refute claims, allegations or facts related to a case [6]. There have been several legal cases where cloud-based evidence has been challenged. Digital evidence provides an objective and often timestamped record of events, communications and actions, which can help establish a factual basis for legal arguments. It is more reliable than traditional paper-based evidence.

Data in the cloud is subject to rapid changes and updates. Real-time applications constantly generate, modify and delete data. Preserving a snapshot of evidence at a specific point in time can be challenging, especially when dealing with dynamic cloud workloads. Data in the cloud is often encrypted both in transit and at rest, thus making it difficult to access and preserve without proper credentials or encryption keys. According to [4, 5], there are many different types of crimes and therefore rendering it almost impossible to acquire complete chain of dependencies in the cloud.

The patent infringement case between Apple and Samsung, cloud-based evidence was a central issue. Apple claimed that Samsung had copied design elements of their products. The case involved examination of emails and documents that were stored in the cloud to demonstrate patent infringement and design similarities. The study found out that the issue was resolved through a settlement [7].

Various criminal and civil cases involving the use of Facebook posts that are often considered cloud-based evidence are solved through established legal processes [8]. These posts are used to establish reasons, motives and challenge the credibility of witnesses. In various legal cases, email evidence stored in cloud-based email services like Gmail has been used to prove or disapprove various claims, including criminal cases, contract disputes and intellectual property disputes.

III. DATA COLLECTION TOOLS AND TECHNIQUES

Specific tools and technologies used in cloud computing patent infringement cases depends on the nature of the patents in question. Data acquisition has been a big issue during investigation of cloud based incidents [9]. According to [10], research to date has failed in giving practical tools that support remote forensic acquisition. The use of guidance Encase in acquiring forensic data remotely is illustrated, but adds that the data may be untrustworthy. [11] proposed a framework for preservation of forensic data from cloud environment but there were no capabilities implemented.

Table 1 shows the digital forensic tools and their functions denoted by the tick [12].

Table 1: Functions of digital forensic tools

	ProDiscover Basic	OSForensics, demo version	Access Data Forensic Tool Kit	Guidance Software EnCase
Acquisition				
Physical data copy	√	√	√	√
Logical data copy	√	√	√	X
Data acquisition formats	√	√	√	√
Command-line processes	X	X	X	√
GUI processes	√	√	√	√
Remote acquisition	X	√	√	√

Better tools having the required features should be considered by the investigators who have the right platform.

[13] cited that EnCase and FTK were the most widely used tools. However, [14] noted that in the year 2007, an authentication vulnerability was found between the remote Encase agent and the server [9], lamented that there was lack of appropriate tools for the data in cloud as many were standardized to today's computing environment.

According to [15], both tools AccesData Forensic Toolkit and EnCase can successfully return volatile and non-volatile data in the cloud environment. The FTK Agent and the Encase Servlet manually installed in their experiment was successful as it was able to acquire hard drive and the memory image remotely. Both Encase and FTK do have a client server feature used for remote forensics. The study compared the two mostly used forensic tools FTK and EnCase on the cloud environment performance.

Table 2: Comparisons of FTK and EnCase forensic tool kits [15].

	FTK tool kit	ENCASE tool kit
Cloud forensics support	Limited integration with cloud services	EnCase supports integration with various cloud platforms, allowing for the collection of evidence from cloud environments.
Cloud platform Integration	Limited integration with cloud services	EnCase supports integration with various cloud platforms, allowing for the collection of evidence from cloud environments.
Incident Response in the cloud	FTK has limited incident response features, especially in the cloud	EnCase is more comprehensive and includes features for incident response, making it more suitable for cloud environments.
Encryption handling	FTK supports the analysis of encrypted data	EnCase has features for decrypting and analyzing encrypted data, providing more robust capabilities in dealing with encryption.
Data collection from cloud service	FTK may have challenges collecting evidence directly from cloud services	EnCase is better equipped to collect evidence from various cloud services, offering more versatility in cloud investigations.
Legal compliance and documentation	FTK adhere to legal standards for evidence handling	EnCase emphasizes legal compliance and provides detailed documentation, making it suitable for legal and forensic requirements.

Apart from Encase proving to be better, EnCase do not provide functionality of verifying or authenticating a person extracting forensic image, therefore identification and prove of integrity becomes questionable. EnCase use MDCs in providing integrity but MDCs are not sufficient in ensuring integrity and therefore it can be forged [16]. General purpose digital forensic tools like the EnCase, Forensic Toolkit (FTK) and the Autopsy can be used in collecting and analyzing evidence from cloud environments. EnCase is installed in virtual machines like AWS, Azure or Google Cloud and then configured to perform digital forensic tasks in a cloud environment.

While Amazon Web Services can offer the infrastructure and tools required for digital evidence preservation, it is imperative for organizations to establish appropriate data retention policies, access controls and also compliance procedures to guarantee preservation of the digital evidence in compliance with legal and regulatory mandates. Retrieving of an image of the virtual disk in a virtual machine is possible in Amazon Web Services. However, [11], argues that there is no mechanism of obtaining a hash of the image in the providers system that should validate the image integrity after download. Amazon Web Services allows one to encrypt data in transit and data at rest and also ensures confidentiality and integrity in digital evidence.

[17], presented a unified logging and monitoring framework- OpVis that could achieve operational visibility across the cloud. The researcher came up with a framework to monitor and provide operational visibility that captures and store real-time logs of system activities. Configuration of custom log collection and retention policies should be done to ensure that logs are preserved for a specified duration.

The study notes that, there are several issues that needs to be resolved for proper performance of digital investigation in the cloud environment.

Chain of custody is the chronological documentation or the paper trail of digital evidence [18]. It is used in a court of law as evidence. Chain of custody is presented as a prove on how the evidence was collected, preserved and analysed. It also documents who accessed the evidence, who modified or who interacted with the evidence and not forgetting the date and time.

According to [19], the ultimate goal of a digital investigator is to safeguard the original evidence. Maintaining the chain of custody preserves the integrity of the evidence. Evidence can be rendered inadmissible if any of the process steps breaks.

Hash functions generate fixed size hash values for data. A comparison is done before and after evidence collection. Legal and regulatory requirements must be followed when handling digital evidence in cloud to ensure data integrity and authenticity in the cloud environment. According to [20], cryptographic techniques can be used to achieve secrecy of data over a network.

The figure 1 illustrates the AES encryption process consisting of multiple rounds. Each round involve series of cryptographic operations. Ciphertext which is the final result represents the encrypted data. The key length determines the number of rounds.

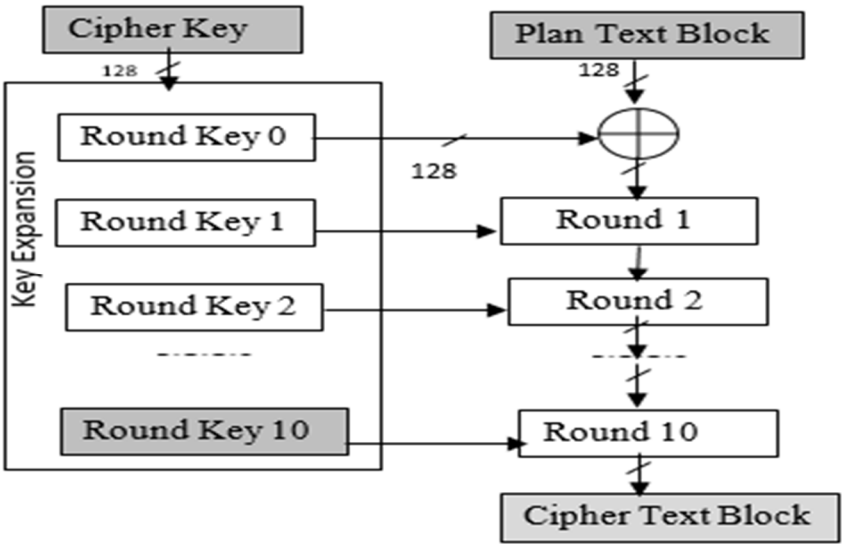


Fig 1: Advanced Encryption Standard Algorithm [21].

RSA algorithm has two keys; public and private and used in encrypting and decrypting data in the cloud storage. The key size and encryption block used is variable and not fixed.

Table 3 compares the SHA 256, RSA and AES cryptographic tools towards preservation of digital forensics evidence in the cloud environment.

Table 3: Comparison between SHA256, RSA and AES cryptographic tools [22].

	SHA 256	Rivest Shamir Adleman (RSA)	Advanced Encryption Standard (AES)
Security	Resistant to collision attacks and ensures data integrity	Secure for key exchange and digital signatures with proper key lengths	Secure for encryption data with proper key management
Efficiency	Fast computation for hashing	Efficient for small amounts of data with proper key sizes	Fast an suitable for bulk data encryption
Performance	Generally fast for hashing	Slower than symmetric encryption, depends on key size	Fast and efficient for bulk data encryption
Implementation in cloud	Commonly used for the file integrity checks, digital signatures	Used in secure communication protocols, certificate-based authentication	Used for encrypting sensitive data during storage or transmission
Preservation of digital evidence	Ensures integrity, detects changes to data	Supports secure key exchange, preserves integrity with digital signatures	Preserves confidentiality, protects against unauthorized access.

This table compares SHA 256, RSA and AES cryptographic tools based on security, performance, implementation in cloud and preservation of digital evidence.

According to the study, these tools may be combined together to achieve data integrity and confidentiality in cloud environment with each serving its specific role in the security strategy.

The image signature stored in a binary file is sent to the verifying person who needs the verification of the image already in the viewer [22].

To ensure admissibility of evidence in court, legal and regulatory considerations should be a gude in choosing of tools and methods. The study examines legal aspects of digital forensic investigations of cloud computing. Various laws and regulations, such as data protection and privacy laws such as GDPR and HIPAA, financial regulations such as Sarbanes-Oxley Act and industry-specific standards such as PCI DSS, impose legal obligations on organizations to maintain the integrity of specific types of data including personal information, financial records and medical data.

Failure to maintain data integrity can have serious legal consequences, including the dismissal of evidence, sanctions against organizations and damage to organization's credibility. This ensures that data remains reliable, accurate and trustworthy throughout its lifecycle. Ensuring data integrity throughout the chain of custody is essential in proving authenticity of evidence in court.

Courts require that digital evidence be tamper evident.

Its integrity being preserved from the point of creation or capture to the time of presentation in court. If data integrity is compromised, the evidence may be challenged and deemed inadmissible.

Digital forensic guidelines explicitly designed for investigating cloud computing systems have not yet been established.

IV. METHODOLOGY

The methodology employed in this study is querying of existing literature like, academic papers, books and articles related to preservation of digital evidence in real time cloud environment, thereby helping in gaining an understanding of the current state of knowledge, best practices and challenges in preservation of digital evidence in a cloud environment. Peer-reviewed research articles, conference papers, and journals related to cloud computing, digital forensics and legal aspects will be reviewed.

Comparative analysis will be employed in the study. This will compare different approaches, methodologies and technologies used in digital evidence preservation within cloud environments. This will help identify best practices and areas for improvement.

Legal databases such as LexisNexis and Westlaw will be reviewed to access court cases, legal precedents, and relevant related to digital evidence and its admissibility.

V. DISCUSSION AND FINDINGS

In figure 2: Comparison of performance of executing time of Rivest Shamir Adleman (RSA), Hashing (SHA 256) and Advanced Encryption Standard (AES).

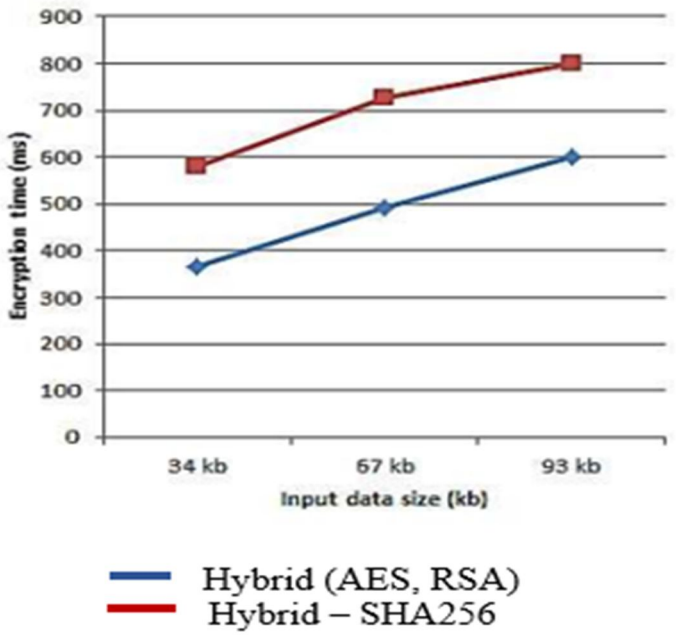


Fig 2: Comparison of performance of executing time [23].

According to the [23], combination of the encryption algorithms is a secure and a convenient technique in data security in cloud storage and achieves integrity. The study analysed two automated tools. The tools claim to protect integrity of digital evidence.

Table 4: Tools comparison on digital forensic investigation process basis [24].

Tool used	Preservation	Collection	Examination	Analysis	Reporting
Encase	Yes	Yes	Yes	Yes	Yes
Autopsy 3.0.0	Yes	Yes	No	Yes	Yes
Access Data FTK Imager	Yes	Yes	Yes	Yes	Yes
Mount Image	No	Yes	Yes	No	Yes

In table 4 digital forensic tools were examined and Mount Image proved not to have the adequate features for keeping track on time and date during acquisition and therefore not valid information in preservation of evidence. Autopsy too lacks the features for examining extracted evidence. The review emphasizes the importance of establishing a robust chain of custody for digital evidence, ensuring that it remains unaltered and admissible in legal proceedings. For digital evidence to be preserved within the cloud environments, there should be a combination of best practices, tools and procedures to ensure the integrity, security and admissibility of the evidence. Encase in cloud computing may have limitations including data transfer, network latency and scalability of cloud infrastructure in meeting the forensic investigations demands.

VI. CONCLUSION

In conclusion, the study sheds light on challenges and solutions related to preserving digital evidence in a cloud environment, especially in real-time scenarios where data is constantly changing and being processed. It provides valuable insights into maintaining the integrity and legal admissibility of digital evidence, offering recommendations for future research and practical implementation. For the data to be trusted, be reliable and accurate, digital evidence should be tamper evident which proves the authenticity of digital evidence in court.

VII. AREAS OF FURTHER STUDY

There is significant impact in preservation of digital evidence in cloud computing. Challenges of preserving digital evidence keep rising as the cloud technology evolves. Further study is to investigate the block chain technology in creation of tamper proof logs of digital evidence to enhance admissibility in courts.

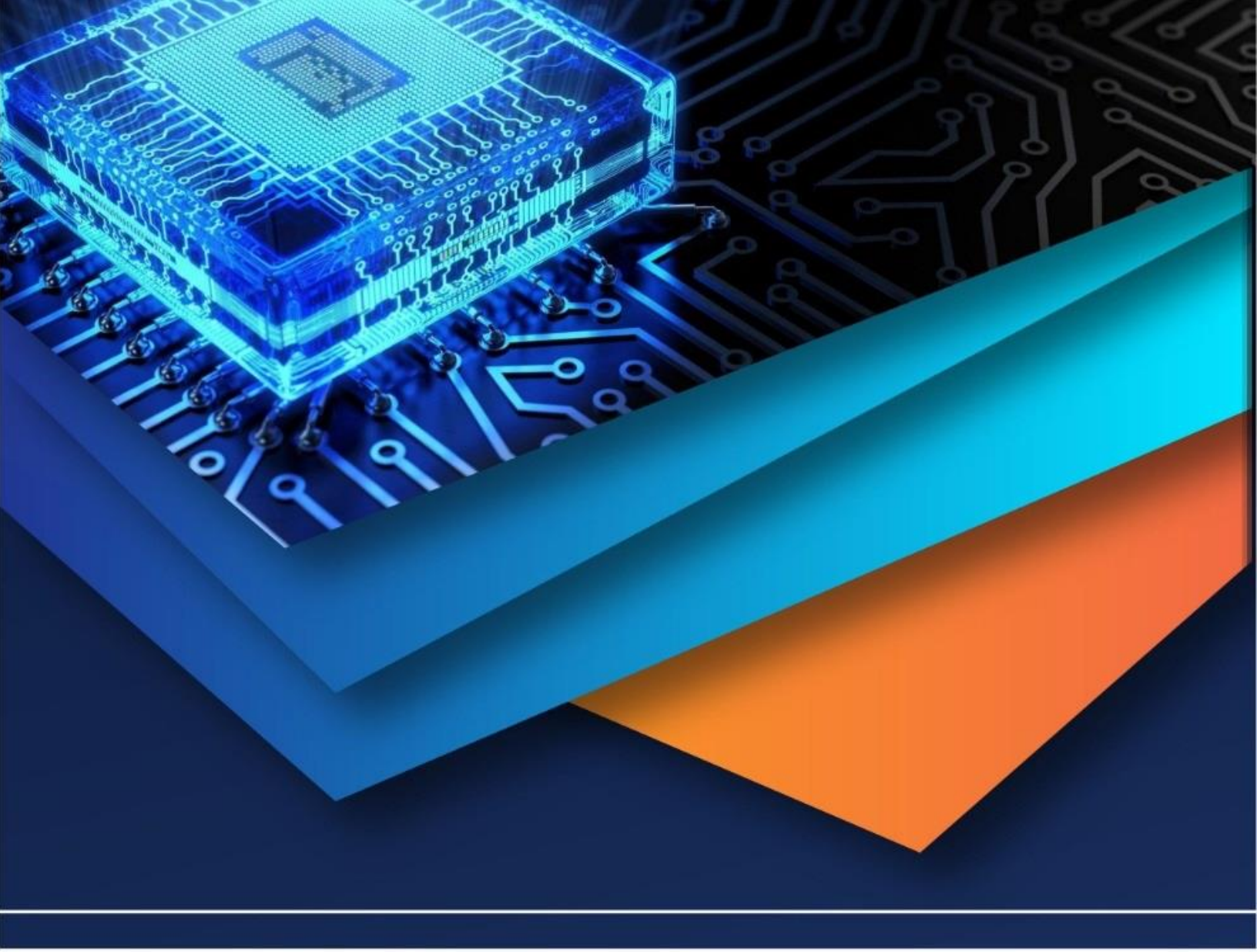
VIII. ACKNOWLEDGEMENT

I would like to express my gratitude to all who have reviewed this paper for their supportive suggestions. My profound gratitude goes to Dr. Andrew Kipkebut for his continuous support, guidance and insightful feedback throughout this paper. Your contributions are truly appreciated.

REFERENCES

[1] Currie, R. J. (2017). Cross-border evidence gathering in transnational criminal investigation: is the Microsoft Ireland case the“next frontier”?. Canadian Yearbook of International Law/Annuaire canadien de droit international, 54, 63-97.
[2] Patil, A., Banerjee, S., Jadhav, D., & Borkar, G. (2022). Roadmap of digital forensics investigation process with discovery of tools. Cyber Security and Digital Forensics, 241-269.
[3] Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., Pricop, E., Dutta, N., ... & Pricop, E. (2022). Introduction to Digital Forensics. Cyber Security: Issues and Current Trends, 71-100.
[4] 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).
[5] Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud forensics: An overview. In Advances in Digital Forensics VII (pp. 16–26).
[6] Prakash, V., Williams, A., Garg, L., Barik, P., & Dhanaraj, R. K. (2022). Cloud-Based Framework for Performing Digital Forensic Investigations. International Journal of Wireless Information Networks, 29(4), 419-441.
[7] Duncan Geoff (2014). Why are Apple and Samsung throwing down? Digital Trends. Retrieved 24 June 2014.
[8] Antoliš, K. (2023). The Challenges of Collecting Digital Evidence Across Borders. Policija i sigurnost, 32(3/2023), 271-289.
[9] M. Taylor, J. Haggerty, D. Gresty, D. Lamb Forensic investigation of cloud computing systems, Network Security, 2011 (3) (2011), pp. 4-10
[10] J. Dykstra and A. Sherman (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques.
[11] Martini, B., & Choo, K. K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. Digital investigation, 9(2), 71-80.
[12] Nelson, B., Phillips, A., & Steuart, C. (2014). Guide to computer forensics and investigations. Cengage Learning.
[13] Heiser, J. (2009). Remote forensics software. Gartner RAS Core Research Note G, 171898, 2009.
[14] R. Giobbi, J. McCormick (2007). Vulnerability Note VU#912593: Guidance EnCase Enterprise uses weak authentication to identify target machines
[15] Josiah Dykstra, Alan T. Sherman, (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques, Digital Investigation, Volume 9, Supplement.
[16] Saleem, S., & Popov, O. (2011). Protecting digital evidence integrity by using smart cards. In Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST (Vol. 53, pp. 110–119). http://doi.org/10.1007/978-3-642-19513- 6_9
[17] Fabio A. Oliveira, Sahil Suneja, Shripad Nadgowda, Priya Nagpurkar, Canturk Isci (2017). A Cloud-native Monitoring and Analytics Framework.
[18] G. Giova, (2011). “Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems,” Int. J. Comput. Sci. Netw. Secur., vol. 11, no. 1, pp. 1–9.
[19] Kruse II, W. G. and Heiser, J. G. (2002). Computer forensics: Incident response essentials. Indianapolis: Pearson.
[20] Jain, R., & Shrivastava, A. (2012). Design and implementation of new encryption algorithm to enhance performance parameters. IOSR Journal of Computer Engineering (IOSRJCE), ISSN, 2278-0661.
[21] Heron, S. (2009). Advanced encryption standard (AES). Network Security, 2009(12), 8-12.
[22] R. T. Rapolu, M. K. Gopal and G. S. Kumar, (2022). "A Secure method for Image Signaturing using SHA-256, RSA, and Advanced Encryption Standard (AES)," 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India, 2022, pp. 1-7, doi: 10.1109/ICDCECE53908.2022.9792989.
[23] AbdElnapi, N. M., Omara, F. A., & Omran, N. F. (2016). A hybrid hashing security algorithm for data storage on cloud computing. International Journal of Computer Science and Information Security (IJCSIS), 14(4).
[24] Muhammad, M. K., Ismaila, I., & Lukman, I. (2020). Integrity Assurance for Small Scale Digital Devices Based Evidence for Cyber Crime Investigation.

	Joyce Chepkemoi Chepkwony holds a Master of Science degree in Information Technology Security & Audit from Kabarak University, Nakuru, Kenya. Research interest mainly include Digital Forensics, Artificial Intelligence, Data Mining and Network Security.
	Dr. Andrew Kipkebut holds a Doctor of Philosophy PhD, in Information Security and Audit - Kabarak University and Msc in Computer Science - University of District of Columbia USA. Research interest mainly include; Algorithm Design and Optimization, Machine Learning, Artificial Intelligence, Cloud Computing, IOT and Data Science.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY