Cloud Forensics Framework to Identify, Gather, and Analyze Cloud Computing Incidents

Rafef Al-mugern
Faculty of Computing, Universiti Teknologi Malaysia, Malaysia | Department of Computer Science, Shaqra University, Saudi Arabia
a-20@graduate.utm.my (corresponding author)

Siti Hajar Othman
Faculty of Computing, Universiti Teknologi Malaysia, Malaysia
hajar@utm.my

Arafat Al-Dhaqm
Computer & Information Sciences Department, Universiti Teknologi PETRONAS, Malaysia
arafat.dhaqm@utp.edu.my

Abdulalem Ali
Institute of Computer Science and Digital Innovation, UCSI University, Malaysia
almaldolah2012@gmail.com

Received: 2 March 2024 | Revised: 8 March 2024, 22 March 2024, and 28 March 2024 | Accepted: 1 April 2024

 DOI: https://doi.org/10.48084/etasr.7185

ABSTRACT

The focus of cloud forensics is cyber-crime cases, no matter the object, the subject, or the environment involved. Each cloud computing environment has a variety of features that make it unique. Challenges associated with cloud forensics can be found at every stage of the digital forensics process. We need to begin by understanding the cloud forensics landscape (the cloud) in order to provide a holistic solution to overcome these challenges. While designing the cloud forensics framework, the elements that make up the cloud should be taken into consideration, which also impact the forensics process within the cloud. An extensive survey of the current state of research in cloud forensics is presented in this paper. Also, a conceptual cloud forensics framework that facilitates the identification, gathering, and analysis of cloud computing events is proposed, utilizing the design science approach. The proposed conceptual cloud forensics framework consists of six stages: identifying incidents, gathering evidence, preserving evidence, analyzing incidents, documenting incidents, and investigating post-incident events. Each stage has several activities and tasks to assist investigators dealing with cloud computing events. Unlike traditional approaches to cloud forensic investigations, the conceptual framework developed in this study is highly applicable.

Keywords-cloud computing; cloud forensics; digital forensics; design science

I. INTRODUCTION

Over the past few years the Cloud has undergone a series of radically improved processes. Due to its growing, it has started to attract the attention of hackers as well. Issues related to trust emerged from the early days of cloud computing [1]. There was a reluctance on the part of organizations to move their data into the cloud. Cloud computing, by contrast, includes many advantages (mainly cost savings). In recent years, technological advancements in the IT industry have resulted in more sophisticated cloud implementations. In recent years, a growing number of experts are available in the cloud domain and most challenges have been addressed [2]. IoT (Internet of Things) and big data analytics are two of the areas where cloud computing has created a plethora of innovation through IoT and big data analytics [3]. Cloud forensics is a branch of the Digital Forensics (DF) field that focuses on gathering and analyzing cloud-related incidents and data [4]. Several models, approaches, and frameworks have been proposed for cloud forensic analysis. These models have their advantages and disadvantages, but their true value lies in their flexibility. The current paper aims to develop a conceptual forensic framework that recognizes, collects, and analyzes cloud computing data. The developed conceptual cloud forensic framework consists of six steps. Each of these stages plays an important role during

the process of conducting an effective and comprehensive investigation into an incident attributed to cloud computing.

This study's findings will allow investigators to collect, preserve, analyze, and document relevant information resulting from their investigations in a more efficient and effective way than they could before. This framework can be used to enhance security, manage resources more effectively, and improve incident response by enhancing the efficiency of these processes. It is essential for organizations to maximize the power of cloud computing in order to remain competitive in a constantly evolving world of cloud computing, giving them valuable insights that will help them drive innovation and success in a constantly changing environment.

II. RELATED WORKS

Authors in [3] presented a comprehensive survey of the research trend in cloud forensics. They also proposed a cloud forensics taxonomy based on the cloud computing paradigms that have an impact on cloud forensics. In [3], a forensic metamodel was proposed for cloud computing to resolve the ambiguities and challenges that arise in cloud computing, such as standardization and heterogeneity of the field. Authors in [5] investigated how a website may be compromised using the cloud. They also carried out a hypothetical case study on cloud-based child pornography. Their study described forensic acquisition, evidence preservation, and chain of custody as the most challenging aspects of cloud forensics. Authors in [6] provided an understanding of cloud forensics through the review of various frameworks proposed in the literature, the essential components in cloud architecture, possible threats against cloud services, and various types of forensic approaches. Authors in [7] compared traditional methods of forensic investigation with those of IoT forensic investigation, and the results showed that IoT forensic investigation was more effective and efficient. They concluded that the approaches presented in their paper are necessary for IoT-based DF to function appropriately. Authors in [8] examined how cloud technologies are impacting DF regarding privacy and security issues, customer issues, and trust issues. Authors in [9] reviewed the existing traditional approaches and found that decentralized data processing rendered those approaches impractical. Accordingly, they reviewed cloud computing implementation issues in traditional DF. Authors in [10] discussed some of the challenges and solutions associated with cloud-based forensic architecture. Authors in [11] focused on the importance of digital evidence in cybercrime and electronic crime, and emphasized that digital evidence plays a key role in DF analysis as it is one of the main factors that influence it. Authors in [12] provided a detailed description of the methodological aspects and the frameworks that are being used in cloud forensics. They also critically reviewed the existing issues in implementing cloud forensics stages and possible resolutions. A detailed comparison of existing methodologies was also conducted to show their similarities and limitations. Based on the perspective and business needs of forensic practitioners, authors in [13] provided a practical log architecture framework. Their framework was tested on ownCloud, a popular open-source platform that is widely used by many companies. Authors in [14] comprehensively reviewed all types of DF, with a focus on cloud forensics. They first discussed various types of forensics classes, their frameworks, weaknesses, and solutions. Then, they focused on the existing challenges of cloud forensics. Their detailed comparative study discussed several cloud computing frameworks, including their advantages, disadvantages, differences, and similarities and provided some research directions for future studies. According to [15], three main legal challenges arise owing to the current technological landscape of cloud-based systems: territoriality (the possibility of losing location), possession (the ownership of cloud content), and confiscation procedure (problems related to user authentication and data preservation). Authors in [16] discussed the challenges associated with cloud and IoT forensics. They also presented various innovative techniques in both domains, which will contribute to a better understanding of these approaches under one umbrella. As reported in [17], log-based cloud forensics has become one of the most important aspects of cloud monitoring. The authors presented a taxonomy based on a literature study. They outlined several issues regarding the existing log-driven cloud forensic schemes and some problems that are still open to research. Authors in [18] developed an investigation framework that leverages DF to investigate cloud servers. Moreover, they reviewed previous related work based on existing cloud forensics practices, fog forensics, edge forensics, and law in order to emphasise the significant role that cloud computing plays in digital forensics. Table I displays the summarization of the existing reviewed works.

III. METHODOLOGY

This study focuses on developing a novel conceptual framework based on the design science approach. The methodology used in the present study is illustrated in Figure 1.

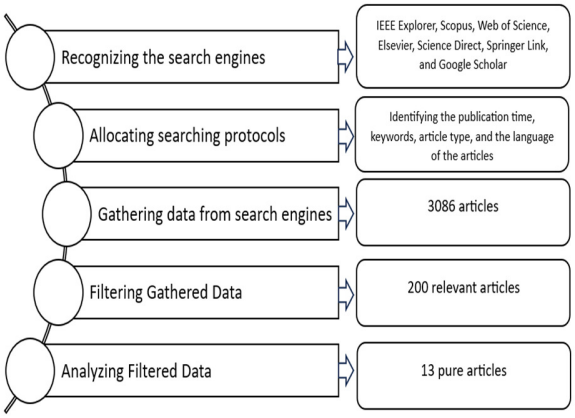

Fig. 1. Methodology used in this study.

According to [19], the design science approach is used to build an artefact that will enable humans to deal with the problem domain in an effective way.

- **Recognizing the search engines**: The purpose of this step is to identify the most popular search engines to gather relevant articles through them. IEEE Xplore, Scopus, Web of Science, Science Direct, Springer Link, and Google Scholar were considered in this study.

TABLE I. EXISTING WORK SUMMARIZATION

Year	Ref.	Description
2022	[3]	Analyzed the current research trends in cloud forensics. A taxonomy for cloud forensics based on cloud computing paradigms is proposed.
2023	[4]	It was proposed that cloud computing should incorporate a forensic metamodel to address ambiguities and challenges, such as standardization and heterogeneity.
2012	[5]	An investigation was conducted into how the cloud could be used to compromise a website and a hypothetical case study on cloud-based child pornography was conducted. The study identified forensic acquisition, evidence preservation, and chain of custody as the most challenging aspects of cloud forensics.
2012	[6]	Provided an overview of cloud forensics methodologies, cloud architecture components, and threats to cloud services, as well as types of forensic approaches.
2013	[7]	The authors conclude that the approaches presented in their paper are critical to the successful operation of IoT-based DF.
2013	[8]	The ways cloud technologies impact digital forensics today were investigated and privacy, security, customer, and trust issues associated with cloud-based DF investigations, were examined.
2015	[9]	Based on a review of existing traditional approaches, the authors concluded that decentralized data processing rendered those approaches essentially unusable.
2016	[10]	Cloud-based forensic architecture was discussed, along with some challenges and solutions. A description of the different categories and investigation processes of digital forensics is provided.
2017	[11]	Major focus was given on the importance of digital evidence in cybercrime and electronic crime.
2017	[12]	This paper describes the methodological aspects and frameworks of cloud forensics in detail.
2018	[13]	The proposed framework provided a practical approach to log architecture.
2019	[14]	All types of DF, emphasizing cloud forensics, were analyzed.
2020	[15]	There are three major legal challenges associated with cloud-based systems today. A number of issues are involved such as territoriality, possession, and confiscation procedures.
2020	[16]	The authors discussed cloud and IoT forensic challenges. Furthermore, they presented various innovative techniques to better understand how these approaches can be combined.
2021	[17]	A literature study led to the development of a taxonomy. The authors summarized several issues with the existing log-driven cloud forensic schemes and outlined some problems that have yet to be addressed.
2023	[18]	The authors investigated cloud servers with a framework that leverages DF. To emphasize the importance of cloud computing in the field of DF, they reviewed previous related work based on established cloud forensics practices, fog forensics, edge forensics, and law.

- **Allocating searching protocols**: This step identifies the search protocols that will govern the search in the search engines. The protocols used in this paper are the publication time, keywords, article type, and the language of the article in the standard form. The publication period was limited to the years from 2010 to 2023, and the keywords were set to "Cloud computing," "Cloud forensics," or "Digital forensics". The article types were set to journal articles, conference papers, and book chapters. Only papers written in English were considered in this research.
- **Gathering data from search engines**: In this step, the required data were collected from the search engines based on the search protocols. The output of this step is shown in Table II and Figure 2. A total of 3086 articles were collected from the search engines. The discussed cloud forensics different aspects are shown in Table III. Since 2010, the authors have put cloud forensics in the direction of the investigation process. As a result, a total of 694 articles were identified. As shown in Table III, the three directions that have received the most attention in the cloud forensics field are challenges, reviews, and surveys (in descending order). They are followed by case studies, blockchains, and framework directions.

TABLE II. SUMMARY OF THE COLLECTED ARTICLES

Search Engines	Keywords	Total papers	Year
IEEE Xplore	"Cloud computing," "Cloud forensics," or "Digital forensics"	128	2010- 2023
Scopus		479	
Web of Science		105	
Science Direct		194	
Springer Link		360	
Google Scholar		1820	
Total	3086		

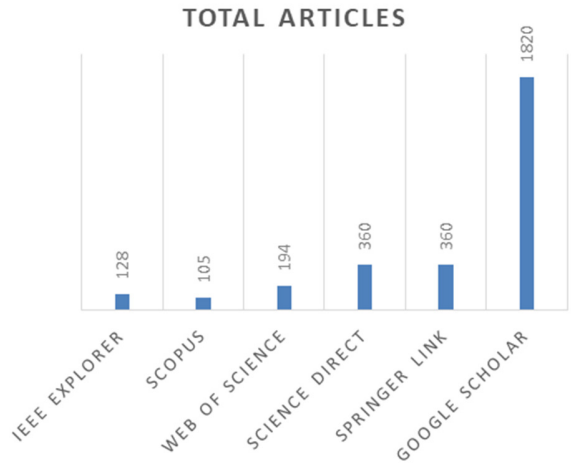

Fig. 2. Summary of the collected articles.

- **Filtering gathered data**: The data gathered in the previous step are filtered based on the criterion of being focused on the investigation process and framework directions.
- **Analyzing the filtered data**: The extracted 800 articles are analyzed by evaluating their investigation processes, contributions, advantages, disadvantages, methodology, results, novelty, and their contributions to the cloud forensics field.

Table IV displays the summarization of the analyzed gathered models.

IV. RESULTS AND DISCUSSION

This section will discuss the development of a conceptual framework for cloud forensic investigation. According to the models presented in Table V, the developed framework consists of 6 distinct processes (see Figure 3), which are described in detail below.

TABLE III. SUMMARY OF THE COLLECTED ARTICLES BASED ON THEIR DIRECTION

Category	Year														Total
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	
Investigation process	2	9	14	28	33	49	64	52	57	66	84	76	87	73	694
Frameworks	0	1	3	5	10	9	18	14	5	7	9	11	8	6	106
Case Studies	3	8	21	24	24	48	58	58	62	79	65	73	83	53	659
Challenges	7	26	56	85	83	146	157	131	144	175	147	175	174	135	1641
Survey	2	13	34	47	56	89	112	97	107	140	110	139	137	115	1198
Blockchain	0	0	0	0	0	0	1	9	16	36	35	81	70	71	319
Review	5	15	31	64	58	84	100	95	121	137	121	153	165	129	1278

TABLE IV. SUMMARY OF THE ANALYSIS OF GATHERED MODELS

Ref.	Focus	Purpose	Advantages	Disadvantages	Methodology	Output
[20]	Virtual Machine (VM) acquisition	To be highly scalable from cloud infrastructures.	Use of cloud infrastructure to acquire VMs from a highly scalable manner.	Did not address integrity validation and large-scale deployment, nor did include additional investigation.	VMware's management SDK	A novel system based on cloud management and allowed cloud-based VM acquisition
[21]	Log acquisition in private cloud environment	Improvement of the use of Eucalyptus log files in a private cloud environment	Secure private cloud environment using Eucalyptus.	Lacks high availability setup for Eucalyptus	Eucalyptus	A dashboard based on Eucalyptus's cloud operating system.
[22]	Underpinning elements of cloud computing, which are required for cloud services to be forensically friendly.	To offer forensics open cloud facilities.	Allows forensic analysis to be easily conducted. Proposes a set of questions to aid cloud forensic analysis.	Need for more comprehensive real-life scenarios that cover a variety of aspects and are supported by case studies.	Literature review	A set of questions that can be used as part of a cloud forensics analysis.
[23]	Discusses the challenges faced in cloud forensics and corresponding solutions.	To collect and analyze data.	Minimizes the time required for forensic investigations.	Lacks real-world implementations.	Struts and Hadoop distributed file system.	A framework for remote data collection and preprocessing.
[24]	An acquisition system in an Infrastructure as a Service (IaaS)	To develop and validate a forensic acquisition system in the IaaS model.	Organizations can truly take back ownership of their data from the cloud service provider.	Scalability issues are not adequately addressed.	Design science approach	Forensic acquisition system in IaaS model
[25]	Examination of cloud forensics solutions in the context of DF investigations.	To understand the challenges and limitations associated with conducting DF in cloud environment	Provided several suggestions, guidelines, and possible solutions for the investigation of forensic issues related to cloud computing.	As cloud data are stored on remote servers, they are vulnerable to unauthorized access attempts	A systematic approach	Addresses the advantages and disadvantages of using cloud forensics in digital investigations and presents recommendations.
[26]	Cloud-based DF investigations.	To determine if forensic investigators will fail to secure all necessary evidence on time.	When performing acquisition from the cloud, hybrid approaches were preferred over complete approaches, especially in time-critical situations	Cloud forensic imaging will never be able to capture the complete evidence, so cloud forensic investigations will always be based on incomplete evidence.	Hypothesis and case study, and FTK remote agent.	Several factors affect remote acquisition, and this results in a non-linear relationship between image acquisition time and storage volume.
[27]	Non-volatile memory in IaaS.	To propose solutions to cloud forensics data acquisition challenges.	Providing forensically reliable images, the approach enables the virtual hard disk to be restored as a forensic image any time.	Lacks a wider and more practical cloud environment that reflects many virtual machines.	Design science approach	A novel technique based on a cluster analysis of non-volatile memory.
[28]	Detecting crimes with cloud-based DF	To inspect the modern state of cloud virtual level forensics.	Reveals the requirements for forensics tools to be developed in order to analyze cloud infrastructure in a sound manner.	It was difficult to acquire and analyze cloud virtual layers using forensics tools because specialized forensics tools are lacking.	Experiments	A framework for assessing the virtual environment's readiness for forensic investigations and applying state-of-the-art forensics tools to cloud environments.
[29]	Cloud computing	To perform forensically sound investigations into cloud cybercrime.	Improve the ability to track attackers, identify virtual machine weaknesses, and gather digital evidence.	A real-world cloud computing environment is not provided for the necessary testing for the proposed model.	Design science method.	A novel cloud forensic investigation model to help users investigate cybercrime in the cloud.

[30]	Digital forensic readiness in the cloud.	To explore a feasible method for implementing digital forensic readiness.	To enable effective incident response procedures through the computation of the agent-based solution large-scale digital evidence.	Lacks real world implementation.	Distributed agent-based solutions.	The proposed approach uses a modified obfuscated Non-Malicious Botnet (NMB) that, when running in a cloud environment in conjunction with forensic logging capabilities for DF readiness purposes, operates as a distributed forensic Agent-Based Solution (ABS).
[31]	Cloud environment	To examine how DF readiness can be performed in cloud computing environments by designing and implementing a feasible technique	Identified several challenges associated with DF investigation in the cloud environment, including technical, operational, and systematic.	There is a drawback of collecting a large amount of forensic information at one time.	Modified obfuscated NMB.	A high-level overview of the model
[32]	Cloud computing	To investigate evidence using forensics-enabled cloud investigation.	Provides a holistic view of cybercrime, encompassing concepts from the viewpoints of organisation, technology, and law.	Lacks the kind of automation that is necessary in order to make the whole investigation efficient and effective.	Modeling	A framework for forensics enabled cloud investigation.
[33]	Cloud forensics readiness	To increase an organization's ability to reply to damages.	It can be possible to develop models using meta-analysis results.	The study focused only on 22 publications.	Meta-analysis approach	Meta-analysis was conducted to propose a cloud forensics readiness model.
[34]	Cloud forensics log security scheme.	To provide cloud forensic investigators with secure and reliable logs.	Provides investigators with secure and reliable logs that can be used for cloud forensics investigations.	Does not have the ability to detect different types of cloud attacks, encrypt files upload by the user, or set some parameters to determine whether CSPs should approve or reject cloud user requests.	Encryption algorithm (AES)	As a result of this secure log system, investigators will be able to provide secure and reliable log files for use in cloud forensics investigations.
[35]	Fitbit Versa	Different extraction and analysis techniques that can be used to recover different databases.	Provides investigators with timely information that can be used in future investigations.	Fitbit trackers typically store only a limited amount of data, which may not provide a comprehensive picture of the user's activities.	Cellebrite UFED and MSAB XRY	During the evidentiary stages of a forensic investigation, some types of data that can be verified as accurate could prove essential to the evidence process.
[36]	A timely and forensically sound investigation is necessary for cloud crimes.	To help users investigate cloud crimes in a timely and scientific manner.	Using this model, VMs in the cloud environment can be identified for future use and help digital investigations.	Lacks real world implementation.	Design science method	A novel cloud forensic investigation model to help users investigate cloud crimes in a timely and scientific manner
[4]	Cloud forensics	To resolve challenges, ambiguities, and issues associated with cloud computing, including standardization and heterogeneity.	Practitioners will be able to derive a unified model for cloud forensics that can be instantiated in the field.	Lacks practical implementation	Metamodeling approach	Proposed a forensic metamodel for the technology to resolve ambiguities, challenges, and issues that arise in cloud computing

- **Incident identification:** A security breach or incident in the cloud environment begins with incident identification. In case of potential incidents or security breaches, it is crucial to promptly identify and acknowledge them. As early as this stage, suspicious activities and abnormal behaviors might be recognized by the security analyst and may be used to detect security incidents. It is essential that these incidents are recognized as soon as possible so that the damage can be mitigated and further problems be avoided. Without the timely detection of security risks and potential data breaches, long-term dangers and security breaches may occur. Identifying incidents effectively requires appropriate monitoring and detection mechanisms. With the help of secure tools and technologies, suspicious behaviors or activities can be detected and alerted to as soon as they occur. Potential security breaches can be detected with the help of network traffic analysis, system log analyzers, and user behaviors analyzers. In an organization, the incident identification process should be clearly defined, communication channels for reporting the potentially escalating incidents should be established, and roles and responsibilities be defined for incident detection.

The importance of identifying and reporting incidents should also be emphasized through regular training and awareness programs. Many aspects of managing incidents and security breaches may exist in the cloud environment, and incident identification plays an important role in developing a framework for managing them. Organizations can ensure the security of their cloud infrastructure and data by recognizing and acknowledging potential incidents promptly and taking appropriate action to mitigate their impacts.

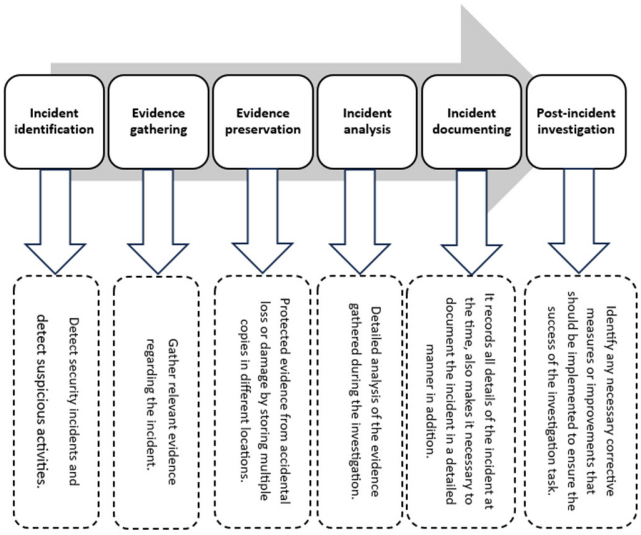

Fig. 3. The novel conceptual cloud forensic investigation framework.

- **Evidence gathering**: Immediately after the identification of an incident, the investigation proceeds to the next stage, gathering evidence, to prove the existence of a crime. It is necessary for the investigators to attempt to gather as much relevant evidence regarding the incident as possible to make a more informed decision. Log files, a computer snapshot, network traffic information, and user actions would be examples of documentation that qualifies as such a record in addition to any other physical or logical information that would provide additional insights. The evidence-gathering process is one of the most essential steps in the incident response process, which is why it is so vital to the effectiveness and efficiency of the entire process. Using this method, the examiner can reconstruct the crime scene that led up to the incident, determine its source reason, govern the influence of the incident on the systems and data affected by it, and evaluate the influence of the incident on the affected systems and data. In addition to recording a wide range of events throughout the day, system log files are essential for gathering evidence. A system may stop working for several reasons. The system may require to log in, change a file, set up a network connection, or even start a process. Depending on the situation, it can mean anything from login attempts to file changes. Using these logs, investigators can gain insights into the behaviors of users and potential attackers, acquiring a lot of information about the actions taken by these attackers or the abnormal behaviors of users. Whenever a snapshot of a system is created at a particular time, it shows its status. Snapshots help a user timely view and gather critical information such as the operating system configuration and running processes. It is possible to identify any anomalies that have occurred by examining the change in snapshots taken before and after the incident. In addition, network traffic data can be used as valuable evidence. This is one of the most valuable tools to prove that a crime has been committed. These data can also include IP addresses, protocol information, and information regarding the data transfer. Investigators may find it quite helpful to analyze network traffic to identify any unusual or malicious activity, such as attempts to gain unauthorized access to network resources or the theft of confidential information. It is also possible to obtain evidence because of the actions of a user. Information such as logins, files accessed, and system commands are some of the information that can be recorded on the system. Investigation of a user's actions may be necessary to determine whether any unauthorized or malicious activities have been carried out by insiders or unknown external actors.
- **Evidence preservation:** The preservation of evidence is one of the most important steps to ensure that the evidence gathered is both complete and authentic. Investigators must prioritize storing and securing evidence carefully to prevent evidence from getting tampered with or altered in any manner that could affect its reliability in the future. To ensure that evidence is protected and that it remains intact over time, it is important to create a secure backup. It is recommended that investigators store multiple copies of the original evidence at different locations to ensure that it is protected from accidental loss or damaged. Reconstruction of the evidence should still be possible even if one of the copies has been compromised. Evidence can be enhanced with cryptographic techniques.
- **Incident analysis:** Analysis of incidents is one of the most important aspects of any investigation into an incident related to cloud computing data. Investigators get engaged in the analysis procedure through the stage of evidence assembly, which is the process of gathering information that will help them acquire better perception into the incident in question. After carefully examining the gathered evidence, the investigators will be able to gain a greater understanding of the incident. To determine whether an incident was caused by a vulnerability or weakness within the cloud environment, it is necessary to perform a detailed analysis of the evidence gathered during the investigation of the incident. By analyzing an incident, the investigators can discover how various factors contributed to the incident in the first place, which in turn will allow them to uncover the underlying causes of future incidents. As a result, it is important to examine the network traffic data in detail along with log files and system configurations.
- **Incident documenting:** To succeed in investigating an accident, several important things need to be documented to ensure accuracy in the investigation process and to provide a detailed explanation of what has taken place during it.

Documentation serves as a comprehensive record of the incident and all its details. Physical evidence can be classified into several types, such as photographs, videos, documents, and any obtained statements or. Each piece of evidence must be correctly chained of custody to maintain its integrity and ensure its admissibility in court.

- **Post-incident investigation**: At this stage, the investigators seek to identify any necessary corrective measures or improvements that should be implemented to ensure the success of the project. One primary objective is to prevent similar incidents from taking place in the future and to enhance the overall security and resilience of the cloud environment. It is the investigators' responsibility to consider the root causes and contributing factors of the incident during the post-incident investigation. The investigation should be meticulously carried out, including a review of all available logs, system configurations, and any other documentation deemed necessary. The investigators can then determine the underlying vulnerabilities that led to the incident and gain a comprehensive understanding of what happened. After an incident has occurred, it is essential to identify any corrective measures that need to be implemented as part of the post-incident investigation process. During this process, the existing security controls are analyzed and determined whether they have been effective in preventing or mitigating the incident in question. It will be possible to recommend appropriate measures for addressing any gaps or weaknesses identified during the assessment. Moreover, the objective of the post-incident investigation is to identify any way in which the security and resilience of the cloud environment could be improved. A critical aspect of this process would be ensuring that existing policies, procedures, and protocols are right up to date and robust. It may also include the assessment of the effectiveness of the incident response plans and the identification of areas for improvement in those plans. Investigators will be composing a comprehensive report as soon as the post-incident investigation has been conducted, which details their findings and makes recommendations based on their findings. Such report will serve as a valuable source for the organization in regard to providing insights into the incident and detailing how similar incidents can be prevented in the future through the implementation of the necessary measures.

The present study concentrates on two dimensions. The first dimension consists of the research directions of the cloud forensics, and the second is the development of the proposed conceptual framework for the cloud forensics. With a look at the first dimension, it can be seen that cloud forensics has evolved into an integral part of the investigation process. In the past few years, this area of the market has steadily expanded. As Figure 4 illustrates, cloud forensics can be considered in seven investigation process directions: investigation process, framework, case studies, challenges, survey, blockchain, and review direction.

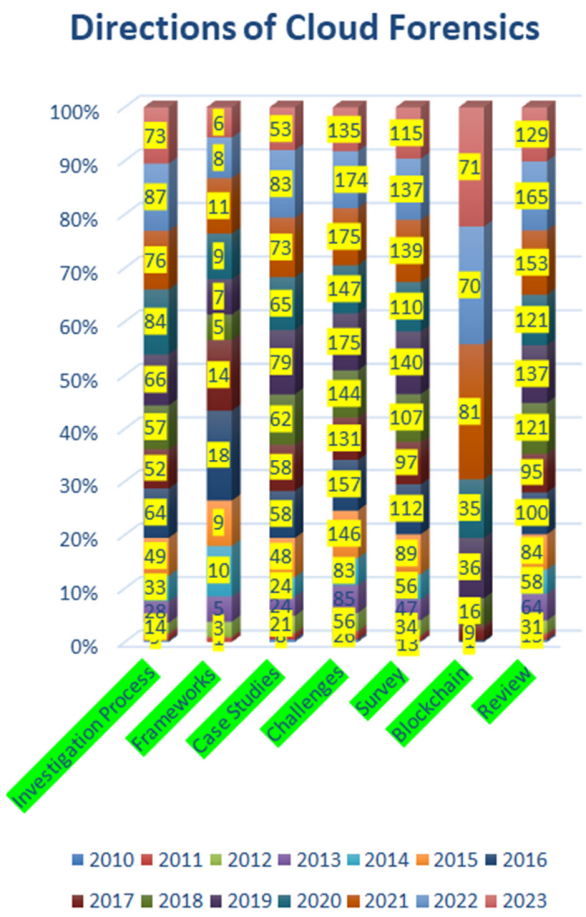

Fig. 4. Summary of the different directions adopted by the gathered articles.

These directions have been highlighted by 694 articles published during the timeframe considered in this study (2010–2023). Cloud forensics has received the most attention in three directions, as shown in Figure 4. Our discovered studies regard mostly challenges, reviews, and surveys. Case studies, blockchains, and frameworks have received less attention (the list is set in a descending order). Researchers working in the field of cloud forensics contribute to the development of robust solutions and methodologies to address the challenges arising from the use of cloud technologies in forensic investigations. Surveys identify emerging trends and areas that require further investigation and contribute to the body of knowledge by providing valuable insights into the field. A case study illustrates cloud forensics techniques in action and offers a practical perspective. Researchers may gain a more comprehensive understanding of challenges and solutions by examining specific cases. The potential implications of blockchain technology for cloud forensics, especially in preserving and securing data, have attracted significant attention. An investigation into cloud forensics is not possible without frameworks, which are vital for providing structure and support. Standardized methods enable efficient and standardized data collection, analysis, and reporting.

TABLE V. COMPARISON OF THE PROPOSED CLOUD FORENSICS FRAMEWORK WITH THE EXISTING MODELS

Year	Ref	Incident identification	Evidence gathering	Evidence preservation	Incident analysis	Incident documenting	Post-incident investigation
2013	[20]	×	√	×	×	×	×
2014	[21]	×	√	×	×	×	×
2013	[22]	×	√	×	√	×	×
2015	[23]	×	√	×	√	×	×
2016	[24]	×	√	×	×	×	×
2016	[25]	√	×	×	×	×	×
2014	[26]	√	√	√	√	√	×
2017	[27]	√	√	√	×	×	×
2017	[28]	√	√	√	√	√	×
2018	[29]	×	×	√	×	×	×
2018	[30]	×	√	√	×	×	×
2018	[31]	√	√	√	√	√	×
2019	[32]	×	×	√	√	√	×
2020	[33]	√	√	×	×	×	×
2020	[37]	√	√	×	×	×	×
2020	[34]	√	√	×	×	×	×
2021	[35]	√	×	×	√	√	×
2021	[36]	√	×	√	×	×	×
2023	[3]	√	√	√	√	√	×
Proposed framework		√	√	√	√	√	√

A conceptual framework for cloud forensics, which is the second dimension of this study, was developed. Based on Table V, it is evident that the developed framework has a unique process referred to as post-incident investigation. The proposed framework for cloud forensics is more comprehensive when compared to existing studies. For example, the incident identification process has been covered by 12 studies, evidence gathering by 14, evidence preservation process by 9, evidence analysis process by 8, and incident documentation by only 6, (Table V). None of the previous studies has covered the post-incident investigation process.

V. CONCLUSION

In recent years, organizations have been able to access, manage, and process information much more efficiently and effectively than before due to the advent of cloud computing. Several new challenges have arisen during the transition to the cloud, due to the number of security incidents that can take place in cloud environments. Traditional forensic techniques cannot address the unique characteristics of cloud environments. To identify, gather, and analyze cloud computing incidents using a design-science approach, this study proposes an innovative conceptual framework that uses the design-science methodology for the analysis of cloud computing incidents. This novel conceptual framework comprises six steps: identifying the incident in question, identifying the evidence, preserving the evidence, analyzing the incident, documenting the incident, and post-incident investigation. Using the framework developed in this study, investigators will be able to identify an incident, collect relevant evidence, preserve the collected evidence, analyze the data, document them, and conduct post-incident investigations in a more efficient and effective manner. As a future study, we recommend the implementation of the developed framework in real-world scenarios.

ACKNOWLEDGEMENT

Authors wish to thank the Ministry of Higher Education under Fundamental Research Grant Scheme (FRGS/1/2022/ ICT07/UTM/02/1). We would like also to thank the Deanship of Scientific Research at Shaqra University for supporting this work.

REFERENCES

[1] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, Nov. 2016, https://doi.org/10.1016/j.jnca.2016.09.002.

[2] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing: Implementation, Management, and Security*. Boca Raton, FL, USA: CRC Press, 2009.

[3] P. Purnaye and V. Kulkarni, "A Comprehensive Study of Cloud Forensics," *Archives of Computational Methods in Engineering*, vol. 29, no. 1, pp. 33–46, Jan. 2022, https://doi.org/10.1007/s11831-021-09575-w.

[4] R. Al-Mugerrn, A. Al-Dhaqm, and S. H. Othman, "A Metamodeling Approach for Structuring and Organizing Cloud Forensics Domain," in *International Conference on Smart Computing and Application*, Hail, Saudi Arabia, Feb. 2023, pp. 1–5, https://doi.org/10.1109/ICSCA57840.2023.10087425.

[5] J. Dykstra and A. T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques," *Digital Investigation*, vol. 9, pp. S90–S98, Aug. 2012, https://doi.org/10.1016/j.diin.2012.05.001.

[6] A. K. Mishra, P. Matta, E. S. Pilli, and R. C. Joshi, "Cloud Forensics: State-of-the-Art and Research Challenges," in *International Symposium on Cloud and Services Computing*, Mangalore, India, Dec. 2012, pp. 164–170, https://doi.org/10.1109/ISCOS.2012.32.

[7] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of Things Forensics: Challenges and approaches," in *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Austin, TX, USA, Oct. 2013, pp. 608–615, https://doi.org/10.4108/icst.collaboratecom.2013.254159.

[8] F. Daryabar, A. Dehghantanha, N. I. Udzir, N. F. binti M. Sani, S. bin Shamsuddin, and F. Norouzizadeh, "A survey about impacts of cloud computing on digital forensics," *International Journal of Cyber-Security and Digital Forensics*, vol. 2, no. 2, pp. 77–95, Apr. 2013.

[9] A. Pichan, M. Lazarescu, and S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," *Digital Investigation*, vol. 13, pp. 38–57, Jun. 2015, https://doi.org/10.1016/j.diin.2015.03.002.

[10] S. Khan *et al.*, "Cloud Log Forensics: Foundations, State of the Art, and Future Directions," *ACM Computing Surveys*, vol. 49, no. 1, pp. 1–42, Feb. 2016, https://doi.org/10.1145/2906149.

[11] M. Harbawi and A. Varol, "An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework," in *5th International Symposium on Digital Forensic and Security*, Tirgu Mures, Romania, Apr. 2017, pp. 1–6, https://doi.org/10.1109/ISDFS.2017.7916508.

[12] M. E. Alex and R. Kishore, "Forensics framework for cloud computing," *Computers & Electrical Engineering*, vol. 60, pp. 193–205, May 2017, https://doi.org/10.1016/j.compeleceng.2017.02.006.

[13] A. Pichan, M. Lazarescu, and S. T. Soh, "Towards a practical cloud forensics logging framework," *Journal of Informatin Security and Applications*, vol. 42, pp. 18–28, Oct. 2018, https://doi.org/10.1016/j.jisa.2018.07.008.

[14] M. Alkhanafseh, M. Qatawneh, and W. Almobaideen, "A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 8, pp. 610–629, Jan. 2019, https://doi.org/10.14569/IJACSA.2019.0100880.

[15] R. Fernandes, R. M. Colaco, S. Shetty, and R. Moorthy H., "A New Era of Digital Forensics in the form of Cloud Forensics: A Review," in *Second International Conference on Inventive Research in Computing Applications*, Coimbatore, India, Jul. 2020, pp. 422–427, https://doi.org/10.1109/ICIRCA48905.2020.9182938.

[16] S. A. Ali, S. Memon, and F. Sahito, "Analysis of Cloud Forensics Techniques for Emerging Technologies," in *International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications*, Tirana, Albania, Dec. 2020, pp. 106–111, https://doi.org/10.1109/CoNTESA50436.2020.9302862.

[17] A. Ghosh, D. De, and K. Majumder, "A Systematic Review of Log-Based Cloud Forensics," in *Inventive Computation and Information Technologies*, S. Smys, V. E. Balas, K. A. Kamel, and P. Lafata, Eds. New York, NY, USA: Springer, 2021, pp. 333–347.

[18] A. A. Khan, A. A. Shaikh, A. A. Laghari, and M. M. Rind, "Cloud forensics and digital ledger investigation: a new era of forensics investigation," *International Journal of Electronic Security and Digital Forensics*, vol. 15, no. 1, pp. 1–23, Jan. 2023, https://doi.org/10.1504/IJESDF.2023.127745.

[19] E. Bunde, "AI-Assisted and Explainable Hate Speech Detection for Social Media Moderators – A Design Science Approach," in *54th Hawaii International Conference on System Sciences*, Maui, HI, USA, Jan. 2021, pp. 1264–1273.

[20] L. A. Holt and M. Hammoudeh, "Cloud Forensics: A Technical Approach to Virtual Machine Acquisition," in *European Intelligence and Security Informatics Conference*, Uppsala, Sweden, Aug. 2013, pp. 227–227, https://doi.org/10.1109/EISIC.2013.59.

[21] A. K. Mishra, E. S. Pilli, and M. C. Govil, "A Prototype Implementation of Log Acquisition in Private Cloud Environment," in *3rd International Conference on Eco-friendly Computing and Communication Systems*, Mangalore, India, Dec. 2014, pp. 223–228, https://doi.org/10.1109/Eco-friendly.2014.52.

[22] S. Almulla, Y. Iraqi, and A. Jones, "Cloud forensics: A research perspective," in *9th International Conference on Innovations in Information Technology*, Al Ain, United Arab Emirates, Mar. 2013, pp. 66–71, https://doi.org/10.1109/Innovations.2013.6544395.

[23] S. Saibharath and G. Geethakumari, "Cloud forensics: Evidence collection and preliminary analysis," in *International Advance Computing Conference*, Banglore, India, Jun. 2015, pp. 464–467, https://doi.org/10.1109/IADCC.2015.7154751.

[24] S. Alqahtany, N. Clarke, S. Furnell, and C. Reich, "A forensic acquisition and analysis system for IaaS," *Cluster Computing*, vol. 19, no. 1, pp. 439–453, Mar. 2016, https://doi.org/10.1007/s10586-015-0509-x.

[25] E. Morioka and M. S. Sharbaf, "Digital forensics research on cloud computing: An investigation of cloud forensics solutions," in *Symposium on Technologies for Homeland Security*, Waltham, MA, USA, Dec. 2016, pp. 1–6, https://doi.org/10.1109/THS.2016.7568909.

[26] N. Thethi and A. Keane, "Digital forensics investigations in the Cloud," in *International Advance Computing Conference*, Gurgaon, India, Feb. 2014, pp. 1475–1480, https://doi.org/10.1109/IAdCC.2014.6779543.

[27] S. Alqahtany, N. Clarke, S. Furnell, and C. Reich, "A forensic acquisition based upon a cluster analysis of non-volatile memory in IaaS," in *2nd International Conference on Anti-Cyber Crimes*, Abha, Saudi Arabia, Mar. 2017, pp. 123–128, https://doi.org/10.1109/Anti-Cybercrime.2017.7905276.

[28] R. Jabir and O. Alfandi, "Cloud Digital Forensics Evaluation and Crimes Detection," in *International Conference on Emerging Technologies for Developing Countries*, Cotonou, Benin, Dec. 2018, pp. 171–180, https://doi.org/10.1007/978-3-319-67837-5_16.

[29] E. E.-D. Hemdan and D. H. Manjaiah, "CFIM: Toward Building New Cloud Forensics Investigation Model," in *Innovations in Electronics and Communication Engineering*, H. S. Saini, R. K. Singh, and K. S. Reddy, Eds. New York, NY, USA: Springer, 2018, pp. 545–554.

[30] V. R. Kebande and H. S. Venter, "On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges," *Australian Journal of Forensic Sciences*, vol. 50, no. 2, pp. 209–238, Mar. 2018, https://doi.org/10.1080/00450618.2016.1194473.

[31] V. R. Kebande and H. S. Venter, "Novel digital forensic readiness technique in the cloud environment," *Australian Journal of Forensic Sciences*, vol. 50, no. 5, pp. 552–591, Sep. 2018, https://doi.org/10.1080/00450618.2016.1267797.

[32] M. A. Pramanik, "CeFF: A Frameword for Forensics Enabled Cloud Investigation," M.S. thesis, University of East London, London, UK, 2019.

[33] S. A. Kristyan, Suhardi, and T. Juhana, "Modeling Cloud Forensics Readiness using MetaAnalysis Approach," in *International Conference on Information Technology Systems and Innovation*, Bandung, Indonesia, Oct. 2020, pp. 364–369, https://doi.org/10.1109/ICITSI50517.2020.9264943.

[34] S. N. Joshi and G. R. Chillarge, "Secure Log Scheme for Cloud Forensics," in *Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, Oct. 2020, pp. 188–193, https://doi.org/10.1109/I-SMAC49090.2020.9243428.

[35] J. Williams, A. MacDermott, K. Stamp, and F. Iqbal, "Forensic Analysis of Fitbit Versa: Android vs iOS," in *Security and Privacy Workshops*, San Francisco, CA, USA, Dec. 2021, pp. 318–326, https://doi.org/10.1109/SPW53761.2021.00052.

[36] E. E.-D. Hemdan and D. H. Manjaiah, "An efficient digital forensic model for cybercrimes investigation in cloud computing," *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 14255–14282, Apr. 2021, https://doi.org/10.1007/s11042-020-10358-x.

[37] V. R. Kebande, N. Karie, R. Ikuesan, and H. S. Venter, "Ontology-driven perspective of CFRaaS," *WIREs Forensics Science*, vol. 2, no. 5, 2020, Art. no. e1372, https://doi.org/10.1002/wfs2.1372.