e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

DIGITAL FORENSIC STUDY ON CLOUD COMPUTING AND CLOUD SECURITY

Katta Ganesh Sai*1, Pandiripalli Tharun*2, Varanasi Manikanta*3, CH MH Saibaba*4, Devarasetsurya Manikanta*5, S Kavitha*6

*1,2,3,4,5,6Department Of CSE, Koneru Lakshmaiah Education Foundation,
Vaddeswaram, AP, India.

DOI : https://www.doi.org/10.56726/IRJMETS45758

ABSTRACT

As cloud computing becomes more prevalent, it is critical to understand the unique characteristics of this technology and its impact on digital forensics and security. This paper covers the body of knowledge on cloud security and digital forensics, highlighting major issues such as data fragmentation, dynamic resource allocation, and data encryption. We present a methodology for conducting digital forensic investigations in cloud systems and talk about the need to implement security controls for protecting sensitive data. This study presents a digital forensic examination of cloud computing and cloud security, focusing on the challenges and potential solutions, to analyze and secure digital data in cloud environments. By giving a thorough overview of the problems and solutions involved in examining and protecting digital data in cloud environments, our study contributes the digital forensics and cloud security.

Keywords: Cloud Security, Genetic Algorithm, Data Encryption, Intrusion Detection System, Security Techniques, Cloud Computing, Security, SPI Model, Vulnerabilities, Threats Cyber Security, Digital Forensic Tools.

I. INTRODUCTION

The term "cloud computing" has been defined by the National Institute of Standards and Technology (NIST) as a complete and developing era inside of someone's day-to-day existence that provides demand for internet services like network systems, storage, servers, and programmers with flexibility and expense performance for customers. There are distinct categories for the many cloud services, such as Infrastructure as a Service. Internet services are available when needed thanks to cloud computing. An internet service provider needs to spend a lot of money on infrastructure and other issues, such as disc failure, system failure, and software defects, among others. For people who no longer wish to set up infrastructure on personal devices, the cloud is the correct solution. Nowadays, a rising number of people have been using clouds to store, send, and retrieve sensitive information, making cloud community protection one of the most pressing issues [1].

The creator of the above artwork conveys some Risk issues that affect cloud protection including information corruption, man-in-the-middle attacks, and violation of private details. This paper's study of cloud computing focuses on how virtualization concerns impact effective issuer models for cloud computing. Cloud computing, which makes use of virtualization, offers a platform for the exchange of assets, both infrastructure and software [2]. A digital signature and the RSA set of rules are used to encrypt data that is kept in the cloud. [3] describes the safety control models, protection specifications, and RSA set of rules with a digital signature that enhances cloud data security when it is being transferred over a network.

In addition to physical attacks, bad people have the option of carrying out cyberattacks to harm sensitive data about people. Avoiding cyberattacks takes time for the protection of businesses, individuals, and the country [4]. The exploration of the security of cloud records in this study makes specific use of data mining and algorithms.

The combination of cloud computing with the Internet of Things (IoT) was the most crucial innovation in our world in 2014. The fact that they will probably still be leased and used makes them the most significant part of the net offer emphasis on the fusion of IoT and cloud computing, adding Cloud IoT.

Distributed denial of service attacks were regarded as one of the largest issues of 2015. These attacks take the form of a group of intruders attacking with the single objective of depriving the user of the targeted device or services. Studying cloud security makes it more difficult to extract evidence from the cloud, forensic investigations can grow hard [5]. Instead of looking into virtual forensics, forensic research uses investigators to deal with numerous challenging situations. The intricacy of the cloud and a way to affect digital investigations were offered by the creator.

The security of a resource that is open-ended and simple to access is still debated, as writers noted in their discussion on cloud security in the year 2012. In their study, they examined the attributes of cloud computing, the cloud transport model, the cloud computing environment, and security risks related to cloud stakeholders [6]. Although virtualization plays a crucial role in cloud computing, its safety has not yet been fully explored [7].

This study's analysis of cloud security focuses on how virtualization attacks affect an effective cloud computing service architecture. Cloud computing makes it possible to share infrastructure and software resources by utilizing virtualization technologies. [2].

A STUDY ON THE ISSUE REGARDING CLOUD COMPUTING SECURITY

In both the corporate and academic worlds, the benefit of cloud computing is becoming more and more widely acknowledged. Access to a shared amount of configurable computing assets (including networks, servers, storage, applications, and services) through a network has become accessible primarily to cloud computing. These resources can be instantaneously provided and released with minimum administration service or labour-provider interaction. In some instances, the development of these platforms and the services they offer are referred to collectively as "cloud computing" in marketing [8]. It is unclear how security at all levels (such as network, host, application, and data levels) may be performed and how services security is transferred to cloud computing because cloud computing is an essentially fresh operating model [9].

Cloud computing is distinguished by its extensive scale and fully distributed, diverse, and virtualized cloud services. Cloud security measures are often like those used in other IT environments.

Compared to conventional IT solutions, cloud computing may provide various dangers to a company. Businesses that are expanding outside of their data centre-controlled networks are very concerned about shifting sensitive data and important apps to the public cloud. Here, we analyze the safety issues for cloud computing with a focus on the so-called SPI model (SaaS, PaaS, and IaaS), highlighting the most serious vulnerabilities in these kinds of systems and the most significant risks discovered in the research relating to cloud computing and its surroundings.

Here, we outline many hazards and weaknesses and explain which cloud service models they may affect. At each tier of the public cloud, the most important security features are thoroughly defined. In a later section, we'll look at cloud computing's security issues, identifying the main cloud weaknesses, the biggest cloud threats, and all workable remedies. The goal of the issue was to identify Cloud Computing's most important challenges, considering security needs, threats, risks, and requirements.

A Model for Cybersecurity in Environments of Cloud Computing.

The search results show that cyber security metrics are tools that help improve decision-making, increase performance, and increase accountability [1]. They serve as measures of how closely the security mechanisms of the system follow relevant protocols, rules, and regulations[5]. The number of reported incidents, any variations in these numbers, the time and expense required to identify an attack, and the number of vulnerable systems are some crucial cybersecurity metrics [1]. The use case, regulatory scope, and risk tolerance of an organization all influence the selection of cybersecurity KPIs [4]. However, it is recommended that companies pick KPIs that non-technical staff, consumers, and other stakeholders can all understand [4]. Mean Time to Detect (MTTD), Mean Time to Resolve (MTTR), and Mean Time to Contain (MTTC) are some of the most common KPIs and metrics used for evaluating cyber security performance [4][6]. The average time to resolve an event for a system that detects intrusions is referred to as MTTR [6].

Risk estimation metrics: -

The use of information systems is prevalent nowadays throughout both individuals and organizations. It is effectively clear that the loss of a significant amount of money, time, and other resources would result from information security attacks on these systems from hackers, viruses, or inside staff members. The information security risk management methodology is used in this situation to save costs without raising risks. Threats and vulnerabilities are strongly related to the features of the assets and, respectively, the security measures. Examples of tangible and intangible assets include software, equipment, and personnel (plans, organization, external factors, and technical factors).

The first stage permits the identification of the system's assets, security demands (confidentiality, integrity, and availability), threat profiles, and key vulnerabilities through interviews with diverse people during workshops.

Digital Forensics in Cloud Computing

Digital evidence is delicate and brittle, and if managed wrongly, it can be manipulated. Data is hard and unstable, therefore protocols must be followed to make sure that it is not changed during processing. Identification, collection, acquisition, and preservation are the first four processes in the first processing of digital evidence. A standard operating procedure (SOP) contains all the guidelines and instructions that must be followed to investigate in a way that ensures the validity of gathered evidence in a court of law, as well as the instruments and other resources required [10]. The application of digital forensic science to cloud computing systems is known as cloud forensics. In terms of technology, it creates digital evidence using a hybrid forensic approach. Facilitating both internal and external investigations involves interactions between cloud actors (such as cloud providers, consumers, brokers, carriers, and auditors) on an organizational level [11].

When using hardware devices like memory cards, flash drives, sophisticated tools, etc., forensic professionals have an easier investigative process. The technique produces a low report when an attack occurs in a cloud computing environment; as a result, we use forensic services to make a more serious report and manage the collection of consumer data and accidental evidence. Digital research allows for time and cost savings; some services may be built on SaaS, PaaS, or IaaS models.

IaaS (Infrastructure as a Service):

It is a service model offered by CSPs that includes physical infrastructure/VM, networking devices, and device security and housing. Customer capability will be determined by necessity. The client has the majority of the power over basic hardware and software infrastructure, including housing, purchasing, and operating it.

PaaS(Platform as a service):

It is a service approach for software deployment. The CSP offers the customer a platform so they may upload and maintain their systems and applications without worrying about system upkeep or infrastructure maintenance. It limits access since it might be challenging for the investigators to have full access.

SaaS (Software as a service):

A centrally hosted software distribution with a subscription-based and license strategy is referred to as SaaS. Due to its partial lack of control over software and hardware development, it also aids in cost reduction. However, it offers less power and might be quite difficult for the investigator.

II. RELATED WORK

The development of digital forensics, which has entered a new stage with the arrival of cloud computing, has been impacted by technological developments. The cloud computing concept makes shared computing resources including networks, servers, storage, applications, and services available by way of the network on demand, making it a widely available and practical option.

An Investigation into the Challenges

Associated with Security in Cloud Computing.

The importance of security in cloud computing requires the resolution of several issues. The lone person or entity accountable for guaranteeing cloud computing security is the cloud service provider, who is in charge of data storage and security maintenance.

DATA SECURITY: -

To prevent unauthorized access, theft, alteration, or destruction of digital information, protocols and precautions are put in place. These measures must be implemented throughout the data's entire lifecycle, including when it is stored, transmitted, and processed. Various security tests and assessments are employed to identify and prevent malicious attacks and ensure the protection of data.

- Cross-site scripting [XSS].

- Hidden field manipulation.
- Access control weaknesses.
- Insecure configuration.
- OS and SQL injection flaws.
- Insecure storage.

DATA SEGREGATION: -

Data segregation is the technique of segregating sensitive data from non-sensitive data and granting only authorized individuals or programs access to sensitive data. Organizations can reduce the risk of illegal access, data leakage, and data loss by separating their data. Data segregation vulnerabilities can be discovered or located using the test following.

1. Data validation.
2. Insecure storage.
3. SQL injection flaws.

Using Digital Forensics Methods in Cloud Computing Environments.

Challenges presented by cloud computing for established digital forensic investigation models are explored in this section, with a focus on the DFRW Investigation Process (DIP) Model and the ACPO principles and guidelines. Digital forensics in cloud environments involves gathering, analyzing, and safeguarding electronic data in cloud-based systems for investigative purposes. When conducting digital forensics in cloud environments, there are several important factors to keep in mind.

Understanding the cloud service model is important since different cloud service models, such as IaaS, PaaS, and SaaS, have various levels of responsibility for security and data management. It's important to understand the service model being used to determine the scope of the investigation. Collect relevant data: Collecting relevant data is crucial in any digital forensics investigation. In cloud environments, this may include data stored in virtual machines, storage buckets, databases, or logs. Preserve the evidence: Cloud environments can be dynamic, and data can change quickly. To protect the evidence's integrity and legal admissibility, it is crucial to utilize proper instruments and storage methods.

III. TYPES OF EVIDENCE IN CLOUDS

Evidence found in cloud environments may include familiar items such as emails, documents, and images created using common software applications. However, there are also additional types of evidence unique to cloud environments, such as activity logs that track user interactions with cloud services. To track how their services are being used, major cloud service providers like Amazon and Google have created a variety of logging techniques. A variety of logging techniques.

1. Message log search:

Message log search refers to the process of searching and analyzing logs generated by messaging systems, such as email servers, instant messaging platforms, and social media platforms. Message logs contain valuable information that can help investigators identify patterns of behaviour, establish timelines, and gather evidence in cases such as cyberbullying, harassment, and data breaches.

2. Logs for the Amazon Simple Storage Service (S3):

A feature of Amazon Simple Storage Service (S3) is logging which enables you to track requests made to your S3 buckets. With logging enabled, Amazon S3 will automatically generate access logs for every request made to your S3 bucket. These logs contain detailed information about the request, such as the IP address of the requester, the date and time of the request, and the item requested.

Enabling S3 logging can be done at the bucket level, and you can choose to send logs to a target bucket or an external destination, such as Amazon S3 or Amazon Glacier. You can also configure the log file format, the frequency of log generation, and the retention policy for your logs.

CLOUD COMPUTING BUILDING BLOCKS & DEPLOYMENT MODELS

Application Service Providers (ASP) use the software-as-a-service (SaaS) method to distribute different software applications via the Internet. In addition to saving the client from having to download and use the application on their personal computer, this also lessens the significant labour associated with software maintenance, including continuing use, protection, and support. [3]. To run and manage the complete solution, The SaaS provider is in charge of setting up and maintaining the IT infrastructure, which includes servers, operating systems, databases, space in data centres, network access, power, and cooling, among other things. Developers can build, release, and manage applications using Platform as a Service (PaaS), a cloud computing architecture, without having to worry about the underlying infrastructure. With PaaS, the user is in charge of supervising the design and deployment of their application while the cloud service provider takes care of the infrastructure's hardware, networking, operating system, and other elements.

Four basic deployment models for cloud computing exist:

Public Cloud: Cloud technologies, which are a subset of cloud computing, make resources like servers, storage, and software available to everyone online. The resources are shared by several companies or individuals, and it is run by external cloud service providers.

Private Cloud: A "private cloud" is a cloud computing infrastructure that is used solely by one business. It is managed and operated by the business or a third-party supplier, and it may be hosted on- or off-site.

Hybrid Cloud: An integrated and smooth cloud computing environment is provided by a hybrid cloud, which is made up of both public and private clouds. With this deployment paradigm, businesses can exploit the scalability and affordability of public cloud resources for workloads that are not sensitive while maintaining sensitive data and applications on their private clouds.

Community Cloud: A community cloud is a sort of cloud computing that is used by a specific group of entities that have identical objectives and worries, like security and regulatory compliance. These clouds can be hosted on-premises or off-premises and are often managed and run by a third-party supplier.

Analysis of cloud computing's anti-forensics approaches and digital forensics challenges

Anti-forensic techniques in cloud computing

- Evidence Destruction
- Obfuscation
- Compromise integrity of evidence
- Data Hiding
- Circumvent VM Isolation

1. Cloud computing evidence destruction: - When the VM is executing or when the VM stops, the evidence can be destroyed. When the VM is terminated, the log files are lost. Data files can be discarded while the VM is executing, and the VM's data itself can be destroyed. After the VM, the evidence is deleted as a result.

2. Obfuscation: -

This approach is used to modify the logs inside the VM and change/update the file timestamps in the disc file. Obfuscation allows file timestamps to be confused, file headers to be altered, and log files to be altered.

3. Data hiding: -

Threats from side channels and covert channels are investigated. These attacks are used to erase crucial information about which VM is ignorant and to bridge the communication gap between VMs. A side-channel assault can likewise do this. The CSP uses several encryption mechanisms, but by taking advantage of specific security features, attackers can transfer the data from one VM to another via covert or side channels.

4. Compromise integrity of evidence: -

The investigators and CSP are primarily responsible for this work. The evidence cannot be changed or altered by any of the attackers. CSP must ensure that the attacker cannot destroy or modify the evidence.

5. Circumvent VM isolation: -

Because towards its main mode, multi-tenancy, the cloud is extensively employed. Side channel assaults are therefore given priority. Attackers may locate two virtual machines (VMs), interrupt their connectivity, damage critical data, or steal vital information. [12].

Cloud forensic challenges

identification: -

Identification in cloud forensics refers to the process of identifying whether a crime has occurred or not in a cloud environment [4]. It is a step in the forensic process that uses a set of predetermined steps to determine the origin of the evidence. Cloud forensics is a subset of digital forensics that may be classified into three areas: client forensics, cloud forensics, and network forensics. The investigator identifies the evidence from the three different sources of cloud service models, namely SaaS, IaaS, and PaaS. The evidence is collected from both the client and server sides. Implementing forensic tools in the cloud environment and trying to log all activities from both application layers can help in identifying evidence for cloud forensics [12].

Preservation-collection: -

Data preservation and collection are critical in cloud forensics investigations. Following a set of predetermined stages, the forensic process is started as a post-incident activity after the crime is committed and identifies the source of the evidence. The decentralized nature of the cloud creates issues for cloud synchronization, and the absence of standard formats of logs is a bottleneck to providing a general solution for all CSPs and all types of logs. Researchers have proposed various ways of addressing the challenges of cloud forensics, including new approaches to testing attacks in real-time [12].

Examination-analysis: -

Examination analysis is a stage in the digital forensic investigation process that involves carefully examining digital evidence to discover relevant information that can help answer investigative queries. It comes after the acquisition phase, in which evidence is gathered, and before the reporting phase, in which the results are presented. During the examination-analysis phase, forensic investigators evaluate the gathered digital evidence using various techniques and tools. Examining file information, monitoring network traffic, studying computer memory, and retrieving lost or damaged data are examples. The purpose is to find and evaluate pertinent information that can aid in the investigation of topics such as who was responsible for a cyber-attack when it occurred, and how it was carried out.

Presentation: -

When referring to cloud forensics, the term "presentation" refers to the stage of the digital forensic investigation process when the investigation results are shared with interested parties. This phase, which comes after the examination analysis phase, involves concisely presenting the investigation's results.

The presentation phase involves the preparation of a report by forensic investigators that includes an overview of the investigation's discoveries along with any relevant data, analysis, and recommendations. The report could also provide suggestions for corrective action and for preventing such situations in the future. The client, management, and legal representation are often included among the stakeholders who receive the report is generally presented. Due to the complexity of Platforms for cloud computing, the location of the data, and the cloud forensic presentation phase investigations can be extremely difficult.

IV. CONCLUSION

Digital forensics in cloud computing presents unique challenges that require specialised knowledge, tools, and procedures. It is essential to provide standardised rules and methods for carrying out digital forensic investigations in cloud environments as more businesses continue to use cloud computing. This study has analysed the body of knowledge on cloud computing's use of digital forensics and has highlighted both significant problems and potential answers. The proposed framework for conducting digital forensic investigations in cloud environments can serve as a starting point for organisations and forensic investigators to develop their procedures. Overall, this study highlights the importance of digital forensics and cloud security in today's technology-driven society and emphasizes the need for continued research and collaboration between digital forensics and cloud computing communities.

V. REFERENCES

[1] Anis Ben Aissa B, Latifa Ben Arfa Rabai A, *Mouna Jouini A. A Cybersecurity Model In Cloud Computing Environments (2013)25.

[2] Hashizume Et Al. Journal Of Internet Services And Applications 2013, 4:5.

[3] Oludare Isaac Abiodun A⇑, Moatsum Alawida B, Abiodun Esther Omolara A, Abdulatif Alabdulatif C. Data Provenance For Cloud Forensic Investigations, Security, Challenges, Solutions And Future Perspectives: A Survey 34(2022).

[4] Dr K. Thirupathi Rao, Divya Vadlamudi, B. Rajasekhar reddy, Pellakuri Vidyullatha. Analysis Of Digital Forensics Challenges And Anti-Forensics Techniques In Cloud Computing7(2.7) (2018).

[5] Tim Storer, William Bradley Glisson, George Grispos. Calm Before The Storm: The Challenges Of Cloud Computing In Digital Forensics (2018).

[6] "Nist Cloud Computing Forensic Science Challenges," August 2020.

[7] Rajnish Choubey1, Rajshree Dubey 2, Joy Bhattacharjee3. A Survey On Cloud Computing Security, Challenges And Threats (2011).

[8] Kashif Munir, Iram Manan, Mubarak Almutairi. Digital Forensics In Cloud Computing Platforms. Ijcsns International Journal Of Computer Science And Network Security, Vol22 No.4, April 2022.

[9] Kalyan Sudia, Santosh Bulusu. A Study On Cloud Computing Security Challenges. Master Thesis Software Engineering Thesis No Mse-2012:82 01 2012.

[10] Rabi Prasad Padhy1 Manas Ranjan Patra, 2 Suresh Chandra Satapathy, 3senior Software Engineer Associate Professor Hod & Professor Oracle India Pvt. Ltd. Dept. Of Computer Science Dept. Of Computer Sc.& Engg. Bangalore, India Berhampur University, India Anits, Sanivasala, India. Iracst - International Journal Of Computer Science And Information Technology & Security (Ijcsits) Vol. 1, No. 2, December 2011.

[11] Archit Kapur. Bachelor In Information Technology Inderprastha Engineering College. Digital Forensics In Cloud Computing. International Journal Of Computer Applications (0975 – 8887) Volume 183 – No. 18, July 2021.

[12] Moatsum Alawida B, Oludare Isaac Abiodun A, Abiodun Esther Omolara A, Abdulatif Alabdulatif C. Data Provenance For Cloud Forensic Investigations, Security, Challenges, Solutions And Future Perspectives: A Survey 34(2022).