INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

PROTECTING CLOUD FORENSIC INVESTIGATION AGAINST ANTI-FORENSIC INVASIONS: A STUDY

AUTHORED BY - ASHUTOSH KUMAR
RESEARCH SCHOLAR
NETAJI SUBHAS UNIVERSITY

ABSTRACT

A computational paradigm is also known as "cloud computing" allows for the cost-effective delivery of computer assets and services to consumers on demand. Because the cloud computing environment's infrastructure, computing power, and storage are so easily accessible, it is accessible to several security threats.

The cloud environment has unique characteristics that make conventional digital forensic investigation techniques inapplicable, including multiple tenancies, the use of virtualization actual lack of access of cloud data, and lack of assurance. The use of several cloud forensic investigation techniques has been examined by researchers. Yet, invaders have targeted such processes directly. Anti-forensic assault is one such documented attack that goes after the cloud forensic procedure itself. The effectiveness of the forensic process gets hampered when an invader performs an anti-forensic invasion against a cloud environment by concentrating on specific stages of the process. It should be noted that there aren't numerous techniques available for preventing anti-forensic attacks in clouds because they are a relatively new attack pathway. The difficulties in identifying anti-forensic assaults are increased by the cloud environment's segmented structure and its amenities.

I examined potential anti-forensic invasions against the cloud forensic investigation process in my research paper, focusing on each of the four steps. This research paper's main goal is to suggest methods for recognizing and preventing cloud anti-forensic invasions. Initially, I suggested classifying cloud anti-forensic attacks using a classification system. Next, I developed a productive method for identifying any dubious virtual PCs (virtual machines) in the cloud. Finding a suspect Virtual Machine (VM) allows us to separate it, preventing any anti-forensic threats. I examined the anti-forensic invasion scenarios in the cloud using invasions diagrams. Additionally, I have suggested effective methods for identifying and

 ISSN: 2582-6433

classifying cloud anti-forensic attacks.

My work contribution is the suggestion of a hashing-based detection mechanism for cloud data objects that have been disguised. Virtual computers in the cloud serve as important sources of evidence for the forensic investigation. To stop Virtual Machine deletion, I have suggested an authentication system. Preserving the obtained proof against non-forensic invasions is just as crucial as it is difficult. My other contribution is the proposal of an integrity-preserving system that can prevent cloud anti-forensic attacks by safeguarding the evidence when it is transferred to the probe the location. The Eucalyptus private cloud test bed was used to verify the techniques suggested research paper.

Keywords: Cloud computing, cloud data, cloud anti-forensic attacks, Virtual Machine.

INTRODUCTION

"Cloud computing represents not only the current scenario and the whole of computing history, but also its prospective or future.

- Larry Ellison

For the past 20 years, cloud computing has been the vogue. At first, only major companies were drawn to adopting cloud computing due to its features as a computing atmosphere for resource utilization and business implementation. These days, medium and lower business businesses are also associated with the utilization of cloud computing. These companies utilize cloud systems for user data storage as well as for the development and delivery of individual applications. More than ninety-five of businesses utilize cloud services, according to the most current data on cloud adoption. The worldwide market for public cloud services is expected to reach $623.3 billion.

One prominent and economic technology strategy nowadays is cloud computing. In recent years, there has been a significant increase in the use of cloud computing applications as businesses and consumers look for lower cost computational services and resources. Both the public and private sectors are beginning to accept cloud computing more and more. A cloud computing system utilizes automation and a multi-tenant utilize pattern to make effective use of the resources.

 ISSN: 2582-6433

These days, a large number of cloud service provider businesses, such as Drop box, Google, and Amazon, can meet clouds customer requirements at inexpensive prices. Security and privacy issues in cloud computing have become more complex as a result of the fundamental shift in cloud computing utilization from the business to the person side. Systems that used to support cloud computing are becoming easy targets for abusive and unlawful assaults. Malicious people have been encouraged to misuse their surroundings by the widespread usage of cloud technology and the quick and simple means of gaining access to it. Local tractability is extremely difficult because of the internet-based platform's remote access abilities and the fact that the service logs are also widely preserved there.

A 2016 analysis on Cyber crime estimated that by the year of 2025, the cost of cyber crimes might reach an unprecedented $10.5 trillion. Numerous nations are making significant investments in implementing different protective and security strategies against Cyber crimes. Such safeguards, meanwhile, have not proven effective in preventing incidents of security breaches. Numerous scholars are working on developing methods to look into cybercrimes and find the perpetrators. Such tool is known as "**Forensic computing**".

Investigative forensic methods can be used to probe into cybercrimes in environments of cloud computing. Conventional computing ecosystems are distinct from cloud-based services in certain ways. Therefore, it is not possible to utilize usual digital forensic strategies for cloud forensic research. There are more than sixty five main challenges listed in the "NIST paper" on internet-based forensics. "Architectural design, gathering and evaluating data, against forensics, incident-first those who responded, and administration's role " are several of them, to mention a few others. While responding to problems in the cloud-based eco mechanism, investigators encounter several kinds of difficulties. Prior to implementing cloud forensics for discovering illegal activity in the cloud, however, there are a number of difficult issues that require our immediate attention. Such comprise of flexibility of cloud computing, forensic scene reorganization cloud data isolation, cloud data origin, and cloud against-forensics.

One of the main obstacles to cloud forensic exploration is anti-forensics. When attempting an assault of such kind, the perpetrators attempt to conceal what they have done, making it more difficult for forensic experts to examine and recreate the criminal activity scene. Anti-forensic invasion detection and mitigation would help researchers to conduct cloud forensic examinations efficiently and quickly, assisting in the gathering of proof that would be

 ISSN: 2582-6433

acknowledged in the court of law.

DEFINITION OF CLOUD COMPUTING

A collective collection of adaptable computing assets (such as networks, servers, storage, apps, and services) that can be quickly provided and issued with little management or provider of services interaction is made feasible by the cloud computing model. This strategy is everywhere, feasible, and on-demand.

CHARACTERISTICS:-

There are 5 features of cloud computing. They are as follow:-

- ***Instantaneous Self-Service:-***

Despite the assistance of an internet service provider, consumers of cloud computing may utilize the services that are offered or computer resources such as processing, storage, network, and virtual machines. Subsequently that allows for obtaining the necessary services genuinely quick and easy.

- ***Wide-Ranging Network Connectivity:-***

Utilizing conventional connection protocols, cloud-based services and digital assets can be obtained from a range of gadgets, including PCs, laptops, and mobile phones, across a network.

- ***Sharing of Resources:-***

Employing a multi-tenant strategy, suppliers of cloud services aggregate their computer assets to provide connectivity to a broad range of cloud users. At execution, multiple resources are allocated according to customer demand. Customers are ignorant of the exact positions of the assets that have been allocated. Virtualizations are a technique that helps maximize the use of the tangible assets that are accessible to achieve this capability.

- ***Swift Flexibility:-***

Customers who use the cloud have the ability to swiftly change the resources that were allocated based on their needs. For example, extra storage space can be readily allocated right away if the individual using the cloud demands it.

- ***Service Measurement:-***

Measurement of service is also known as “pay-per-use”. Utilization of the provided cloud computing services is monitored. The basic unit of assessment is hours. Such feature is advantageous to cloud supplier as well as consumers.

 ISSN: 2582-6433

Models of Cloud Service

There are various models of cloud services. They are as follow:-

- ***User-friendly Software:-***

It is popularly known as Software as a Service (SaaS). With this type of service model, consumers of cloud computing can access programs managed by the cloud company that provides as a kind of service. People who use the cloud may utilize programs instantly from their web browser while installing or downloading them on their gadget. Some instances are Drop box, Face book, Gmail, and so on.

- ***Web-Based Program:-***

It is popularly known as Platform as a Service (PaaS). Such model service designs give consumers of cloud computing a platform to execute their own programming. In order to build their own software or task, people who use the cloud are not required to upgrade their computer programs or have a computer with an operating system; they may access cloud computing directly from their web browser. Some instances are Google Application Engine, Microsoft's Azure cloud platform, etc.

- ***Services for Infrastructures:-***

It is popularly known as Infrastructure as a Service (IaaS). Cloud customers can access resources such as computing power, data storage, memory, and connectivity to networks through the cloud computing paradigm. Customers have control over the cloud network according to the service provider that provides it. Some instances are Rack space as well as VMware, and Amazon Web Services and so on.

The following approaches to deployment will be utilized for setting up such service models. They are as follow:-

- ***Internal Cloud:-***

Internal cloud is also known as private cloud. An internal cloud is frequently operated and regulated by a single business or by several of them, each of which sets its own standards for connectivity, safety, and secrecy. Customers inside the enterprise which manages the internal cloud can access the provided services, increasing its adaptability and reliability. However, it comes at a substantial expense with respect to of labor and computer equipment. One can set up a internal cloud with programs like Open Stack, VMware, and Eucalyptus, etc.

- ***Community Cloud: -***

A community cloud is usually set up by a collection of institutions who are part of the same

 ISSN: 2582-6433

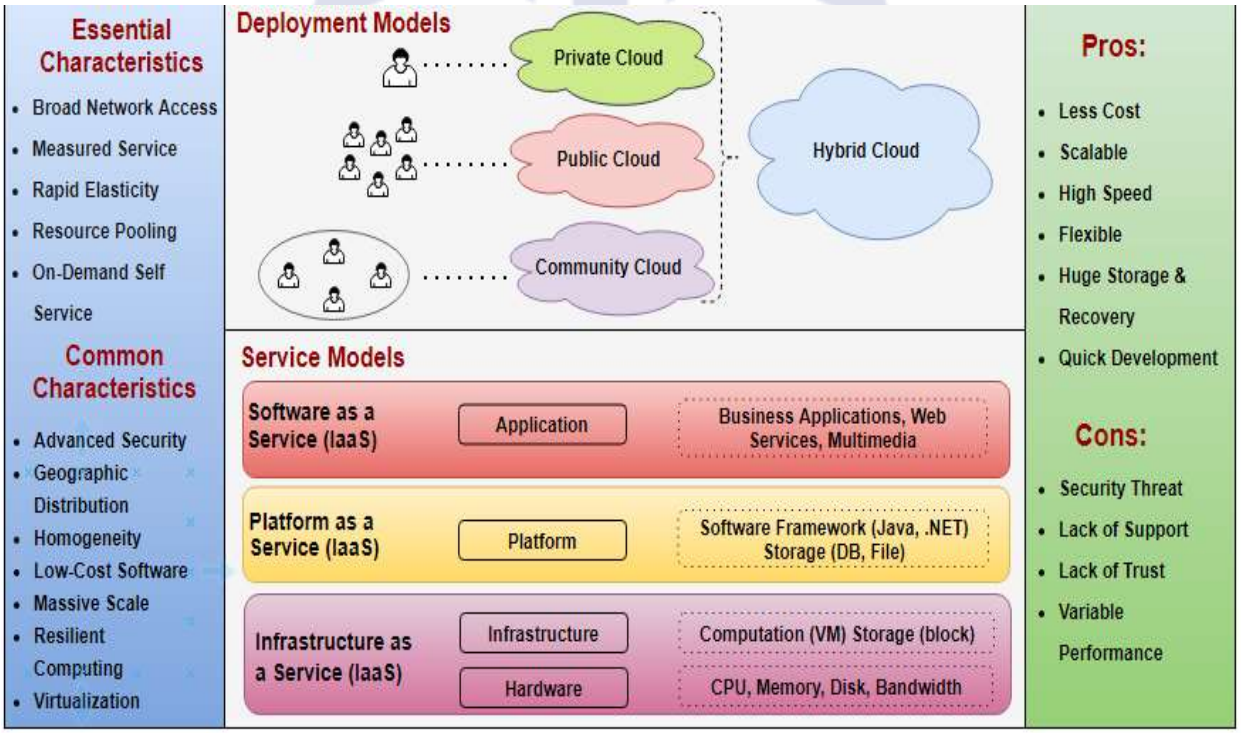
group or have similar objectives in order to utilize all of the assets. Because of their common interests, most of the consumers of the community cloud have been established on a basis of trust. When contrasted with private clouds, such an approach is economical for cloud customers and has a higher degree of confidence than public clouds. Yet rigorous safety and confidentiality rules are required for this kind of implementation paradigm. Community cloud installation can be done via public cloud providers like as Microsoft, Amazon, and so on.

- ***Open Cloud*:-**

It is popularly known as public cloud or external cloud, where facilities and amenities are provided by a third party or cloud computing supplier. To access the services and resources of an open cloud, people who use the cloud must have a service level agreement (SLA) with their provider of cloud services. In contrast to all installation strategies, open cloud computing is less economical. The main issue with this approach, though, is the shortage of confidence that exists between cloud service suppliers and cloud consumers. Amazon, Google, and Microsoft are the three most well-known open-source cloud providers.

- ***The Cloud Hybrid:-***

Hybrid clouds are created by integrating public, private, and community clouds. In addition to being more reliable than private clouds, this approach is also cheaper to operate. Cooperation between methods of deployment along with application adaptability is necessary, though. A few instances of hybrid clouds are Microsoft, Amazon Web Services, etc.



Structure of Cloud Services

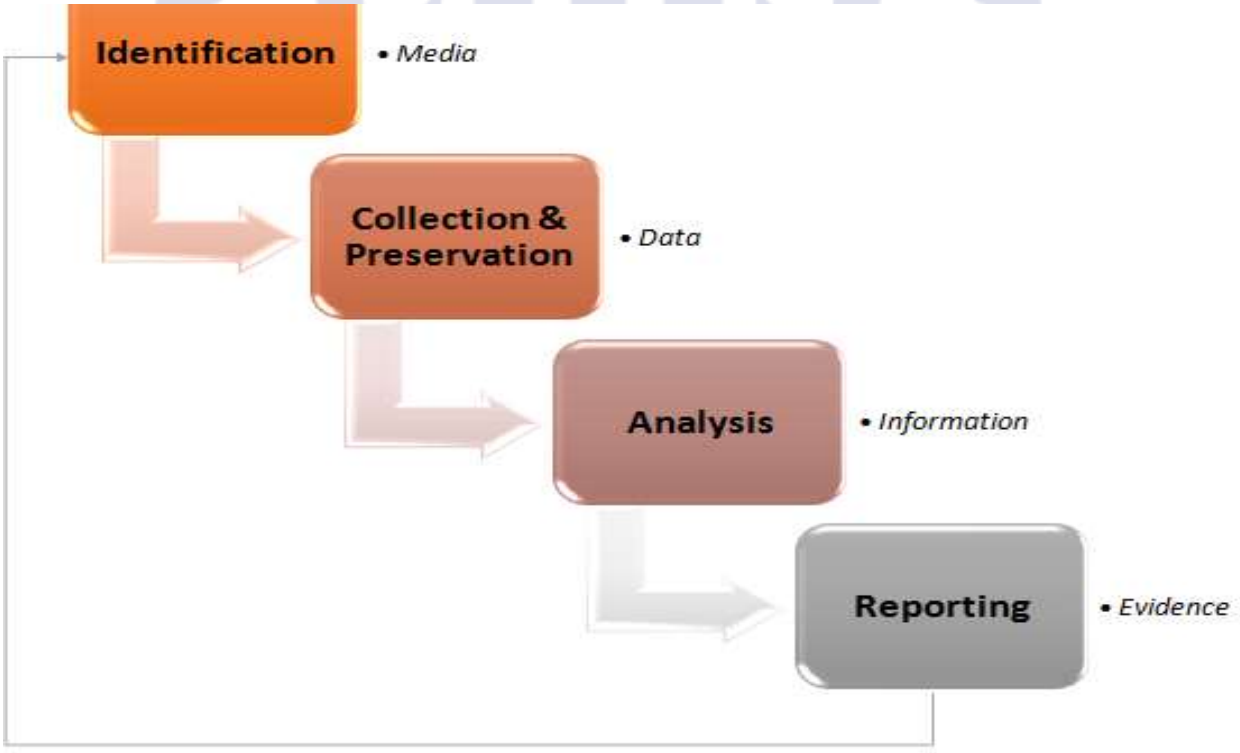
 ISSN: 2582-6433

CLOUD FORENSICS

Cloud crimes are becoming more prevalent as the amount of computing power used in instances of cloud computing rises. The distinct features of the cloud make the current online forensic techniques and instruments unsuitable for use in forensic investigations. It therefore demands a new kind of cloud-based forensic research. We describe cloud forensics in this section and go through the issues that need to be resolved before we can use digital forensics in a cloud setting. We also go over the main types of difficulties that cloud forensic investigations suffer according to the report of "The National Institute of Standards and Technology, USA."

Cloud Forensics is defined as the use of digital forensic science in systems that use cloud computing. In technical terms, it is a hybrid forensic method to the collection of electronic proof such as virtual, network, live, large-scale, customers. To facilitate both internal and external examinations, it involves collaborations among various cloud participants such as cloud service provider, cloud customers, cloud agent, cloud the carrier, cloud assessor etc. In terms of law, it frequently refers to conditions involving several tenants and territories.

Cloud Forensic is defined as technological approaches, scientific principles, and developed and tested procedures to identify, gather, preserve, examine, evaluate, and report digital evidence in order to recreate previous cloud computing.



Electronic Forensic Investigation Model

 ISSN: 2582-6433

- ***Problems associated with Cloud Forensics:-***

Several research projects have covered a range of problems and difficulties associated with cloud forensics. It was indicated in the previous part, conventional digital forensics research techniques are unable to be utilized in the cloud because of the distinct features of the cloud. The field of electronic forensics is divided into four stages: ***"identification, collection, analysis, and reporting."*** The cloud services utilized and the procedures followed to obtain access to the cloud resources determine the sources of the proof.

By technically confiscating the hardware, the origin of the proof is located in traditional disk forensic. However, since the hardware in the cloud's framework could be dispersed among many places in the world, we are unable to capture it. Since the data has been secured and gathered from many sources, it is not possible to examine and analyze the data using the forensic tools that are now available. It's possible that the obtained evidence is unreadable by the forensic instruments now from the existing technology. It's possible that the information gathered from the cloud services is not in a proper format that can be used in court of laws. Therefore, the chain of custody should be maintained during the reporting and disclosure of the cloud environment proof. The various challenges or problems in cloud forensics are as follow:-

- ***Identification: -***

The identification process will recognize the sources that are needed to gather the proof when the investigator receives a complaint about illegal usage of cloud systems from a cloud service provider or another third party. Virtual cloud instances, the network layer, client systems, etc. are possible sources of proof. Unless a virtual machine (VM) seeks for extra storage, the Cloud Service Provider (CSP) typically offers dynamic storage to Virtual Machines. The removal of forensic data from the volatile memory when the virtual machine (VM) stops is the challenging issue at this phase. Installation models influence how illicit use of cloud technologies is detected. Consumers and companies that provide services are both able to recognize this type of illegal utilization. Whether utilizing the provided services, consumers are able to recognize whether something is prohibited. Service providers must keep an eye on the cloud system to spot any unauthorized data storage, deletion, or virtual machine (VM) use.

- ***Gathering and preserving the data***

In this stage, proof is gathered through the designated origins and stored to protect against taint and manipulation of evidences. There are numerous difficulties in gathering evidence throughout the cloud forensics process. They are as follow:-

i. Large amount of data stored in cloud.
ii. The nature of data on the cloud is volatile.

 ISSN: 2582-6433

iii. Consistency of data.
iv. Restoring erased data in a computerized scenario.
v. Inability to fully scan all of the cloud's evidence for forensic purposes.

ANALYSIS:-

The analysis of cloud debris presents numerous difficulties for the researchers. They are as follow:-

i. Relation between forensic proof cloud service providers.
ii. Rebuilding the incidents using Virtual Machine pictures.
iii. Integrity of Information in Metadata.
iv. Evaluating the recording information's timeline.
v. Synchronization of time stamps.

ANTI-FORENSICS: -

Introduction of counter-forensic methods may provide significant obstacles. Some obstacles are as follow:-

i. Malware could avoid virtual machine separation.
ii. Ensuring the authenticity of the proof.

Legal Obstacles:-

There are following legal obstacles. They are as follow:-

i. Recognizing territorial concerns to obtain data lawfully.
ii. Service Level Agreements lack appropriate conditions and terms of service.
iii. Inadequate systems for worldwide collaboration and communication during the inquiry.
iv. Confiscating of cloud resources affects the other people's ability to use the identical assets.
v. Serving summons without providing the actual position of the evidence.

ROLE of MANAGEMENT:-

There are following obstructions produced in managing the shareholders. They are as follow:-

- Account proprietors' distinct identity.

 ISSN: 2582-6433

- Separation between cloud login details and real users.
- Establishing fraudulent identities and remaining anonymous are simple tasks.
- Authorization along with restricted entry.

Obstacles of Cloud Forensics.

COUNTER-FORENSICS:-

Counter forensics is also known as anti forensics. Recently, "Hidden Computing," "Art of tarnishing," or "Counter Forensics" have recently come to be considered as crucial components of Cyber Forensics Research.

According to Ryan Harris, Anti-forensics is defined as “techniques used to stop or act against the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system”. A clear and accepted definition of counter-forensics is "Any attempt to compromise the usefulness and availability of electronic proof to the forensics process" is the accepted definition of counter-forensics.

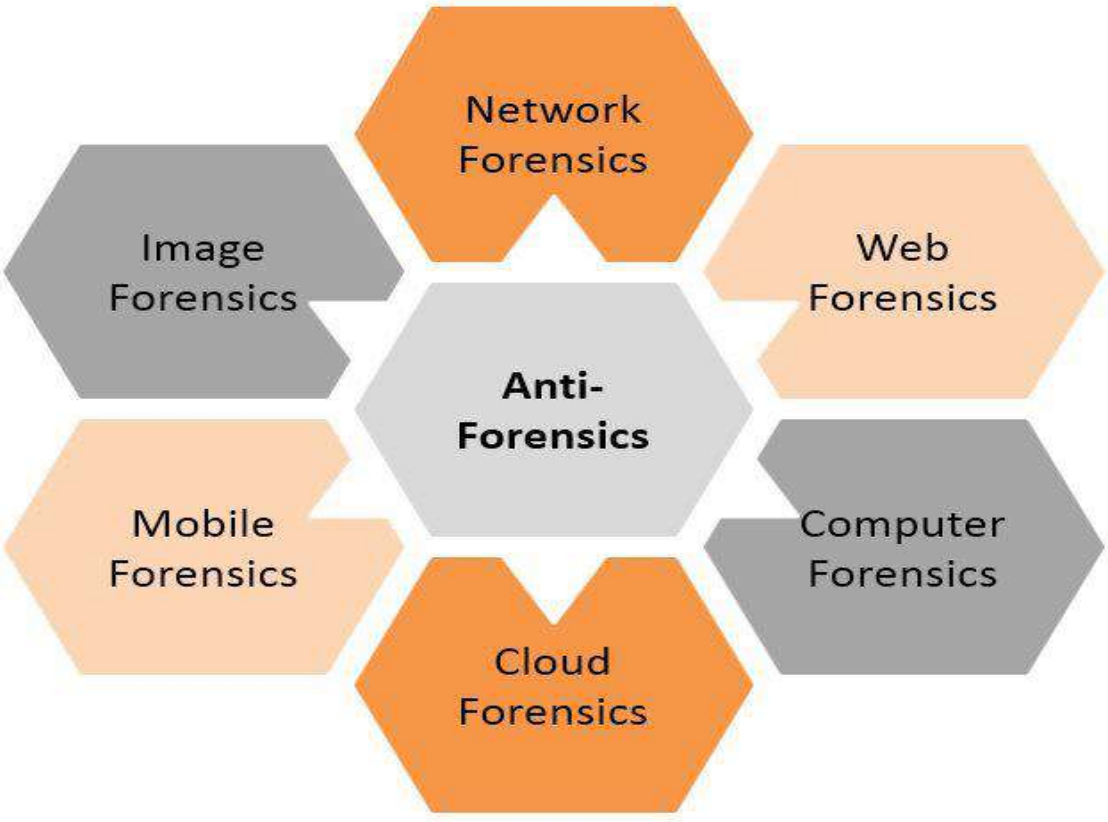
 ISSN: 2582-6433

Effect of Counter-forensics:-

A set of methods and resources known as "Counter-forensics" have the objective to disrupt forensics. The goals of the counter-forensics field are as follow:-

- Transform the proof in a way that makes it impossible to retrieve or return it to its original state.
- Stop the process of recognizing suspicious incidents through investigations.
- Obstruct the forensic investigator's efforts to gather appropriate proof from the site of the offense.
- Extend the duration of the investigations. This could irritate the law enforcement officer and cause them to give up trying to solve the crime.
- Obstruct the forensic instruments being utilized to counter an inquiry.
- Examine the reports produced during a forensic examination with suspicion. It's possible that these findings could not hold up in court.

Thus, Invasions using counter-forensics are extremely important to the forensic examination procedure as well as established and developing fields, such as clouds and smart phone computing.



Areas of Forensic Investigation

 ISSN: 2582-6433

Significance of Cloud Counter-Forensics:-

Since several companies are considering the cloud as a legitimate revenue model for computing infrastructure, several companies have moved their old infrastructure to the cloud. Even if cloud-based services have been demonstrated to be technically reliable gadgets, breaches of safety and cybercrimes continue to happen on them. For the company's financial interests, any documented event involving a breach of privacy or electronic crimes in the cloud will therefore appear to be expensive. For this purpose, numerous numbers of businesses these days strengthen their cloud safety measures. It is impossible to provide 100% privacy, yet. Digital assaults and other crimes continue to be a risk in cloud-based environments. This implies the development of an extensive and adaptable system for investigating into, evaluate, and notify about cloud crimes in order to prevent similar offenses.

Intruders attempt to obstruct the forensic examination and modify evidence in a variety of techniques. The significance of counter - forensic assaults in cloud computing lies in their ability to disrupt the efficient and effective performance of forensic examination by the perpetrator of the invasion.As a result, we must develop defenses towards counter-forensic assaults in the cloud.

Difficulties in tracking down Cloud Counter-forensic Attacks

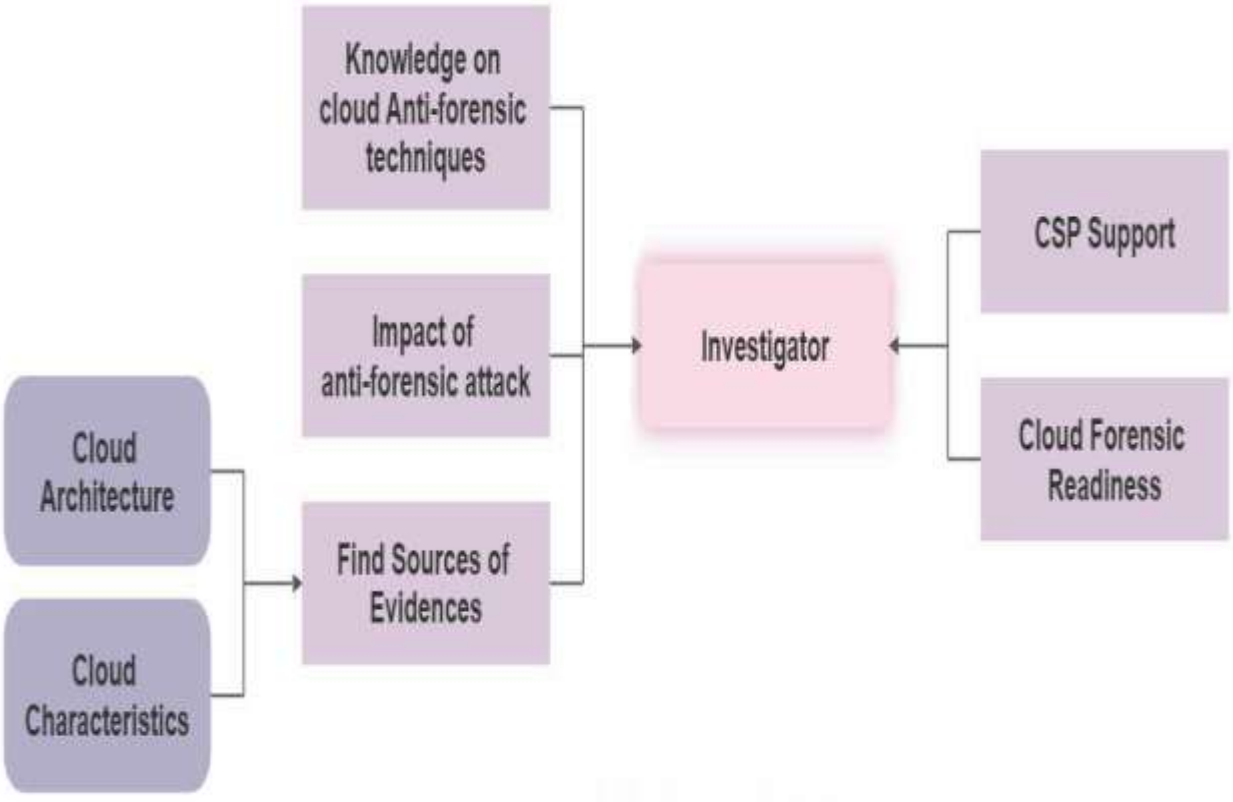
Counter-forensic assaults were formerly restricted to specific computers and networks. Researchers have found that counter-forensics in the cloud is proving to be a significant barrier for cloud forensic investigation, with the development of cloud computing as a new computational paradigm. Because cloud computing is changing, conventional invasion identification algorithms cannot be used to detect cloud counter-forensic invasions. We determined the following difficulties in identifying cloud counter-forensic invasions .They are as follow:-

- It is difficult to identify the exact place of an attack due to the cloud's design and features.
- Forensic cloud computing requires appropriate established processes and techniques as a result. Counter-forensics in cloud computing is a serious and challenging problem.
- The task is difficult to compile, evaluate, and identify the various sources of proof. Cloud service providers must grant approval for the law enforcement agency to collect

 ISSN: 2582-6433

the proof, therefore Cloud service providers (CSPs) should indicate that they are prepared and willing to assist with the inquiry.

- In order to gather evidence, forensic investigators need to be properly educated regarding various kinds of anti-forensic attacks and their range.
- In a cloud context, it is generally difficult to identify attacks; however, analyzing events records is more difficult and necessitates substantial assistance from the cloud service provider. The Service Level Agreements (SLAs) that now exist are not designed to satisfy the needs of conducting an external forensic investigation. In order to minimize the danger of diminished trust, the majority of the time, the incidence of an assault is not reported to the public with the anticipated clarity.



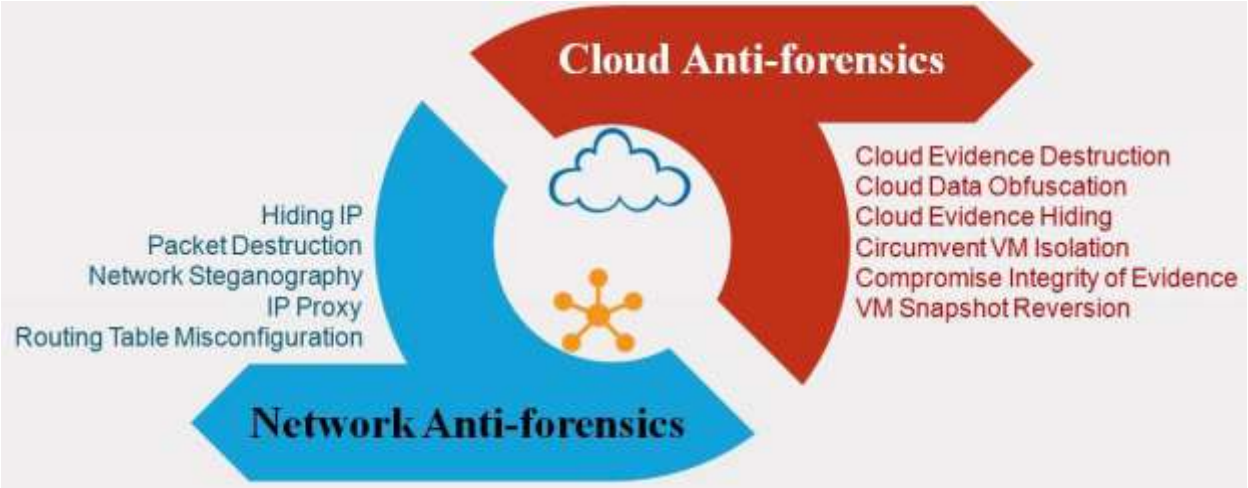
Obstacles in the identification of Cloud Counter-forensic Invasion.

Cloud Counter-forensic Invasions.

Hackers are also aware of the improved techniques for cloud forensic analysis that have been developed. People create their own methods and instruments for altering and erasing cloud data. Cloud anti-forensic assaults are those that attempt to compromise the cloud forensic investigation process itself, thus decreasing the standard and quantity of evidence.

 ISSN: 2582-6433

A significant obstacle for cloud forensics is anti-forensics. The assault target can be used to categorize anti-forensic attack scenarios." Concealing IP, Forwarding Table Incorrect configuration, IP Proxy, Network Steganography, or packet destruction, and conceals information within TCP Links and carrier folders" are the six areas into which cloud counter-forensics falls. The category is based on network counter-forensics. The primary goal of a perpetrator initiating an anti-forensic assault on a cloud computing system is to lead the forensic investigator misled while he does the forensic inquiry. Categorization of counter-forensic invasion methodologies in the context of networks and cloud computing surrounding.



Types of anti-forensic techniques in network and cloud computing

A Proposed Structure for the Investigation of Cloud-Based Forensic Invasion

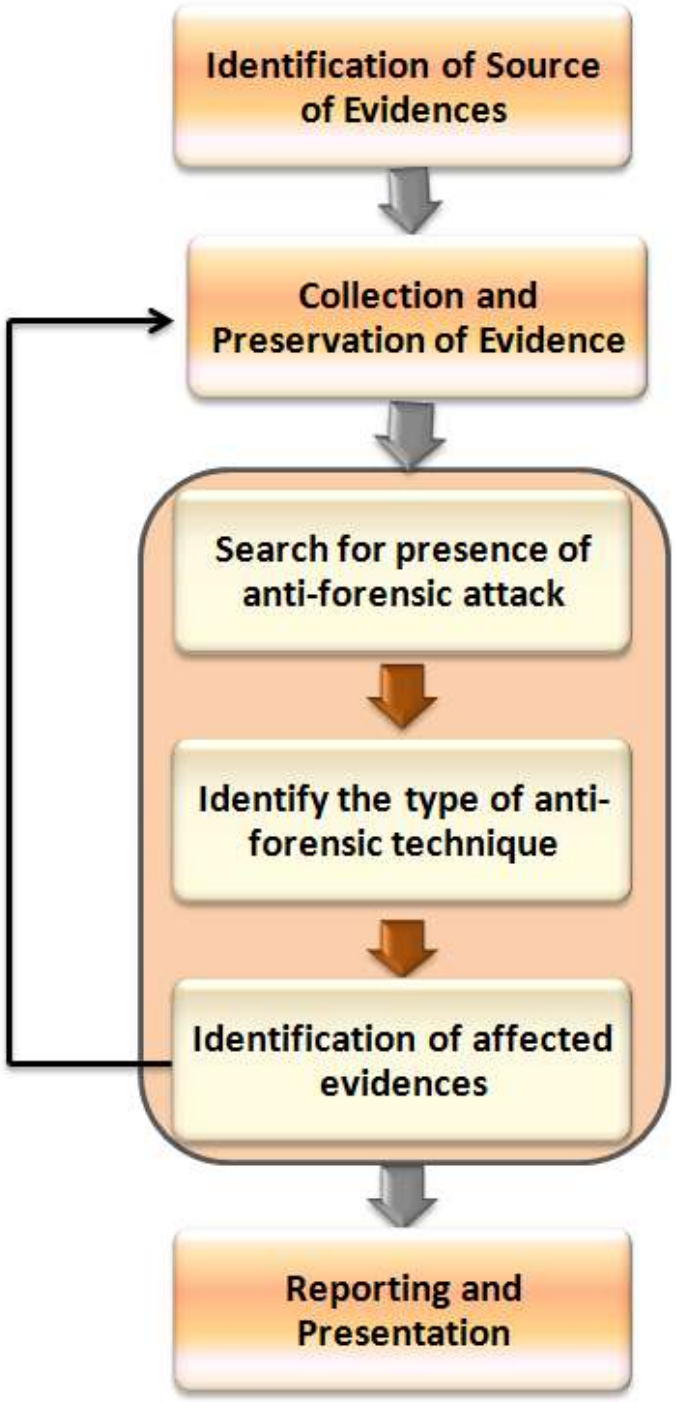
We suggest an innovative framework that can help in the process of cloud forensic examination by making it easier to identify anti-forensic attacks. The origins that provide proof are identified by the CSP/investigator upon receiving a complaint from a customer regarding the illegal utilization of cloud computing resources. The nature of the reported assault determines the type and source of proof. The gathering and storage of proof comes immediately after the origins of proof have been discovered. The proof from the virtual machine example must be segregated for effective investigation in order to avoid tampering or alteration.

Delport's research suggests that proof of authenticity can be protected by separating data collected from cloud instances. The evidence is then analyzed to determine which anti-forensic attack it was. The range of the evidence is narrowed, developed, and gathered here. The

 ISSN: 2582-6433

analysis phase in the structure we recommend is divided into three smaller stages, which include:-

- Check if an anti-forensic assault is present.
- Determining the kind of anti-forensic method and,
- Recognizing the affected pieces of proof. Following the recognition of the harmed evidence is also gathered and stored.



Structure for cloud counter-forensic invasion investigation

 ISSN: 2582-6433

Conclusions:-

The distinct features of the cloud ecosystem make cloud forensics difficult to perform. In order to determine the difficulties with cloud forensics, we carried out a thorough review of the literature. I concentrated on anti-forensics as a significant issue that can impede the process at different phases of cloud forensic examination. The primary contributions of the work are:

- Suggested different obstacles in detecting anti-forensic attacks in cloud environments and proposed classification of different types of invasions that can be launched in the cloud environment. A general paradigm for examining anti-forensic assaults in cloud computing was suggested by us.
- Concentrated on two anti-forensics problems: managing transitory proof and a broad search area. Researchers suggested a method to preserve dynamic proof to detect anti-forensics by isolating the suspicious virtual machine to the permanent storage through snapshots. Additionally, we suggested an arrangement to target virtual machines to detect dubious packages in order to narrow down the search space.
- Suggested a two-step procedure for identifying anti-forensic threats in cloud environments. In the first stage, all potential assaults in a cloud environment are recognized by destroying proof and displaying the threat vectors, which creates an anti-forensic database. To visualize the assault route, we developed a method based on attack graphs. Using the anti-forensic database, the anti-forensic attack is located in the second stage.
- Researchers suggested an innovative application of hashing to identify and prevent cloud data concealment. In order to authenticate the virtual machine (VM) removal requests, we additionally presented an authentication mechanism. We developed a method for encryption cloud proof before transferring it to the researcher in order to maintain proof authenticity.

Thus, One of the biggest obstacles to cloud forensic inquiry is cloud anti-forensics. We discussed several approaches to cloud anti-forensics in this study. As part of the cloud forensic process, we expect that the work provided in this paper will assist the cloud ecosystem in protecting its systems from anti-forensic attacks.

 ISSN: 2582-6433

REFERENCE

1. Nick Galov Cloud Adoption Statistics for 2021. URL: https:// hostingtribunal.com/blog/cloud-adoption-statistics/ (visited on 01/19/2021).
2. Steve Morgan. Cyber warfare In the C-Suite. URL: https:// cybersecurityventures.%20com/hackerpocalypse-cybercrime-report-2016/ (visited on 11/13/2020).
3. Cloisters Security in the cloud. URL: http://www.clavister.com/documents/ resources/white-papers/clavister-whp-security-in-the-cloud-gb.pdf (Visited on 05/07/2016).
4. Rounak Jain. Data leak of over 100 million debit and credit cardholders. URL: https://www.businessinsider.in/tech/news/over-100-million-debit-and-credit-card-users-data-has-been-leaked-online-from-payments-processor-juspay-amazon-and-swiggy/articleshow/80096472.cms (Visited on 04/01/2021).
5. Neeta Sharma. Digital India Sees 63.5% Increase In Cyber Crime Cases. URL: https://www.ndtv.com/india-news/digital-india-sees-63-5-increase-in-cyber-crime-cases-shows-data-2302958 (Visited on 21/09/2020).
6. Peter Mell, Tim Grance, et al. "The NIST definition of cloud computing". In: (2011).
7. Ian Foster et al. "Cloud computing and grid computing 360-degree compared". In: 2008 grid computing environments workshop 2008.
8. Luis M Vaquero et al. A break in the clouds: towards a cloud definition. 2008.
9. Keyun Ruan."Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results". In: Digital Investigation
10. NIST Cloud Computing Forensic Science Working Group et al Nist cloud computing forensic science challenges. Tech. rep. National Institute of Standards and Technology, 2014.
11. Crenshaw, A. Anti-forensics: Occult computing. 2012. URL: http://www.irongeek.com/downloads/anti-forensics-aide.pdf (Visited on 21/09/2020).
12. haxf4rall. Complete guide to anti-forensics leave no trace. 2015. URL: http://www.haxf4rall.com/2015/04/13/complete-guide-to-anti-forensics-leave-no-trace/ (Visited on 21/09/2020).