iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VI **Month of publication:** June 2024

DOI: https://doi.org/10.22214/ijraset.2024.63399

www.ijraset.com

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

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

Cloud Forensics: Challenges and Blockchain Based Solution

Anusha VC[1], Rutuja Karate[2], Prof. Hrishikesh Mogare[3]
[1, 2]PG Student,[3]Associate Professor, Dept. Of Master of Computer Application, KLS Gogte Institute of Technology, Belgaum, Karnataka

***Abstract:** As digital forensics has advanced, it has now become a crucial aspect of cloud computing. The standard process for digital forensics includes five key steps: identifying the problem, collecting relevant data, investigating the crime scene, analyzing the evidence, and documenting the case. However, performing digital forensics in the cloud presents unique challenges, especially related to security and privacy. This paper reviews different digital forensics methods, particularly focusing on cloud computing. One approach we highlight is the use of blockchain technology in cloud forensics. Blockchain's decentralized, tamper-proof ledger enhances the security and integrity of forensic evidence, ensuring reliable chain of custody and improving the credibility and admissibility of evidence in legal proceedings. Cloud forensics offers significant advantages such as large storage capacity, powerful computing abilities, and tools to identify criminal activities, which are crucial for thorough investigations. We examine the problems and challenges at each stage of the cloud forensics process and discuss how blockchain technology can provide effective solutions. Our goal is to help new researchers better understand these issues and encourage the development of new ideas to address the challenges in cloud forensics.*

***Keywords:** Cloud Forensic, Digital Forensics, Blockchain, Challenges, Solution, Implementation*

I. INTRODUCTION

The reliance on cyberspace, particularly the internet, has significantly increased in recent years. Technological advancements have given rise to new paradigms such as fog and cloud computing, with cloud computing being one of the most widely used today. Cloud computing has created numerous economic opportunities and introduced promising technologies that are now essential in modern computing. This paradigm allows for the private storage of large amounts of data and helps ensure data security over the internet.

However, investigating large-scale cloud data can be challenging if an attacker targets the cloud network. To address these challenges, a new field called digital cloud forensics has emerged. Cloud forensics combines traditional digital forensics with cloud computing, leveraging networks, digital storage devices, and computers to identify and investigate criminal activities. This integration of digital forensics with cloud technologies is known as cloud forensics [1,3].

Cloud forensics aims to identify crimes committed in the cloud and conduct investigations with minimal complexity. Over the years, various branches of digital forensics have developed, including computer forensics, network forensics, mobile device forensics, digital image forensics, digital audio forensics, and memory forensics. Traditional forensic investigation methods are often less effective due to the decentralized nature of data processing. Integrating digital forensics with cloud computing addresses these limitations but also introduces new challenges [2,7].

The investigation process in any platform typically involves several phases: identifying the problem, collecting data, examining the crime scene, analyzing the evidence, and presenting the case findings. Research indicates that implementing cloud-based digital forensics is complex, with numerous issues and challenges at each stage. These challenges include accessing logs, collecting stable data, handling vast amounts of data, recreating crime scenarios, navigating multinational laws, and presenting evidence in court [5,6].

This paper provides a detailed review of the issues and challenges in each phase of the cloud forensics process. Solutions such as maintaining logs, using separate planes for cloud data retrieval, and legislative measures are suggested [4,10].

Given the growing interest in cloud forensics, this paper aims to conduct a thorough analysis based on existing literature, presenting an analytical review of the major challenges, existing solutions, and open problems in the field. The review includes the concept of cloud digital forensics, Blockchain-based approaches in digital forensics, the issues and challenges in cloud-based forensics, and possible blockchain solutions to these problems.

Blockchain technology, known for its potential to preserve and track the chain of custody in digital forensics, enables stakeholders to create a digital ledger for documenting and storing transactions over a distributed network. This can ensure the security and privacy of digital evidence in cloud forensics [9,10].

A. *Cloud computing*

Cloud computing is a term used to describe technology, services, and applications that deliver hosted services over the internet, transforming them into a self-service utility. According to the National Institute of Standards and Technology (NIST), cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [13]. " Cloud computing services are generally divided into three main categories based on what they offer to the end user:

1) Software as a Service (SaaS): Providers host their applications on their own servers and users access these applications over the internet. Examples include file storage services, social networking platforms, and email services.
2) Platform as a Service (PaaS): Cloud providers offer a platform where users can develop, deploy, and run their own applications. The underlying hardware, network, and tools are managed by the service provider. Examples include Google App Engine, Microsoft Azure, Engine Yard, and Cloud Enabled Application Platforms (CEAP) [14].
3) Infrastructure as a Service (IaaS): Users purchase basic computing and storage resources and have control over the infrastructure, including the operating systems, software, and networks. Examples include Amazon EC2 and Rackspace Cloud Services [14].
4) Cloud services can also be categorized based on their deployment model:
5) Private Cloud: The infrastructure is used exclusively by a single organization.
6) Community Cloud: The infrastructure is shared by a specific community of organizations with common concerns.
7) Public Cloud: The infrastructure is available for public use.
8) Hybrid Cloud: This involves a combination of two or more different types of cloud infrastructures (private, community, or public).

B. *Cloud Forensic*

Cloud forensics involves the growing use of networks, digital devices for storage, and computers in identification of several criminal activities being performed in both Hi-Tech and traditional forensics [1]. The traditional digital forensics process is integrated with Cloud-based technologies which are often referred to as Cloud forensics.

In short, cloud forensics is the combination of digital forensics with cloud computing [2].

Cloud forensics is an application inside the framework of digital forensics which identifies the crimes performed on the cloud and performs the required investigation with minimum overhead and complications.

The cloud computing evolution poses several challenges and issues mostly in digital forensics and crime investigation. The investigation process for any kinds of platform includes several phases such as- identification of problem, data collection, examination of crime scenes, and analysis of the investigation and presentation of the case findings [6,8].

C. *Digital Forensic*

Digital forensics is a field within forensic science focused on using digital data (created, stored, and transmitted by computers) as evidence in investigations and legal cases. The first Digital Forensics Research Workshop in New York in 2001 defined it as: “The use of scientifically derived and proven methods to preserve, collect, validate, identify, analyze, interpret, document, and present digital evidence from digital sources to help construct events found to be criminal or to anticipate unauthorized actions that could disrupt planned operations [13].”

McKemmis defines digital forensics as the “process of identifying, preserving, analyzing, and presenting digital evidence in a way that is legally acceptable.[13]”

Digital Forensic involves main 3 Steps and first step involves the different Activities as follows:

1) Identification: Define the case and identify the evidence and incident.
2) Collection and Preservation: Gather evidence from digital devices and securely preserve it.
3) Examination and Analysis: Organize, analyze, and interpret the evidence to draw conclusions.

4) Presentation: Prepare and present a report of the findings for court.

The second step Chain of Custody tracks the collection and handling of evidence, documenting who collected it, when, and why. This ensures the evidence remains reliable for legal use.

The final Documentation step involves continuously recording details about the evidence, including where it was found and its condition. Accurate documentation is crucial for future investigations and legal cases.

Fig1: Activities involves in Digital Forensic

D. Blockchain

A block chain is a distributed ledger technique in which a plurality of peers manage and store data by mutually agreed rules. The nodes (peers) that want to manage the data participate in the P2P network and each node can verify the integrity of the block. Each peer can create a block, where the block of the first successful peer propagates to all peers, and if all the peers agree that the block is justified, the block is added to all peers. If the new block is properly created, it means that the verification of the previous block is also completed. Therefore, the longer the block length, the higher the reliability of the entire block. Verification of the integrity of a block can also verify that all past blocks are correct by comparing the hash value. However, this does not guarantee that the block is completely trustworthy, and that it has been acknowledged that it has done a lot of work proofing. Therefore, the more peers participating, the safer it is [11,12].

New blocks are created using the Proof of Work (PoW) or Proof of Stake (PoS) method. The PoW method is a task to find a hash value that satisfies a certain condition, and it is operated by adjusting the degree of difficulty for an average of 10 minutes in case of Bitcoin. The PoS method is a method for saving the cost and maintenance cost of hardware equipment and is a concept to solve the problem of PoW method in the field of cryptocurrency. Recently, cryptocurrency has been developed that combines both methods properly due to system maintenance cost and security problems. In addition, research is underway to apply not only cryptocurrency but also the fields that need to guarantee the integrity of data. For example, the blockchain based digital content distribution system, using blockchain for medical data access management, a framework for preventing double-financing[13], blockchains and smart contratcs for the Internet of Things are researched [12,13,14].

II. CLOUD FORENSICS AND CHALLENGES

Fig 2:Cloud Fornsic Challenges.

A. Identification

Determining the type of crime, software and hardware used by the suspect and possible evidence locations. In a cloud computing environment, identifying the digital forensic requirements to conduct a sound investigation is considered to be the main building block in the process of identification.

The first step in computer forensic in identification of the case and it involves two main steps as evidence and incident identification, which will be helpful to prove the incident that has happened in the case scenario. Identification is reporting of malicious activity in cloud such as illegal use of cloud for storing files, deleting files and so on.

This phase arise in cloud by the complaint made by individual, by CSP authority reporting misuse of cloud or any other. Digital evidence is both fragile and volatile in context of cloud therefore requires the attention of special personnel and methods in order to ensure that evidence data can be proper isolated and evaluated [5].

1) Access to Evidence in Logs

Logs play a vital role in an investigation. Having access to log files in order to identify an incident is the first priority for the investigators. In cloud environments where data are stored in unknown locations due to systems' distribution locating logs is a hard and painful process. The availability of system statutes and logs files is depending on the cloud service model. It is not feasible in SaaS and PaaS models due to the limited access which the client has; whereas it is partly applicable in the IaaS model as the client has access to the Virtual Machine (VM) which behaves like an actual machine. Many CSPs do not provide services to gather logs and sometimes intentionally hide the details from customers [12].

2) Volatile Data

When the power is turned off, volatile data cannot sustain. Likewise, when a VM is turned off or restarted, all the data will be lost unless the image is stored somewhere. This reflects to the loss of important evidence such as registry entries, processes and temporary internet files. volatile data that resides within the virtual environment including registry entries and temporary internet files are likely to be lost when the IaaS's customer restarts their machines. The extra storage can be utilized in data-recovery, data-safety for client and ease the data collection for investigators. For this reason, it should be globalized between CSPs in order to provide the Clients with their persistent storage. In case an adversary launches an attack on a VM with no persistent storage synchronization, when the attack is completed, the adversary can shut down the Virtual Machine instance leading to a complete loss of volatile data, if no further countermeasures are installed.

3) Dependence on CSP

CSPs are responsible for helping and assisting the investigators and the clients with all the information and evidence they can get in their cloud infrastructures. Both customers and investigators are heavily depended upon the CSP in collecting the digital evidence from cloud computing environment as they have limited control on the system. The problem arises when the CSPs are not willing to provide the information reside in their premises. In SaaS and PaaS we need to depend on the CSP to identify, preserve and collect all the evidence that could lead us to the incident. Another major issue is the CSPs dependence on third parties. CSPs sign contracts with other CSPs in order to be able to use their services. This means that the investigation has to cover all the parties involved with an immediate impact to the chain of custody.

B. Data Collection & Preservation

Data collection refers to physical acquisition of forensic data. Any digital forensic procedure consists of physically taking the custody of hard disk being investigated and then taking bitwise copy of same maintaining the integrity of data. But in case of cloud this is impossible. Physical seizure is difficult and dependent step in cloud. The investigator has to contact CSP for physical acquisition of data which is distributed among many data centers. According to data collection phase of cloud forensics should also consider the storage capacity for collecting evidence. The amount of data for evidence would be large due to distributed and wide nature of cloud. The author suggests collecting the evidence a separate cloud can be used because data would be very large. Another issue in evidence collection and preservation is chain of custody which is nothing but a path that shows how evidence was collected and preserved and analyzed. Due to remote nature of cloud this property again violates the digital forensic rule [9].

1) *Data Integrity:* One of the main issues faced by investigators in cloud based cases is the data preservation. Data integrity is a critical component of the forensic process. It is crucial that the original evidence is not changed at all. The integrity preservation and the stability of the evidence is essential in cloud investigation for IaaS, PaaS and SaaS. We must preserve data in our effort to acquire evidence in multi-jurisdiction environments, a difficult task to deal with, without violaany law. If the integrity is not preserved (could be compromised by the CSP or the hypervisor then the evidence will not be admissible to the court of law. Finally, it is difficult to maintain the stability of the data because of the transient nature and dedicated description of the data in a Cloud. It is a challenging task to prove the integrity of cloud-based evidence to the court in an admissible manner. For example, if the client was involved with the malicious activities, she can claim that her authentication credentials were stolen and might be misused by somebody else. Yet, it is difficult to evaluate the authenticity of that claim.
2) *Time Synchronization:* The synchronization of time (Stamps) are very important as it can be used as a source of evidence. Nevertheless, the date and time stamps of the data are questionable when they are from multiple systems. Moreover, the difference in time zones between cloud servers and cloud clients can affect the integrity, reliability and admissibility of evidence. In all three service models the time concerning data is also crucial and requires hard work to come with the correct results. This is due to the fact that data are stored in multiple geographical regions with different time zones. Investigators need to gather all the time stamps from the devices and establish an accurate time line of events. Currently, the cloud infrastructure is a strongly dependent on whether the VM guest OS are using a network protocol to synchronize with a network time server.
3) *Privacy:* The virtualization of the systems in IaaS and multi-jurisdiction affect the privacy of the clients. Investigators must ensure that all regulations and standards are retained in order to collect the evidence without breaching clients' privacy. CSPs also must find a mechanism to ensure clients that their information will not be accessed by any member of the staff even if they have been deleted.
4) *Chain of Custody:* For conventional forensic process, chain of custody can be defined as "a roadmap that shows how evidence was collected, analyzed and preserved in order to be presented as evidence in court". The most important thing to present evidence in a court of law is to make sure that the chain of custody of the evidence is maintained throughout the investigation. Any interruption in the chain of custody will be a problem and the evidence will be questionable. The chain of custody has to illustrate how the evidence was collected, analyzed and preserved at the aim of presenting the evidence in admissible way at the court of law. Imagine an investigation where the CSP has to submit data to the investigators. The personnel responsible for collecting the data are not trained to preserve evidence according to specific forensic techniques. In this case the chain of custody will not be maintained. For a case to stand in court the investigators have to ensure that the chain of custody should contain information such as, who collected the evidence, how and where the evidence was collected, how the evidence was stored, who accessed the evidence, etc.
5) *Multi-jurisdiction:* To acquire evidence from the three models in cloud from different jurisdictions is another issue for the investigators. Due to cloud characteristics system's data are usually spread in places around the globe. Thus, it is very difficult, almost impossible, to conduct evidence acquisition when investigators are dealt with different legal systems, where the related laws or regulations may vary by countries [15]. Any evidence retrieval must be according to the laws and privacy policies of the specific jurisdiction where forensic investigation took place in order to maintain the chain of custody. Otherwise, the evidence cannot stand in a court of law.
6) *Multi-tenancy:* In cloud environments where IaaS and PaaS services are used, customers share the same storage in VMs. This has an immediate effect on the investigation. Evidence retrieval in multi-tenant environments must maintain the confidentiality, preserve the privacy of the tenants and finally ensure that the data to be collected concern specific tenant and no other. Due to the multi-tenancy the data can be contaminated by people who have access into the same storage unit with result of losing important evidence.

C. Analysis& Examination

Analysis: Organizing the evidence and it involves analysis of the devices for evidence as digital clues. The investigator interprets and correlates the data to know the fact and draw conclusion whether the evidence is proved or not. This phase consists of analysis of logs collected from different layers of cloud. In context of cloud this phase has significant challenges. First is the decentralized log mechanism which is spread over multiple tiers of cloud. The logs are located over different servers at different data center location. Again the logs are sometimes volatile in nature due to virtualization property of cloud.

Examination: Organizing the evidence involves examination of the devices for evidence as digital clues. The investigator extracts the information for examination of the case and inspects the extracted data and their characteristic. Studying the collected data and its attributes. Current computer forensics practices examine well-structured storage e.g., hard disks; however, in cloud computing a significant proportion of the target data may be held in memory/network dumps and/or log files [6].

1) *Lack of Forensics Tools:* Data analysis in cloud environments requires appropriate forensic tools. Many of the tools used for a cloud investigation, have been designed and introduced for digital forensic investigations. With the systems distributed all over the world and with no physical access to the computer devices, these kinds of tools cannot fully cover the investigations in IaaS, PaaS and SaaS models. New software tools must be developed to assist in the preservation – collection stage acquiring data more efficient and new certified tools must be produced to help the investigators in data examination and analysis. It is a common understanding that the available forensics tools have various limitations and cannot cope up with the distributed and elastic characteristic of the cloud computing. Also, there is a high level of demand upon forensic-aware tools for the CSP and the clients to conduct forensics investigation in cloud environment. Hence, it is crucial to develop tools which can be utilized to identify, collect and analyze cloud forensics data. A combination of computer forensics and network forensics tools is needed at aiming of acquiring forensics data and then analyzing them in a timely fashion. Encryption: Encryption is done by and large generally utilized by cloud client as a measure of securing the information, or to fulfil legitimate and consistence prerequisites. In any case, culprits can likewise utilize encryption for unlawful reason. pointed out the wide spread usage of encryption by criminals to hide illegal images. Many cloud customers in all three service models store their data in an encrypted format to protect them from criminal activities. When an investigation is conducted the encrypted data will not be useful once the encryption keys cannot be acquired. The evidence also can be compromised if the owner of the data is the only one who can provide the key, or if the key is destroyed. Furthermore, many CSPs are using encryption methods to store clients' data in the cloud.
2) *Crime Scene Reconstruction:* It is crucial to reconstruct the crime scene in order to understand how illegal activities were committed. Unfortunately, this could be a problem in the cloud environment. In cloud environments where data are spread across different regions and countries with time differences, to reconstruct the crime scene and place the facts in a logical order might be a difficult work. On the other hand, if a VM instance is forced to shut down, all data and potential evidence will be lost and the reconstruction phase cannot be executed. In traditional digital forensics, the investigator can identify the number of devices used in the crime or the people involved in the crime easily. The cloud context, however, implies real-time and autonomous interaction between various nodes, which makes it almost impossible to reconstruct the crime scene and to identify the scope of the damage, due to the highly dynamic nature of the communication.
   However, regeneration event can be used where a snapshot is done due to occurrence of every attack.

D. Presentation

Finally, the investigator prepares the reports from the findings about the findings of the investigation and makes it appropriate enough with evidence to finally present it to the court. Presentation is the phase of presenting data in front of jury as evidence for crime provenance. Due black box and abstract nature of cloud the jury member is unable to understand the validity of evidence in cloud. The findings will be presented to either the management of an organization or a court of law [10].

1) *Complexity of Testimony:* In a court of law where the jury (often) consists of people with only the basic knowledge in computer systems, the investigators must be ready to deal with this situation. They have to be prepared to give a clear and simple understanding on the terms of cloud computing, cloud forensics and how they work and explain how the evidence acquired preserved and documented during the investigation. This is an important issue towards the progress of the trial.
2) *Documentation:* Another challenge is to persuade the jury that the evidence acquired during the investigation has been documented properly and there had been no changes to the evidence in the previous stages. Investigators must ensure that all parties have been involved in the investigation, followed methods and principles in order to maintain the chain of custody of the evidence that has been collected. Documentation of digital evidence concerns all stages.

III. BLOCKCHAIN BASED SOLUTION

Blockchain technology has become a revolutionary tool for enhancing security and privacy in various fields such as eHealth, IoT, industries, and voting. It operates as a decentralized, shared, and tamper-proof ledger on a peer-to-peer network.

Initially popularized by Bitcoin, blockchain records transactions in blocks, which are then verified through a process called Proof of Work. Incorporating blockchain into Digital Forensics and Incident Response (DFIR) can significantly improve the credibility and admissibility of evidence by maintaining an immutable chain of custody [10].

A. Blockchain-Based Forensic Solutions

1) Data Storage and Integrity Management

A proposed framework uses blockchain to store evidence securely and manage data integrity, comparing its efficiency with existing cryptocurrencies. Simulation and TPS (transactions per second) calculations using Hyperledger are suggested for future improvements.

2) Digital Evidence Processing with IoT:

A system integrating blockchain with IoT forensics enhances the credibility, legitimacy, and non-repudiation of evidence. It includes cryptographic solutions to address identity privacy concerns and employs smart contracts for various forensic transactions. Future work includes testing the system in a diverse IoT environment.

3) IoT Forensic Chain (IoTFC):

This platform provides proof of presence and privacy for forensic investigations, ensuring traceability and auditability of evidence. IoT devices submit evidence to the blockchain, documenting the origin, storage, examination, and presentation of the evidence.

4) IaaS Cloud Blockchain Technology

This approach solves centralized evidence collection issues by distributing evidence across multiple peers in the blockchain. It includes advanced security measures like Secure Ring Verification based Authentication (SRVA), Sensitivity Aware Deep Elliptic Curve Cryptography (SA-DECC), and Secure Hashing Algorithm-3 (SHA-3). The system allows users to track their data through Fuzzy based Smart Contracts (FCS) and constructs Logical Proof Graphs (LGoE) for evidence analysis.

5) Log Protection and Auditing

Maintaining the confidentiality of log files is crucial for incident monitoring. A public model using a third-party auditor verifies the accuracy of cloud logs without revealing log content. The system aggregates log block tags using a Merkle hash tree, storing the root node on the blockchain to prevent tampering. This method reduces computational costs and enhances the security audit of cloud logs.

Blockchain technology offers significant advantages for cloud forensics by providing a secure, transparent, and immutable way to handle digital evidence. These benefits make blockchain-based solutions far superior to traditional methods, ensuring that digital evidence remains credible, verifiable, and tamper-proof throughout the forensic process.

Blockchain technology offers significant advantages for cloud forensics by providing a secure, transparent, and immutable way to handle digital evidence. These benefits make blockchain-based solutions far superior to traditional methods, ensuring that digital evidence remains credible, verifiable, and tamper-proof throughout the forensic process.

B. Tools For Cloud Forensics

FROST is a forensics tool for the OpenStack cloud computing platform. This tool acquires data from API logs, virtual disks and guest firewall logs in order to carry out the digital forensic investigation. FROST provides Infrastructure-as-aService (IaaS) cloud. This tool stores the log data in Hash trees and returns it in Cryptographic form. It works at the cloud management plane and hence does not need to interact with the operating system inside the guest virtual machines. Therefore no trust is needed in these machines. The FROST tools are user driven so no interaction of the forensic examiners and customers with the Cloud service providers are needed for law enforcement. The latest features of these tools allow forensic experts to extract the required forensic data from the OpenStack cloud without the provider's interaction. The outline has an extensible arrangement of scientific goals, including the future expansion of other information safeguarding methods, revelation techniques, checking procedures, measurements and reviewing abilities [11].

Hence, clients of open cloud administrations do not require the help of their cloud supplier for any forensic examination.

Law authorization depends on the bulky and tedious court order procedure to acquire cloud information, and requires the cloud supplier to execute every inquiry in the interest of the requester. In [11] it has been reasoned that the administration plane is an alluring answer for client driven scientific abilities since it gives access to criminological information without expecting to believe the visitor virtual machine (VM) or the hypervisor, and without requiring help from the cloud supplier. Putting away and getting reliable proof from anoutsider supplier is non-paltry.

Its commitments are-

1) Description of the engineering, outline objectives, and execution of client driven measurable obtaining of API logs, virtual disks, and firewall logs from the administration plane of Open Stack.

2) A calculation for putting away and recovering log information with uprightness in a hash tree that coherently isolates the information of every cloud client in his or her own particular sub tree.

3) Evaluation results demonstrating that the proposed arrangement fulfills mechanical and lawful prerequisites for acknowledgment in court and scales properly for a cloud environment.

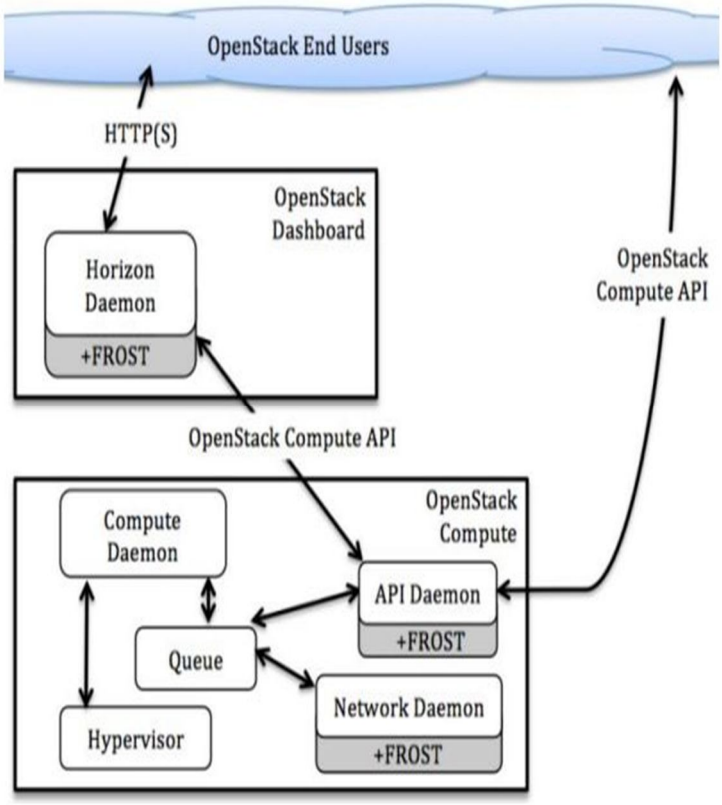


Fig. 3: Open Stack architecture showing where Open Stack Compute (Nova) and Open Stack Dashboard (Horizon) have been modified to add FROST [11].

So we can say that FROST suite for OpenStack is a collection of forensic tools which is integrated into the management plane of a cloud architecture. These tools can be used by law enforcement, cloud consumers, law enforcement and forensic investigators for acquiring trustworthy forensic data independent of the cloud provider. This tool can also be used for metrics, real-time monitoring or auditing. User accessible concrete capabilities are offered by FROST. While numerous organizations are still reluctant to embrace cloud arrangements in light of security concerns, FROST arms them with capable and quick reaction capacities. All commercial cloud services should be using these types of tools so that the cloud forensic problems can be solved.

IV. PROPOSED SOLUTION IMPLEMENTATION

Blockchain technology can address several challenges in cloud forensics by providing a secure, transparent, and immutable way to track and verify digital evidence. Here is a real example where blockchain technology is applied to solve cloud forensic challenges:

Example: Guardtime's Blockchain-Based Integrity Solutions for Cloud Forensics

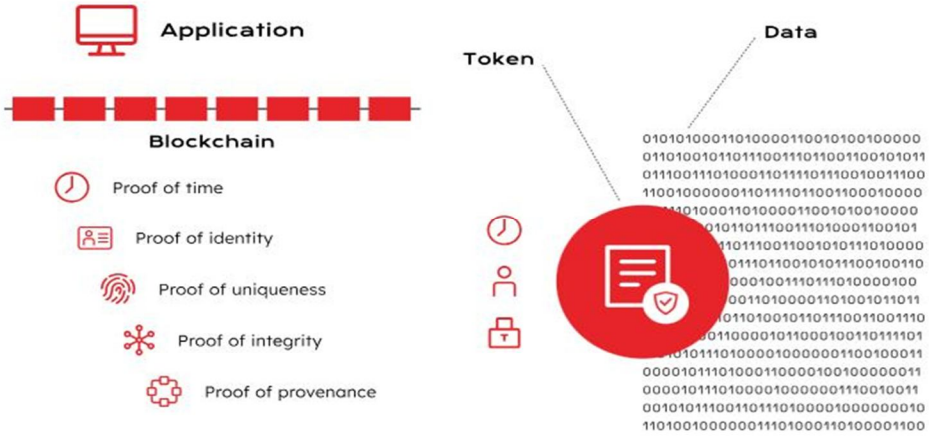


Fig 4: Guardtime's Blockchain-Based Integrity Solutions for Cloud Forensics

Company Overview: Guardtime, an Estonia-based company, provides blockchain-based solutions to ensure data integrity and security. Their technology is used in various sectors, including government, healthcare, and cybersecurity.
Challenges Faced by Guardtime in Cloud Forensics and Blockchain-Based Solutions:

A. Challenges

1) Data Timestamping and Integrity:

Solution: Guardtime's KSI blockchain timestamps and cryptographically hashes every piece of data, such as log entries or files. These hashes are aggregated and anchored in the KSI blockchain.
Benefit: This creates a tamper-evident record, ensuring the integrity and authenticity of the data. Any alteration attempts would change the hash value, which would no longer match the hash stored in the blockchain.

2) Tamper-Evidence and Verification:

Solution: The KSI blockchain enables investigators to verify the integrity of the data by comparing its hash to the blockchain record.
Benefit: This ensures that the data has not been tampered with since it was recorded. Any discrepancies in the hash values would indicate potential tampering.

3) Immutable Audit Trail:

Solution: The blockchain creates an immutable audit trail of all digital events and data.
Benefit: Forensic investigators can use this audit trail to track the history of digital evidence, proving the chain of custody and authenticity of the data, which is critical for legal proceedings.

4) Compliance and Reporting:

Solution: Organizations can log all relevant events and activities in the KSI blockchain.
Benefit: This provides a verifiable and immutable record, helping organizations demonstrate compliance with regulatory requirements and enhancing transparency.

5) Data Provenance:

Solution: The blockchain tracks and verifies the provenance of digital assets, including their origin and any modifications.
Benefit: This ensures a comprehensive and tamper-proof history of data changes, allowing investigators to establish the authenticity and integrity of the digital evidence.

B. Real-World Deployment Examples:

1) Estonian Government: The government uses Guardtime's KSI blockchain to secure its digital services, ensuring the integrity of records and logs in its e-government systems.

2) Healthcare: Guardtime's technology protects patient records, ensuring they remain untampered and providing a reliable source of data for forensic investigations if needed.

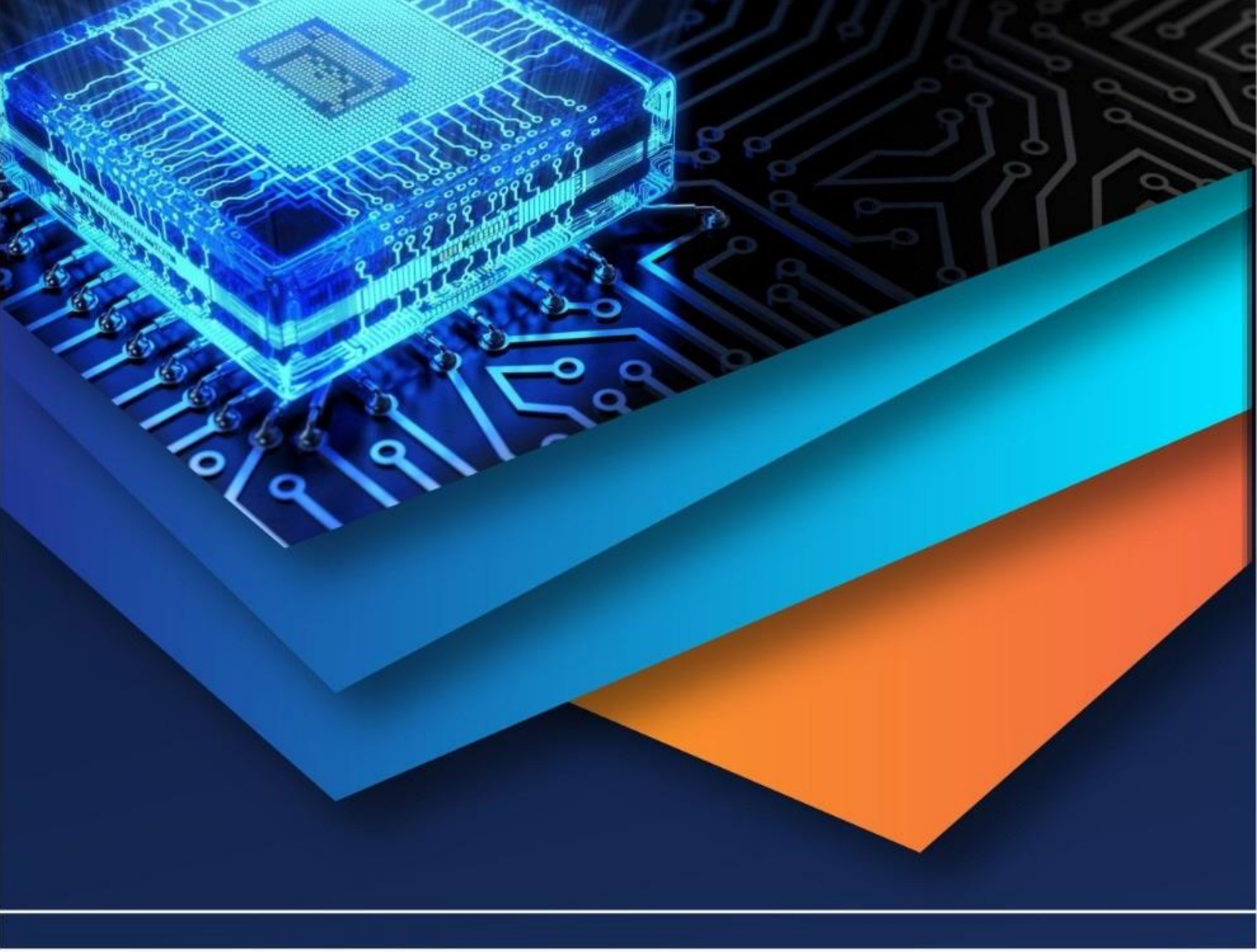
By using blockchain technology, Guardtime addresses key challenges in cloud forensics, such as ensuring data integrity, maintaining an immutable audit trail, and verifying the authenticity of digital evidence. This real-world application demonstrates the practical benefits of integrating blockchain into forensic investigations in cloud environments.

V. CONCLUSION

Forensic investigators are facing huge challenges to cope with the criminal activities, which were not as complex in traditional forensic approach as the cloud, due to its complex structure. The paper identified the challenges in cloud forensic and the cutting edge solutions to counter these challenges found on the literature have been discussed. Given the growing interest in cloud forensics, this paper aims to conduct a thorough analysis based on existing literature, presenting an analytical review of the major challenges, existing solutions, and open problems in the field. The review includes the concept of cloud digital forensics, IoT-based approaches in digital forensics, the issues and challenges in cloud-based forensics, and possible blockchain solutions to these problems.

REFERENCES

[1] Cloud forensics: identifying the major issues and challenges S Simou, C Kalloniatis, E Kavakli, S Gritzalis Advanced Information Systems Engineering: 26th International Conference, CAiSE …, 2014
[2] Cloud forensics: a review of challenges, solutions and open problems S Alqahtany, N Clarke, S Furnell, C Reich 2015 international conference on cloud computing (ICCC), 2015
[3] Technical challenges of cloud forensics and suggested solutions MY Arafat, B Mondal, S Rani Int. J. Sci. Eng. Res, 2017
[4] PDF] Block chain based data logging and integrity management system for cloud forensics JH Park, JY Park, EN Huh Computer Science & Information Technology, 2017
[5] Simou, S., Kalloniatis, C., Kavakli, E., Gritzalis, S. (2014). Cloud Forensics: Identifying the Major Issues and Challenges. In: Jarke, M., et al. Advanced Information Systems Engineering. CAiSE 2014. Lecture Notes in Computer Science, vol 8484. Springer, Cham. https://doi.org/10.1007/978-3-319-07881-6_19
[6] A survey on cloud forensics challenges and solutions S Simou, C Kalloniatis, S Gritzalis, H Mouratidis Security and Communication Networks, 2016•Wiley Online Library
[7] Cloud forensics issues and opportunities A Aminnezhad, A Dehghantanha, MT Abdullah, M Damshenas International Journal of Information Processing and Management, 2013•academia.edu
[8] Cloud forensics solutions: A review S Simou, C Kalloniatis, E Kavakli, S Gritzalis Advanced Information Systems Engineering Workshops: CAiSE 2014 International …, 2014•Springer
[9] Cloud forensics: a review of challenges, solutions and open problems S Alqahtany, N Clarke, S Furnell, C Reich 2015 international conference on cloud computing (ICCC), 2015•ieeexplore.ieee.org
[10] Could block chain technology help resolve the cloud forensic problem? Y Zhao, B Duncan - Cloud Computing, 2018 - researchgate.net
[11] A blockchain-based process provenance for cloud forensics Y Zhang, S Wu, B Jin, J Du 2017 3rd IEEE international conference on computer and …, 2017•ieeexplore.ieee.org
[12] Block chain based data logging and integrity management system for cloud forensics JH Park, JY Park, EN Huh - Computer Science & Information Technology, 2017 - csitcp.net
[13] Cloud forensics: identifying the major issues and challenges S Simou, C Kalloniatis, E Kavakli, S Gritzalis Advanced Information Systems Engineering: 26th International Conference, CAiSE …, 2014•Springer
[14] Cloud forensics: issues and challenges JJ Shah, LG Malik 2013 6th International Conference on Emerging Trends in …, 2013•ieeexplore.ieee.org



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY