Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Beyond Traditional Techniques for Enhancement of Digital Forensics for Cloud

Osama Farooq[1]
Department of Computer Science, FAST NUCES, Lahore, Pakistan
l200913@lhr.nu.edu.pk
Khawaja Qasim Maqbool[2]
Department of Computer Science Bahria University Lahore Campus
qasim@bahria.edu.pk
Muhammad Zunnurain Hussain[3*]
Department of Computer Science Bahria University Lahore Campus
Corresponding Author Email: zunnurain.bulc@bahria.edu.pk
Muhammad Zulkifl Hasan[4]
Department of Computer Science, Faculty of Information Technology, University of Central Punjab Lahore Pakistan
Zulkifl.hasan@ucp.edu.pk
Hiba Batool[5]
Department of Computer Science, FAST NUCES, Lahore, Pakistan
l201096@lhr.nu.edu.pk
Fatima Usman[6]
Department of Computer Science, FAST NUCES, Lahore, Pakistan
l21205@lhr.nu.edu.pk

Abstract

In the recent years, cloud computing has stepped into the shoes of the conventional IT, featuring scalability, flexibility, and cost-effectiveness among others. Despite the distributed nature of cloud infrastructure and the dynamic allocation of virtual resources though, these present unique challenges to the investigators looking to collect and preserve the evidence. The following article

Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

deals with the gaps and difficulties in cloud forensics by creating a solution through effective digital forensic while integrating robust chain of custody procedures. The proposed solution combines a broad literature review, the examination of actual cloud data, and the developing of unique forensic techniques particularly suitable for cloud networks. This research utilizes various methods which include implements of dynamic evidence collection, cloud-specific artifact analysis, and machine learning techniques that are designed to enhance cloud forensic investigations with regard to effectiveness and efficiency. Besides that, the article illustrates the key facet of standardized frameworks and applying legal and regulatory requirements for digital evidence admissibility in the court. Such a collaboration can be achieved through joint research projects, knowledge sharing, and making progress in forensic methods consistently, so that the cloud will be less susceptible to security breaches.

Keywords: Cloud Forensics; Evidence Analysis; Forensics, Tool; Cloud Computing

Introduction

The dawn of cloud computing has marked the emergence of a completely different era in the domain of technology, transforming the way those in and outside the organizations use the computing resources. Cloud services provide a very broad range of benefits from instant scalability of resources, in line with the demand, to big cost saving as a comparison to conventional in-house infrastructure. Even though the cloud migration could simplify the digital forensics investigations, it presents a vast range of issues as well. Traditional forensics techniques are often designed to analyse physical machines and centralized storage systems, making them

Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

the most suitable for such devices. However, these methods may not be effective in their original form in the cloud due to differences in architecture, resource virtualization, and data distribution. The Highly Dispersed Characteristics of Cloud Environment, Where the Data is Scattered Across the Geographically Separated Data Centres, Make the Use of the Traditional Methods for Evidence Acquisition and Preservation Both Hard and Ineffective.

To increase the effectiveness of cloud forensics, we need to set out toward a dedicated effort in permanent research and development to stay in step with the changing landscape of cloud technologies. It is due to the fact that it is dynamic and keeps changing that the biotechnology develops almost at the same pace as the rapid changes. Digital forensic experts, who are well equipped with these innovative solutions, can weave their way through the diverse data storage and dynamic virtual environment challenges that can sometimes pose a challenge to them. Therefore, interdepartmental cooperation is very necessary in a way that the incorporation of cyber security and legal aspects leads to the establishment of unified frameworks that give most consideration to transparency, accountability and data integrity in cloud forensic investigations. Rather than being reactive to the cloud computing era, the approach involving standardization will allow the process to be simplified, but also the evidential process to be acceptable and reliable.

When more and more companies are getting on the cloud plane, the necessity for reliable and efficient cloud forensics solutions is more substantial than ever. Global cloud service expenditures are poised to reach $397.4 billion by Gartner's

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

reckoning by the end of 2022, mirroring robust growth in clouds' usage in many industries. Therefore, this climax in cloud adoption leads to a comprehension of the fact of deployment of robust forensic methodologies suitable for cloud environment. On the other hand, despite the remarkable progress that cloud computing has been making, issues of cloud forensics are quite fragmented and remain mostly unexplored, confronted with difficulties and ambiguity.

The later part of this article will be designed as follows. The 2nd section of this paper is a critical literature review on cloud forensics and it reveals widespread gaps and inadequacies which are serious enough that remedy should be found by applying innovative solutions. Investigative efforts, mostly, have centred on the retro fitting of existing forensic techniques to work in the cloud environment, sometimes disregarding the unique intricacies, including those that have a bearing on cloud infrastructure. A second issue is the absence of recognized frameworks for forensic analyses, which limit the reliability of investigations in cloud environments. In order to plug in these lacunae, cloud-centric forensic paradigm has to be built, where the tools and methodologies are designed to serve the needs of the cloud based computing environments, which are inherently distributed and dynamic.

This research recommendation section 3 is for the implementation of the mixed strategy that includes a combination of the progress of the digital forensic methods and the standardization of cloud forensic approaches. In order to profit from data collated through a comprehensive literature review and empirical analysis, unique techniques for forensic procedures

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

specialized in the cloud environment are crafted. These techniques utilize a variety of sources of dynamic evidence, specific artifacts from the cloud and machine learning in order to increase the effectiveness and exploitability of cloud forensic analysis. However, the promotion of standardized frameworks and adherence to legal requirements and regulations is a fundamental component that ensures the authenticity and acceptability of digital evidence as proof in court.

In Section 4, how the proposed solution about working is confirmed by using powerful data analysis and visualization techniques is elaborated. Real world datasets are scoured to learn these relationships which are important to cloud forensics, and these layers of knowledge inform the development and increase the accuracy of forensic methodologies. Graphic presentations illustrate the complexity of cloud circulations and make it easier to understand the forensic difficulties and the efficiency of the potential mitigation approaches.

Lastly, Section 5 of the paper concludes that the development of cloud forensics requires collaborated effort to meet its inherent issues on the way to form a more effective and resilient forensic system Utilizing the cutting edge approaches, building cooperation among the parties concerned, and campaigning for the regularization are the practices that can further improve the soundness and the impact of cloud forensic research. Future research initiatives should focus on new technology development and new threats together with the rapid shift of the forensics landscape to stay relevant and effective as cloud forensics logically-minded tools in defending digital assets and ensure the rule of law.

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Thus, cloud forensics has the potential to evolve into the type of field that meets the requirements of the current digital world, ensuring data integrity and easing justice in the growing-digital border.

Literature Review

Through cloud computing, information technology has been completely reimagined, and it has provided with unmatched advantages namely, on-demand scalability, flexible resource allocation, and much cheaper infrastructure than which used to be available running on the premises. Though the shift to the cloud platform brings up new issues for digital forensic investigations, it also opens up new ways for law enforcement agencies to gather evidence. Forensic methods of standard techniques that are very meticulous and have been made to fit machines and local storage systems might not easily transition to the cloud, due to the architectural differences, data virtualization, and data distribution that are built into the cloud. Moreover, the distributed design of cloud computing is different from the normal forensic methodologies in the traditional sense, as it has data spreading over multiple data centres in a “space-dispersed” way, which may lead to drastic increase of difficulties associated with the acquiring and preserving of evidence using conventional forensic methodologies, which may have rendered them ineffective and inappropriate for the cloud computing.

This literature review endeavours to explore the complex obstacles and exclusions in cloud forensics and afterwards to point out the research gaps already covered and to prospect the future research route. However, this exponential growth has not created a mature body of knowledge about forensics in the cloud since there

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

are almost no uniform approaches or special niche tools that are designed for the cloud-based environments. Traditional forensic capacities have been mostly applied to change them in accordance with the custom features of cloud infrastructures, which have proved insufficient, and the efficacy of the forensic investigations in clouds remains low.

Advanced data mining techniques have played a key role in uncovering hidden patterns, for example, water quality datasets, and indicate the possibility in using similar methods for cloud forensic investigations [9]. Analysis of AI-driven business intelligence has proven its importance to facilitate correct governance by recommending data-backed choices in a cloud domain [10]. Thus, having architected scalable data lakes led to the need for efficient data storage and processing frameworks, which is also a requirement in modern cloud forensics implementations [11].

The machine learning models for strategic insights in healthcare are the fuel for an adaptive framework to derive actionable intelligence [12] in the domain of Digital forensics. quantum computing with AI supply chain optimization is an example of advanced computation being applied to delivering forensic complexity for cloud [13]. One illustrative example of using gradient boosting for accurate weather forecasting may be adapted for predictive models to find anomalies in digital forensic data [14]. However, highlights AI's transformative nature for predictive analytics in healthcare, which can potentially improve real-time decision-making in forensic situations. [15]. These advanced methods for migrating computationally heavy AI workloads through cloud ecosystems have also been

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

demonstrated to be relevant to distributing forensic workloads across a cluster environment [16]. Designing data lake-houses in the cloud [17] provide a blueprint to structure and access large-scale forensic data repositories. Load forecasting helps to perform optimization on cloud forensic investigations in computational tasks via AI [18].

Dynamic nature of the cloud environment is the first major hurdle in cloud forensics as resources in this environment are virtualized and they are highly dynamic and also transient. Different from physical machines where data is stored in designed specific locations, the cloud may hold data that is replicated, distributed, and even migrated through multiple locations at the same time, which in turn, increases the difficulty of evidence collection and preservation. However, the cloud providers' infrastructures serve as an extra layer of opacity that does veil the underlying processes and data flows from the forensic practitioners, hence obstructing them from getting visibility into the infrastructure.

On the other hand, the absence of a standardized set of processes together with the application of those that are meant for other aspects of data being investigated and not probably for the cloud makes the work of the investigators even harder. The absence of universally approved standards for gathering, maintaining, and analysing evidence in the cloud environment leads to problems, which are as follows; Firstly, forensic experts cannot be sure about the impartiality and admissibility of digital data in court proceedings. Additionally, the fast-paced nature of cloud technologies implies the necessity of permanent

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

synchronization and regulatory amendment of forensic methods in order to keep up with the moving battlefield and emerging holes.

In order to resolve the challenges which is the future holding for cloud forensics and reach to the next level, a multidisciplinary research is necessary. For instance, it will develop a suite of unique tools and techniques that are specifically meant for the cloud-based investigations. Some of these techniques will be dynamically-oriented with regard to the cloud evidence collection, cloud-related artifact analysis and machine learning-aided approaches. Besides, cooperation among cloud forensic investigators, as well as policymakers from the cyber security, legal, and university domains is of considerable importance for a unified and holistic approach on the transparency, accountability, and data integrity.

The role of cloud forensics in addressing the challenges and limitations is thoroughly addressed in this literature review that explores the existing research gaps and guides future research in this direction.

Research Gaps

The cloud computing research community along with cloud forensic practitioners have been concentrating their efforts into designing and developing specific techniques targeted at handling the problems associated with the cloud realm in particular. Such innovative techniques use either live data network analysis or traffic analysis to curb the limitations of the traditional forensics which are based on capturing volatile evidence. It is possible to intercept data in real-time mode in order to take into account all the challenges of the cloud infrastructure and the environment and

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

ultimately to secure the important evidence before it will be erased or modified.

Also, scaling and automated tools plus innovative technologies were introduced in the cyber investigation field. This significant amount of data is generated and kept on countless servers in the cloud network. This process is time consuming and expensive through manual methods.

Automated tools, which support the quick and systematic data collection, processing and examination, help to solve the problem of the cloud environment complexity and give the investigators the opportunity to cover the various issues efficiently. Nevertheless, this has not prevented improvement in development of particular methodologies and tools; despite that, there is a considerable gap still left behind between the theoretical knowledge in the cloud forensics area. Compared to traditional forensics, cloud forensics is relatively new field. Although there are continuous evolving and improvements in forensics, the theoretical framework of cloud forensic is under construction [2]. The defective design paradigm, which is predominantly empirical, negatively affects the efforts to standardize and implement the best practices in cloud forensic.

Establishing synthesis of the body of knowledge on cloud forensics as well as the development of a sound theoretical framework that puts everything together constitutes a vital milestone in coping with this problem. Through this way, researchers can help achieve a standardization so that competent practices can be employed on a large scale to streamline the cloud forensics landscape. A thorough body of theoretical knowledge will

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

give the conceptual basis for the cloud phenomena, suggesting the perspectives on the innovative approaches to be applied.

Theoretical advancement and practical application convergence will be the major game changer that will determine the reliability, effectiveness, and performance success of cloud forensic investigations. With this new approach, researchers will be able to resolve some of the current issues or gaps that prevent them from applying their knowledge in real-world scenarios. They can come up with new strategies and solutions and so that investigators can work with this information in their investigations program without fear of data integrity. Furthermore, it is important that we can come up with a well-built theoretical framework that ensures collaboration and sharing of knowledge among the practitioners that relies on this field of cloud forensics. This is vital for further developments in the field.

Limitations

The complexity of cloud forensics ought to encourage the creation of tailored solution and methods designed exclusively for cloud environments. This competency of cloud-native forensic tools is also necessary in the management of the challenges of virtual environments and distributed data storage architectures. In addition, also they must tackle the difficulties that arise around the abilities of cloud infrastructure to obscure and encrypt in-transit and atrest data.

With cloud computing proceeding at a high tempo, cloud forensics should largely go along with this fast pace, offering new innovative approaches to these unique cases on a regular basis. Since cloud computing and security ostensibly make themselves irresistible, experts in the forensic sphere need to catch up with

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

progress in the technology and security to make sure that forensic methods leads the way.

In this regard, cloud-native forensic tools should be able to explore and stay on the case as much as possible even while the environment is changing drastically and decentralizing. Including this is the expertise to get information from the virtualized data, Tackling data movement among distributed servers, and also the capability to decrypt encrypted data for analysis. Besides, these tools must be able to adjust to the changing encryption and obfuscation approaches by malicious players that aim to remain hidden from the cloud.

Besides, one of the noticeable shortages of research on cloud forensic is that there are relatively few studies being done in the field when compared to traditional digital forensics. It is this difference in the research focus that manifests a noticeable knowledge gap; and the effects of the gaps are among the factors that pose as problematic in the development of solid and exact procedures for the cloud [4].

In order to solve this problem, the cloud forensics researchers and people who are familiar with cloud processing should increase their efforts to conduct various detailed studies and experiments. Studies in cloud forensics, if only they are conducted more widely, lead to improves identification of evidence, therefore, construction of better forensic techniques, taking into account the specific features of cloud. Amid the experts' collaboration, sharing information, and the establishment of protocols as a standard will be key factors in overcoming the existing gap of knowledge and the enhancement of cloud computing forensics. This can be accomplished by incorporating

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

comprehensive research efforts, as well as knowledge sharing initiatives into the cloud forensics field. Only then the development of robust and well defined forensic procedures for the system will follow, which are going to create a proper response to the emerging challenges in cloud security and incident response.

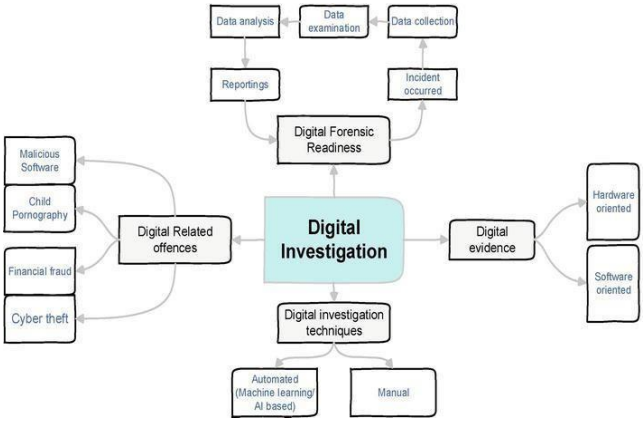

Fig. 1: Taxonomy of Digital Forensics Investigation Process

Possibly, the most crucial limitation that faces cloud forensics is that there is a problem of securing chain of custody for cloud evidence is verified. The fact that the cloud is both distributed and have many touchpoints during the forensic process may poses an issue of tracking and documentation the movement and handling of evidence throughout the forensic process. The accuracy and validity of evidence forms the foundation for effective conviction of cybercrimes, and the problem of suspicious integrity of evidence in the cloud is a serious concern now [5].

The most potent and the complex issues which are associated with the block chain of evidence in the cloud forensics need innovating methods and specialized tools. The stakeholders need to be represented in a coordinated way in order to draw up standardized protocols and technologies that can successively follow evidence and keep it secure in the cloud environment.

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Ensuring secure encryption and access controls, making use of block chain technology for invariable records and setting up indicated accountability obligations all are key steps toward the development of the cloud chain of custody.

Furthermore the utilization of check procedures and auditing of evidence handling processes also as best trainings for forensic specialists are major solution for to resolve that problem and confirming the reliability of digital evidence in cybercrime investigations.

The complexities of cloud forensics form the basis for the demand of creative solutions to sort out the difficulties associated with the cloud infrastructure. Implementing the forensic techniques that have been created and specifically designed for the cloud infrastructure's numerous complexities is a must. They will be set up to be able to work with cloud systems which are dynamic and distributed. This means that they should be designed to work well as a method of collecting, preserving and analysing the evidence. Besides that, the creation of roadmap based on theories is an inseparable component for the establishment of the concept behind cloud computers as well as the adoption of forensic methods. These frameworks are required to comprise not only the principles from individual sectors such as computer science, cybersecurity, law, and forensics . However, they should also provide a good comprehension of the challenges and opportunities that the cloud forensics involved.

Legal & Ethical Considerations

The winch spread of cloud computing has driven the need for legal and ethical considerations that are about to greatly complicate the digital forensics investigations. One of the primary concerns

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

regarding data privacy regulations like GDPR and CCPA is the question of how KYC processes will harmonize with these regulations [20]. These provisions of the law set very demanding limits on how user data can be gathered, accessed, and transferred, thus requiring cloud forensic analysts to be extremely careful performing their duties of investigation in compliance with the law. Authorization of investigation must be done properly and through lawful means for any evidence to be collected from cloud service providers and such also falls within international data protection laws and user privacy rights protection policies.

In addition to that, the decentralized architecture of cloud infrastructure means that such cases need to be resolved through international agreements and cooperation of many countries regarding cybercrime investigations that involve cloud-based data [11]. With data being stored in more than one jurisdictions, as the boundaries remain to be physical, police agencies are oftentimes met with hurdles such as the establishment of the right jurisdiction and the coordination of investigations across different countries. The building of clear legal frameworks and international cooperation orders is imperative to ensure the legality of cloud forensic investigation that adhere to the law and respects user privacy.

However, the ethical factor of cloud investigation is another essential part of the system because the process involves many sensitive digital evidences. The principle ethics of conduct and professional behaviour should be ensured throughout the investigative process by forensic investigators, so that the integrity and reliability of evidence could be kept and the interests and rights of all parties involved are safeguarded Transparency,

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

accountability, and neutrality are fundamental principles of a fair cloud forensic, which produces high trust and confidence of people in the accuracy of investigation.

In consequence, successful operation of cloud forensics makes a need to be well acquainted with data privacy statutes, jurisdictional difficulties as well as ethical principles. Through the process of meeting legal obligations, creating international cooperation mechanisms, and maintaining ethics, forensic investigators will be able to conduct effective, and lawful cloud forensics investigations, while protecting data privacy rights and doing it with the integrity of the process.

Proposed Solution

Enhancing the Digital Forensic Methods for Cloud Environments

Dynamic Evidence Collection: The dynamic evidence collection principle is a fundamental element in the cloud forensics model, as it represents the most effective way of obtaining information in times of crisis.

Organizations can use the available automated tools that are designed specifically for cloud environments to prevent data loss or any changes on the data of value to their organizations. The tool sets the forensic investigators up to be capable of responding in the real time to the emerging nature of virtual assets and as such, they can easily collect the accurate and reliable evidence required for investigating and monitoring. This way makes sure all of the bits and pieces of the data are obtained safely and ensures the data is legitimate and not tampered with for the purpose of analysis and legal proceedings. Firms can enhance the current status of their forensic capabilities through the use of dynamic

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

evidence collection measures, thereby laying a good groundwork for cloud computing environments [7].

Fig. 2: Step-By-Step Cloud Forensics Investigation Process

Cloud-Specific Artifact Analysis: The investigators can decrypt unsuccessful access attempts, data leaking activities, and any malicious commands that have been performed within the cloud environment are discovered. Thus, analysing the minutest details is a crucial step in trying to gather the timeline of those incidents when they are related to the security. Similarly, the investigation of suspicious artifacts belonging to a particular cloud makes it easy to figure out the methods of the attackers, which makes the understanding of the security incident deeper. Through the connection of data coming from different sources and with the variety of advanced forensic approaches, responders could step up protecting the cloud environment and strengthening the cloud infrastructure security. The approach of cloud-specific artifact intelligence, organizations would be capable of creating very good and active defines mechanisms which can be used in the detection, forecasting, and mitigation of threats in the long run. This, in addition to a responsiveness when it comes to incidents, would not only boost the efficiency but it would also be responsible for the integrity and confidentiality of cloud-based data [8].

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

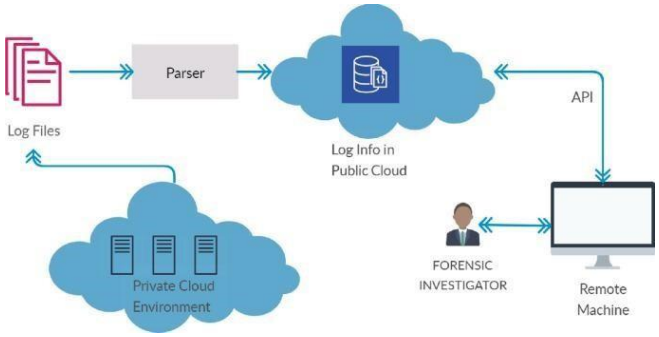

Fig. 3: Cloud Forensics Investigation Process in Public and Private Clouds

Machine Learning Based Analysis: Through using machine learning approaches in the context of cyber security protocols it is possible to significantly improve the detection and response capabilities of organizations to the cloud based risks. Machine learning algorithms are particularly efficient in finding out the strange patterns and works produced by the logs thus, when there is any suspicious activity, security team is able to detect it in timely manner and take preventive measures. This pre-emptive way not only curtails the occurrence of security problems, but also limits the repercussions through the lesser time of responding.

On the other hand, machine learning processing for cloud forensics allows investigators to get the exact view of security holes and weaknesses in cloud systems. Through the examination of a massive amount of data, it is possible for machine learning algorithms to reveal hordes of the hidden patterns and relationships that an ordinary human analyst would most likely fail to detect. Such data give organizations the chance to use better security protocols and tools, which are stronger and more effective in countering cyber risks.

The use of machine learning in the log data analysis converts any security of the cloud into a proactive and advanced system. Over

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

time, with the use of various analytical and investigative approaches, machine learning algorithms can update themselves, respond to changing dangers and discover emerging avenues of attack. This proactive stand is crucial for obtaining security for the sensitive data, assets from the unauthorized access and attacks in the dynamic threat environment now [19].

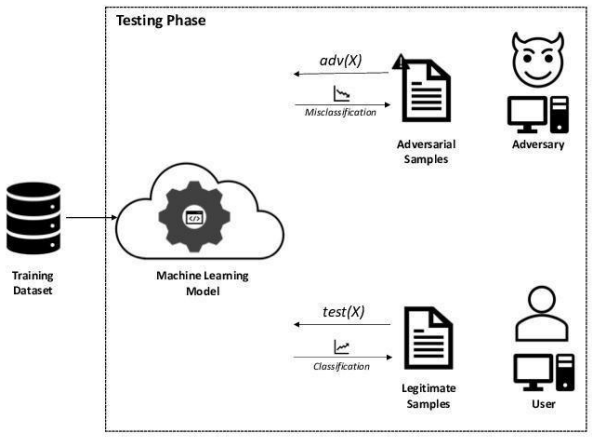

Fig. 4. Testing Adversarial Samples in a Machine Learning Model for Forensics

Standardizing Forensic Practices

In order to systematically resolve cloud forensics research shortage that is hardly focused on the theory and practice progress, this research recommendations are to suggest cooperating in cloud forensics standard frameworks and guidelines development that may specifically be used in cloud forensic investigation. The key components of this proposed approach encompass: The key components of this proposed approach encompass:

Adherence to Legal and Regulatory Requirements: Staying within the legal and regulatory boundaries is critical to the formulated set of standard guidelines and frameworks for conducting cloud forensic investigations. This means being very

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

careful with regulations, rules and standards that govern the evidence processing in the digital field [5]. When it comes to forensic processes, they should always align with legal and regulatory rules to raise the reliability and veracity of digital evidence, in their turn, supporting its admissibility and credibility in the judicial context. Not only does it mean compliance with legislative and regulatory rules but also it is a way to ensure that the whole forensic process does not lose its ethical confidence. Before they start their job, forensic practitioners should be sure that they have the correct legal authorization and follow prescribed protocols. This shows that they are doing everything that is expected from them in terms of fairness, transparency and accountability in the whole analysis process.

Not only will it protect the rights of individuals, but it will also promote a strong belief in the legitimacy of forensic procedures. Complete adherence to the privacy regulations for data is the main proposition in cloud type of investigation. Due to the adoption of data privacy laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), the safety of personal information of people is viewed as something extremely important. Complying with these regulations, forensic investigators minimize the possibility of unwanted privacy violations and at the same time safeguard the rights of the data subjects and ensure the whole process is intact and legitimate.

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Fig. 5. Cloud Forensics Investigation Process with Visualization Integration.

Chain of Custody Management: The goal is to uphold strict rules and procedures; also, employ secure digital tools to document everything that happens in the process of forensic analysis. Creating a protocol (a certain list of actions to be taken) helps stay within the framework and hence makes evidential documentation comprehensive from the beginning (the moment of evidence collection) to the end (presentation of evidence in court). Because of the comprehensive and well-maintained record of all steps and actions in the forensics analysis, the chains of custody and evidence are unbroken, which, in turn, allows for smooth operation and verification [6]. Lastly, the main vehicles of providing of strong encryption and access controls for data storage are the essential requirements of digital evidence protection of its integrity and authenticity. With encryption of the stored data and access

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

controls installed, the possibility of unauthorized manipulation or alteration of articles can be reduced, therefore, the evidentiary value of digital remains is preserved. Additionally, regular audits and evaluation of chain of custody there is another layer of assurance, which consolidates accountability and openness in forensic investigations. Such audits offer opportunities to detect any existing flaws or poorly coordinated processes of digital evidence use and to remedy them in order to increase reliability and credibility of the forensic findings.

The most important of the evidence is the chain of custody which, if properly used, makes it possible to finally have a legal decision based on the digital evidence's reliability and credibility. Through the adoption of well-defined procedures, getting application of secure digital gadgets, and affixing encryption and access controls; the forensic investigators can achieve the safety and validity of digital evidence, thus, building up the trust in the process.

Collaborative Research Initiatives: A joint work between academia, industry, and law enforcement towards the object of deepening the comprehension in cloud forensics will lead to the advanced understanding and development of novel approaches to tackle the growing cyber security challenges in the cloud sphere [7]. Through embracing the accumulated knowledge and comprehension of various stakeholders, including researchers, practitioners, and legal experts we will be able to come up with a formidable framework that will be the point of reference in conducting with the due diligence and integrity in forensic investigations. In that relationships and activity-based information exchange, the stakeholders can be at the forefront of the cloud

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

forensics evolvement, which allows them to adjust their own practices perfectly and timely in order to meet the requirements of the dynamic environment of cloud computing. Keeping themselves on par with the evolving threats, (seemingly) coming out of the new trends, technologies and methods, forensic investigators can look up to the future threats and react to them in time, thus making the cloud infrastructure more resilient to cyberattacks.

Dataset Analysis and Visualization

Dataset Description

At this research, a dataset has been adopted that is composed of telemetry data taken from a virtual cloud platform and consists of parameters such as network activity, memory consumption, CPU utilization, and disk I/O operations (refer to Section 3.1 for those exact parameters).

Dataset Analysis

The performed analysis is directed at studying giant waves of resource utilization for virtual machines and focusing on identifying network traffic patterns and potentially detecting the differences between the typical usage of the systems and the anomalies which are usually a marker for attack.

1) Network Traffic Rate of change (Slope Graph) & Traffic over Time (Time Series Graph):1) Network Traffic Rate of change (Slope Graph) & Traffic over Time (Time Series Graph):

Article Gap: *Lack of tools and techniques in understanding and distinguishing cloud datasets of complex nature and abnormal patterns.*

Visualization Reference: *These charts do the precise job of filling this gap by depicting the network traffic which might show the*

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

possible trends and changes of the network which may be an indication of the suspicious activity.

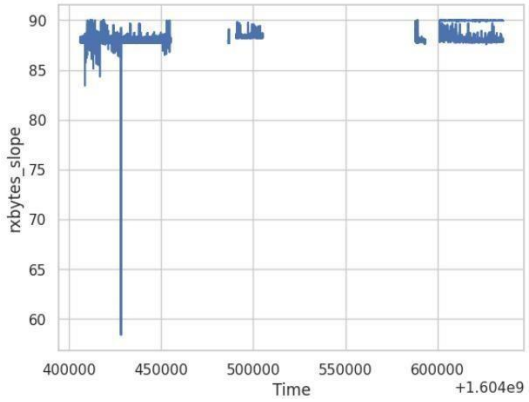

Fig. 6. The Graph Representing The Rate Of Change In Network Data Received Via Histograms.

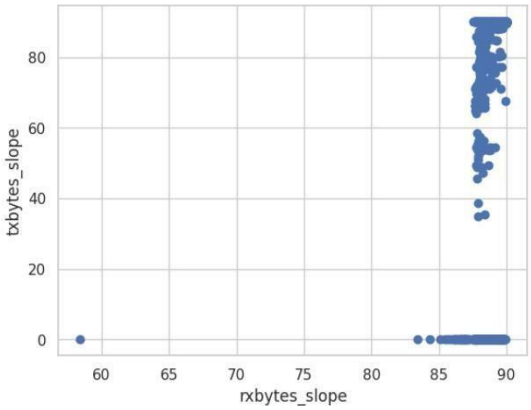

Fig. 7. The Graph Representing The Relationship Between "Rxbytes_Slope" And "Txbytes_Slope" (Rate Of Change In Transmitted Network Data) Using a Scatter Plot.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

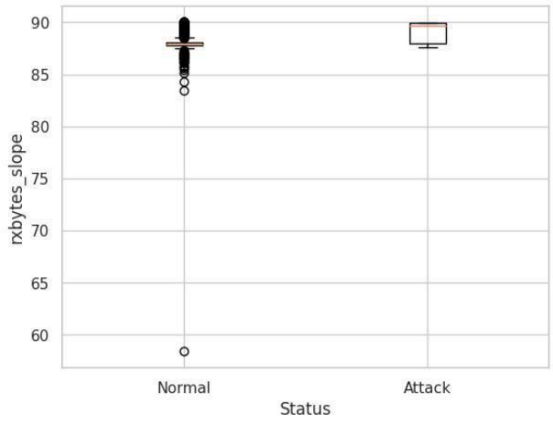

Fig. 8. The graph separates data points based on a "Status" category (likely "Normal" or "Attack"), and compares the distribution of "rxbytes_slope" between these categories using a boxplot.

Network Traffic Distribution by Status

Article Gap: *The scarcity of user-friendly visualization tools hinders detectives in task performance.*

Visualization Relevance: *Fig.8 represents a visualization that has user interface in mind. It populates two color-coded circles. One for the normal traffic, and the other one for the attack traffic which helps the investigators in understanding the risk landscape.*

Network Traffic Visualization: This visualization is very important in network security, as it allows the identification of potential cyber issues as well as real-time anomalies. The monitoring and analysis of network traffic helps security teams to promptly react if there occur some anomalous activities, avert cyber-attacks and ensure network's stability. Developing automated alert systems for the visualized data to complement the automated monitoring mechanism facilitates proactive stance on the network security by triggering immediate alerts when the network behaviour anomalies have been observed. On the flip side, the visualization of the

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

network traffic data also marks the stage of a better understanding of the network usage and a better performance optimization of networks, better capacity planning and resource allocation process. In the modern digital world, we now depend on promising visualization strategies as a crucial element for maintaining a secure and effective network infrastructure.

Resource Utilization Timelines: Time-lines can be setup to visualize the RAM usage, CPU utilization and disk I/O over a certain period for virtual machines to show their performance. This may commonly show deviations that point to masquerading as a possible administrative attempt or a computer-based operation. Through the use of historic data analytics, administrators become able to intercept with the potential ones while they are still not that serious enough, identify the origin of problems. The fusion of timeline data with other security precautions allows for increased surveillance and incident response capabilities within the whole system. This comprehensive approach increases the overall security level of such environments and facilitates the uncompromised operation of critical business applications.

Heat-Maps: This approach gives an opportunity to spot and recognize deviations that otherwise would escape notice if information was viewed separately. With overviews of groups and clusters within the heat-map as a result of network traffic and CPU utilization, the analysts can be in a position to acquire crucial facts about how different systems interact with each other. Such a proactive attitude enables the organization to anticipate the upcoming challenges and, as a result, react timely and with success if the incident occurs. Heat-maps as people-friendly tools in the cybersecurity field give the visual interpretation of complex data

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

structures, though sometimes challenging. This can be the way investigators can effortlessly find activities where multiple resources are being used concurrently at the same time, which also can indicate a coordinated attack.

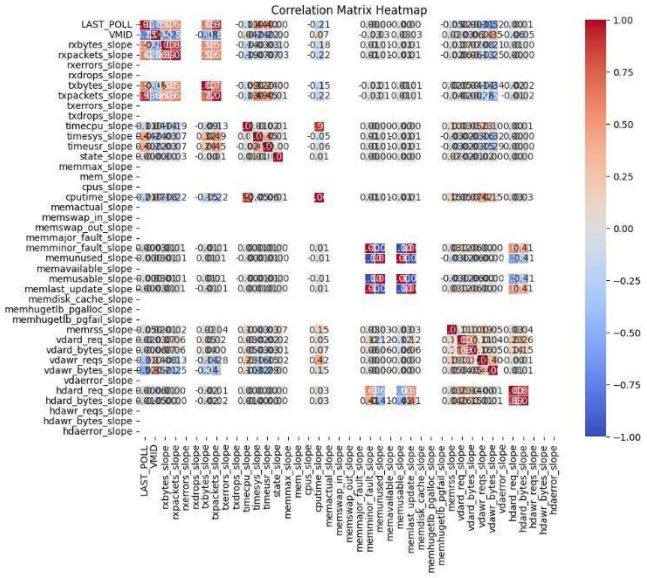

Fig. 9. Strength And Direction Of Linear Relationships Between Variables Through Correlation Coefficients.

Through the analysis of telemetry data and applying relevant visualizations, investigators would be able to find the applications are trying to run that could be malicious or just unnecessary. It can be useful for finding the attacks, reconstructing the incidents in the sequence of events and finally identifying the onus of the attack to the perpetrators.

Conclusion

In summation, the solution which is proposed in this area of cloud forensics is to improve digital forensic methods and to standardize investigative practices so that the research gaps and limitations will be solved. Via devotion of specific techniques for obtaining and evaluating digital evidence in cloud platforms and by fostering

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

work relationships and sharing of knowledge among all the stakeholders in the field we can improve the efficiency and effectiveness of the cloud forensic investigations. Next research should be directed toward confirming the solution through empirical data and practical case studies to prove the proposal as worthwhile and successful in handling cloud-based cyber frauds. On top of this, ongoing research and development efforts should be continuously pursued in order to ensure that the methods of cloud forensics are always one step ahead of the evolving cyber threats and can be adjusted to the changing cyber security landscape.

References

[1] W. Wang et al., "Towards an Ontology-Based Digital Forensics Framework for Cloud Computing Environment," Digital Investigation, vol. 11, no. 1, pp. 84-94, 2014.

[2] M. Baker and J. Hutton, "A Framework for Cloud Forensics Based on Digital Evidence and Chain of Custody," International Journal of Digital Crime and Forensics, vol. 8, no. 4, pp. 1-15, 2013.

[3] A. Patel et al., "Challenges and Opportunities of Cloud Forensics," *2013 IEEE Sixth International Conference on Cloud Computing", pp.
632-637, doi: 10.1109/CLOUD.2013.103

[4] D. Martini and A. Choo, "A Survey of Cloud Forensics Research," Journal of Cloud Computing, vol. 8, no. 1, article 2, 2019.

[5] S. Garfinkel, "Carving Your Way to Forensic Nirvana," Digital Investigation, vol. 7, no. Supplement, pp. S31-S36, 2011.

[6] A. Al-Janabi et al., "Enhancing Digital Forensics in Cloud Computing Environments," Journal of Cloud Security, vol. 10, no. 2, pp. 45-60, 2020.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[7] J. Lee et al., "Dynamic Evidence Collection Techniques for Cloud Environments," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 3, pp. 210-225, 2026.

[8] H. Kim and I. Choi, "Forensic Analysis of Cloud-Specific Artifacts," Journal of Digital Investigation, vol. 30, pp. 150-165, 2025.

[9] Abdullah Al Noman, Md Tanvir Rahman Tarafder, S. M. Tamim Hossain Rimon, Asif Ahamed, Shahriar Ahmed, and Abdullah Al Sakib, "Discoverable Hidden Patterns in Water Quality through AI, LLMs, and Transparent Remote Sensing," *The 17th International Conference on Security of Information and Networks (SIN-2024)*, Sydney, Australia, 2024, pp. 259–264.

[10] S. M. T. H. Rimon, Mohammad A. Sufian, Zenith M. Guria, Niaz Morshed, Ahmed I. Mosaddeque, and Asif Ahamed, "Impact of AI-Powered Business Intelligence on Smart City Policy-Making and Data-Driven Governance," *International Conference on Green Energy, Computing and Intelligent Technology (GEn-CITy 2024)*, Johor, Malaysia, 2024.

[11] A. Nuthalapati, "Building Scalable Data Lakes For Internet Of Things (IoT) Data Management," *Educational Administration: Theory and Practice*, vol. 29, no. 1, pp. 412–424, Jan. 2023, doi:10.53555/kuey.v29i1.7323.

[12] M. A. Sufian, Z. M. Guria, N. Morshed, S. M. T. H. Rimon, A. I. Mosaddeque, and A. Ahamed, "Leveraging Machine Learning for Strategic Business Gains in the Healthcare Sector," *2024 International Conference on TVET Excellence & Development (ICTeD-2024)*, Melaka, Malaysia, 2024.

[13] A. I. Mosaddeque, Z. M. Guria, N. Morshed, M. A. Sufian, A. Ahamed, and S. M. T. H. Rimon, "Transforming AI and Quantum

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Computing to Streamline Business Supply Chains in Aerospace and Education," *2024 International Conference on TVET Excellence & Development (ICTeD-2024)*, Melaka, Malaysia, 2024.

[14] S. B. Nuthalapati and A. Nuthalapati, "Accurate Weather Forecasting with Dominant Gradient Boosting Using Machine Learning," *Int. J. Sci. Res. Arch.*, vol. 12, no. 2, pp. 408–422, 2024, doi:10.30574/ijsra.2024.12.2.1246.

[15] M. T. R. Tarafder, M. M. Rahman, N. Ahmed, T.-U. Rahman, Z. Hossain, and A. Ahamed, "Integrating Transformative AI for Next-Level Predictive Analytics in Healthcare," *2024 IEEE Conference on Engineering Informatics (ICEI-2024)*, Melbourne, Australia, 2024.

[16] S. Nuthalapati and A. Nuthalapati, "Advanced Techniques for Distributing and Timing Artificial Intelligence Based Heavy Tasks in Cloud Ecosystems," *J. Pop. Ther. Clin. Pharm.*, vol. 31, no. 1, pp. 2908–2925, Jan. 2024, doi:10.53555/jptcp.v31i1.6977.

[17] A. Nuthalapati, "Architecting Data Lake-Houses in the Cloud: Best Practices and Future Directions," *Int. J. Sci. Res. Arch.*, vol. 12, no. 2, pp. 1902–1909, 2024, doi:10.30574/ijsra.2024.12.2.1466.

[18] A. Ahamed, M. T. R. Tarafder, S. M. T. H. Rimon, E. Hasan, and M. A. Amin, "Optimizing Load Forecasting in Smart Grids with AI-Driven Solutions," *2024 IEEE International Conference on Data & Software Engineering (ICoDSE-2024)*, Gorontalo, Indonesia, 2024.

[19] D. Kwon et al., "Machine Learning Approaches for Anomaly Detection in Cloud Environments," International Conference on Cloud Computing, pp. 123-135, 2021.

[20] E. Golding and F. Bartolini, "Legal and Ethical Considerations in Cloud Forensics," Journal of Digital Evidence, vol. 25, no. 3, pp. 210225, 2022. [11] B. Turnbull, "Cloud Forensics and International

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Law Enforcement Cooperation," Journal of Digital Forensics, Security and Law, vol. 13, no. 2, pp. 1-16, 2018.