
# International Journal of Information Technology, Research and Applications (IJITRA)

**B. MENAKA, S. ARULSELVARANI (2025). EXPLORING CLOUD NETWORK FORENSICS: A COMPREHENSIVE SURVEY OF TOOLS AND TECHNIQUES ENHANCED WITH DEEP LEARNING MODELS, 4(2), 14-28.**

**ISSN: 2583-5343**

**DOI:10.59461/ijitra.v4i2.174**

The online version of this article can be found at:
https://www.ijitra.com/index.php/ijitra/issue/archive

Published by:
PRISMA Publications



**International Journal of Information Technology, Research and Applications (IJITRA)** is a journal that publishes articles which contribute new theoretical results in all the areas of Computer Science, Communication Network and Information Technology. Research paper and articles on Big Data, Machine Learning, IOT, Blockchain, Network Security, Optical Integrated Circuits, and Artificial Intelligence are in prime position.

PRISMA
PUBLICATIONS

https://www.prismapublications.com/

# EXPLORING CLOUD NETWORK FORENSICS: A COMPREHENSIVE SURVEY OF TOOLS AND TECHNIQUES ENHANCED WITH DEEP LEARNING MODELS

**B. MENAKA[1], S. ARULSELVARANI [2]**

[1-2]Department of Computer Science, Urumu Dhanalakshmi College, Tiruchirapalli, India

**Article Info**

***Article history:***

Received March 15, 2025
Revised April 04, 2025
Accepted May 02, 2025

***Keywords:***

Cloud Network Forensics
Deep Learning
Security Incidents
Threat Detection
AI-driven Analysis

**ABSTRACT**

A comprehensive investigation into cloud network forensics, providing an in-depth survey of tools and techniques while integrating advanced deep learning models for enhanced analysis. By examining various cloud environments, including public, private, and hybrid infrastructures, the study explores the challenges and opportunities in detecting, analyzing, and mitigating security incidents. This survey provides an overview of forensic tools and techniques used to investigate cyber incidents, focusing on the integration of deep learning models for enhanced threat detection and analysis. Through the utilization of deep learning methodologies, the research aims to enhance the efficiency and accuracy of forensic investigations, offering valuable insights into emerging trends and best practices for securing cloud-based systems. It highlights key challenges, including data privacy and real-time threat detection, while discussing future trends in AI-driven forensics.



**Corresponding Author:**

B. Menaka, Research Scholar
Department of Computer Science
UrumuDhanalakshmi College
Tiruchirapalli
India

Email: menaka01.mphil@gmail.com

## 1 Introduction

Cloud network forensics has seen advancements through deep learning models [14]. Traditional methods for cloud detection based on rules and physical models are being surpassed by deep learning-based approaches, particularly in handling optical remote sensing images[9]. However, the challenge lies in the size and complexity of these deep models, limiting their applicability and explain ability [13]. A recent proposal introduces a lightweight network, CDFM3SF, tailored for cloud detection in multi-spectral images like Sentinel-2A, outperforming traditional and state-of-the-art deep learning methods inaccuracy and speed [7]. This fusion of multi-scale spectral and spatial features in the proposed method showcases the potential of deep learning in enhancing cloud detection techniques for cloud network forensics [2].


Figure 1: Process Flow of Cloud Forensic Model

## 2 Contribution Of Research

Cloud computing provides a new way of computing that is different from traditional computing. Traditional computing lacks in providing confidentiality, integrity, and privacy about user data. Reduced level of control over the cloud, absence of standard log format, multi-tenancy and decentralization [15]. There is a lack of support for Cloud Computing and Forensics, Challenges in Cloud Forensics, Cloud service models, and Existing Gaps and Solutions [16]. Cloud computing has become a mainstream processing paradigm, offering on-demand resources at a low cost [17]. However, there is a lack of support for cloud forensic analysis within cloud computing environments. In cloud computing, analyzing various logs (such as network logs, process logs, or activity logs) is essential. These logs serve as valuable sources of information for cloud forensic investigations. Existing secure logging mechanisms are designed for traditional systems rather than the complexities of the cloud environment.

The authors propose an alternative approach for secure logs in a cloud setting. In their proposed system, different log records are encrypted using unique user public keys, ensuring that other users cannot decipher the content. This approach significantly reduces the verification time to prevent unauthorized log modifications. The study focuses on cloud forensics, cloud logs, cloud computing, cloud security, and proof of past logs1. The main contributions of this paper are as follows:

Table 1: Contributions of this Paper

| Paper Title | Key Points |
|---|---|
| Cloud Forensic Overview | Investigating cybercrimes related to the cloud. Challenges due to cloud diversity. Research trends include trust, network forensics, evidence collection, privacy and data provenance. |
| Comprehensive Survey | Proposed taxonomy based on Cloud Computing paradigms. Strategies for efficient cloud forensic. Early focus on network forensic and data preservation. |
| Deep Learning Models | **Convolutional Neural Networks (CNNs):** Image analysis and feature extraction<br>**Recurrent Neural Networks (RNNs):** Sequential data analysis (Eg., log files, network traffic)<br>**Generative Models:** Synthetic data generation and evidence enhancement.<br>**Deep Reinforcement Learning (DRL):** Decision-making tasks. |
| Examination and Analysis | Use tools and methodologies to examine digital evidence. Insights from log files, network activity patterns, metadata decoding, and data recovery. Technical expertise is required. |

## 3 Structure of Survey

This paper is organized as follows section I-C Background and Related Work, section II reviews Cloud Network Forensics Techniques domains including Log Analysis, Traffic Monitoring, Packet Inspection, Memory Forensics, Behavioral Analysis, Metadata Examination, and Flow Analysis; Section III includes details about Deep Learning Models in Cloud Forensics domain include Anomaly Detection, Intrusion Detection, Behavioral Profiling, Malware Detection, Log Analysis and Sequence Modeling, and Resource Attribution forensics; Section IV includes details about powerful cloud network forensic toolkits Wireshark, Volatility, Cloud Trail (AWS), Azure Monitor (Microsoft Azure), Google Cloud Logging (GCP),and Snort; section V presents Challenges and Future Directions regarding proposed research work.

## 3.1 Background and Related Work

Cloud network forensics is a rapidly evolving field driven by the increasing adoption of cloud computing services across various sectors. It encompasses the methodologies, techniques, and tools used to investigate security incidents, breaches, andOther malicious activities within cloud environments Unlike traditional digital forensics, cloud network forensics faces unique challenges due to the distributed and virtualized nature of cloud infrastructures as well as issues related to multi-tenancy, dynamic resource allocation, and data privacy. Researchers in this field aim to develop innovative approaches to collect, preserve, analyze, and interpret digital evidence from cloud-based systems. By advancing our understanding of cloud network forensics, researchers contribute to enhancing the security, trustworthiness, and resilience of cloud-based services, there by supporting the continued growth and adoption of cloud computing technologies.

Table 2: Several researchers worked on different technologies of Cloud network forensics

| Ref No. | Title | Authors | Year | Summary | Methodology | Data Source |
|---|---|---|---|---|---|---|
| 1 | Adversarial Attacks Against Deep Learning-Based Network Intrusion Detection Systems and Defense Mechanisms | Chaoyun Zhang, Xavier Costa-Perez, Paul Patras | 2024 | Investigates adversarial attacks on NIDS and proposes defense mechanisms. | Attack modeling, deep learning-based defenses, empirical evaluation. | CICIDS2017, NSL-KDD datasets. |
| 5 | Digital Forensics in Cloud Computing: Techniques and Challenges for Investigating Cybercrimes | Vikas, Shruti Aggarwal, Himani, AnnuYadav, Prashant Kumar | 2023 | Discusses forensic methodologies, challenges, and tools for investigating cybercrimes in cloud environments. | Forensic frameworks, digital evidence acquisition, legal aspects. | Case studies from cloud investiga-tions. |
| 8 | Classification and Pattern Extraction of Incidents: A Deep Learning-Based Approach | SobhanSarkar, Samman-giVinay, ChawkiD-jeddi, J. Maiti | 2022 | Uses deep learning for classifying incidents and extracting risk patterns. | Neural network-based classification, pattern mining. | Industrial incident reports. |
| 18 | Entropy State-Regularized Recurrent Neural Network-Long Short Term Memory (ESRRNN-LSTM) and Classifier for COVID-19 Vaccine | A. Sathya, M. S. Mythili | 2023 | Proposed an ESRRNN-LSTM model to enhance COVID-19 vaccine classification accuracy using entropy-optimized LSTM layers. | The ESRRNN-LSTM leverages entropy measures to regularize and optimize LSTM states for better feature extraction and prediction. | COVID-19 Vaccine dataset |

## 3.2 Cloud Forensics Analysis

A secure block verification mechanism (SBVM) is proposed to secure the device from unauthorized users in a cloud environment, secret keys are optimally generated using a backtracking search optimization algorithm [11]. The authors designed and implemented an automated monitoring system for the IBM CloudPlatform, which utilizes deep learning neural networks to detect anomalies in near-real-time in multiple Platform components simultaneously [12]. The researchers present a comprehensive survey of the research trend in cloud network forensics. The proposed taxonomy provides cloud forensics solution

strategies for efficient cloud forensics [10]. Cloud computing provides a new way of computing that is different from traditional computing. Traditional computing lacks in providing confidentiality, integrity, and privacy about user data. Such as no physical access to cloud logs due to its distributed nature, reduced level of control over the cloud, absence of standard log format, multi-tenancy and decentralization [15].There is a lack of support for Cloud Computing and Forensics, Challenges in Cloud Forensics, Cloud service models, and Existing Gaps and Solutions [16].

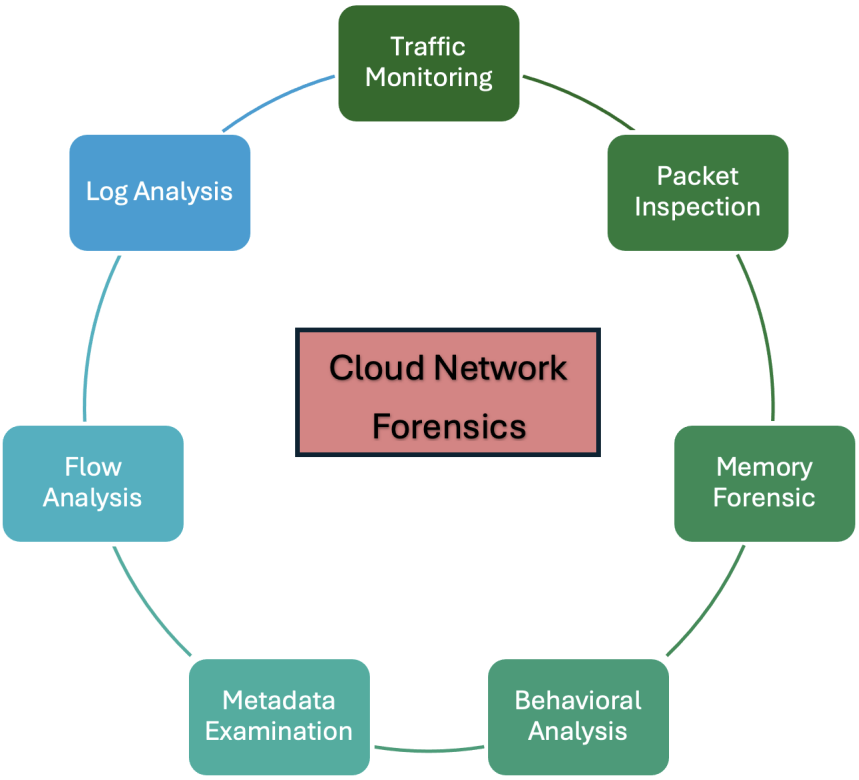


Figure 2: Cloud Network Forensics Domain

### 3.2.1 Log Analysis

Analyzing logs generated by various cloud services (e.g., web servers, databases, virtual machines). Detecting anomalies, identifying security incidents, and reconstructing events.Handling large volumes of logs, dealing with log formats specific to different cloud providers.

### 3.2.2 Traffic Monitoring

Monitoring network traffic within the cloud infrastructure.Identifying suspicious patterns, unauthorized access, or data exfiltration. Encrypted traffic, dynamic resource allocation, and multi-tenancy.

### 3.2.3 Packet Inspection

Examining network packets to extract relevant information.Identifying malicious payloads, analyzing communication patterns, and reconstructing network sessions.Encrypted packets, scalability, and real-time processing.

### 3.2.4 Memory Forensics

Analyzing memory dumps from cloud instances. Extracting process information, identifying injected code, and recovering deleted data.Accessing memory in a virtualized environment, handling memory snapshots.

#### 3.2.5 Behavioral Analysis

Profiling normal behavior of cloud resources. Detecting deviations from expected behavior. Defining normal behavior in dynamic cloud environments.

#### 3.2.6 Metadata Examination

Scrutinizing metadata associated with cloud resources (e.g., instance creation time, IP addresses, storage details). Linking events, tracking resource movements, and identifying potential security incidents.Ensuring metadata integrity and availability.

#### 3.2.7 Flow Analysis

Analyzing flow records (NetFlow, IPFIX) to understand communication patterns. Identifying communication paths, detecting anomalies, and mapping network relationships. Aggregating flow data from distributed cloud resources.

### 3.3 Deep Learning Models In Cloud Forensics Domain

Deep anomaly analytics is a rapidly evolving field that leverages the power of deep learning to identify anomalies in various datasets as discussed by the authors, however, there are also many challenges associated with deep anomaly analytics [6]. Overview of research on crime prediction using machine learning and deep learning approaches is presented, highlighting potential gaps and future directions that can enhance the accuracy of crime prediction [3]. In this article, the authors explore the potential of graph convolutional networks to learn patterns among networked criminals and to predict various properties of criminal networks, including missing criminal predict the amount of money exchanged among criminal agents, and even anticipate partnerships and recidivism of criminals during the growth dynamics of corruption networks [4].

#### 3.3.1 Anomaly Detection

Deep learning models, such as auto encoders or recurrent neural networks(RNNs), can learn normal patterns from network traffic or system logs. Detecting anomalous behavior within cloud environments, such as unauthorized access, data exfiltration, or suspicious resource usage.

#### 3.3.2 Intrusion Detection

Convolutional neural networks (CNNs) or long short-term memory (LSTM)networks can analyze network packets or log entries to identify potential intrusions. Real-time detection of malicious activities (e.g., DDoS attacks, SQL injection) in cloud-based systems. Deep learning models can handle complex patterns and generalize across different attack vectors.

#### 3.3.3 Behavioral Profiling

Recurrent neural networks (RNNs) or attention-based models can learn temporal dependencies in cloud resource behavior. Malware DetectionUsing CNNs or hybrid architectures (e.g., CNN-LSTM), deep learning models can analyze binary files or memory dumps. Identifying malicious software (e.g., Trojans, ransomware) within cloud instances. Deep learning can handle feature extraction directly from raw data.

#### 3.3.4 Log Analysis AND Sequence Modeling

LSTM networks excel at sequence-to-sequence tasks, making them suitable for log analysis. Parsing and understanding complex log entries (e.g., system logs, API logs) in cloud environments. Deep learning models can learn contextual dependencies and handle noisy data.

#### 3.3.5 Resource Attribution forensics

Graph neural networks (GNNs) or attention mechanisms can link cloud resources based on their interactions. Tracing resource movements, identifying shared dependencies, and attributing actions to specific instances. Deep learning models capture graph structures effectively

## 3.4 Cloud Forensic Toolkits

Cloud Forensics to provide the best toolkit for the investigators. We present a review of significant characteristics of Cloud Forensic toolkits comprising Wireshark, Volatility, Cloud Trail (AWS), Azure Monitor (Microsoft Azure), Google Cloud Logging (GCP), and Snort.

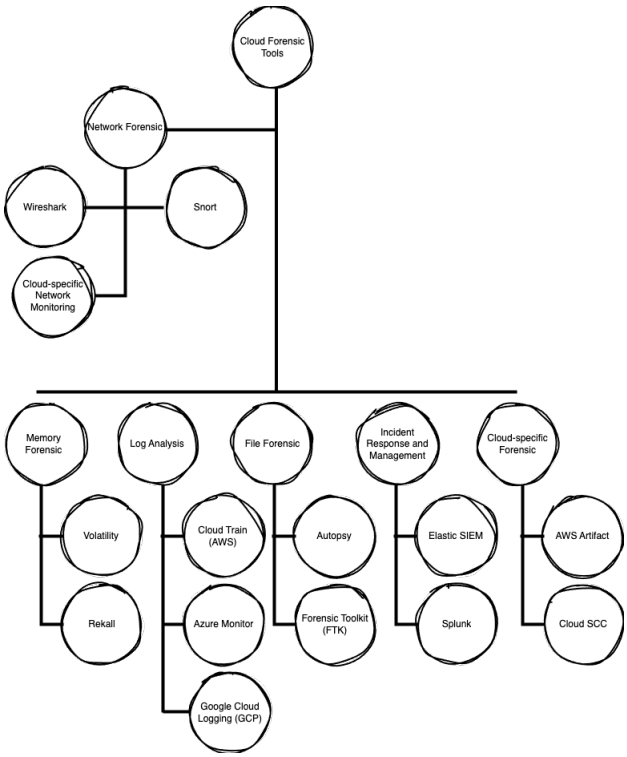


Figure 3: Classification of Cloud Forensic Tools

Table 3: Comparison of general features of Cloud Forensic Tools

| Feature | Wireshark | EnCase | Autopsy | Volatility | Cado Security | Xplico | Snort | The Sleuth Kit(TSK) | Magnet AXIOM |
|---|---|---|---|---|---|---|---|---|---|
| Live Network Capture | Yes | No | No | No | Yes | Yes | Yes | No | No |
| Packet Analysis | Yes | No | No | No | Yes | Yes | Yes | No | No |
| Memory Forensics | No | No | No | Yes | Yes | No | No | No | Yes |
| Cloud-Specific Forensics | No | No | No | No | Yes | No | No | No | Yes |
| Disk Imaging | No | Yes | Yes | No | Yes | No | No | Yes | Yes |
| Intrusion Detection | No | No | No | No | Yes | No | Yes | No | No |
| Log & Data Extraction | No | Yes | Yes | No | Yes | No | No | Yes | Yes |

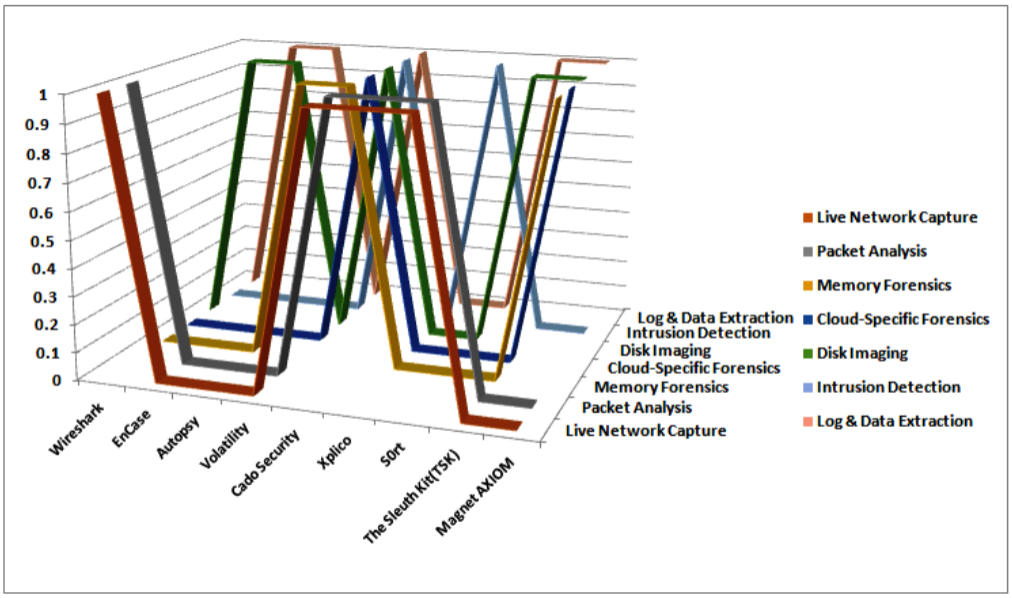


Figure 4: Comparison of general features of Cloud Forensic Tools

## 3.5 Domain Wise Analysis Of Cloud Network Forensics Tools

Cloud network forensics tools analyze digital evidence across cloud environments, helping detect security threats and breaches. AWS GuardDuty, Azure Sentinel, Google Chronicle, and Splunk specialize in log-based threat detection, anomaly detection, and SIEM integration, making them ideal for cloud-native security monitoring. Zeek(Bro), in contrast, focuses on packet-level analysis and deep traffic inspection, crucial for network forensics. These tools collectively support real-time monitoring, data collection, and forensic investigations, ensuring a comprehensive approach to incident response and cybersecurity in cloud environments.

### 3.5.1 Incident Response Cloud Network Forensics Tools

GuardDuty, Azure Sentinel, Google Chronicle, and Splunk excel in real-time threat detection, automated incident response, cloud log monitoring, and SIEM integration, making them ideal for cloud security operations. Zeek (Bro), unlike the others, specializes in packet-level analysis but lacks automated threat response and SIEM integration. All tools support behavior-based anomaly detection, enhancing their ability to detect sophisticated threats. While cloud-native tools (GuardDuty, Sentinel, and Chronicle) focus on cloud security, Zeek and Splunk provide broader forensic capabilities across network environments.

Table 4: Feature-wise comparison of Incident Response Cloud Network Forensics Tools

| Feature | AWS GuardDuty | Azure Sentinel | Google Chronicle | Splunk | Zeek (Bro) |
|---|---|---|---|---|---|
| Real-Time Threat Detection | Yes | Yes | Yes | Yes | No |
| Automated Incident Response | Yes | Yes | Yes | Yes | No |
| Packet-Level Analysis | No | No | No | No | Yes |
| Cloud Log Monitoring | Yes | Yes | Yes | Yes | No |
| Behavior-Based Anomaly Detection | Yes | Yes | Yes | Yes | Yes |
| SIEM Integration | Yes | Yes | Yes | Yes | No |

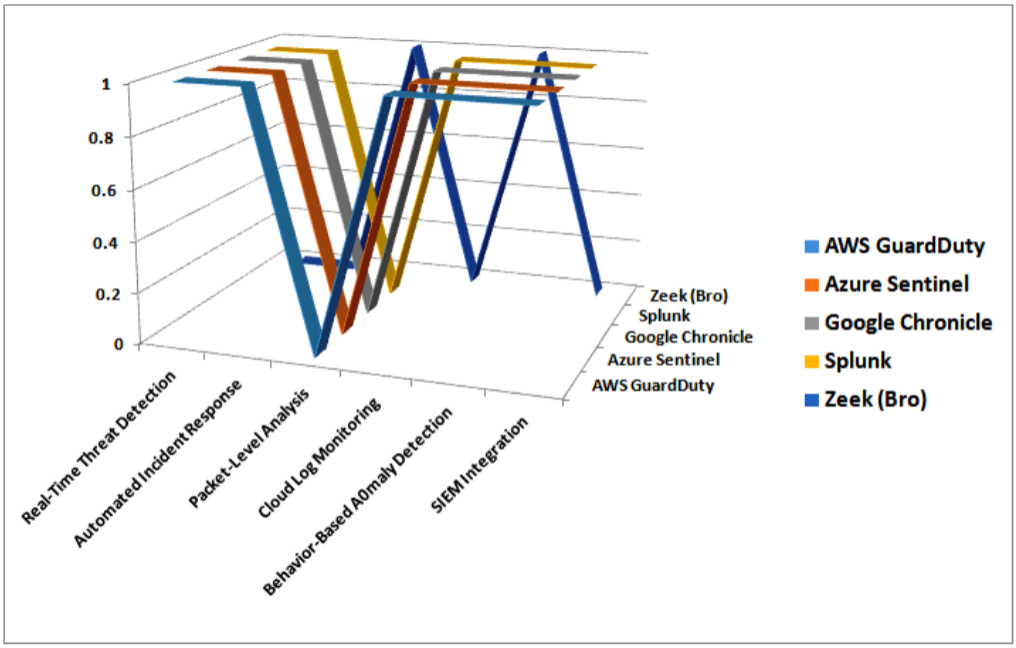


Figure 5: Comparison of Incident Response Cloud Network Forensics Tools

### 3.5.2 Data Collection for Cloud Network Forensics Tools

Cloud network forensics tools differ in their data collection approaches, with AWS GuardDuty, Azure Sentinel, Google Chronicle, and Splunk excelling in cloud log collection, event-based data collection, and behavioral data monitoring, ensuring comprehensive security insights. Zeek (Bro), on the other hand, focuses on network traffic capture and packet-level data collection, making it ideal for deep network analysis. While cloud-native tools aggregate and analyze large-scale cloud logs, Zeek provides a granular view of network activity, complementing other forensic methods.

Table 5: Feature-wise comparison of Data Collection for Cloud Network Forensics Tools

| **Feature** | **AWS GuardDuty** | **Azure Sentinel** | **Google Chronicle** | **Splunk** | **Zeek (Bro)** |
|---|---|---|---|---|---|
| Cloud Log Collection | Yes | Yes | Yes | Yes | No |
| Network Traffic Capture | No | No | No | Yes | Yes |
| Packet-Level Data Collection | No | No | No | No | Yes |
| Event-Based Data Collection | Yes | Yes | Yes | Yes | No |
| Behavioral Data Collection | Yes | Yes | Yes | Yes | Yes |

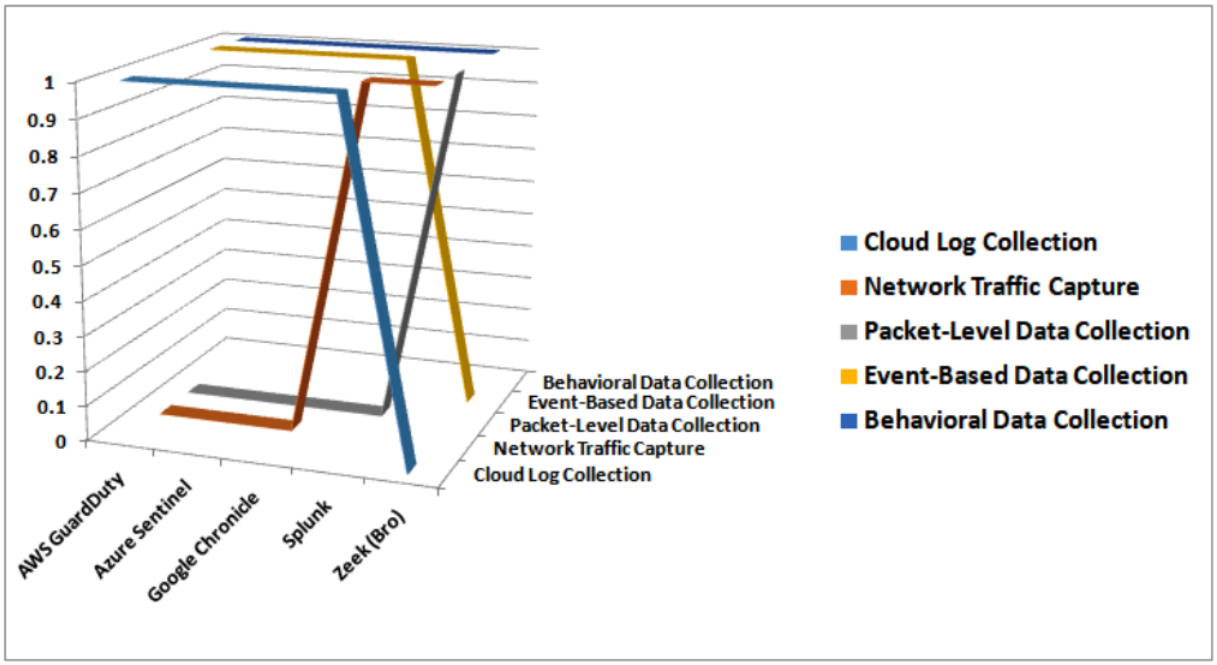


Figure 6: Comparison of Data Collection for Cloud Network Forensics Tools

### 3.5.3 Data Analysis for Cloud Network Forensics Tools

Cloud network forensics tools vary in data analysis capabilities, with AWS GuardDuty, Azure Sentinel, Google Chronicle, and Splunk excelling in log data correlation, threat intelligence integration, machine learning-based anomaly detection, and real-time processing, making them essential for cloud security monitoring. Zeek (Bro), in contrast, specializes in deep packet inspection (DPI) but lacks advanced log correlation and intelligence integration. While cloud-native solutions focus on large-scale automated analysis, Zeek provides a network-centric approach for forensic investigations.

Table 6: Feature-wise comparison of Data Analysis for Cloud Network Forensics Tools

| **Feature** | **AWS GuardDuty** | **Azure Sentinel** | **Google Chronicle** | **Splunk** | **Zeek (Bro)** |
|---|---|---|---|---|---|
| Cloud Log Collection | Yes | Yes | Yes | Yes | No |
| Network Traffic Capture | No | No | No | Yes | Yes |
| Packet-Level Data Collection | No | No | No | No | Yes |
| Event-Based Data Collection | Yes | Yes | Yes | Yes | No |
| Behavioral Data Collection | Yes | Yes | Yes | Yes | Yes |

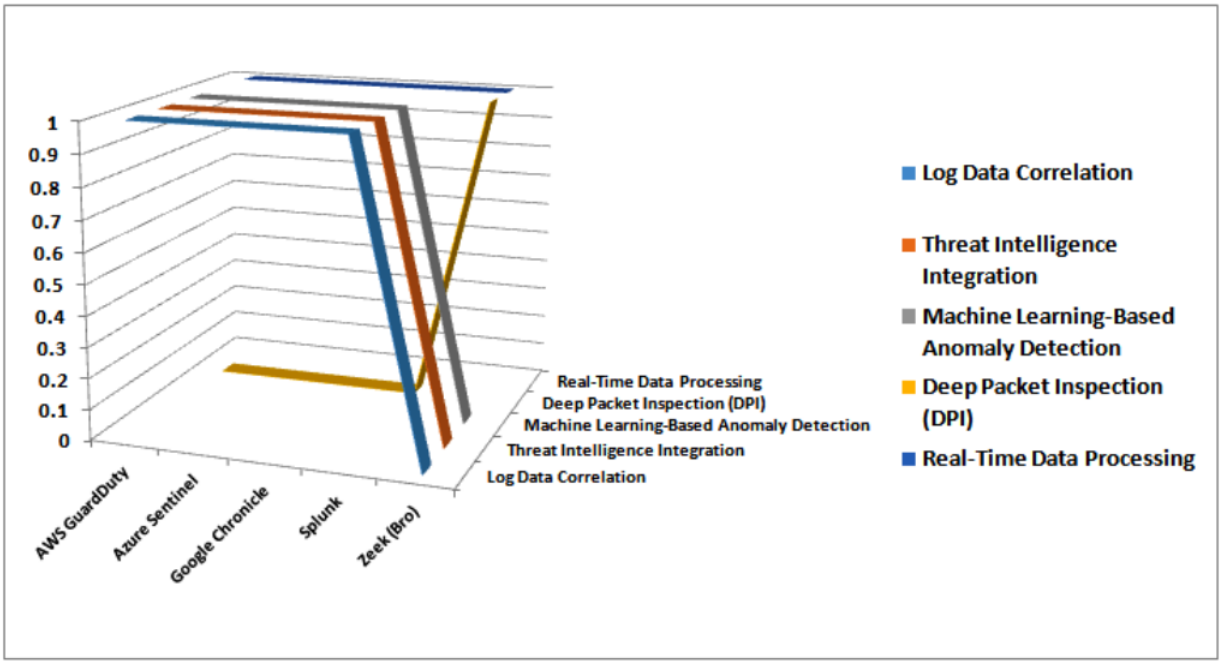


Figure 7: Comparison of Data Collection for Cloud Network Forensics Tools

### 3.5.4 Log & Data Extraction for Cloud Network Forensics Tools

Cloud network forensics tools vary in their capabilities, with AWS CloudTrail, Azure Monitor Logs, Google Chronicle, and Splunk excelling in cloud log collection, real-time monitoring, SIEM integration, and forensic timeline reconstruction, making them ideal for cloud-based investigations. The Sleuth Kit (TSK) and Magnet AXIOM focus on data extraction from logs and forensic timeline reconstruction, while Wireshark specializes in packet capture and analysis for network traffic investigations. Combining log-based and packet-based tools ensures a comprehensive forensic approach for cloud security.

Table 7: Feature-wise comparison of Log & Data Extraction for Cloud Network Forensics Tools

| Feature | AWS CloudTrail | Azure Monitor Logs | Google Chronicle | Splunk | Wireshark | The Sleuth Kit (TSK) | Magnet AXIOM |
|---|---|---|---|---|---|---|---|
| loud Log Collection | Yes | Yes | Yes | Yes | No | No | Yes |
| Real-Time Log Monitoring | Yes | Yes | Yes | Yes | No | No | No |
| Data Extraction from Logs | Yes | Yes | Yes | Yes | No | Yes | Yes |
| SIEM Integration | Yes | Yes | Yes | Yes | No | No | No |
| Packet Capture & Analysis | No | No | No | No | Yes | No | No |
| Forensic Timeline Reconstruction | Yes | Yes | Yes | Yes | No | Yes | Yes |

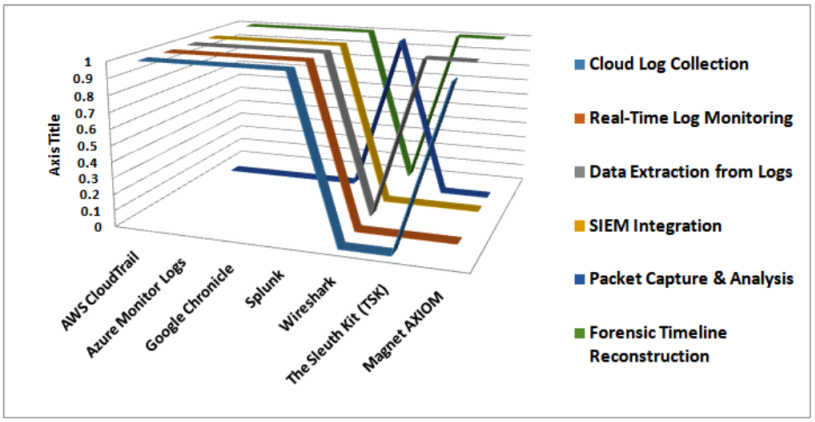


Figure 8: Feature-wise comparison of Log & Data Extraction for Cloud Network Forensics Tools

## 3.6 Domain Wise Comparison of Cloud Network Forensics

Cloud network forensic tools serve different functions based on their focus areas. AWS GuardDuty, Azure Sentinel, Google Chronicle, and Splunk excel in cloud log collection, real-time threat detection, and intrusion detection, making them ideal for cloud-based security monitoring. Wireshark and Zeek (Bro) specialize in packet-level analysis and network intrusion detection, useful for deep traffic inspection. The Sleuth Kit (TSK) and Magnet AXIOM are strong in memory and disk forensics, helping recover and analyze digital evidence. Behavioral anomaly detection is a shared strength across multiple tools, aiding in proactive threat identification.

Table 8: Comparison domain wise cloud network forensic tools

| **Domain** | **AWS GuardDuty** | **Azure Sentinel** | **Google Chronicle** | **Splunk** | **Wireshark** | **Zeek (Bro)** | **The Sleuth Kit (TSK)** | **Magnet AXIOM** |
|---|---|---|---|---|---|---|---|---|
| Cloud Log Collection | High | High | High | High | Low | Low | Medium | Medium |
| Real-Time Threat Detection | High | High | High | High | Low | Medium | Low | Low |
| Packet-Level Analysis | Low | Low | Low | Low | High | High | Low | Low |
| Intrusion Detection | High | High | High | High | Medium | High | Low | Low |
| Memory & Disk Forensics | Low | Low | Low | Medium | Low | Low | High | High |
| Behavioral Anomaly Detection | High | High | High | High | Medium | High | Low | Medium |

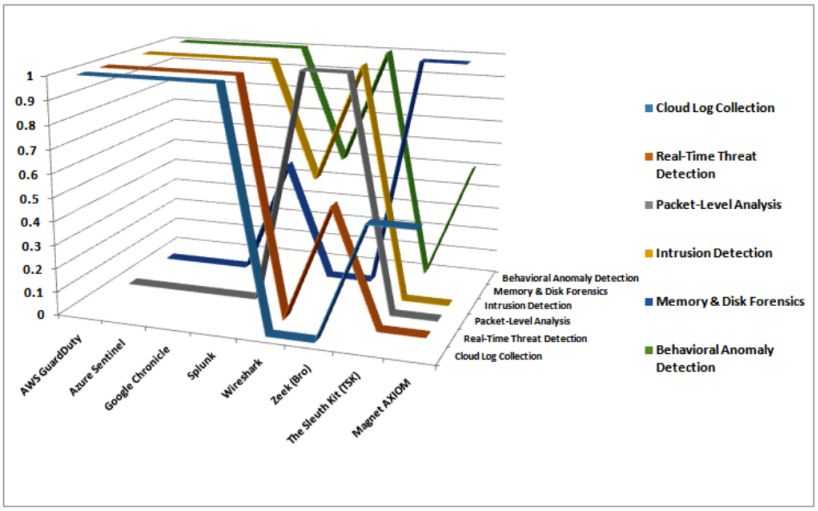


Figure 9: Domain wise cloud network forensic tools

# 4 Challenges and Future Directions of Cloud Network Forensics

## 4.1 Challenges

These different areas of cloud network forensics work together to help organizations detect, analyze, and respond to security threats and incidents within cloud environments effectively. By leveraging specialized tools and techniques in each area, organizations can enhance their ability to protect sensitive data, maintain compliance, and mitigate the risks associated with cloud based infrastructure.

Table 9: Overview of Cloud Network Forensics

| Paper Title | Challenges |
|---|---|
| Dynamic Infrastructure | Cloud environments are highly dynamic and scalable, making evidence collection and preservation challenging due to constant resource provisioning and de-provisioning. |
| Data Encryption | Encryption of data in transit and at rest within cloud environments hinders access and analysis, as decryption keys may not always be readily available |
| Multi-Tenancy and Shared Resources | Shared resources in multi-tenant cloud environments complicate investigations, making it difficult to isolate and attribute specific activities to individual users. |
| Complexity of Virtualized Infrastructure | Virtualization technologies add complexity to forensic analysis, requiring specialized tools and knowledge to examine virtualized components effectively. |
| Legal and Jurisdictional Issues | Cloud forensic investigations must navigate complex legal and jurisdictional frameworks, including data sovereignty and cross-border data transfer regulations. |
| Interoperability Challenges | Lack of standardization and interoperability among cloud service providers hinders forensic investigations due to disparate logging formats and data storage methods. |
| Emerging Technologies | The rapid adoption of new technologies like server-less computing and containerization introduces novel challenges for forensic investigators to address emerging threats. |

### 4.2 Future Directions

Cloud network forensics involves addressing emerging challenges and leveraging advancements in technology to enhance investigative capabilities. Here are some potential future directions:

- Advanced Threat Detection: Develop advanced techniques for detecting and responding to sophisticated cyber threats within cloud environments.
- Privacy-Preserving Forensics: Research and develop techniques for conducting forensic analysis while preserving user privacy and compliance with data protection regulations. This may involve methods for anonymizing sensitive data during investigation processes.
- Dynamic Evidence Collection and Analysis: Investigate methods for dynamically collecting and analyzing digital evidence in highly dynamic and scalable cloud environments. This includes developing automated tools and workflows for real-time data capture and analysis.
- Cloud-Specific Forensic Tools: Develop specialized forensic tools and methodologies tailored to the unique characteristics of cloud environments. This may include tools for analyzing virtualized infrastructure.
- Legal and Regulatory Compliance: Address legal and regulatory challenges related to cloud network forensics, including data sovereignty, cross-border data transfers, and jurisdictional boundaries. Develop guidelines and best practices to ensure compliance with relevant laws and regulations.
- Standardization and Interoperability: Promote standardization efforts and interoperable frameworks for cloud network forensics. This includes developing standardized data formats, protocols, and interfaces to facilitate cross-platform investigations and data sharing among cloud service providers.
- Digital Forensic Readiness: Enhance organizations' digital forensic readiness by developing comprehensive incident response plans, conducting regular training and exercises, and establishing forensic response teams.
- Collaboration and Information Sharing: Foster collaboration and information sharing among cybersecurity professionals, law enforcement agencies, cloud service providers, and regulatory bodies.

## 5 Conclusion

In conclusion, cloud network forensics is indispensable for maintaining the security and integrity of cloud-based systems and data in today's digital landscape. As organizations increasingly rely on cloud services, the need for effective forensic investigation and analysis becomes paramount in detecting, responding to, and mitigating security incidents. Despite the challenges posed by the dynamic nature of cloud environments, ongoing advancements in technology and collaboration efforts hold promise for enhancing the capabilities of cloud network forensics. Looking ahead, continued innovation and collaboration will be key to addressing emerging threats, refining techniques, and establishing best practices in this critical field. By investing in robust forensic capabilities and fostering cooperation across industries, organizations can better protect their cloud-based assets and ensure trust in the cloud computing paradigm.

### 5.1 Future Work

Future work in cloud network forensics will focus on developing automated tools for dynamic and scalable investigation processes. Additionally, there will be efforts to integrate advanced technologies like machine learning for real-time threat detection and response. Standardization initiatives will play acrucial role in ensuring interoperability among forensic tools across various cloud platforms. Furthermore, research will continue to explore privacy-preserving techniques to address data privacy concerns in forensic investigations. Collaboration among stakeholders will be essential for driving innovation and establishing best practices in this evolving field.

### 5.2 Limitation

Cloud network forensics faces limitations due to the dynamic and distributed nature of cloud environments, complicating evidence collection and attribution. Encryption and multi-tenancy further hinder investigations, impeding access to crucial data and complicating analysis. Moreover, the lack of standardized practices and interoperability among cloud service providers restricts the effectiveness of forensic tools and techniques.

## ACKNOWLEDGEMENT

I, B. Menaka, as the author of this review paper, express my heartfelt gratitude to the dedicated researchers and academic institutions for their valuable contributions to cloud network forensics and deep learning. I am deeply appreciative of Assistant Professor Dr. Arulselvarani for his unwavering guidance, assistance, and encouragement in ensuring the successful completion of this research work at a high standard.

## References

[1] Zhang, C., Costa-Perez, X., & Patras, P. (2024). Adversarial attacks against deep learning-based network intrusion detection systems and defense mechanisms. IEEE/ACM Transactions on Networking. https://doi.org/10.1109/TNET.2021.3137084

[2] Ojha, A. A., Thakur, S., Ahn, S.-H., & Amaro, R. E. (2023). DeepWEST: Deep learning of kinetic models with the Weighted Ensemble Simulation Toolkit for enhanced sampling. Journal of Chemical Theory and Computation. https://doi.org/10.1021/acs.jctc.2c00282

[3] Mandalapu, V., Elluri, L., Vyas, P., & Roy, N. (2023). Crime prediction using machine learning and deep learning: A systematic review and future directions. IEEE Access. https://ieeexplore.ieee.org/ielx7/6287639/10005208/10151873.pdf

[4] Ribeiro, H. V., Lopes, D. D., Pessa, A. A. B., Martins, A. F., da Cunha, B. R., Gonçalves, S., Lenzi, E. K., Hanley, Q. S., & Perc, M. (2023). Deep learning criminal networks. arXiv preprint. https://arxiv.org/pdf/2304.08457

[5] Vikas, Aggarwal, S., Himani, Yadav, A., & Kumar, P. (2023). Digital forensics in cloud computing: Techniques and challenges for investigating cybercrimes. JETIR. https://www.jetir.org/papers/JETIR2307004.pdf

[6] Xia, F., Akoglu, L., Aggarwal, C. C., & Liu, H. (2023). Deep anomaly analytics: Advancing the frontier of anomaly detection. IEEE Transactions on Knowledge and Data Engineering. https://ieeexplore.ieee.org/ielx7/9670/10111508/10111514.pdf

[7] Li, J., Wu, Z., Hu, Z., Jian, C., Luo, S., Mou, L., Zhu, X. X., & Molinier, M. (2022). A lightweight deep learning-based cloud detection method for Sentinel-2A imagery fusing multi-scale spectral and spatial features. arXiv preprint. https://arxiv.org/pdf/2105.00967

[8] Sarkar, S., Vinay, S., Djeddi, C., & Maiti, J. (2022). Classification and pattern extraction of incidents: A deep learning-based approach. Neural Computing and Applications, 34, 13559–13574. https://doi.org/10.1007/s00521-021-06780-3

[9] Shlezinger, N., Whang, J., Eldar, Y. C., & Dimakis, A. G. (2022). Model-based deep learning. arXiv preprint. https://arxiv.org/pdf/2012.08405

[10] Purnaye, P., & Kulkarni, V. (2022). A comprehensive study of cloud forensics. Archives of Computational Methods in Engineering, 29, 33–46. https://doi.org/10.1007/s11831-021-09575-w

[11] Khan, Y., & Varma, S. (2021). An evolutionary algorithmic framework: Cloud-based evidence collection architecture. Research Square. https://doi.org/10.21203/rs.3.rs-630503/v1

[12] Islam, M. S., Pourmajidi, W., Zhang, L., Steinbacher, J., Erwin, T., & Miranskyy, A. (2021). Anomaly detection in a large-scale cloud platform. arXiv preprint. https://arxiv.org/pdf/2010.10966

[13] Lathuilière, S., Mesejo, P., Alameda-Pineda, X., & Horaud, R. (2020). A comprehensive analysis of deep regression. arXiv preprint. https://arxiv.org/pdf/1803.08450

[14] Li, J., Sun, A., Han, J., & Li, C. (2020). A survey on deep learning for named entity recognition. arXiv preprint. https://arxiv.org/pdf/1812.09449

[15] Joshi, S. N., & Chillarge, G. R. (2020). Secure log scheme for cloud forensics. International Journal of Current Engineering and Technology. http://inpressco.com/category/ijcet

[16] Schlepphorst, S., Choo, K.-K. R., & Le-Khac, N.-A. (2020). Digital forensic approaches for cloud service models: A survey. In Cyber Security in Parallel and Distributed Computing (pp. 175–199). Springer. https://link.springer.com/chapter/10.1007/978-3-030-47131-6_8

[17] Sawant, A., Vanjari, A., Sahare, S., & Wasade, S. (2020). A survey on cyber forensics for securing cloud logs. International Journal of Scientific Research in Engineering and Development, 3(1), 14. http://www.ijsred.com/volume3/issue1/IJSRED-V3I1P38.pdf

[18] Sathya, A., & Mythili, M. S. (2023). Entropy state-regularized recurrent neural network-long short-term memory (ESRRNN-LSTM) and classifier for COVID-19 vaccine. Indian Journal of Science and Technology, 17(3). https://doi.org/10.17485/IJST/v17i3.2426

## BIOGRAPHIES OF AUTHORS

**Menaka B**
B. Menaka is currently a full-time Research Scholar in the Computer Science Department at Urumu Dhanalakshmi College, Trichy-19. With 15 years of extensive teaching experience at MIET Institution in Trichy (2006–2021), she has developed a strong foundation in education and research. She earned her B.C.A. and M.C.A. from Bharathidasan University and an M.Phil in Computer Science from Salem University.. She published works include the journal article "Remote Database Controller" on Wireless (2012, ISBN No: 978-3-8473-7273-8) and "Short Message Services" in Data Communication Networks (2013, ISBN No: 978-3-659-34683-5). She has also authored a book on "Mobile Communications" (2021, ISBN NO: 978-93-93253-10-1), further expanding her contributions to the field. She can be contacted at email: menaka01.mphil@gmail.com.

**Arulselvarani S, Ph. D**
Head, Department of Computer Application has completed her Doctorate degree in Mother Teresa Women's University, Kodaikannal, Tamil Nadu,India(2014). Currently she is working as Assistant Professor and Research Supervisor in PG and Research Department of Computer Science at Urumu Dhanalakshmi College, Kattur, Tiruchirappalli. She has published many National and International Journals and presented papers in various conferences. She has published two books (Interactive Visual Basic and An Overview of DBMS). She has 23 years of teaching experience. She is a member in ISTE. Her area of interest includes E-Learning, Simulation,Datamining and Machine Learning,Software Engineering and DBMS.