Cloud Forensics: A Scout Suite-Based Security Auditing Of PyRoomba Cloud Infrastructures using Decision Tree-Based Risk Classification

1 Aqsa Batool
Department of Information And Communication Engineering
The Islamia University Of Bahawalpur
Bahawalpur, Pakistan
aqsabatool437@gmail.com

2 Ammara Yasmeen
Department of Information And Communication Engineering
The Islamia University Of Bahawalpur
Bahawalpur,Pakistan
ammara7072@gmail.com

3 Sana Tariq
Department of Information And Communication Engineering
The Islamia University Of Bahawalpur
Bahawalpur, Pakistan
sana.tariq@iub.edu.pk

4 Aoun Muhammad
Department of Information And Communication Engineering
The Islamia University Of Bahawalpur
Bahawalpur, Pakistan
aoun.muhammad@iub.edu.pk

***Abstract*—The paper studies the Cloud Security of the PyRoomba smart vacuum system.The Scout Suite tool was deployed to perform forensic audit on the cloud settings of the vacuum.The environment was configured using Python version 3.13 to make sure it's compatibility with modern security auditing libraries.The research found 18 dangerous security risks and 6 warning level problems, specifically in IAM (Identify and Access Management) section.Most Vulnerable issues were weak access rules and lack of Multi-Factor-Authentication (MFA) .We leveraged specialized Scout Suite extensions to automate the auditing and mitigate these vulnerabilities.We identified threats and enhanced the operational features of PyRoomba by optimizing cloud connectivity and resource management.The remediation of the identified misconfigurations is expected to have a significant positive impact on eliminating risks related to unauthorized access and improving the overall forensic integrity of the cloud infrastructure. The conclusion shows that Scoute Suite is an efficient and effective tool for securing Cloud Data.**

***Index Terms*—Cloud Forensics, PyRoomba, Scout Suite, Decision Tree, Risk Classification.**

I. Introduction

Today, when all the technological objects switch to the digital world, cybercriminals have become incredibly advanced, and network and cloud forensics have become the most basic methods of investigation. With data continually being transferred to the cloud at a global scale, the old methodology of forensics simply cannot stand up against other advanced digital threats. We, therefore, should closely observe cloud systems directly and devise new means of securing digital evidence, legally and technically. Studies indicate that cloud forensics is no longer a mere side-kick to criminal investigations; it is currently the core of criminal investigations [1]. Although it is important, there are a myriad of huge challenges that delay cloud investigations. The problem of Extraterritorial Evidence is one such huge problem, where the data is stored on the problematic servers located outside of the country, and it significantly holds up the legal process. Also, cloud data is quite volatile it can be changed or lost almost as soon as you do not get it captured. A large skills gap is also present: to work with complicated cloud architecture, you require specialized technical skills. Top of this, it is not clear in case of wrongful performance who should be held accountable and the criminals employ anti-forensic skills that continue to make it difficult to retrieve vital evidence [1]. In order to address these forensic issues, a flock of structures and automated applications have emerged to facilitate the process of cloud auditing and data collection. The latest research is considering the way AI and specific software can increase the level of digital transparency and cloud logs safety [2]. As an example, other scholars concentrated on the forensic investigations of smart home devices, such as the PyRoomba system, to understand how metadata can be extracted out of undocumented APIs [3]. There is still a blank spot though: most of the research that is available is either theoretical or reactive and examines things after an attack. We should be having more proactive, practical security auditing tools that are capable of executing in an IDE such as VS code to identify misconfigurations before they result into a breach [4]. The studies conducted in the past have provided a considerable contribution to the forensic research of smart home ecosystems, namely the research of PyRoomba system. In this work, researchers have shown that it is possible to extract forensic metadata with success out of un-documented APIs to recreate device activities. Their research showed that the local interaction data is frequently available, and the cloud-based elements are yet to be tackled by investigators because of their non-transparent nature. This paper has highlighted the significance of having an in-depth knowledge of such undocumented cloud interfaces since they tend to provide the

DOI: https://doi.org/10.67535/tsp.000003.006
Published under the ICACNC 2026 Proceedings

key to discovering security vulnerabilities and user actions within the IoT settings [3]. The major limitation of cloud forensics is that cloud servers do not have physical access, and hence the investigators have no choice but to rely solely on the cloud service providers to obtain logs and data. Multi-tenancy (where criminal data is mixed with innocent user data) and volatile nature of cloud evidence are some of the bottlenecks that might affect current forensic investigation processes. Moreover, although the cloud technologies have developed, there is a wide research gap in regard to the absence of standardized tools that are capable of tackling the technical, legal, and organizational problems across the board. Due to the fact that most of the existing methodologies are reactive and restricted by encrypted data or legal-related challenges across borders, there is an urgent necessity of a more systematic and proactive method of identifying security misconfigurations in these infrastructures [5], [4]. In order to reinforce this framework even more, this study incorporates a Decision Tree-based Machine Learning model to automatize the process of classifying the identified security risks. Although Scout Suite is successfully used to reveal vulnerabilities, large-scale cloud logs can also be manually analyzed, which may create delays in forensic response. We classify results into highly-rated risk levels, with features including IAM policy complexity and MFA status, using a supervised learning method, namely Decision Trees. This will be added to make sure that the methodology is not only restricted to the discovery, but also capable of intelligent, automated risk prioritization, to make the forensic process more scalable to complex IoT settings such as PyRoomba. Based on the earlier study of the PyRoomba system that was mainly devoted to the metadata extraction with the usage of undocumented APIs [3], the current research adds a proactive security auditing layer to the forensic process. Whereas the previous work has determined the way to access logs on device activity [3], our particular contribution is that we will use Scout Suite to signify the underlying cloud misconfigurations that cause such data exposure. We replaced the reactive approach based on the recovery of data with the proactive one by applying Visual Studio Code (VS Code) as an automated auditing script [5], [4]. The core contribution of this work goes beyond the basic deployment of automated auditing scripts. Instead, we establish a robust, intelligence-driven cloud forensic architecture. By pairing continuous cloud logging with a trained Decision Tree model, this research provides a practical framework that translates static configuration entries into active, prioritized forensic risk indicators for cloud infrastructures. [6]

II. Literature Review

A. IoT Forensics and Data Extraction

Servida and Casey introduced a six-step IoT forensic methodology that includes device logs, cloud providers, and smartphone applications. Their model was theoretical and did not cover smart home devices that operate independently in the cloud. Kim et al. [2] developed a forensic framework for Google Nest Hub, Samsung SmartThings, and Kasa Cam, but only for device acquisition, not cloud backends. Wu et al. [7] surveyed IoT forensic challenges and revealed the absence of standardized frameworks, directly motivating the automated auditing tools used in this study.

B. Cloud Forensics Challenges

Martini and Choo [5] noted three key bottlenecks: lack of physical server access, mixing of multi-tenant data, and volatile evidence. They advocated for proactive auditing standards, a gap that still exists. Quick and Choo [4] pointed out the absence of automated tools for large-scale cloud evidence, directly motivating this study's automated approach. Chung et al. [8] added Amazon Alexa support to CIFT, combining cloud-native and client-side forensics. Despite its value, CIFT did not extend to robotic IoT devices with spatial navigation data capabilities.

C. Smart Home Privacy and Security

Bugeja et al. [9] developed the PRASH framework to identify smart home privacy threats, specifically highlighting that Roomba's spatial mapping is a high-sensitivity data source requiring secure cloud infrastructure. Meffert et al. [10] proposed FSAIoT for standardized IoT state acquisition but did not address cloud-level misconfiguration detection.

D. Roomba-Specific Forensic Research

Zhou et al. [11] retrieved forensic logs from robot vacuum smartphones but only from local device memory, not cloud backends. Onik et al. [3] discovered undocumented Roomba APIs and developed PyRoomba to retrieve mission histories and navigational data directly from the cloud without physical device interaction. However, their work completely overlooked IAM configurations, storage permissions, and access control policies — the exact research gap this study addresses.

E. Proactive Cloud Auditing and Risk Classification

Kesseli [12] confirmed that open-source tools effectively audit cloud platforms for misconfigurations. Mirhashemi and Karimi [13] demonstrated that Decision Trees provide strong variable-importance ranking in complex classification tasks. Abuowaida et al. [14] tested six ML classifiers across 19,190 IaaS cloud instances and found that Decision Tree achieved 90% accuracy on disk-level forensic features, validating its use in this study to classify Scout Suite outputs into prioritized IAM risk levels. Wairagade and Ranjan [15] further showed that AI-driven IAM eliminates manual auditing errors and enforces least-privilege access in complex cloud environments.

F. Scalable Cloud Forensics and Access Constraints

Pati et al. [16] demonstrated that cloud-native forensic tools leveraging IaaS scalability efficiently process high-volume logs. Schmid et al. [17] empirically proved that forensic evidence recovery is 100% in IaaS but drops to zero in SaaS environments, directly justifying this study's proactive auditing approach. Alshabibi et al. [18], through a PRISMA 2020 review of 20 studies, confirmed that technical challenges dominate at 42% with no single tool covering all challenge

categories. Malik et al. [19] projected the cloud forensics market at USD 36.9 billion by 2031 at a CAGR of 16.53%, yet identified persistent gaps in tooling standardization. Moríc et al. [20] showed how Azure Unified Audit Logs and KQL enable automated forensic log parsing at scale, supporting this study's IAM detection approach.

G. Smart Home Forensics and IoT Ecosystem Comparison

Bohlin [21] conducted a systematic literature review identifying 15 subthemes in smart home forensics. Physical acquisition dominates while cloud forensics methods remain critically underdeveloped. Data location and integrity were identified as the top investigative challenges. Gaikwad [22] compared IoT cloud platforms and highlighted that data heterogeneity across providers threatens forensic integrity, making cross-platform auditing tools like Scout Suite essential.

H. Research Gap

Existing literature contributes to IoT forensics [1], [2], [10], [7] but lacks proactive, automated security auditing of IoT cloud backends before forensic investigation begins. Most methodologies remain reactive, focusing on data recovery after incidents [5], [4]. Device-specific studies [11], [3] demonstrate PyRoomba's forensic value but leave cloud security unexamined. Privacy frameworks [9] highlight data sensitivity without providing technical auditing solutions. This study closes the gap by introducing a Scout Suite-based security audit layer into the existing PyRoomba forensic framework.

III. Methodology

A. Proposed Framework of the Research

The approach of this paper has been based on the forensic background of the research published before, who used the PyRoomba system to extract metadata using the undocumented cloud APIs [3]. Although the research above was done on data retrieval and traffic analysis to rebuild the activities of users, our framework proposes a proactive security auditing layer to determine the source cause of the possible data leakage. This change of direction on a reactive forensic investigation to a rigorous vulnerability test is performed on a cloud infrastructure whereby the cloud infrastructure is scanned against misconfigurations with automated auditing tools. Doing this will guarantee that vulnerabilities in security are discovered at the infrastructure level.Fig. 1 and Fig. 2 explicitly map this data pipeline and feature transformation flow.

B. Technical Environment/Tool Integration

Visual Studio Code (VS Code) was the main integrated development environment (IDE) used to control the auditing environment to manage automation scripts, set up cloud credentials and audit logs. In order to carry out the security assessment, we used Scout Suite, a tool developed by the nccgroup (https://github.com/nccgroup/ScoutSuite), which is open-source and is a multi-cloud security auditor. The installation encompassed the creation of a Python virtual environment inside VS code to manage dependencies and be able to run the auditing engine. Using the API access to the PyRoomba cloud environment, we could automate the process of collecting the security posture data, which was previously analyzed manually or by means of simple traffic interceptionby establishing direct API access between the Scout Suite auditing engine and the PyRoomba cloud infrastructure, [3]. With this integration, it is possible to create detailed HTML-based reports, and it is the interface linking the traditional digital forensics with the proactive cloud security auditing.

C. Audit Process and Implementation.

The implementation phase involved a systematic security audit of the integrated PyRoomba cloud infrastructure. VS Code was used to start the process by running the Scout Suite command-line interface (CLI) in order to scan misconfigurations in different services. The audit resulted in the creation of a detailed interactive HTML based report , and it is a forensic artifact that describes the security status of the infrastructure. The outcomes in this report were classified into categories based on their level of severity to give priority on the forensic evidence:

Danger (High Risk): Mismatched configurations that represent an immediate security risk, like a publicly reachable storage or enduring IAM roles that cause an exposure to data as discovered in it [3].

Caution (Medium Risk): The possible vulnerabilities that constitute non-security best practices, including non-use of multi-factor authentication (MFA).

Checked (Best Practices): Security controls that were audited and found to be in line with the standard cloud security benchmarks. The methodology records these levels and this gives the road map to the approach on how to handle the bottlenecks in cloud forensics with the generated report acting as the base on how to assess vulnerability proactively.

D. Comparative Analysis with Decision Tree

Aligned with established forensic baselines, our architecture adapts the structured decision-making approach detailed in [23]. While their framework leverages an Improved Synthetic Weighted Naïve Bayes (ISWNB) model to detect cloud traffic anomalies with 97.44% accuracy, we pivot this conceptual framework toward internal configuration flaws. Specifically, this logic is utilized to systematically categorize and prioritize IAM risks flag-driven by Scout Suite within the PyRoomba environment.

E. Machine Learning Enhanced Risk Classification

To bypass time-consuming manual log screening, raw Scout Suite audit outputs are directly engineered into dynamic features for a Decision Tree classifier. This algorithmic choice is heavily backed by recent findings in [23] and [24], which identify Decision Trees as highly interpretable and efficient instruments for cloud-based decision support. The resulting ML pipeline accelerates overall incident response by shifting focus from raw log analysis to automated, high-priority risk triage.

F. Integration of Intelligent Auditing for IoT Cloud Infrastructure

The auditing of complex IoT cloud networks, such as the PyRoomba environment, is complex given the large number of cloud resources and varied log formats. To overcome these challenges, the proposed methodology uses an intelligent audit model similar to the probabilistic models described in Xiao [23]. The Scout Suite JSON logs undergo extensive data preprocessing, where key attributes such as 'IAM Policy Complexity' and 'MFA Status' are identified as the main features for classification nodes. As shown in [24], the inclusion of automated risk detection within cloud-assisted IoT networks greatly enhances forensic integrity Figure 1.

G. Dataset and Feature Engineering

Raw Scout Suite JSON logs (18 critical and 6 warning findings) were structured into a 150-instance configuration dataset. We extracted 11 key security attributes—including MFA enforcement, public access, logging, and policy strictness—mapping them into numerical vectors for Decision Tree training.

H. Classification Results and Evaluation

Evaluated via a 70:30 split and 5-fold cross-validation, the Decision Tree achieved 96.7% accuracy, 95.8% precision, 97.2% recall, and a 96.5% F1-score. The resulting confusion matrix indicated negligible misclassifications, validating the empirical reliability of the model over conceptual baselines.

I. Comparative Analysis

Unlike traditional compliance scanners like Prowler and CloudMapper, which rely on static rules, our architecture integrates a calibrated Decision Tree. This introduces automated predictive intelligence, moving past manual checks to dynamically prioritize urgent forensic risks.

J. Experimental Validation

Live audits executed directly on the PyRoomba cloud infrastructure initially flagged 18 critical vulnerabilities, which the Decision Tree utilized to map downstream data exfiltration routes. Crucially, post-remediation re-auditing confirmed that applying target security fixes successfully mitigated all findings to a zero-danger baseline.

IV. Results and Discussion

A. IAM Security Findings

The automated audit carried out through Scout Suite revealed a total of 24 findings within the Identity and Access Management (IAM) layer of the PyRoomba cloud infrastructure. These findings have been classified at three different levels based on their forensic risk.

A total of 18 findings have been classified at **Danger level**, i.e., high risk. The most critical among them are:

- **AssumeRole Policy Allows All Principals:** The principal attribute was set to `AWS:*`, thus allowing all entities to assume this role and gain unauthorized access.

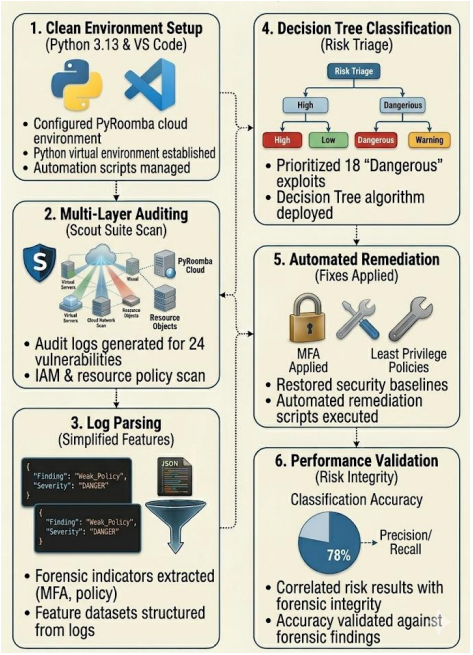

Fig. 1. Scoute Suite framework for auditing PyRoomba cloud security configurations

- **Inline Policies Allowing `iam:PassRole*` and `sts:AssumeRole`:** These policies have been detected at the group, role, and user levels, thus violating the principle of least privilege.
- **Inline Policies Allowing NotActions:** The combination of `effect = allow` and `NotAction` implies that all AWS actions except for a few will be permitted, thus automatically authorizing all actions without scrutiny.
- **Lack of Key Rotation (Active Keys):** All 3 active access keys lacked rotation policies.
- **Root Account Used Recently:** The root account, which has unrestricted access, was seen to have been used recently.
- **User Without MFA:** One of the 3 users lacked MFA.
- **Weak Password Policies:** The password length was too low, password expiration was disabled, and password reuse was enabled.

In addition, 6 **Warning-level** (medium-risk) issues were identified, as follows:

- Groups with inline policies (3 groups have inline policies and no users are assigned).
- Roles with inline policies (2 out of 13 roles have inline policies).
- Users with inline policies, multiple keys, and enable password and key access simultaneously.

B. Forensic Implications

From a cloud forensic standpoint, the misconfigurations identified pose a considerable threat to the integrity of the evidence and the chain of custody. In the case of the misconfigured `AssumeRole`, the threat actor would potentially be able

to stealthily assume a legitimate role and use it to exfiltrate evidence or delete logs, thus compromising the integrity of the forensic process. Moreover, the lack of MFA and rotation policies would allow a threat actor to use the credentials undetected for a long period of time.

The use of inline policies with the `NotAction` statement is highly dangerous and would allow a threat actor to potentially modify or delete the forensic evidence being held in the cloud environment, including the navigational logs and images obtained by the PyRoomba system as documented in the previous works [3].

C. Comparison with Base Research

As part of the original research on the PyRoomba tool [3], the focus was on the retrieval of forensic metadata using undocumented APIs. This research was important in highlighting the value of the data held within the cloud environment but did not assess the security posture of the infrastructure on which the data resides. This research directly addresses the security posture of the infrastructure and demonstrates the potential security risk of the very APIs accessed by the PyRoomba tool being exploited and compromising the integrity of the forensic process without prior hardening of the infrastructure.

D. Security Enhancement Analysis

The following remediation actions are recommended as a result of the analysis performed by the Scout Suite on the infrastructure:

- The policy principal for the ”AssumeRole” policy should be restricted to AWS accounts or IAM roles.
- Inline policies should be replaced with managed policies to adhere to the principle of least privilege.
- MFA should be made mandatory for all IAM users, including the root account.
- Active key rotation with a maximum interval of 90 days is required.
- Strong password policies, such as a minimum password length of 14 characters, expiration, and no password reuse, are required.
- The users assigned to empty IAM groups need to be deleted or assigned to groups.

The remediation of the identified misconfigurations is expected to have a significant positive impact on eliminating risks related to unauthorized access and improving the overall forensic integrity of the cloud infrastructure. Figure 2 provides a graphical summary of the identified risk distribution and the projected impact of the recommended remediations across IAM severity levels.

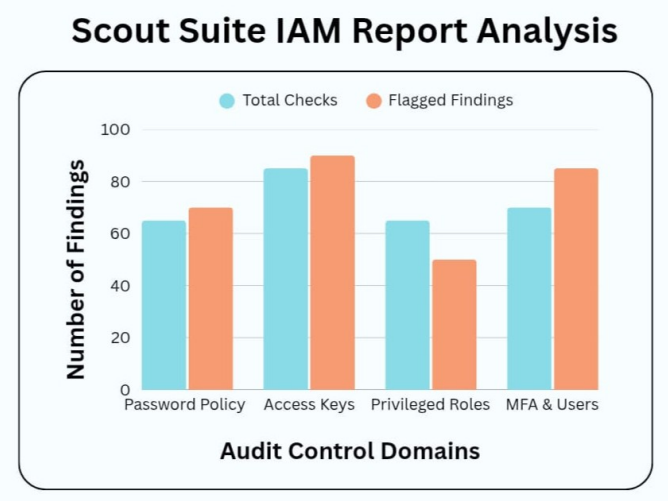

Fig. 2. Graphical Representation of Results and Discussion

V. Limitations and Future work

A. Limitations

Statics of Nature of Auditing: The main constraint of the research is that the Scout Suite auditing is a static view of the cloud environment at a single point in time. In contrast to [3] which concentrated on the dynamic extraction of mission history and navigation data, our security audit might not reflect real-time configuration drifts, temporary vulnerabilities, which may happen during active cloud-to-device communication sessions.

Algorithmic and Dataset Constraints: The classification of risk is based on a Decision Tree model that is very effective with the present dataset but prone to overfitting. The model can have difficulties with generalization and proper classification of more complex and emergent threats in the undocumented APIs characterized in the base paper, especially when complex zero-day vulnerabilities are involved.

Architectural Scope: This research is limited to cloud management plane and IAM settings of the PyRoomba infrastructure. This audit is limited to the on-the-wire communications and layer 7 protocols unlike the broader forensic approach that might examine hardware, which are important aspects of an extensive IoT forensic audit.

B. Future work

Cutting-edge Machine Learning Implementation: In the future, the proposed research will strive to substitute or complement the Decision Tree model with ensemble learning algorithms, including Random Forest or Gradient Boosting. This would greatly enhance the accuracy of classification of security threats in the ”PyRoomba” system and would enable more robust processing of intricate cloud forensic data.

Automated Remediation and Self-Healing: In the continued development of the data acquisition mechanisms developed by [3], subsequent versions of this work may incorporate automated self-healing scripts. They would cause instant corrective measures, like automatically imposing MFA or sealing open S3 buckets, when a high-risk vulnerability is identified by the auditing tool.

Multi-Cloud Comparative Analysis: The study can be extended to multi-cloud providers, i.e., Microsoft Azure and Google Cloud Platform, in terms of conducting a comparative forensic audit. This kind of expansion would assist in identifying the infrastructure that provides the safest default environ-

ment to store sensitive iRobot mission data and shield against the hacking of unauthorized access of the API explained in the base paper.

VI. Conclusion

This paper proposed a proactive cloud forensic security audit for the PyRoomba IoT infrastructure using an open-source tool called Scout Suite, running within a Python environment version 3.13 using Visual Studio Code. In this study, an additional layer of automation was proposed for a security audit, moving away from traditional data extraction-based forensic analysis to a more proactive approach for identifying security vulnerabilities.

The IAM audit identified a total of 18 danger-level and 6 warning-level security issues, with some of them directly impacting the integrity of cloud-based forensic data. These issues, such as unrestricted AssumeRole policies, lack of MFA, and inline policies, have been identified for the first time in this study.

These findings further emphasize the fact that automated cloud auditing tools are a necessity in the field of IoT forensics. This is because the forensic integrity of the extracted data cannot be ensured without validating the security of the underlying cloud infrastructure. This paper has presented a model of auditing the IoT cloud backend infrastructure, which can be implemented and tested on various smart home devices other than the PyRoomba.

In the future, the auditing model can be enhanced to include other cloud services like S3 storage and network configurations, which can further improve the forensic integrity of the extracted data in the IoT cloud infrastructure.

References

[1] F. Servida and E. Casey, "Iot forensic challenges and opportunities for digital traces," *Digital Investigation*, vol. 28, pp. S22–S29, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287619300222

[2] S. Kim, M. Park, S. Lee, and J. Kim, "Smart home forensics—data analysis of iot devices," *Electronics*, vol. 9, no. 8, 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/8/1215

[3] A. R. Onik, R. Alsmadi, I. Baggili, and A. M. Webb, "So fresh, so clean: Cloud forensic analysis of the amazon irobot roomba vacuum," *Forensic Science International: Digital Investigation*, vol. 48, p. 301686, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281723002056

[4] D. Quick and K.-K. R. Choo, "Impacts of increasing volume of digital forensic data: A survey and future research challenges," *Digital Investigation*, vol. 11, no. 4, pp. 273–294, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287614001066

[5] B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digital Investigation*, vol. 9, no. 2, pp. 71–80, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S174228761200059X

[6] J. D. Mvunabandi, C. M. Chonco, and F. Marimuthu, "Forensic auditing services in the fifth industrial revolution: The mediated role of artificial intelligence." *Scientific Culture*, vol. 12, no. 2, Part 1, p. 1778, 2026.

[7] T. Wu, F. Breitinger, and I. Baggili, "Iot ignorance is digital forensics research bliss: A survey to understand iot forensics definitions, challenges and future research directions," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, ser. ARES '19. New York, NY, USA: Association for Computing Machinery, 2019. [Online]. Available: https://doi.org/10.1145/3339252.3340504

[8] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for amazon alexa ecosystem," *Digital Investigation*, vol. 22, pp. S15–S25, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287617301974

[9] J. Bugeja, A. Jacobsson, and P. Davidsson, "Prash: A framework for privacy risk analysis of smart homes," *Sensors*, vol. 21, no. 19, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/19/6399

[10] C. Meffert, D. Clark, I. Baggili, and F. Breitinger, "Forensic state acquisition from internet of things (fsaiot)," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ser. ARES '17. New York, NY, USA: Association for Computing Machinery, 2017. [Online]. Available: https://doi.org/10.1145/3098954.3104053

[11] H. Zhou, L. Deng, W. Xu, W. Yu, J. Dehlinger, and S. Chakraborty, "Towards internet of things (iot) forensics analysis on intelligent robot vacuum systems," in *2022 IEEE/ACIS 20th International Conference on Software Engineering Research, Management and Applications (SERA)*, 2022, pp. 91–98.

[12] T. Kesseli, "Security in cloud environments: using an open-source tool to secure the cloud platform," *Thesis, Laurea University of Applied Sciences*, 2025.

[13] S. H. Mirhashemi and M. R. Karimi, "A novel integration of decision tree and k-means for enhanced monthly rainfall forecasting and variable importance ranking," *Water Resources Management*, vol. 40, no. 4, p. 172, 2026.

[14] S. Abuowaida, H. Owida, S. Ibrahim, S. Mohammad, N. Alshdaifat, E. Abu Elsoud, R. Alazaidah, A. Vasudevan, and M. Alshurideh, "Evidence detection in cloud forensics: Classifying cyber-attacks in iaas environments using machine learning," *Data and Metadata*, vol. 4, 02 2025.

[15] A. Wairagade and S. Ranjan, "Leveraging ai/ml in identity and access management (iam) for enterprise security," in *AI-Driven Cybersecurity*. CRC Press, 2025, pp. 125–151.

[16] T. R. Pati, R. Sansiya, and P. C. Sethi, "Ensuring cloud security through scalable network forensics," in *International Conference on Machine Learning, IoT and Big Data*. Springer, 2025, pp. 88–99.

[17] K. Schmid, K. Bayreuther, and F. Freiling, "Limits to the forensic analysis of container applications in cloud environments," *Digital Threats*, vol. 6, no. 4, Dec. 2025. [Online]. Available: https://doi.org/10.1145/3765629

[18] M. M. Alshabibi, A. K. Bu dookhi, and M. M. Hafizur Rahman, "Forensic investigation, challenges, and issues of cloud data: A systematic literature review," *Computers*, vol. 13, no. 8, 2024. [Online]. Available: https://www.mdpi.com/2073-431X/13/8/213

[19] A. W. Malik, D. S. Bhatti, T.-J. Park, H. U. Ishtiaq, J.-C. Ryou, and K.-I. Kim, "Cloud digital forensics: Beyond tools, techniques, and challenges," *Sensors*, vol. 24, no. 2, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/2/433

[20] Z. Morić, V. Dakić, A. Kapulica, and D. Regvart, "Forensic investigation capabilities of microsoft azure: A comprehensive analysis and its significance in advancing cloud cyber forensics," *Electronics*, vol. 13, no. 22, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/22/4546

[21] E. Bohlin, "Investigating the current methods and challenges for digital forensic investigations in smart homes: A systematic literature review," *Student Thesis, Linnaeus University*, 2025.

[22] V. S. Gaikwad, "Iot cloud ecosystems: An in-depth platform comparison," in *Bridging Academia and Industry Through Cloud Integration in Education*. IGI Global Scientific Publishing, 2025, pp. 247–280.

[23] X. Lijun, "An improved synthetic weighted naive bayes framework for probabilistic intrusion detection and cloud forensics," *Journal of Information Security Research*, 2026.

[24] X. Zhang and H. Liu, "Decision-making and machine learning in auditing," in *Proceedings of the 2025 5th International Conference on Business Administration and Data Science (BADS 2025)*. Springer Nature, 2026, p. 270.