Investigating Advanced Persistent Threat Tactics in Cloud Environments: A Forensic Study of AWS CloudTrail Log Data

Adeolu Opeyemi Ojo[1]; Mohammed Benmubarak[2]

[1;2]University of Greater Manchester, Deane Road, Bolton, BL3 5AB, UK

Publication Date: 2025/08/07

Abstract: The focus of this study is to identify and reduce Advanced Persistent Threats (APTs) in the cloud environment of Amazon Web Services (AWS). Popular security frameworks like MITRE ATT&CK, Cyber-Kill Chain and Pyramid of Pain were employed to improve effectiveness of forensic investigation in cloud environments. Tactics, techniques and procedures (TTPs) using Cloud Trail log data were analyzed in order to discover the efficiency of these frameworks in attack patterns identification. Findings from the study reveals that logs are crucial for identifying attack trends such as lateral movement, exfiltration of data, escalation of privileges in order to help improve understanding and analysis of APT activities in AWS environment, and the integration of frameworks such as MITRE ATT & CK, Cyber-Kill Pains and Pyramid of Pain provides strategies that are proactive to quelling advanced cyber adversaries

Keywords: *Forensic Analysis, CloudTrail, Advance Persistent Threats (APTs), Amazon AWS, Cloud, MITRE ATT&CK, Cyber Kill Chain, Pyramid of Pain.*

How to Cite: Adeolu Opeyemi Ojo; Mohammed Benmubarak (2025) Investigating Advanced Persistent Threat Tactics in Cloud Environments: A Forensic Study of AWS CloudTrail Log Data. *International Journal of Innovative Science and Research Technology*, 10(7), 3170-3176. https://doi.org/10.38124/ijisrt/25jul1786

I. INTRODUCTION

It has become important to analyze the security architecture of any enterprise in this era where threats associated with cybersecurity are becoming more advanced. Adoption globally of cloud computing technology has redefined how computer resources of businesses can be managed thus repositioning the information and communication technology, however advancement in cloud computing comes with huge benefits and at the same time significant risks such as losses financially, breaches of data, damage reputation and operational disruptions in the area of forensic investigation and security [1].

The need for a more informed understanding of forensic investigation associated to APT incidents is important as a result of several cloud environments migration. Most traditional tools for forensics were not initially designed for cloud environments hence creating several difficulties like evidence chronology and inherent complexities in cloud architectures for investigators [2]. Also the modern techniques and tactics used by APT actors has necessitated advanced forensics tools in order to identify and mitigate recent cyber security issues.

Through Cloud Trail logs analysis, this study intends to enhance how to investigate APTs in cloud environment such as AWS. In order to achieve this, an emulation scenario within AWS will be designed to discover, identify and analyze APT's attacks behavior using security frameworks such as MITRE ATT&CK, Cyber Kill Chain and Pyramid of Pain concurrently.

Several papers [3-11] have carried out investigations and improvements on cloud forensics. The current studies reveal several critical gaps in the domain of enhanced threat detection within cloud systems. Firstly, there is a notable lack of research that effectively integrates advanced persistent threat (APT) detection techniques with cloud forensics methodologies. Though existing studies addresses the problems associated with cloud forensics and the complexities of APT attacks, they often fail to explore the intersection of these two fields, particularly within cloud computing environments. Additionally, although various advanced threat detection methods have been developed, there is limited research on their optimal application within cloud infrastructures, especially in terms of scalability and real-world performance. Addressing these gaps through empirical studies and practical implementations will significantly enhance cloud cybersecurity practices and provide valuable insights for both researchers and industry professionals. The base paper [3], investigates the strategies employed by APT actors within Amazon Web Services (AWS) through the analysis of CloudTrail log data forensically using only the Cyber Kill Chain and MITRE ATT&CK, However, the Pyramid of Pain framework was not examined. In contrast, as mentioned earlier, this research aims to examine the behavior of APT's within AWS environments incorporating three security framework. Through a thorough examination of recent cloud forensic analysis methodologies, the development of APT emulation scenarios, and the implementation of an integrated framework. this study seeks to contribute meaningfully to the evolving field of cloud security and forensic investigation.

Section 2 introduces Advanced Persistent Threat (APT) and different techniques employed by several studies for Tactics and techniques in cloud environments, Also, it explains the concept of cloud forensics. Section 3 discusses the methodology. Results were presented and discussed in sections 4 and 5, while the conclusion and the future work were summarized in section 6.

II. LITERATURE REVIEW

Advanced threat detection techniques, cloud forensics methodology, AWS security mechanisms, and advanced persistent threats (APTs) will be covered in this section.

➢ *Advanced Persistent Threats (APTs)*

The oldest recorded attack on military research facilities occurred in the late 1980s, which is when Advanced Persistent Threats (APTs) first appeared. The phrase "advanced persistent threat" was initially used by the US Department of Defence in the late 2000s to refer to Chinese cyber-espionage attempts directed against American national security objectives. In cybersecurity, APT stands for Advanced Persistent Threat. It describes a highly coordinated and well-funded attacker, such as nation-states or elite hacker groups, launching a focused and sophisticated cyberattack. APT attacks are distinguished by their stealth, perseverance, and desire to stay hidden inside a target network for a considerable amount of time [12]. They often involve a number of stages, including data exfiltration, movement laterally, foothold establishment, reconnaissance, and exploitation.

APT as defined by the National Institute of Standards and Technology's [21] is "A well-resourced, highly sophisticated and basically a long-running cyber-attack wherein a threat actor accesses a network and remains undiscovered for a long period". It can also be defined as a kind of cybercrime that focuses on business and political targets. To succeed, APTs need to stay extremely covert for the duration of their operations. Attackers usually have longer-term aims than just making money, and even after major systems have been penetrated and their initial objectives have been accomplished, compromised systems remain operational [13].

➢ *Cloud Forensics*

Cloud forensics refers to the field of inquiry focused on crimes primarily involving the cloud. It integrates elements of small-scale digital device forensics, network forensics, and conventional computer forensics [14]. Today, law enforcement now understands that digital forensics may be used to exploit criminals in the cybercrime sector, and the field has grown in popularity. Collecting the evidence also entails using digital tools like computers, smartphones, and smart sensors that can support law enforcement investigations, the following steps are involved in the Cloud Forensics process: event identification, evidence identification, evidence collection, analysis, and interpretation [15].

Cloud computing provides individuals and organizations with an elastic and adaptable infrastructure, it has become a vital part of today's technology environment. However, because cloud forensics necessitates gathering, examining, and protecting digital evidence kept in cloud computing settings, this growth also poses new difficulties for digital forensics investigators such as the location of data, and ownership of data, encryption of data, and legal challenges [16].

➢ *Related Works*

Numerous researchers have carried out investigations and improvements on cloud forensics. [4] and [5] provides an overview of methodologies in existence and cloud forensics tools, including their inherent problems and solutions. AI and Machine Learning were proposed to enhance cloud protection in [6-8]. Hybrid intrusion detection technique that combines fuzzy analytical hierarchy processing with Bayesian classification proposed in [9], it created a clever APT-Dt-KC method for identifying and stopping cyberattacks.

An algorithm based on Double Q-learning(DQL) for APT defense was proposed in [10], which can efficiently quell the motivation of APT attackers and improve legitimacy in mobile fog computing environment. It outperforms existing methods like Q-learning, Sarsa, and Greedy algorithms. Unsupervised machine learning methods can effectively detect advanced cyberattacks, including new attack types undiscovered in training data. [11] proposes using multi-stage autoencoders for discovering APT attacks in network datasets. The multi-stage autoencoders show further improvements by adapting detection thresholds and testing on new, comprehensive datasets for APT attack detection.

According to Changwei Liu in [3] both Cyber Kill Chain and MITRE ATT & CK can be used in cloud environments to conduct forensic analyses of advanced persistent threat attacks. Findings from the study reveals that it enhances aggregation of evidence and automation of attack steps construction [3]. Though existing studies may have address cloud forensics challenges and APT attacks sophistication but they have failed to find a pivotal ground between this two fields in the context of cloud computing environments using examination of only two security frameworks (MITRE ATT & CK and Cyber Kill Chain) and excluding the Pyramid of Pain methodology. Based on this, there is lack of notable research that effectively examines three security frameworks for identification and investigation of advanced persistent threats (APT's).

III. METHODOLOGY

An experimental cloud environment was used to emulate APT scenarios in an AWS environment and evaluate the security frameworks qualitatively. AWS CloudTrail service is used for forensic data collecting. The utilization of the experimental environment and assaults demonstrates how cloud forensic examination can be advanced by combining the

Pyramid of Pain, MITRE ATT&CK and Cyber Kill Chain approaches.

➢ *Frameworks*

This section briefly defines the three frameworks used in this research below:

- *MITRE's ATT&CK –.*

This is a knowledge based model and technique that has been curated for cyber security behaviors. It reveals identifiable assault in phases and targeted platforms [18]. Version 8 of this framework addresses reconnaissance, weaponization and distribution. This model explains tactically how an attacker could achieve their goal. It is more beneficial than Cyber Kill Chain because it focuses on
indicators of compromise (IOC), tactics and strategies [17].

- *Cyber Kill Chain –*

This is a military term for the series of events that occur during an attack is the "kill chain" [16]. As the opponent progresses through their many life phases, the objective is either to protect against or take advantage of their strikes. The stages of the chain are Reconnaissance, weaponization, delivery, exploitation, installation, C&C, and actions on objectives [18].

- *Pyramid of Pain –*

This is a conceptual framework that depicts the many degrees of difficulty and expense an adversary would face in order to avoid discovery and carry out their attack. It is organized as a pyramid that classifies various indicators and attributes associated with cyber threats [19].

➢ *Research Design*

The study uses a qualitative research methodology, which captures the variety of viewpoints and difficulties surrounding cloud computing environments and digital forensics. This makes it a good fit for cloud forensic analysis. Through in-depth examination of the subjective experiences, beliefs, and actions of those engaged in cloud forensics, this method will assist in gaining important insights that may not be fully captured by quantitative methodologies [20].

The research design employs methodologies, such as assault pattern analysis and case studies. Fig. 1 details the procedures for implementing the research design.

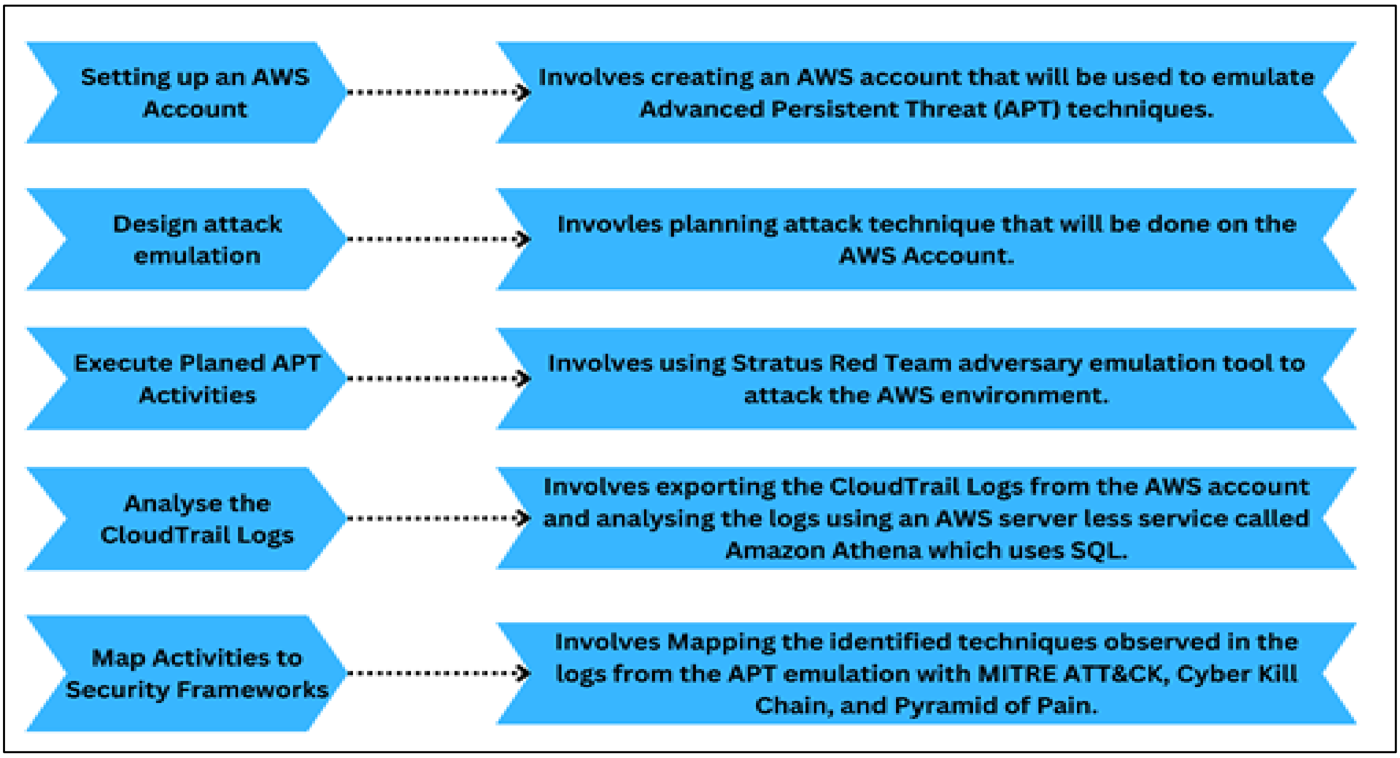
Setting up an AWS Account
Involves creating an AWS account that will be used to emulate Advanced Persistent Threat (APT) techniques.
Design attack emulation
Invovles planning attack technique that will be done on the AWS Account.
Execute Planed APT Activities
Involves using Stratus Red Team adversary emulation tool to attack the AWS environment.
Analyse the CloudTrail Logs
Involves exporting the CloudTrail Logs from the AWS account and analysing the logs using an AWS server less service called Amazon Athena which uses SQL.
Map Activities to Security Frameworks
Involves Mapping the identified techniques observed in the logs from the APT emulation with MITRE ATT&CK, Cyber Kill Chain, and Pyramid of Pain.

Fig 1 Approach for the Research Design

The methodology employed involves using an adversary emulation tool known as Stratus Red Team. This enables an AWS environment to be attacked while an API event call would be generated and documented in AWS CloudTrail.

➢ *Proposed Workflow*

This study proposes that APT groups compromise an Amazon Web Services (AWS) account by emulating Advanced Persistent Threat (APT) techniques using the Stratus Red Team cloud offensive tool, and then correlating the results of the attacks to the three security frameworks as shown in Fig. 2. The steps involved in the emulation of APT technique are described below:

- *Setting up an AWS Account:*

In order to mimic Advanced Persistent Threat (APT) strategies, such as deleting the CloudTrail path and establishing an IAM user access key, this stage entails creating an AWS account. The objective of this simulation is to mimic the actions of an attacker and provide a dataset that closely resembles real-world APT activity. This phase also involves turning on AWS

CloudTrail Logs, including Insight, Data, and Management events.

- *Design Attack Emulation:*

This step entails organizing the attack strategy that will be used on the Amazon account. This study uses a tool from DataDog called Stratus Red Team Tool. It is an offensive tool which is cloud based that uses granular and self-contained MITRE ATT&CK attack tactics [21].

- *Execute Planed APT Activities:*

In this step, the AWS environment will be attacked utilizing methods like stealing EC2 instance credentials, deleting CloudTrail trail, stopping CloudTrail Trail, and so forth, using the Stratus Red Team adversary emulation tool. CloudTrail Logs containing API calls and activity will be generated by this emulation.

- *Analyze the CloudTrail Logs:*

Logs from the CloudTrail are exported from the AWS account, then analyzed using Amazon Athena, this allows analyzes of datasets using a structured query language (SQL). Techniques used by APT attackers to compromise an AWS environment is then identified through this analyses.

- *Map Activities to Security Frameworks:*

At this stage noticeable tactics discovered in the logs from APT emulation are then correlated with the three security frameworks [20].

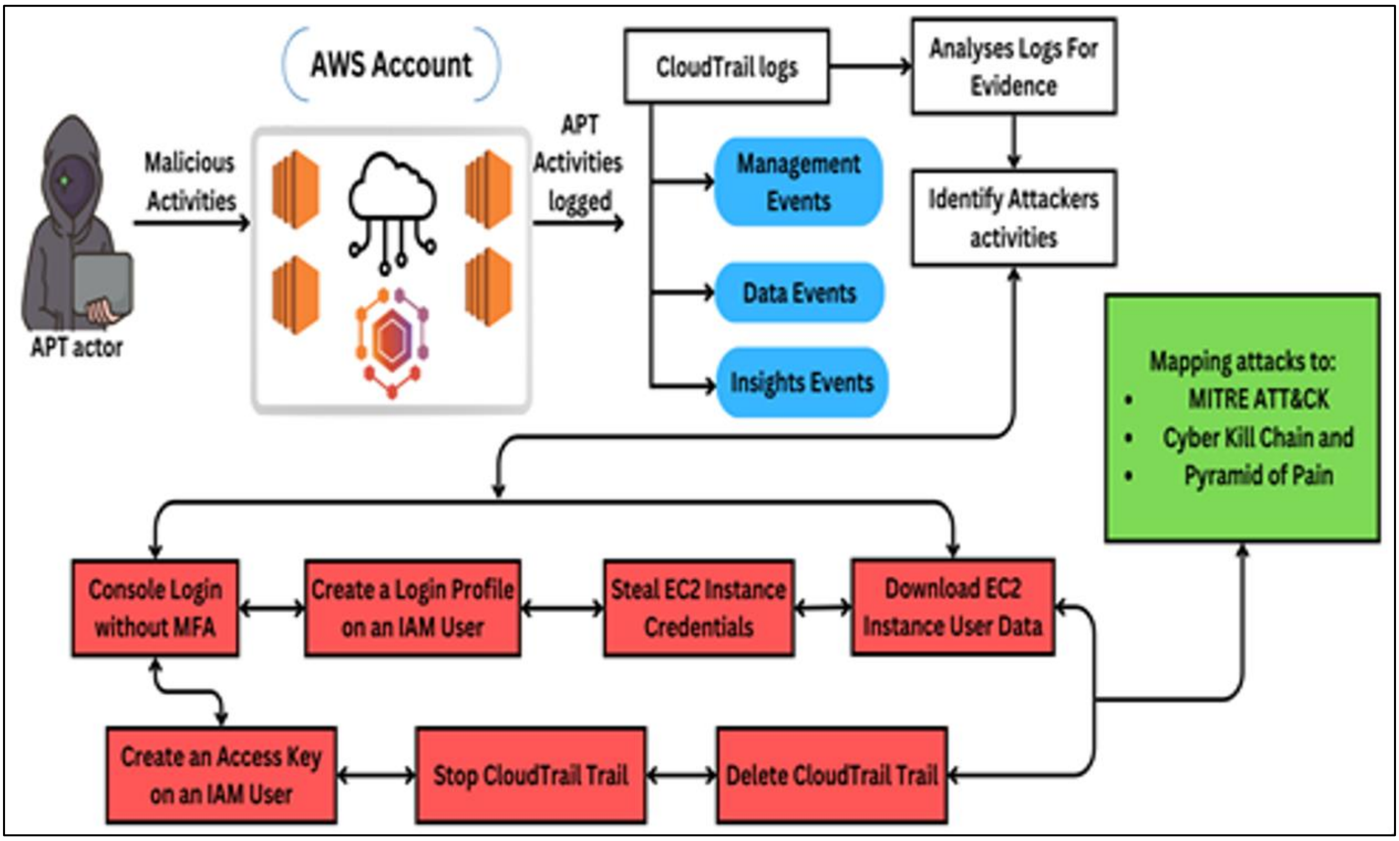

Fig 2 Proposed Workflow

IV. RESULTS

This section discusses the results discovered from the Advanced Persistent Threat (APT) emulation in terms of behavior on the Amazon web Services (AWS) environment. In order to replicate real-world APT actors, the emulation was performed by using a tool called Stratus Red Team adversary, then the findings were logged thoroughly for forensic collection of data by using CloudTrail service. After a detailed analysis of the logs, specific APT patterns and tactics identified were aligned with the three security frameworks to enhance investigations on cloud forensic.

➢ *Mapping to MITRE ATT & CK*

A total of 11 methods aiding attacker's behavior were identified and mapped as shown in Table 1.

Table 1 Mapping to MITRE Attack

MITRE Attack Tactics	Attackers Method Detected	MITRE Attack techniques
Initial Access	Creation of an administrative IAM User	Persistence & Privilege Escalation
Execution	Creation of an Access Key on an IAM User	Persistence & Privilege Escalation
Persistence	Backdoor an IAM Role	Persistence
Privilege Escalation	Exfiltration of RDS Snapshot by Sharing	Ex-filtration
Defence Evasion	Exfiltration of EBS Snapshot by Sharing It	Ex-filtration

Credential Access	Open Ingress Port 22 on a Security Group	Exfiltration
Discovery	Launching of an Unusual EC2 instances	Execution
Lateral Movement	File deletion of S3 Ransomware	Impact
Exfiltration	Stoping of an CloudTrail Trail	Defence Evasion
Impact	Deletion of CloudTrail Trail	Defence Evasion

➢ *Mapping to Cyber Kill Chain*

The study's observations of APT (Advanced Persistent Threat) activities are linked to the seven steps of Lockheed Martin's Cyber Kill Chain paradigm. They are discussed below in Table 2.

Table 2 Mapping to Cyber Kill Chain

Cyber Kill Chain Tactics	**Attackers Method Detected**
Reconnaissance	The login detail of AWS console was compromised.
Weaponization	Rather than creating a payload weaponization, the attackers might use inherent vulnerabilities in the AWS environment.
Delivery	At this stage , there was no applicable strategy used by the attacker.
Exploitation	Creation of an IAM User Access Key, an administrative IAM User and a IAM Role Backdoor.
Installation	At this stage, it was observed that attack was at the instance of launching an Unusual EC2
Command and Control (C2)	Port 22 Open Ingress was observed which could be used communicate with AWS account that was compromised.
Actions on Objectives	Sharing of RDS Snapshot through Exfiltration. Sharing of EBS Snapshot through Exfiltration. Deletion of individual file by S3 Ransomware. Stopping CloudTrail Trail. CloudTrail Trail Deletion

➢ *Mapping to Pyramid of Pain*

In order to comprehend and categorize the indicators of compromise (IoCs) connected to threat actors in the AWS environment, the attack techniques seen during the APT (Advanced Persistent Threat) simulation attack on the AWS environment were mapped to the Pyramid of Pain. As illustrated in Fig. 3, many of the techniques used by the attackers are classified as TTPs as against using artifacts.

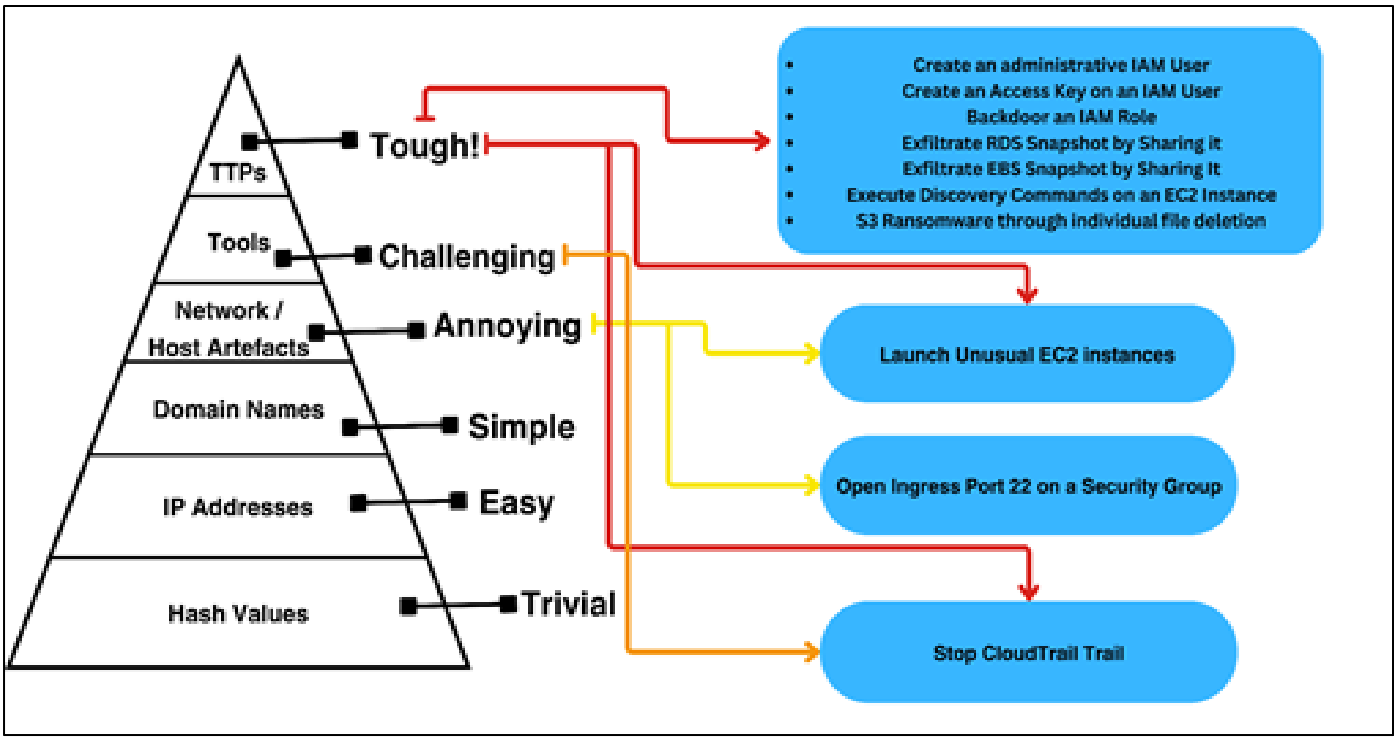
TTPs
Tools
Network / Host Artefacts
Domain Names
IP Addresses
Hash Values
Tough!
Challenging
Annoying
Simple
Easy
Trivial
Create an administrative IAM User
Create an Access Key on an IAM User
Backdoor an IAM Role
Exfiltrate RDS Snapshot by Sharing it
Exfiltrate EBS Snapshot by Sharing It
Execute Discovery Commands on an EC2 Instance
S3 Ransomware through individual file deletion
Launch Unusual EC2 instances
Open Ingress Port 22 on a Security Group
Stop CloudTrail Trail

Fig 3 Mapping Attack Methods Observed to Pyramid of Pain

- *The Mapping to the Pyramid of Pain as Shown in Figure 3 is Explained Below:*

✓ *TTPs - An administrative IAM User Creation:* This refers to a technique for management of user permissions and roles.

✓ *TTPs - An Access Key on an IAM User Creation:* Basically this refers to a strategy for managing credentials for IAM User Access.

✓ *TTPs - An IAM Role Backdoor:* This method allows persistent access through manipulation of user roles and permissions.

- ✓ *TTPs - Sharing of RDS Snapshot through Ex-filtration:* This technique uses ex-filtration of data on relational database particular to AWS environment.
- ✓ *TTPs - Sharing EBS Snapshot through Ex-filtration:* This technique uses exfiltration of data on EC2 storage peculiar to AWS environments.
- ✓ *Network/Host Artefacts*: Port 22 Open Ingress which allows connection remotely through the internet by changing configurations on the security group.
- ✓ *TTPs & Network/Host Artefacts*: Launching of an instance of EC2 which involves a method for creation of network.
- ✓ *TTPs - EC2 Instance through Execution of Discovery Commands:* This technique uses reconnaissance strategy in an AWS environment that has a compromised EC2 instance.
- ✓ *TTPs - Individual File Deletion of S3 Ransomware :* This involves targeting availability of data in S3 bucket.
- ✓ *TTPs & Tools - CloudTrail Trail Stoppage:* This involves the intent to evade detection and manipulation directly of AWS tool.
- ✓ *TTPs & Tools - CloudTrail Trail Stoppage*: This is also similar to stoppage of CloudTrail.

V. DISCUSSION

Based on mapping to MITRE attack, this study observed APT actors often acquire privileges early, maintaining their persistence and concurrently remain hidden as against the mapping to Cyber Kill Chain where attackers must pass through several stages, this allows quick facilitation in early detection and threat mitigation at any stage, while mapping to Pyramid of pain shows that actors compromise AWS environment employing TTPs and Artefacts which may be network or Host, this is possible because both technique are at the top of the pyramid thus making it difficult for APT actors to change their general method in order not to jeopardize their objectives.

This study establishes that mapping the collection of evidences in an experimental APT scenario emulation through forensic examination of logs from CloudTrail to three security frameworks, strategies and tools can be established for early detection, threat analyses and thorough comprehension of tactics, techniques and procedures(TTPs) being used by APT actors within AWS environment. The findings and implications are discussed:

- **Enhancing Cloud Forensic Methodologies** – The study advocates for integration of Pyramid of Pain, MITRE ATT & CK, and Cyber Kill Chain security frameworks in order to enhance prompt detection and understanding APT actor's behavior in cloud environments.
- **Detection of APT and Challenges -** Diverse configurations and technological dependencies are the major challenges preventing quick detection of APTs, in order to mitigate this attacks, this study recommends usage of forensic tools that has been adapted for any particular cloud platform.
- **Utilizing CloudTrail for Improved Investigations -** Through the collection of logs from CloudTrail, the study provides further insights depicting how APT actors behave in AWS.
- **Developing and Validating SQL Scripts** –The introduction of SQL scripts from logs from CloudTrail for detection is a valuable contribution thereby aiding security analysts to quickly identify severe APT actions such as escalation of privileges and exfiltration of data in real time.
- **Practical Recommendations for Cloud Security-** By advancing integration of different security frameworks and enhancing defense techniques, this study justifies the gap between theory and practice thus ensuring findings when applied to any cloud platform can help improve security.

Summarily, by mapping evidences collected to three different security frameworks, this study provides how APT actors behave in addition to their preferred methods within cloud environments, also by classifying and linking levels of Pyramid of pain to particular APT methods like IAM User creation or EC2instances, this research advances knowledge on prioritization of defense techniques based on inability to alter attack methods, however the use of Stratus Red Team tool for the emulation highlights the potential limitations and biases which may affect the accuracy of several attack scenarios. Finally, the AWS-based emulation platform might not completely denote the complexity and intricacies of real-world cloud architectures, thereby potentially limiting the findings generalizability.

VI. CONCLUSION

In conclusion, by examining Advanced Persistent Threat (APT) methods within AWS platform, mapping and linking observed patterns to established security frameworks, this research advocates for efficient defense techniques in quelling advanced cyber-attacks. Additionally, by acknowledging the shortcomings of this study which includes experimental restrictions, however the findings of this study illustrates how to identify APT actors behave and how it is very important for security experts to modify their defense techniques accordingly. Future research could further broaden this scope of this study by examining other architectures other than AWS environment in order to determine the applicability to other platforms. Also by investigating more advanced methods such as anomaly detection based on machine learning and automated response mechanisms, APT detection and mitigation skills can be designed for cloud environments.

REFERENCES

[1]. M. Irfan et al., "A framework for Cloud Forensics Evidence Collection and analysis using security information and event management," Security and Communication Networks, vol. 9, no. 16, pp. 3790–3807, 2016. DOI: 10.1002/sec.1538.

[2]. M. Herman et al., "NIST Cloud Computing Forensic Science Challenges," [Online]. Available: https://doi.org/10.6028/nist.ir.8006, 2020.

[3]. C. Liu, A. Singhal, and D. Wijesekera, 2020 "Forensic Analysis of Advanced Persistent Threat Attacks in Cloud Environments," in Proc. 16th IFIP International Conference on Digital Forensics (DigitalForensics),

New Delhi, India, 2020, pp. 161-180. DOI: 10.1007/978-3-030-56223-6_9.

[4]. K. Alattas and M. Bayoumi, "Reviewing the Existing Methodologies and Tools of Cloud Forensics: Challenges and Solutions," International Journal of Cyber-Security and Digital Forensics, vol. 9, pp. 147-154, 2020. [Online]. Available: https://doi.org/10.17781/P002677.

[5]. 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, p. 433, 2024. [Online]. Available: https://doi.org/10.3390/s24020433.

[6]. S. Myneni et al., "Unraveled — a semi-synthetic dataset for Advanced persistent threats," Computer Networks, vol. 227, p. 109688, 2023. DOI: 10.1016/j.comnet.2023.109688.

[7]. R. Abhinav, K. N. Raghav, S. S. Reddy, P. S. Koushik, S. K. Thangavel, and K. Srinivasan, "A Cloud-Based Intrusion Detection System for Advanced Threat Detection and Prevention using Machine Learning Techniques," in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2023, pp. 1-8.

[8]. P. Shanmurthy, P. Thangamuthu, B. Balusamy, and S. Kadry, "ThreatNet: advanced threat detection, region-based convolutional neural network framework," Indonesian Journal of Electrical Engineering and Computer Science, 2022.

[9]. M. Panahnejad and M. Mirabi, "APT-Dt-KC: advanced persistent threat detection based on kill-chain model," The Journal of Supercomputing, vol. 78, pp. 8644-8677, 2022.

[10]. M. Waqas, S. Tu, J. Wan, T. M. Mir, H. Alasmary, and G. Abbas, "Defense scheme against advanced persistent threats in mobile fog computing security," Comput. Networks, vol. 221, p. 109519, 2022.

[11]. H. Neuschmied et al., "APT-attack detection based on multi-stage autoencoders," Applied Sciences, vol. 12, no. 13, p. 6816, 2022. DOI: 10.3390/app12136816.

[12]. National Institute of Standards and Technology. (2014) NISTIR 7628 Revision 1: Guidelines for Smart Grid Cybersecurity. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[13]. Ghafir, I., & Prenosil, V. (2015). Advanced Persistent Threat and Spear Phishing Emails.

[14]. Mohammed, S., & Rangu, S. (2023). The cloud forensics frameworks and tools: A brief review. International Journal of Science and Research Archive, 08(01), 173–181.

[15]. Yassin, W., Abdollah, M. F., Ahmad, R., Yunos, Z., & Ariffin, A. (2020). Cloud Forensic Challenges and Recommendations: A Review. OIC-CERT Journal of Cyber Security, 2(1), 19–29.

[16]. Mandal, P., & Rajput, I. (2023). Cloud Forensics: Exploring the Challenges and Mapping Out Solutions for the Future. International Journal for Research Trends and Innovation, 8(4).

[17]. MITRE ATT&CK, "Available at: https://attack.mitre.org/matrices/enterprise (Accessed March 18, 2024)," 2022.

[18]. M. Tatam, B. Shanmugam, S. Azam, and K. Kannoorpatti, "A review of threat modelling approaches for APT-style attacks," Heliyon, vol. 7, no. 1, p. e05969, 2021. DOI: 10.1016/j.heliyon.2021.e05969.

[19]. D.T. Salim, M.M. Singh, and P. Keikhosrokiani, "A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model," Heliyon, vol. 9, no. 7, p. e17156, 2023. DOI: 10.1016/j.heliyon.2023.e17156.

[20]. Blue Report, "What Is Pyramid of Pain?" Available: https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain#:~:text=The%20Pyramid%20of%20Pain%20defines,to%20enhance%20cybersecurity%20defense%20strategies (Accessed March 5, 2024), 2023.

[21]. L. Daubner, R. Matulevičius, and B. Buhnova, "A Model of Qualitative Factors in Forensic-Ready Software Systems," in S. Nurcan, A. L. Opdahl, H. Mouratidis, & A. Tsohou (Eds.), Research Challenges in Information Science: Information Science and the Connected World, Springer, 2023, pp. 251-266.

[22]. DataDog, "Home - Stratus Red Team," [Online]. Available: https://stratus-red-team.cloud/. Accessed: 13 March 2024, 2021.