STM JOURNALS

Journal of
Network Security

https://journals.stmjournals.com/jons

ISSN: 2395-6739 (Online)
ISSN: 2321-8517 (Print)
Volume 12, Issue 3, 2024
September–December
DOI (Journal): 10.37591/JoNS

Review JoNS

CLA0D1T—Auditing AWS Services S3 and IAM

Lisshutharan Segaran[1,*], Yousif Elamin[2], Garima Sinha[3]

Abstract

The swift embrace of cloud computing has revolutionized how organizations handle and provide their services, delivering unmatched scalability, flexibility, and cost-effectiveness. However, this shift has also introduced a range of new security challenges and vulnerabilities, particularly concerning data access and identity management. This project specifically aims to address these issues within the context of Amazon Web Services (AWS), focusing on auditing the Simple Storage Service (S3) and Identity and Access Management (IAM) services. The primary objective is to identify, analyze, and prioritize potential misconfigurations in access policies and permissions, which are critical components in safeguarding networks, applications, and data storage. Through a structured and comprehensive methodology, this auditing process will systematically classify various misconfigurations, assess their severity, and propose effective remediation strategies. The audit will encompass a detailed review of access control policies, ensuring that they adhere to the principle of least privilege, and scrutinize IAM roles, policies, and permissions to detect any deviations from best practices. By evaluating the impact of identified vulnerabilities, the project will prioritize them based on the potential risk to the organization's security posture. The anticipated outcomes of this project aim to empower organizations to proactively enhance their cloud security measures, ultimately fostering a safer and more robust cloud computing environment. By addressing these critical security aspects, the project will contribute significantly to mitigating risks associated with cloud adoption and help organizations better protect their digital assets against emerging threats.

Keywords: Cloud computing, cloud security challenges, IAM, S3, auditing services, access policies

INTRODUCTION

The introduction of cloud computing has brought about a paradigm shift in how businesses operate and provide services [1]. The cloud's unparalleled scalability, agility, and cost efficiency have empowered businesses to migrate critical workloads and data to cloud environments. However, this paradigm shift towards cloud infrastructure has ushered in a new era of security challenges and vulnerabilities. The shared responsibility model in cloud computing requires collaborative effort between cloud service providers (CSPs) and their customers to secure the cloud ecosystem.

***Author for Correspondence**
Lisshutharan Segaran
E-mail: lisshu94@live.com

[1,2]Student, Department of Computer Science & Engineering, Jain (Deemed-to-be University), Kochi, Bengaluru, Karnataka, India
[3]Professor, Department of Computer Science & Engineering, Jain (Deemed-to-be University), Kochi, Bengaluru, Karnataka, India

Received Date: May 28, 2024
Accepted Date: July 12, 2024
Published Date: September 14, 2024

Citation: Lisshutharan Segaran, Yousif Elamin, Garima Sinha. CLA0D1T—Auditing AWS Services S3 and IAM. Journal of Network Security. 2024; 12(3): 1–12p.

This paradigm places a significant onus on organizations to ensure the security, integrity, and privacy of their data and applications. In this context, the core components of cloud security have risen in prominence, and among them, Identity and Access Management (IAM) and Amazon Simple Storage Service (S3) stand out as critical domains. The IAM service defines the fundamental framework of user access and permissions within the cloud, whereas S3 serves as the cornerstone for cloud storage solutions. Understanding the nuances, intricacies, and vulnerabilities within IAM and S3 services is pivotal for ensuring the security and compliance of the cloud infrastructure.

A web service that assists in securely managing access to Amazon Web Services (AWS) resources is AWS IAM. Permissions that restrict user access to AWS resources can be centrally managed using IAM [2]. When misconfigured, IAM policies, roles, and permissions can inadvertently expose sensitive data, leading to security breaches and data leaks. Moreover, the complexity of cloud environments makes it increasingly challenging to ensure that user access is appropriately configured, making auditing IAM a multifaceted endeavor.

Amazon S3, Amazon Simple Storage Service, on the other hand, provides performance, security, scalability, and data availability that are among the best in the business [3]. Every volume of data can be stored and protected for almost every use case, including data lakes, cloud-native apps, and mobile apps by clients of all sizes and sectors. However, the flexibility of S3 configurations can introduce inadvertent data exposure, making it vital to scrutinize and secure S3 buckets. Misconfiguration, whether through open permissions or incorrect storage classes, can lead to data breaches and unauthorized data access.

In response to the dynamic landscape of cloud security, the focus of this project was to conduct rigorous auditing of IAM and S3 services within the AWS cloud infrastructure. Auditing is a systematic process of evaluating and validating configurations, access controls, and security practices and emerges as a critical component of a resilient cloud ecosystem. The primary objective is to identify, analyze, and prioritize potential misconfigurations and security gaps that may exist within the IAM and S3 services.

PROBLEM DEFINITION

The rapid adoption of cloud computing has redefined the landscape of modern business operations by offering unprecedented scalability, flexibility, and cost-effectiveness [4]. However, this transition to a cloud infrastructure has brought forth a new frontier of security challenges and vulnerabilities. Organizations, entrusting their critical data and operations to cloud platforms such as AWS, face the imperative of navigating a complex terrain of potential risks. These risks encompass a spectrum of concerns, ranging from unauthorized access to sensitive data to misconfigurations that could expose vulnerabilities in cloud-based services. As organizations increasingly rely on AWS S3 (Simple Storage Service) and IAM services, ensuring the security and integrity of these components becomes paramount.

AWS S3 and IAM services play fundamental roles in cloud ecosystems. S3 serves as the cornerstone for scalable and durable object storage, accommodating vast amounts of data critical to an organization's functioning [3]. On the other hand, IAM governs access to AWS resources, providing a framework for identity management and permissions [2]. Given their central roles, misconfigurations or vulnerabilities in S3 and IAM services pose direct threats to data security, system integrity, and regulatory compliance. Organizations grapple with the challenge of comprehensively auditing these services to identify potential misconfigurations and enhance their security.

One of the primary challenges is the inherent complexity of AWS configurations, where a single misconfiguration can have cascading effects across the entire cloud environment. Misconfigurations in access policies and permissions within S3 and IAM services can result in unintended exposure to sensitive data, unauthorized access, or compromised identity management. Identifying and rectifying such misconfigurations requires a nuanced understanding of the intricacies of AWS services, making the auditing process a non-trivial undertaking. Furthermore, the dynamic nature of cloud environments introduces an additional layer of complexity, which requires continuous monitoring and adaptability in security measures.

In addition to internal security concerns, organizations must contend with an ever-expanding landscape of regulatory and compliance standards. Adhering to industry-specific regulations such as GDPR, HIPAA, or regional data protection laws is not only a legal requirement, but also a critical aspect

of maintaining trust with customers and stakeholders [4]. Auditing S3 and IAM services is integral to ensuring compliance with these standards, as misconfigurations may lead to inadvertent breaches of regulatory requirements, resulting in legal consequences and reputational damage.

The overarching problem to be addressed by this project is the need for a comprehensive auditing solution tailored to AWS S3 and IAM services. The objectives include the identification and prioritization of potential misconfigurations, the evaluation of their severity, and the proposal of effective remediation strategies. This project aims to contribute to the field of cloud security by providing organizations with actionable insights to enhance their AWS security posture, align with regulatory standards, and foster a safer and more resilient cloud computing environment.

LITERATURE REVIEW

The literature survey conducted for this report navigates the multifaceted landscape of cloud security, focusing on key elements integral to auditing the AWS cloud infrastructure. Cloud compliance audits, AWS vulnerability scanning, Amazon S3 as a robust object storage solution, and AWS IAM collectively shape the security framework within the AWS environment. This exploration delves into the objectives, best practices, and functionalities of these components, setting the stage for a comprehensive understanding of the intricacies involved in securing AWS S3 and IAM services.

The literature survey conducted by Lehtinen (2023) emphasizes the integration of automation and manual auditing techniques to comprehensively assess the functionalities, security, and cost implications of AWS [5]. This approach combines manual testing and automation for a thorough evaluation of AWS services, acknowledging the complexity and resource-intensive nature of the need for continuous monitoring, automation, and manual auditing.

Huy and Hung (2019) focus on auditing AWS services and optimizing cloud usage for cost savings within enterprises with multiple AWS accounts [6]. Their work addresses the lack of support for cost optimization in comparison to certain third-party products, such as Dome9, highlighting the importance of efficient cost management alongside security considerations.

Ismail and Islam (2020) presented a unified framework, Security Transparency and Audit Framework (STAF) to aid organizations in assessing CSPs' security for improved transparency [7]. Despite this, their work pointed out the challenge of achieving complete automation and the associated risk of human error in cloud security assessments.

Lins et al. (2016) introduced continuous auditing as a mechanism to enhance the trustworthiness and security of cloud services [8]. Their approach focuses on providing ongoing assurance through the continuous monitoring of certification criteria. However, they acknowledge the potential risk of data manipulation by CSPs, which could undermine the trustworthiness of a continuous auditing process.

Paolo Bellavista, Antonio Corradi, Luca Foschini, and Michele Solimando (2019) contributed to Audit4Cloud, an open-source platform designed for auditing public cloud provider networking performance [9]. The tool offers visibility to performance indicators and historical data, but their work highlights the challenge of potential variability in volunteer involvement for auditing, affecting consistency over time and across different geographical locations. This variability may affect the reliability of the auditing process.

Umar Mukhtar Ismail and Shareeful Islam (2020) highlighted the challenge of achieving complete automation in cloud security assessments [7]. CLA0D1T addresses this concern by providing a robust automated auditing framework that specifically caters to IAM policies, roles, and permissions as well as S3 bucket configurations and access policies. This targeted automation ensures a comprehensive evaluation of security postures without sacrificing depth of analysis.

Compared with the continuous auditing approach introduced by Sebastian Lins et al. (2016), CLA0D1T provides a more tailored and task-focused solution [8]. Rather than continuously monitoring certification criteria, CLA0D1T zeroes in on IAM and S3 services, offering a more specialized tool for organizations seeking precise and actionable results within the AWS environment.

While Audit4Cloud by Paolo Bellavista, Antonio Corradi, Luca Foschini, and Michele Solimando (2019) focuses on auditing public cloud provider networking performance, CLA0D1T complements such efforts by addressing security configurations and permissions, providing a holistic solution for organizations concerned with both security and performance aspects in their AWS infrastructure [9].

In essence, CLA0D1T stands out for its targeted and specialized approach, providing organizations with a dedicated tool for auditing AWS S3 and IAM services efficiently and comprehensively, thereby enhancing their cloud security posture.

RELATED WORK

Comparative analysis of tools plays a pivotal role in assessing the efficacy of auditing solutions in a cloud infrastructure. In this section, we compare "CLA0D1T," the tool developed for auditing services in AWS cloud infrastructure, with "s3audit-ts," a widely used auditing tool specifically designed for Amazon S3 services.

s3audit-ts is a notable auditing tool tailored to Amazon S3 services [10]. It primarily focuses on evaluating and reporting misconfigurations within S3 buckets, such as open-access permissions, data exposure risks, and privacy concerns. This tool offers valuable insights into the security of S3 storage, enabling users to identify and rectify critical S3 misconfiguration. Its lightweight and straightforward design makes it accessible to security practitioners and administrators, aiming to enhance the security of their S3 resources.

By contrast, "CLA0D1T" is a multifaceted auditing tool developed for auditing services within the AWS cloud infrastructure. While it includes capabilities for auditing IAM and S3 services, it extends beyond S3 auditing and encompasses a broader range of AWS services. The tool was designed to automate the auditing processes for IAM policies, roles, permissions, and S3 bucket configurations. This comprehensive approach ensures that both IAM and S3 storage are audited for security vulnerabilities and misconfigurations.

When assessing the two tools, it is evident that s3audit-ts excelled in auditing Amazon S3 services, providing granular insights into S3 misconfigurations. It serves as a valuable asset for organizations primarily concerned with S3 storage security. In contrast, "CLA0D1T" offers a more holistic approach by not only auditing S3 but also IAM services and potentially other AWS services. It presents a versatile solution for organizations seeking comprehensive auditing of their AWS cloud infrastructure, covering identity management, storage security, and potentially more services (Table 1).

Table 1. Related work comparison.

Comparison	s3audit-ts	CLA0D1T
Focus	Primarily focused on auditing Amazon S3 configurations, permissions, and related security aspects	Audit a broader scope of AWS services, including S3, IAM, and potentially other services.
Functionality	Analyzes S3 bucket configurations, access policies, and permissions to identify security misconfigurations	Assess S3 configurations and permissions, auditing IAM configurations, policies, roles, and user permissions, and may include auditing of other AWS services.
Scope	Limited to auditing Amazon S3	Comprehensive auditing for Amazon S3, IAM, and potentially other AWS services.

METHODOLOGY

The methodology for this research project was structured to comprehensively audit services within the AWS cloud infrastructure, with a primary focus on IAM and S3 services, as shown in Figure 1.

The method begins with project initiation and definition phases. During this stage, we laid the foundation by clearly defining the project's objectives and specifying the AWS services targeted for auditing. This initial step ensures that the project's direction is well-established and aligned with its goals.

Once the project is initiated and objectives are defined, we proceed to the automating and conducting audit phase. We employ "CLA0D1T," a specialized auditing tool, to automate the auditing processes for IAM and S3 services. Automation enhances the efficiency and accuracy of auditing, ensuring that configurations, access policies, and permissions are systematically reviewed and assessed [11].

Following the automated audits, we entered the validation and extension phases. The focus is on validating the results generated through automation to ensure accuracy and completeness. Simultaneously, we extend the scope of our auditing efforts to encompass additional AWS services beyond IAM and S3. This extension allows for a more comprehensive evaluation of the AWS cloud infrastructure, adapting it to the evolving service landscape.

The subsequent step is to manually verify the results and assess the vulnerabilities. While automation is powerful, manual analysis is essential to validate the findings and address the nuances that automated tools might overlook. This verification phase adds an extra layer of scrutiny to ensure the reliability of audit results.

The methodology includes a prioritization and mitigation stage to effectively address the identified issues and vulnerabilities. The audit findings are assessed based on severity, potential business impact, and likelihood of exploitation. This prioritization informs the development of mitigation strategies and recommendations that are critical for remedying identified security weaknesses.

The final step in the methodology is the documentation and reporting phase. Here, the project's findings, audit results, risk assessments, prioritized issues, and mitigation recommendations were systematically documented. A comprehensive assessment report is prepared, which not only serves as a record of the audit but also provides valuable insights and guidance for stakeholders and decision-makers.

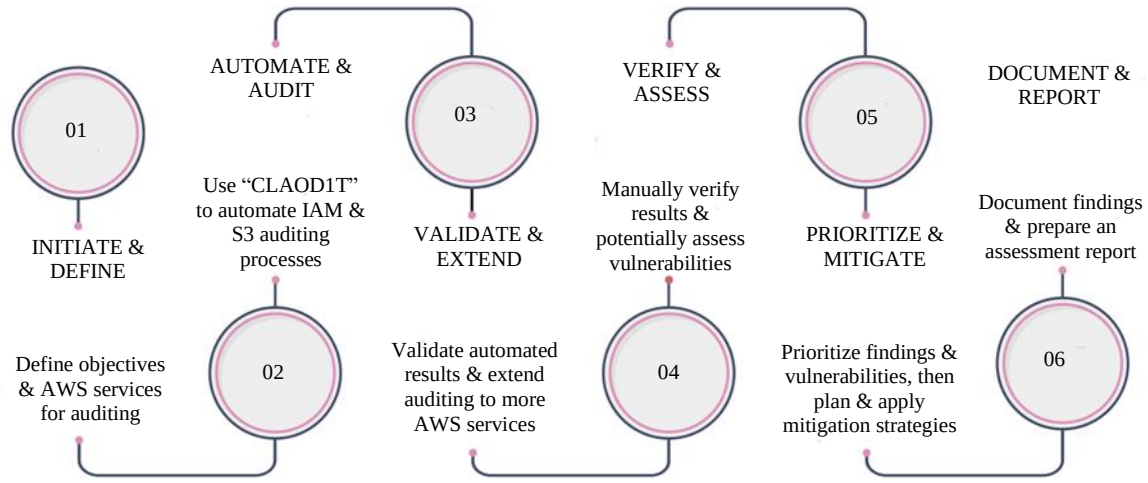

Figure 1. CLA0D1T methodology.

PROPOSED WORK

The CLA0D1T workflow was designed to streamline and enhance the processes involved in managing cloud-based services, ensuring optimal performance, efficiency, and scalability. This workflow encompasses the following key areas (Figure 2):

CLA0D1T Auditing Tool

Develop and implement CLA0D1T for automated auditing processes [12]. CLA0D1T serves as the backbone of the auditing process, automating the evaluation of the IAM services and S3 buckets. CLA0D1T has automated capabilities for the analysis of IAM policies, roles, and permissions along with an in-depth examination of S3 bucket configurations and access policies. It also processed and interpreted the data for subsequent analyses.

IAM Service

Evaluation of access controls, identity management, and authentication mechanisms [2]. IAM services are audited to identify and rectify misconfigurations related to unauthorized access and privilege escalation. Capabilities include the examination of IAM policies and user data as well as the analysis of permissions associated with IAM roles.

S3 Service

The objective is to review the security configurations for AWS S3 services, to assess S3 bucket configurations to identify misconfigurations and inadequate security settings [3]. Capabilities encompass the scrutiny of S3 bucket configurations and the analysis of permissions and access policies for S3 buckets.

Analysis Engine (Processing)

The objective was to process and interpret the data collected by CLA0D1T for detailed analysis. Functionality involves utilizing the analysis engine to interpret the automated results and extract meaningful insights. Capabilities include the aggregation and correlation of IAM and S3 auditing data as well as data normalization for efficient analysis.

IAM Policies, Permissions, User Data

The objective was to collect and analyze IAM policies, permissions, and user data. The functionality encompasses evaluating IAM policies for potential misconfigurations, assessing permissions, and analyzing user data. Capabilities include the identification of excessive permissions and the examination of user attributes and access patterns.

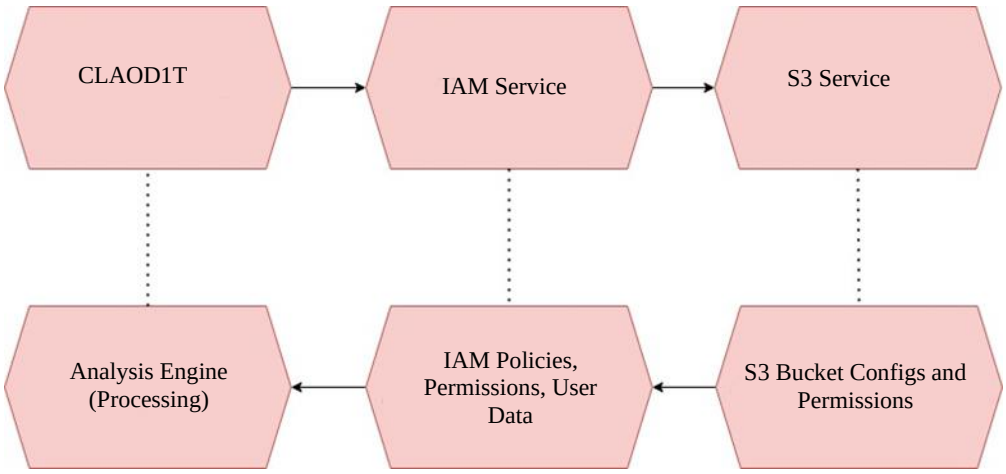

Figure 2. Representation of CLA0D1T workflow.

S3 Bucket Configs and Permissions

The objective was to collect and analyze S3 bucket configurations and access permissions. The functionality involves scrutinizing S3 bucket configurations for vulnerabilities and assessing access permissions. Capabilities include the detection of public or misconfigured S3 buckets and the analysis of access policies associated with S3 buckets.

Integration

The proposed system seamlessly integrated CLA0D1T into the IAM and S3 auditing processes. CLA0D1T acts as a unified auditing solution, automating the assessment of the IAM policies, roles, and S3 bucket configurations. The analysis engine processes the collected data, allowing for a holistic examination of security postures and facilitating strategic decision-making based on audit outcomes. This integrated approach ensures a thorough and efficient auditing process and enhances the overall security of the AWS cloud infrastructure.

IMPLEMENTATION

The architecture of the auditing tool, CLA0D1T (Cloud Audit Tool), was designed as a Command Line Interface (CLI) tool, providing a powerful and streamlined solution for checking misconfigurations and enhancing security settings within the client's AWS environment (Figures 3–5).

The key components of the architecture are:

Command Line Interface

CLI serves as the primary interface for users to interact with the CLA0D1T. Users initiate audits, configure parameters, and view the results through a text-based interface, making it efficient for automation and scripting. Python's Argparse or Click library was used to build a robust and user-friendly CLI.

Auditing Engine

The Auditing Engine forms the core of CLA0D1T and is responsible for interacting with AWS services and collecting data related to the IAM and S3 configurations. It implements automated checks to identify misconfigurations and assess security vulnerabilities. Boto3, the AWS SDK for Python, was employed for seamless communication with AWS services (Figure 6).

IAM Auditing Module

The IAM auditing module focuses on auditing IAM configurations, checking policies, roles, and user permissions, and ensuring access control compliance [13]. Boto3 was used for IAM API interactions and Python was employed to process IAM-specific data (Figure 6) [14].

S3 Auditing Module

The S3 Auditing Module is dedicated to auditing Simple Storage Service (S3) configurations and examining bucket settings, access policies, and encryption configurations for security adherence [15]. Boto3 was utilized for S3 API interactions and Python was employed for processing S3-specific data (Figure 7) [14].

Analysis Engine Module

The Analysis Engine Module processes raw data collected by the Auditing Engine, applies analysis algorithms, and categorizes findings based on severity levels, thereby enabling the prioritization of vulnerabilities. Python was used for data analysis and processing.

Reporting Module

The Reporting Module generates detailed reports based on the analysis conducted by the analysis engine. Reports are presented at the CLI, providing users with actionable insights. Text-based formatting within CLI and Python was used for report generation.

Figure 3. CLA0D1T CLI tool (S3 Audit).

Figure 4. CLA0D1T CLI tool (IAM Audit).


```
{
    "AccountAliases": [],
    "AccountAuthorizationDetails": {
        "GroupDetailList": [],
        "Policies": [
            {
                "Arn": "arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy",
                "AttachmentCount": 1,
                "CreateDate": "2018-02-22 21:24:25+00:00",
                "DefaultVersionId": "v12",
                "IsAttachable": true,
                "Path": "/aws-service-role/",
                "PermissionsBoundaryUsageCount": 0,
                "PolicyId": "ANPAJH4QJ2WMHBOB47BUE",
                "PolicyName": "AWSTrustedAdvisorServiceRolePolicy",
                "PolicyVersionList": [
                    {
                        "CreateDate": "2024-01-18 16:25:15+00:00",
                        "Document": {
                            "Statement": [
                                {
                                    "Action": [
                                        "autoscaling:DescribeAccountLimits",
                                        "autoscaling:DescribeAutoScalingGroups",
                                        "autoscaling:DescribeLaunchConfigurations",
```


Figure 5. output.json file (IAM Audit Output).

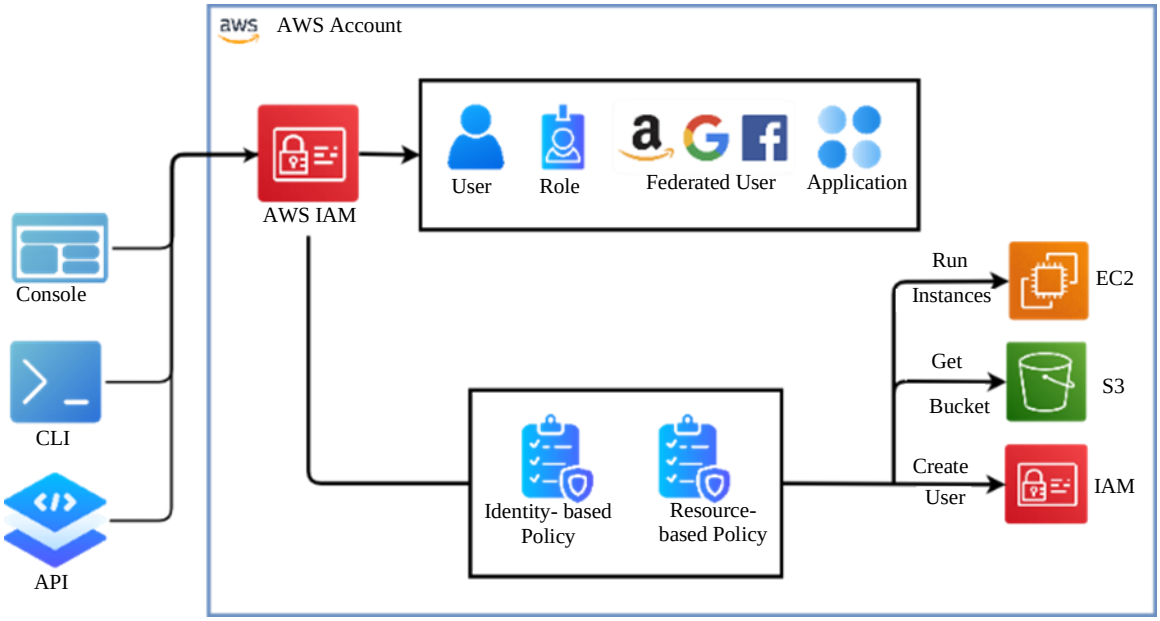

Figure 6. IAM overview [13].

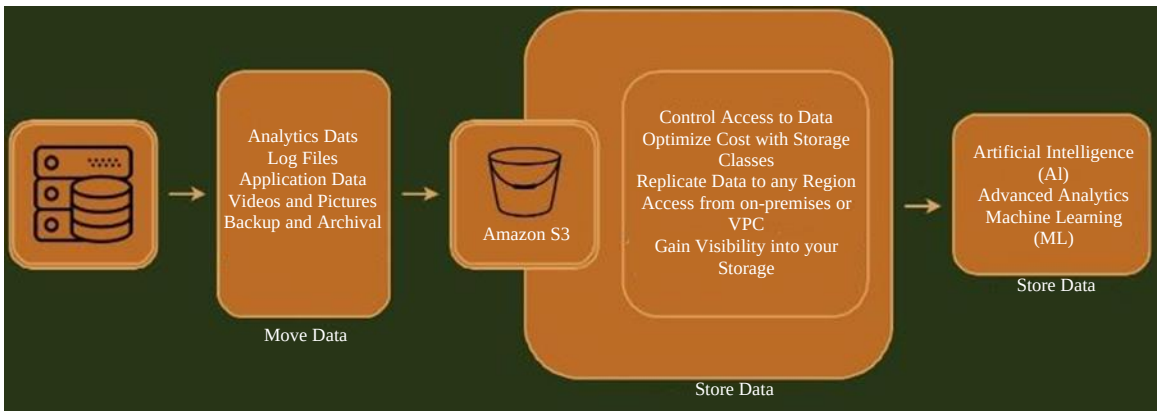

Figure 7. S3 overview [15].

Security and Compliance Integration

This component integrates security and compliance frameworks to ensure that audit checks align with the industry standards. This provides a comprehensive security assessment. Integration of APIs and Python modules was employed for compliance checks.

Database

The database stores configuration data, audit results, and historical data for trend analysis. It facilitates data retrieval for reporting and supports continuous monitoring. A scalable and secure database solution, such as SQLite or a lightweight database, has been employed for data storage.

Workflow

Users initiate an audit through CLI, configure parameters, and specify the scope of the audit. The Auditing Engine triggered to interact with AWS services, collecting data related to IAM and S3 configurations. The IAM and S3 Auditing Modules process specific configurations, conduct checks, and gather relevant data. The Analysis Engine Module processes raw data, evaluates the findings, and categorizes misconfigurations based on severity. The Reporting Module generates detailed reports within the CLI, presenting the identified misconfigurations, their severity levels, and suggested remediation strategies. Users access reports and results within the CLI, thereby gaining insights into the security posture of the IAM and S3 services. This tool supports continuous monitoring, allowing users to schedule and automate periodic audits for proactive security management.

Security Measures

Secure communication channels and data encryption are implemented to protect sensitive information during transit. Access to the tool and its components is managed through IAM roles following the principle of least privilege. A comprehensive audit trial is maintained within the CLI, documenting user actions, audit configurations, and accountability and traceability results.

CONCLUSION

In conclusion, the audit project conducted through CLA0D1T has been instrumental in evaluating and fortifying the security landscape of AWS IAM and simple storage services (S3). The rapid evolution and widespread adoption of cloud computing have transformed how organizations manage their services, making robust security measures essential. The findings and analysis presented in this report shed light on critical misconfigurations and vulnerabilities within IAM and S3, offering a proactive approach to address security challenges.

The IAM auditing module meticulously examines policies, roles, and user permissions, providing a comprehensive view of access controls. Misconfigurations related to over-permissive policies or role-based access control were identified and categorized by severity. The S3 Auditing Module highlighted critical aspects of data storage, including access policies, encryption configurations, and public access settings. These insights collectively provide valuable resources for organizations aiming to improve their cloud security posture.

Future Scope

Although CLA0D1T has achieved its primary objectives, there are several avenues for future enhancements and expansions.

Machine Learning Integration

Explore the integration of machine learning algorithms to enhance the tool's ability to automatically detect anomalous patterns and potential security risks. This contributes to more advanced threat detection capabilities [16].

User-Friendly Interfaces

Develop user-friendly interfaces, including graphical representations and dashboards, to simplify the interpretation of audit results and facilitate better decision-making by security administrators.

Collaborative Security Workflows

Facilitate collaborative workflows for security teams by integrating features that allow seamless communication, documentation, and task assignment within the tool.

Scalability Enhancements

Ensure scalability to accommodate the growing complexities of cloud environments and support organizations as they expand their infrastructure and services.

REFERENCES

1. Amazon. (2023). Amazon S3. [online] Available from: https://aws.amazon.com/
2. Amazon IAM. (2023). AWS Identity and Access Management. [online] Available from: https://aws.amazon.com/iam/
3. Amazon. (2023). Amazon S3 – Cloud Object Storage. [online] Available from: https://aws.amazon.com/s3/
4. Innovatureinc. (2023). Top 10 cloud computing trends in 2023. [online] Available from: https://innovatureinc.com/top-10-cloud-computing-trends/
5. Lehtinen J. Technical Review Setup for Amazon Web Services: Assessing Amazon Cloud Computing Service Configurations. 2023
6. Huy AQ, Hung PD. Security and cost optimization auditing for Amazon Web Services. In: Proceedings of the 2nd International Conference on Software Engineering and Information Management; 2019. p. 44–48. DOI: 10.1145/3305160.3305181
7. Ismail UM, Islam S. A unified framework for cloud security transparency and audit. J Inf Secur Appl. 2020;54:102594. DOI: 10.1016/j.jisa.2020.102594
8. Lins S, Schneider S, Sunyaev A. Trust is good, control is better: Creating secure clouds by continuous auditing. IEEE Trans Cloud Comput. 2016;6:890–903. DOI: 10.1109/TCC.2016.2522411
9. Bellavista P, Corradi A, Foschini L, Solimando M. The Audit4Cloud platform for auditing the networking performance of public clouds. In: IEEE Global Communications Conference (GLOBECOM); 2019. IEEE Publications. p. 1–6. DOI: 10.1109/GLOBECOM38437.2019.9013870
10. The Scale Factory. (2019). GitHub - scalefactory/s3audit-ts: CLI tool for auditing S3 buckets. [online] GitHub. Available from: https://github.com/scalefactory/s3audit-ts.
11. CodiumAI Team. (2023). Creating powerful command-line tools in Python: A practical guide. [online] Available from: https://www.codium.ai/blog/creating-powerful-command-line-tools-in-python-a-practical-guide/
12. Episyche Technologies. (2022). How to build a CLI Tool using Python? [online] Available from: https://episyche.com/blog/how-to-build-a-cli-tool-using-python
13. Digital Cloud Training. (2022). AWS IAM. AWS Cheat Sheet. [online] Digital Cloud Training. Available from: https://digitalcloud.training/aws-iam/
14. Bohara MS. (2020). Programming AWS IAM using AWS python SDK boto3—Part 3. [online] Available from: https://medium.com/geekculture/automating-aws-iam-using-lambda-and-boto3-part-3-3100088a4454
15. Amazon. (2018). Amazon S3, Object storage built to retrieve any amount of data from anywhere. [online] Available from: https://aws.amazon.com/s3/
16. Maheta D. (2023). Python with machine learning: Make user experience interactive. [online] Available from: https://www.bacancytechnology.com/blog/python-with-machine-learning

