Automated Cloud Auditing and Remediation System

Amaravarapu Pramod Kumar[1], Cherukuri Keerthana[2], Chintala Varun Teja[3], K. Prajwala Saffronia[4] and Rajavarapu Avinash[5]

[1] Department of CSE-(CyS,DS) and AI&DS,VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India
[2] Department of CSE- Cybersecurity, VNR Vignana Jyothi Institute of Engineering and Technology,Hyderabad, India
[3]Department of CSE- Cybersecurity, VNR Vignana Jyothi Institute of Engineering and Technology,Hyderabad, India
[4]Department of CSE- Cybersecurity, VNR Vignana Jyothi Institute of Engineering and Technology,Hyderabad, India
[5]Department of CSE- Cybersecurity, VNR Vignana Jyothi Institute of Engineering and Technology,Hyderabad, India.

Abstract: A properly designed cloud deployment strategy gets its implementation handled through security posture management systems. As a defense mechanism for cloud infrastructure the *Automated Cloud Configuration Audit and Remediation System* contains built-in automation to audit and repair cloud infrastructure. A continuous set of cloud configuration checks occurs at all times through automatic repair processes that ensure compliance with existing cloud policy rules.

Multiple project components utilize their available resources to develop better security measures and decrease noncompliance incidents as they simultaneously improve operational resource management. Organizations need strong audits together with supervised remediation initiatives because they build better defensive security systems.

Safe cloud management requires the protection of every organizational security aspect which forms part of the security objective. Cloud technology development requires compliance and enactment management to establish itself as fundamental operational aspects. Organizations need to build an automated system with secure functionality that implements dynamic cloud structure through the Automated Cloud Configuration Audit and Remediation System.

Keywords: Cloud Configuration, Risk Assessment, Monitoring and Reporting, Remediation and Enforcement.

1 INTRODUCTION

Just like in today's corporate setting, with the advent of technology, businesses have transformed the manner in which the IT frameworks of an organization is maintained. It is a highly effective resource for all business types because it provides unmatched flexibility, scalability, and cost efficiency. At the same time, the exponential growth of

cloud resources has brought new complexities in the supervision and protection of cloud space. These days, misunderstandings and security flaws are some of the major issues resulting in data breaches, loss of data, as well as, violations of compliance processes. This illustrates the strong need for an effective cloud management system have in place.

In the recent years, however, the increase in the offering of the cloud services have created considerable complications in the maintenance and protection of cloud environments. Having said that, the lack of sufficient management systems in clouds, combined with the constant presence of ‘misconfiguration’, and security gaps represent some of the most dangerous culprits for data breaches, data loss, or compliance failures. Such issues indicate that there is a need for unduly effective management systems in clouds.

In terms of these issues, this research aims to create an Automated Cloud Configuration and Remediation System. This set of activities is conducted by implementing state-of-the-art machine learning, supervision, and remediation. Its main focus is the autonomous anomaly detection, configuration suspension, and ‘cloud’ continuous control. This is accomplished through bounds engineering which modifies the environment to enable reduction of human exposed errors. The goal of this project is to nurture the security of cloud environments, while easing the attainment of compliance with regulatory documents and maximum industry standards. Thorough solution needs development to handle current method flaws effectively while utilizing existing method advantages.

The Automated Cloud Configuration and Remediation Systems improves cloud security, operational efficiency, and compliance with some policies and norms. Through the use of automation, machine learning, and continuous surveillance, the technology independently finds, and fixes misconfigurations, which reduces the possibility of human error, the industry standards, and rules set by authorities are followed, all while offering full and proper accountability. It results in cost reductions, along with maximizing the allocation of manual tasks, and minimizing the need for systems' outage. Overall, this initiative builds more confidence in the cloud computing prowess and changes how businesses operate their clouds.

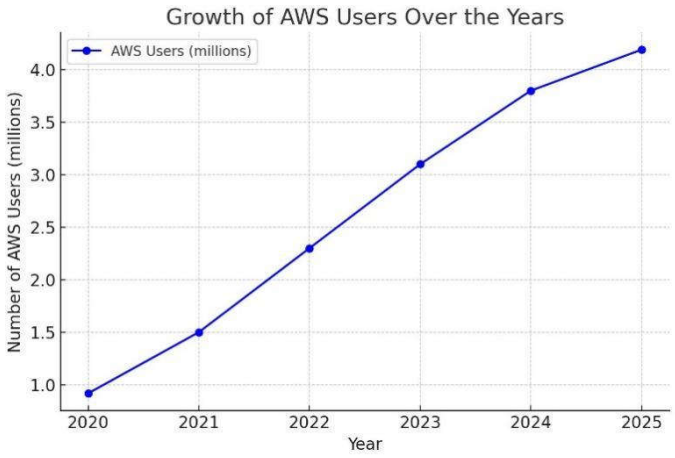

Fig. 1. AWS User Growth (2020 – 2025)

2 LITERATURE SURVERY

The swift growth of cloud computing in recent years has demanded newer, stronger security measures to safeguard shared data and meet diverse compliance mandates. Tools to "audit" the cloud and "remediate" it automatically when troubles are found have become essential in this new landscape. Yet much of the discussion around them remains rather vague. This literature review thus undertakes a straightforward exploration of some of the existing systems, their effectiveness and potential difficulties

Automated Conformity Verification Concept of Cloud Security [01] develop an advanced automated method for configuring and managing public cloud accounts and subscriptions on prominent platforms such as AWS, GCP, and Azure. This method involves the application of standardized configurations to ensure optimal performance and security compliance. Enhancing Cloud Security-Proactive Threat Monitoring and Detection Using a SIEM-Based Approach [03] includes a virtual network comprising virtual machines, load balancers, Microsoft Defender for Cloud, and an application gateway that functions as a web application firewall (WAF). This WAF scans incoming Internet traffic and provides centralized protection against common exploits and vulnerabilities, securing web applications within the cloud environment.[03]

CLAMS- Cross-layer Multi-Cloud Application Monitoring-as-a-Service Framework [05] is capable of: (a) performing QoS monitoring of application components that may be deployed across multiple cloud platforms (e.g., Amazon and Azure), and (b) giving visibility into the QoS of individual application component, which is something not supported by current monitoring services and techniques. Logs2Vul: Vulnerability Detection from Logs for CSPM [14] The framework not only indicates the vulnerability classes corresponding to cloud error logs but also computes a CVS Score (Common

Vulnerabilities Severity Score) against each error log. CVS Score indicates the seriousness of threats and thus provides key information for CSPM. The framework uses Deep Learning algorithms such as CNN, LSTM and transformers to build Machine Learning models that are trained on Cloud error logs augmented with CVE descriptions.[14]

3 SYSTEM ARCHITECTURE

Instructing You to Enter Your AWS Credentials data If you are going start the process, you need to insert your AWS credentials. This is a key bit of information to prove who they are and leverage the various products in their cloud space

• Backend Authorization : Backend now authorizes with the credentials you have sent. If there are certain discrepancies in couple of the fields, the system maybe asking you to provide your details again. Cloud environment is well confirmed with credentials, you can start post analysis to the cloud.

• Checking outside the perimeter: once logged in, you undergo perimeter check authentication. After Success, the system will review the configuration data tied to your cloud stack. This analysis involves taking the existing resources, as well as their configuration and how well they are secured.

• Producing a Security Report: As soon completion of the processing, the system arranges these findings into a well- structured security report. The document assesses any security holes, other configurations required to be done and/or if a cloud architecture is missing compliance.

• Provides Remediation Guidance: The system identifies all security defects and recommends remediations. The recommendations for remediation are grounded in common security and policy practices.

• Automated Corrective Actions: Other the system chooses to automate the remediation; it will move on with the one i defined before. This can encompass things like containment of affected assets, applying any patches or changing the security policies.

• Executing Corrections: So the system proceeds with these commands of automated fixes. In case that something does not appear to work as well during this step, the system will react by reversing the fixes and/or escalating to user.

• Monitoring Repair Rundowns and Results: The procedure monitors all acts and processes into the calendar and delivers results at the time. This is to make sure that nothing out of the ordinary has been thrown away, and also there are records needed for regulation review.

• Report: Finally, system catch all and delivers a report of the whole process being processed. It covers the initial stage of security till when the stacking measures issued and whether or not applied in the cloud, are up to date

4 METHODOLOGY

A methodological study exists to describe the design process and deployment of the Automated Cloud Configuration Audit and Remediation System. The system carries

out automatic audits along with repairs of cloud configuration problems that enhance security infrastructure and decrease security vulnerability exposure. The methodology carries out structured methods for these objectives by using automated protocols yet needs manual processes for completion.

A. Requirement Analysis and System Design

The latter was followed by the discovery of the key-system components of automated AWS cloud configuration audit. The system detects the security risks and gives automatic correction of the risks. Some of the common security misconfigurations have been discussed by security professionals using CIS Benchmarks, AWS Well- Architected Framework, learnings and best practice frameworks like PCI DSS, GDPR. Its architecture involved the mapping of data flow, communication protocols, selection of the frontend and backend technologies.

B. Cloud Interaction and Data Collection

The system talks to cloud environment safely, due to AWS SDK, and receives the information about the configuration (IAM roles, S3 buckets, security groups). The credentials get entered by a user in a secure web page and this data is fetched by the backend through the AWS APIs.

C. User Interface and Report Generation

The frontend developed using React. js, HTML, CSS, and Bootstrap can be used by its users to input AWS credentials and find the outcome of an audit. There are reported vulnerabilities and the weakness levels as well as the directions of how to fix. The buttons are termed as fix, which offer an automatic answer to the problems at hand.

D. Vulnerability Remediation

On the one hand, automation fixes are carried out such activities, as an update IAM policy, setting up security groups, and setting S3 encryption. They are made via the calls of AWS SDK and are logged. Where there is automation, where there is no provision of doing it, step by step guidance of how to handle the job manually may be given.

E. Compliance Check

The system examines the settings with regard to a range of standards which includes GDPR, HIPAA, and PCI DSS. Compliance reports ensure that any non-conformity is pended, and possible solutions that can be undertaken in an attempt to ensure compliance with security and legal standards by the organizations concerned.

F. Testing and Validation

A comprehensive testing makes it reliable. Unit tests are done on modules whereas integration tests can test the entire work flow. User Acceptance Testing (UAT) tests the system capacity in real life situations.

G. Deployment and Monitoring

After testing it is installed on AWS EC2 or locally on the servers. The monitoring tools are used to measure the system and user performance and errors. Failure can also be detected using real-time logs and assist audit trail. Unsuccessful remediations may be reverted of escalated.

H. Continuous Improvement and Updates

The system is constantly modified with the help of new security threats, user responses and modification of AWS services. Backend changes, UI modifications and compliance rule modifications guarantee long-term efficiency and relevance.

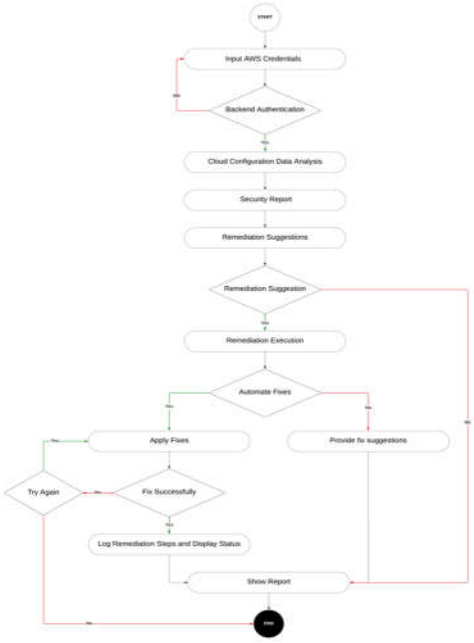

Fig. 2. Control Flow

5 RESULT

An automated cloud configuration audit system along with a remediation system automatically secured and complied AWS resources through misconfiguration identification and resolution capabilities. The system managed broad cloud configuration scanning by running its custom rule engine to classify vulnerabilities in Good, Warning and Danger severity levels through machine learning. Through exploiting logistic regression the system performed precise risk prioritization thus security threats were addressed in a manner that focused on critical issues first.

The audit showed that existing resources were non-compliant to a great extent leading to immediate action needs. High-risk vulnerabilities were automatically remediated by the system which brought configurations into compliance with industry standards for security best practices. The system operated through continuous monitoring to immediately identify newly discovered misconfigurations and always keep security proactive.

The audit process generated detailed information about misconfiguration types and instances which enabled data-based security enhancement plans. The system used historical patterns alongside current data monitoring to detect recurring system weak points which it used to create early defense mechanisms. The predictive features enhanced security policies while implementing best practices thus lowering the possibility of upcoming misconfigurations.

Logistic regression adoption for vulnerability classification served to create risk assessment priorities and improve the remediation system. The classification system organized vulnerabilities into severity bands therefore remediation efforts received effective allocation which started with critical issues and followed with lower-priority vulnerabilities. The methodical system structure protected resources while generating the greatest security results while avoiding extensive operational interruptions.

A major strength of the system consisted of its automatic remediation system that expedited repairs to resources not conforming with industry standards. The remediation engine used predefined security policies together with compliance frameworks to automate fix applications thus reducing the need for manual work and cutting down the chance of human error. This automated approach allowed security teams to manage strategic threats while working on security development improvements instead of tending to separate misconfigurations.

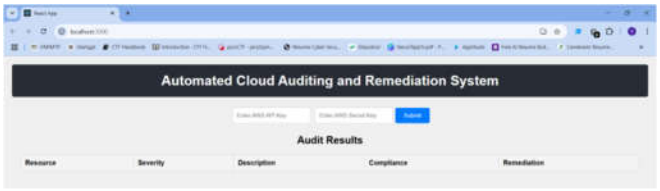

Fig. 3. Result produced 1

The project interface shows the input form which users interact with through fig .3.

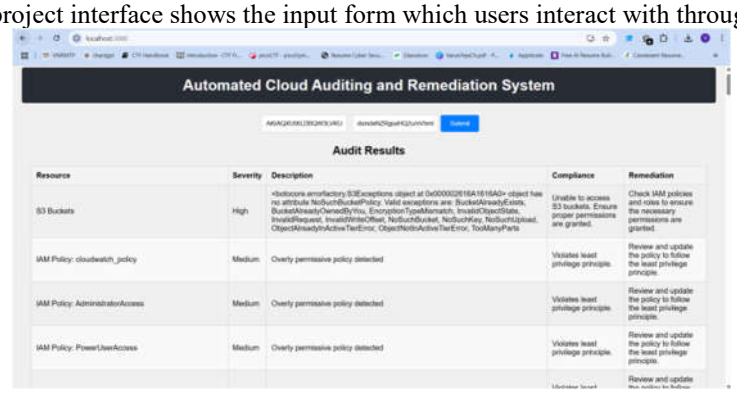

Fig. 4. Result produced 2

Fig .4 presents the cloud vulnerability and similarity interface of the project as shown in the user interface.

Metric	Precision(%)	Recall (%)	F1 Score (%)
Confidentiality Impact	86.57	83.38	84.80
Integrity Impact	87.7	85.81	86.67
Availability Impact	86.84	67.4	71.07
Attack Vector	86.73	71.75	77.61
Attack Complexity	91.30	72.91	79.15

User Interaction	92.73	91.81	92.24

Table. 1. Performance Matrix

6 CONCLUSION

The security of the cloud is significantly enhanced with an automated configuration and repair system. Proactive scanning and fixing of misconfigurations and vulnerabilities in the system ensures that environments are safe, compliant, and optimized in real time. Automation like this lessens manual effort, optimizing the entire organization, while allowing the IT team to allocate resources to important tasks.

Moreover, this system is integrated with other existing cloud systems, lessening the chances of breaches to security and minimizing interruptions to business operations. This also improves compliance to current standards and regulations in order to mitigate penalties and damage to brand reputation.

Ultimately, the automation of cloud configuration systems responds to security concerns in a reliable and scalable manner. The adoption of this system furthers the ability of businesses to protect and optimize their cloud-based configurations which fosters growth and innovation without hindrance.

References

1. Martseniuk, Y., Partyka, A., Harasymchuk, O., & Korshun, N. (2024). Automated Conformity Verification Concept for Cloud Security. *Cybersecurity Providing in Information and Telecommunication Systems 2024*, *3654*, 25-37.
2. Jim, M. M. I. (2024). Cloud Security Posture Management Automating Risk Identification And Response In Cloud Infrastructures. Academic Journal on Science, Technology, Engineering & Mathematics Education, 4(3), 10-69593.
3. Tuyishime, E., Balan, T. C., Cotfas, P. A., Cotfas, D. T., & Rekeraho, A. (2023). Enhancing cloud security—proactive threat monitoring and detection using a siem-based approach. Applied Sciences, 13(22), 12359.
4. Sharma, H. (2020). Effectiveness of CSPM in Multi-Cloud Environments: A study on the challenges and strategies for implementing CSPM across multiple cloud service providers (AWS, Azure, Google Cloud), focusing on interoperability and comprehensive visibility. International Journal of Computer Science and Engineering Research and Development (IJCSERD), 10(1), 1-18.
5. Alhamazani, K., Ranjan, R., Mitra, K., Jayaraman, P. P., Huang, Z., Wang, L., & Rabhi, F. (2014, June). Clams: Cross-layer multi-cloud application monitoring-as-a-service framework. In 2014 IEEE International Conference on Services Computing (pp. 283-290). IEEE.
6. Suriya, B. J., Amarnath, B. K., Raghuraman, A. R., & Arumugam, C. (2024, March). Cloud Security: Upgradation in CSPM Configuration Setting. In 2024 4th International Conference on Data Engineering and Communication Systems (ICDECS) (pp. 1-4). IEEE.
7. Yadav, G. S., Karthick, G., & Mukundha, C. H. (2024). DYNAMIC CLOUD SENTINEL FRAMEWORK (DCSF) FOR CSPM AND OPTIMAL SECURITY IN DYNAMIC

CLOUD ECOSYSTEMS. JOURNAL OF BASIC SCIENCE AND ENGINEERING, 21(1), 2004-2025.

8. Torkura, K. A., Sukmana, M. I., Cheng, F., & Meinel, C. (2021). Continuous auditing and threat detection in multi-cloud infrastructure. Computers & Security, 102, 102124.
9. Bundela, R., Dhanda, N., & Gupta, K. K. (2024, March). Identification and Analysis of Security Issues in Cloud Computing. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 1685-1690). IEEE.
10. Majumdar, S., Madi, T., Jarraya, Y., Pourzandi, M., Wang, L., & Debbabi, M. (2019). Cloud security auditing: Major approaches and existing challenges. In Foundations and Practice of Security: 11th International Symposium, FPS 2018, Montreal, QC, Canada, November 13–15, 2018, Revised Selected Papers 11 (pp. 61-77). Springer International Publishing.
11. Martseniuk, Y., Partyka, A., Harasymchuk, O., & Korshun, N. (2024). Automated Conformity Verification Concept for Cloud Security. Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654, 25-37.
12. Chieu, T. C., Singh, M., Tang, C., Viswanathan, M., & Gupta, A. (2012, September). Automation system for validation of configuration and security compliance in managed cloud services. In 2012 IEEE Ninth International Conference on e-Business Engineering (pp. 285-291). IEEE.
13. Reddy, M. V., Charan, P. S., Devisaran, D., Shankar, R., & Kumar, P. A. (2023, March). A systematic approach towards security concerns in cloud. In 2023 Second International Conference on Electronics and Renewable Systems (ICEARS) (pp. 838-843). IEEE.
14. Jois, O., Roshni, G., Baisak, R., & Upadhyaya, S. R. (2024, January). Logs2Vul: Vulnerability Detection from Logs for CSPM. In 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) (pp. 1-7). IEEE.
15. Prakash, C., & Dasgupta, S. (2016, March). Cloud computing security analysis: Challenges and possible solutions. In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) (pp. 54-57). IEEE.