International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677● Website: www.ijsat.org● Email: editor@ijsat.org

Leveraging AWS Config and Custom Rules for Automated Security Compliance Auditing in Cloud Infrastructure

Vivek Somi

Somivivek@gmail.com

Abstract

This research paper investigates how tailored AWS Config rules could greatly improve cloud security and compliance. These guidelines let companies modify their programs of monitoring and assessing to satisfy legal and operational requirements. By letting complete control over AWS resources, AWS Lambda helps companies to surpass conventional compliance assessments. Real-time compliance status data from AWS Config enable early on security issue discovery by constant monitoring. Automated notifications and corrective action help to lower compliance violations, so lowering the risk of security breaches and so aiding proactive risk management. Considering the complexity of cloud systems, good compliance solutions become especially important. Apart from streamlining adherence to regulations such GDPR, HIPAA, and PCI DSS, bespoke AWS Config rules increase operational efficiency and accountability. Including these guidelines into cloud security plans helps to create a compliance culture in which every AWS resource meets best criteria. Eventually, tailored AWS Config rules let companies efficiently manage regulatory environments using AWS capabilities for innovation and business success, hence building the basis for complete cloud security.

Keywords: AWS Config Rules, Cloud Security, Compliance, AWS Lambda, Regulatory Standards

I. INTRODUCTION

Cloud security is first concern since cloud architecture has a dynamic and sophisticated character. Unauthorized access to sensitive data resulting from data breaches—which could occur from misconfigurations, inadequate authentication systems, or insider threats—is one of the main challenges. While cloud service providers manage the fundamental infrastructure, customers are in charge of safeguarding data, programs, and network configurations, therefore aggravating security concerns. Because of limited view and control over data and network traffic, companies find it far more difficult on cloud systems to properly manage and defend their assets. Strict privacy requirements and data security standards—including GDPR, HIPAA, and PCI DSS—must also be followed; non-compliance has very serious repercussions. Identity and access management (IAM) is becoming more and more important as more customers and services search for access to cloud resources and run the risk of misusing their rights or improper authorization. Moreover taken advantage of by attackers might be dynamic and fast scaling of cloud systems resulting in misconfiguration. Not least of all, strong and

automated security procedures must be in place to protect cloud systems against additional advanced cyberthreats and distributed denial of service (DDoS) attacks. This will motivate allegiance and protect you from always changing hazard.Another main challenge to cloud security is the complexity of multi-cloud setups, in which companies use several cloud service providers to fulfil different operational requirements. When security regulations, data protection, and compliance are handled differently on numerous platforms, misconfigurations and security posture issues are more likely to arise. Lack of homogeneity among providers introduces still another level of challenge and affects the acceptance of fundamental security policies. Another challenge still comes from the security of the APIs and microservices of cloud-native companies. Usually found on outside networks, APIs are easy exploited. Either constructed or improperly secured APIs carry the danger of data leaks, disrupted services, or underlying infrastructure damage. The fact that cloud resources are transient by nature adds to the challenge. Usually avoiding conventional security mechanisms, one can quickly spin up and down instances, containers, and workload. Consistent threat identification, patch management, and security monitoring could all be challenging in such dynamic settings. At last, cloud computing presents a special threat from insiders. Remote work and third-party providers gaining access to cloud resources make it more and more difficult to identify detrimental or unintended behaviors by approved individuals. Companies looking to protect their cloud resources look for advanced solutions including automated monitoring and behavioral analytics to find suspicious activities [1]–[3].

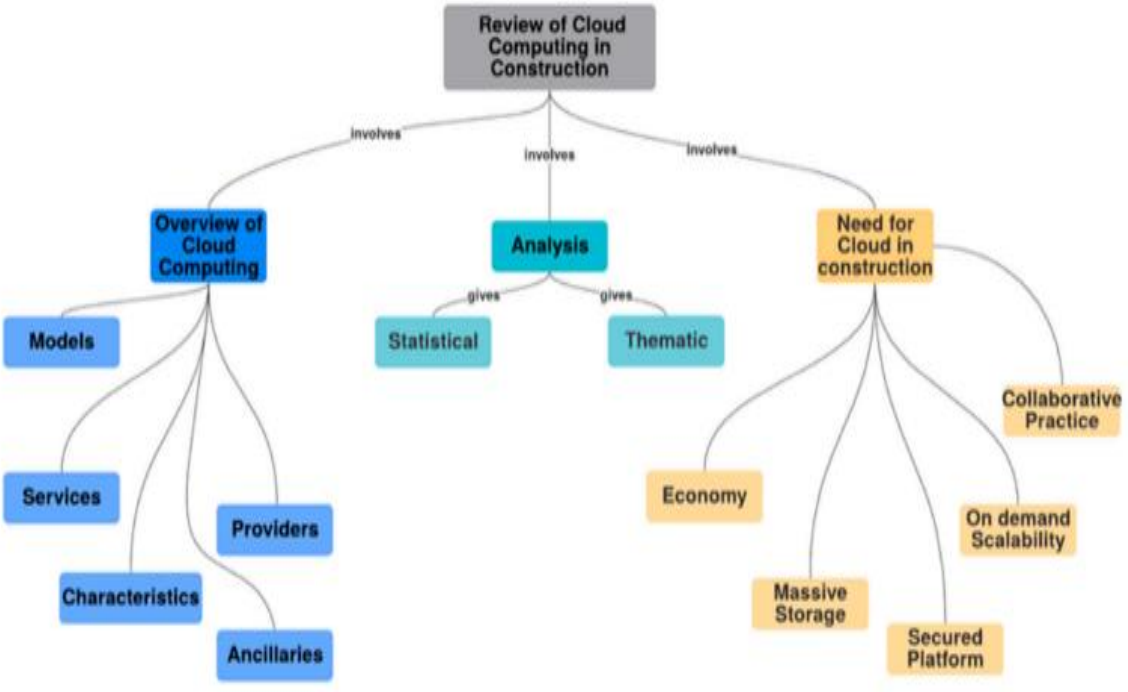

Fig. 1 Cloud computing construction[4]

Companies that wish to keep their data and services safe, current, and confidential while still fulfilling legal, regulatory, and industry needs must follow security criteria in cloud architecture. Companies have to follow compliance guidelines including GDPR, HIPAA, and PCI DSS as the use of cloud computing keeps rising to safeguard private data and stop fines, financial losses, or damage of brand. Cloud compliance guarantees the existence of security systems to protect data from the always growing risk of cyberattacks, unauthorized access, and breaches in the digital environment of today[5], [6]. By proving

their dedication to safe operations and data protection, businesses may win over consumers' and partners' confidence by security compliance. Compliance is already vital in cloud environments, but in these shared and continually changing environments it becomes much more important since businesses have to guarantee that their setups, data management, and access control policies match standards. Under continual monitoring, automated solutions including AWS Config, custom rules, and compliance auditing methods help cloud resources remain compliant with always changing needs. Noncompliance could lead to expensive fines and disturbances in sectors like banking and healthcare that call on great security. Security compliance mostly aims to guarantee that the infrastructure is strong against both internal and external threats while running under the constraints of legal and regulatory frameworks; so, it helps to prevent vulnerabilities, reduce risks, and support business continuity[7].

II. RELATED WORK

Kharade 2022 et al. Closed because of the COVID-19 epidemic. To maintain the academic activities going, most educational institutions have turned to online learning platforms. Still unclear, nevertheless, are issues regarding the readiness, design, and efficacy of e-learning, especially in states like Goa where the technical limitations such as device appropriateness and bandwidth availability are a major obstacle. The study investigates the preferences of the students for certain characteristics of online courses, therefore guiding the construction of a successful online learning environment. According to the findings, most of the respondents—80%—are prepared to choose online courses to help control the curriculum during this epidemic. Most of the kids would rather utilise their smart phones for online learning. While broadband connectivity problems in rural locations makes it difficult for students to make use of online learning efforts, the students said that flexibility and ease of online classes make it appealing alternative[8].

Sreeharsha 2022 et al. has stayed a hassle even if few programs offer special qualities. This work intends to create a voice chatbot as the hotel reservation communication tool with Facebook Messenger and Amazon Lex Service. By means of Amazon Web Services (AWS) in the form of a service called Amazon Lex for producing the bot with utterances and responses and Lambda Functions to validate the responses, running operations using Facebook Messenger service helps the chatbot to be constructed. Running a script gathering plain text or speech recognition using the microphone linked to it, the lambda function sends the output to the Amazon Lex to be handled via several services offered by Amazon Web Services. The chatbot then either in plain text or via the voice connected to the gadget gives the user a suitable answer. Moreover connected with a Facebook profile, this bot also finds practical uses. As necessary, the page administrator can set the necessary access to whole communications gathered via the chatbot [9].

Ahmad 2022 et al. has attracted ever more interest among professionals and scholars. Still, the performance evaluation of those authorizing systems gets little attention. This work presents a comprehensive experimental study of cloud- and edge-based access control techniques for smart home applications in order to cover this gap. We discuss the main architectural decisions, namely (a) where the access control logic is implemented (in the cloud or the edge) and (b) how the attributes needed for policy evaluation are supplied to the policy evaluation point and identify possible deployment models for cloud-based or edge-based access control mechanisms. We empirically assess the found deployment

strategies—mostly AWS IoT and Greengrass—into the IoT platforms provided by Amazon Web Services (AWS) using a smart lock system in order to investigate their effect on smart home performance. Our experimental investigation produces recommendations for practitioners as well as for academics[10].

Van 2022 et al. have produced significant data leaks and security events. Their dynamic and sophisticated character allows incorrectly set (e.g., too permissive) access controls to be easily introduced and unnoticed for a good period of time. Such mistakes must so be found before they could be taken advantage of. We introduce in this work new AWS access and identity management rules misconfiguration detection method. Our method is based on the realization that policies might be regarded as graphically modelled as permissions between objects and entities. Our main point of view is that, given such a graph representation, misconfigurations can be found rather easily as anomalies. Using data from three corporate clouds on genuine identity and access control policies, we assess our strategy. Although with a significantly lower accuracy than rule-based methods, we show that our method correctly detects between 3.7 and 6.4 times as many misconfigurations[11].

Pedro 2022 et al. have substantially cut the delivery times of its customers, but as this method of software development cannot match the speed of the DevOps Software Development Life Cycle, it poses issues for the way security is usually executed. We must so rethink how we include security into this growth paradigm. To try to solve this, moving security to the early phases of development and combining security techniques into DevOps processes helps. This approach simplifies otherwise more time-consuming and difficult processes by means of testing automata. Although academic research has not attracted as much attention to this sector, industry practitioners today find DevSecOps to be a popular topic as the grey literature production of this discipline demonstrates. This dissertation presents how to include security elements, such dynamic application security testing (DAST) and static application security testing (SAST), into CI/CD pipelines, and what impact these new stages would have in the safety of the code used to build container artefacts, time to deploy and security of the pipeline itself. First, in order to get at this, a reference CI/CD pipeline architecture was designed with respect to the specific use-case. One then turned to study the vulnerability reports generated by the DevSecOps toolbox. The efficiency and effectiveness of the tests were assessed in relation to the performance criteria of the system. At last, using the previous comprehensive analysis and pipeline design description, results on the impact of the security testing phases on the CI/CD process emerged[12].

Table no. 1 Literature summary

Author/year	Methods	Findings	Research gap	Results
Podeschi/2022 [13]	Cloud computing course integrates AWS skills for IS students' careers.	Course enhanced cloud skills, preparing students for AWS certification.	Limited studies on cloud integration in broader computing curricula.	Students gained practical AWS skills, boosting employability and certification success.
Tissir/2021 [14]	OpenStack	OpenStack's	Limited research	OpenStack

	security vulnerabilities analyzed over ten years, trends identified comprehensively.	common vulnerabilities identified, revealing trends over ten years.	on long-term security solutions for OpenStack vulnerabilities.	vulnerability trends revealed, improving security understanding and mitigation efforts.
Bhatt/2021 [15]	Proposed ABAC model enhances AWS IoT access control and security.	ABAC model improves access control, enhancing security for AWS IoT.	Insufficient dynamic access control models for securing IoT environments.	Proposed model demonstrated effective access control for AWS IoT applications.
Han/2020 [16]	VM resource contention affects performance; prediction models improve cloud efficiency.	Resource contention degrades VM performance; prediction models yield accurate results.	Limited studies on predicting VM co-residency in public clouds.	Predicted VM co-residency accurately using linear regression and random forest.
Sokolowski/ 2020 [17]	Hybrid HPC deployments enhanced through multitier reactive programming for optimization.	Multitier reactive programming improves execution flexibility for hybrid HPC.	Limited research on optimizing HPC applications for hybrid cloud environments.	Effective hybrid cloud deployment demonstrated using multitier reactive programming approach.

III. Role of AWS in Cloud Security

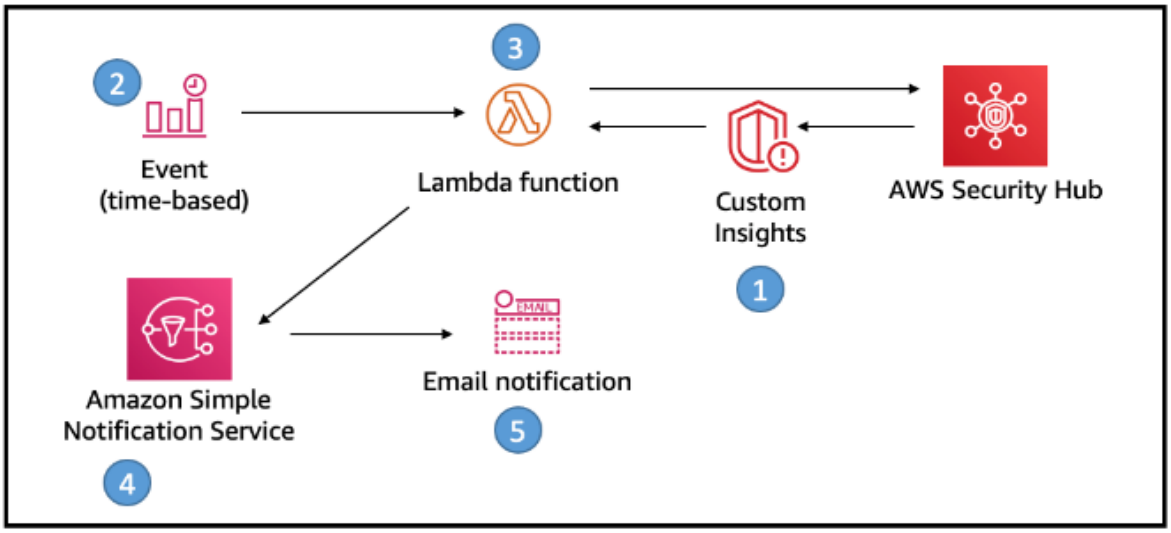

Fig. 2 AWS in cloud security [18]

A. Shared Responsibility Model

Under AWS's shared responsibility approach, data security falls both on consumers and the company. Under this approach, AWS owns the layer of physical, network, and virtualization security of the cloud architecture. Protected also has to be the hardware and software powering cloud services. On the other hand, AWS does not own the security of operating systems, apps, client data, or running systems. This exact explanation enables companies to better grasp their specific security responsibilities and apply suitable procedures and controls. Companies may better control risks and make use of the scalability and adaptability of the cloud by means of AWS's collaborative security approach [19], [20].

B. Comprehensive Security Services

To let cloud apps and data to be safer, AWS offers a wide range of security services. AWS Identity and Access Management (IAM) supports businesses in correctly managing user rights and access restrictions. For some, this gives total control over the resources they can get hold of. Across several services, the AWS Key Management Service (KMS) allows customers quickly create and maintain encryption keys for their data. Moreover offering strong protection against network and application-layer vulnerabilities, AWS online Application Firewall (WAF) protects programs against common online exploits and Distributed Denial of Service (DDoS) attacks.

C. Data Encryption

Strong encryption capabilities of AWS let consumers rest knowing their data is stored both at rest and in transit. Users of systems like Amazon S3 (Simple Storage Service) can encrypt stored data by means of server-side or client-side encryption options, therefore shielding critical data from illegal access. Also built-in security mechanisms of Amazon RDS protect database instances and snapshots. Since it enables encryption, all data—including backups—is safely stored on volumes kept under Amazon EBS (Elastic

Block Store.). These encryption devices help businesses to keep customer privacy and follow all pertinent policies [21]–[24].

D. Continuous Monitoring and Compliance

Two of AWS CloudTrail and AWS CloudWatch, two of its continuous monitoring technologies, are vitally essential for cloud security and compliance. By means of real-time application and resource monitoring, Amazon CloudWatch exposes operational data, system health, and resource utilization for businesses. By tracking user activity and resource changes across AWS services, AWS CloudTrail helps businesses keep an audit trail of events created within their account. Together, these technologies allow more open, responsible, and readily visible cloud operations and resource management, therefore enabling compliance with GDPR, HIPAA, and PCI DSS.

E. Network Security

The broad range of network security technologies available from AWS helps to protect cloud resources and communications. By allowing users create their own virtual networks, Virtual Private Cloud (VPC) consumers can improve security by establishing isolated environments for their resources. Acting as virtual firewalls, security groups in a virtual private cloud (VPC) let users regulate incoming and leaving traffic for their instances. Network Access Control Lists (NACLs) give still another degree of security by discreetly screening traffic at the subnet level. Moreover, AWS Transit Gateway streamlines and protects communication between virtual private clouds (VPCs), therefore enabling fast data transfer with strong security over all networks [29] .

IV. CLOUD INFRASTRUCTURE AND SECURITY COMPLIANCE

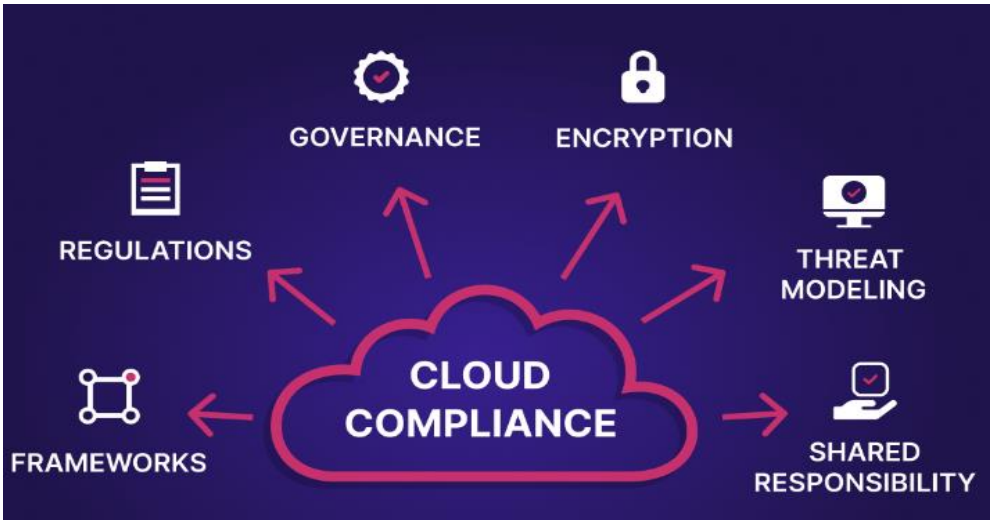

Fig.3 Cloud compliance [27]

Cloud architecture has revolutionized how companies approach their IT expenditures by providing scalability, agility, and cost-efficiencies. Still, given growing reliance on cloud services, strict security compliance is quite important. The degree to which a cloud infrastructure complies with guidelines required to protect private data, guard sensitive information, and ensure ongoing operation of cloud

services is known as "security compliance". Particularly those based on data security and privacy and include GDPR, PCI DSS, and HIPAA, organizations migrating to the cloud must negotiate a complex set of compliance standards. By following these guidelines, which specify high standards for data management, storage, and processing, one promotes a strong understanding of the shared responsibility paradigm in cloud computing. Under this model, clients are in responsibility of safeguarding their applications and data; cloud service providers as Microsoft Azure, Amazon, and Google Cloud supervise the basic infrastructure. Clearly defining these roles helps businesses understand their compliance obligations and deploy appropriate security procedures. Companies that combine data encryption, identity and access management, continuous monitoring, and incident response planning—all of which help to meet cloud security needs—will be more suited.

Sensitive data encrypted both at rest and in transit guarantees it remains free from illegal access. Strong user identification and authorizationutilizing identity and access management systems can considerably reduce the danger of data breaches, therefore helping businesses to meet legal responsibilities. Tools like AWS CloudTrail and CloudWatch enable real-time anomaly detection, resource change monitoring, and compliance violations identification that helps businesses. Moreover, well-written incident response plans help to minimize the consequences and help to regulate security occurrences. For companies, using best practices and implementing evolving compliance regulations into their cloud security strategies is absolutely vital. In an always changing technological environment, data protection largely rely on staff member education, compliance culture development, and use of automated technology. Prioritizing security compliance not only protects private data but also helps partners and consumers to feel confident, so improving the online presence and reputation of a business[28]–[32].

V. CUSTOM AWS CONFIG RULES FOR ENHANCED AUDITING

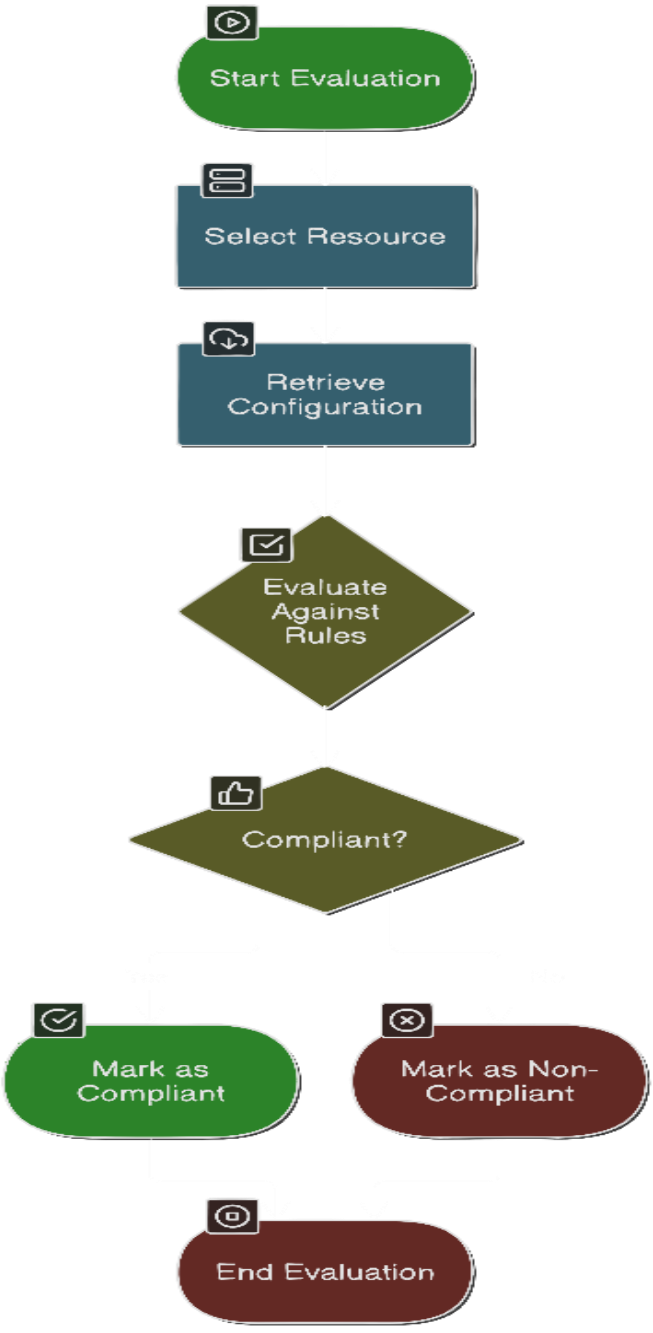

Fig. 4 AWS Config Evaluation Workflow

A. Tailored Compliance Checks

Custom AWS Config Rules let companies fit their operational needs to the regulatory requirements unique to their industry. When users can add custom criteria, AWS resources are always evaluated against relevant standards. This flexibility allows businesses to build compliance strategies suitable for their risk profile and corporate objectives. These tailored solutions enable companies to better administer their cloud environments, maintain regulatory compliance, and enhance security policies by means of proactive monitoring.

B. Automated Monitoring and Evaluation

AWS Config tracks constantly and automatically tests AWS resources against predefined compliance requirements. Real-time compliance status data makes it easy to spot any deviations from set criteria. Using AWS Config helps businesses quickly find security flaws—like improperly configured security groups or exposed storage buckets—before they become major problems. By means of enhanced security posture and fast corrective action, this proactive approach helps companies to more successfully handle regulatory issues. AWS Config thus distributes more responsibility and offers smart analysis for improved administration and control of cloud resources[33]–[34].

C. Integration with AWS Lambda

Apart from tailored AWS Config Rules, AWS Config may monitor resources and match them to set compliance criteria on their own. Real-time compliance level statistics quickly highlights any deviations from defined criteria, therefore supporting continuous assessment. Using AWS Config helps businesses rapidly identify security flaws—such as incorrectly configured security groups or exposed storage buckets—before they become more critical. This proactive approach not only improves security posture but also enables quick fixes, therefore helping businesses to adequately manage regulatory concerns. AWS Config therefore promotes prudent and competent use of cloud resources for optimum control.

D. Automated Remediation and Notifications

Should a resource fail to meet the standards established by a custom AWS Config Rule, the service can instantly sound alerts and start remedial action, therefore enabling businesses to respond rapidly to potential security concerns. AWS Config can notify management using Amazon SNS (Simple Notification Service), therefore encouraging quick research on the non-compliance issue. Automated corrective actions can impose specific settings to reverse improperly configured ones or bring resources into compliance. By means of automation, simplifying the compliance process and thereby lowering the exposure to security hazards helps companies to keep a solid security posture [35].

E. Support for Regulatory Compliance

Maintaining compliance with several regulatory systems, including GDPR, HIPAA, and PCI DSS, mostly depends on the application of tailored AWS Config Rules. These guidelines guarantee that, under constant monitoring of AWS resources, deployments regularly satisfy particular compliance criteria. They assist companies show regulatory compliance by including thorough audit trails tracking resource configurations and modifications over time. Companies can reduce the possibility of infractions and react fast to any problems by aggressively controlling compliance. More openness is ultimately attained by means of adjustable rules, therefore fostering responsible and ethical cloud resource management [36].

VI. CONCLUSION

In conclusion, Custom AWS Config Rules improve cloud security and compliance by matching operational needs with monitoring and assessment systems. Including AWS Lambda allows companies to ensure complete control of AWS resources by extending their monitoring capability outside of

standard compliance audits. Constant monitoring by AWS Config provides real-time compliance data that allow businesses to identify security problems before they become more significant. Automated alarms and remedial actions, through proactive risk management, provide quick responses to compliance deviations, therefore reducing security vulnerabilities. Maintaining continual compliance becomes essential since companies depend more and more on cloud architecture. While simplifying compliance with GDPR, HIPAA, and PCI DSS, Custom AWS Config Rules boost operational efficiency and responsibility. Including these rules into cloud security strategies helps to foster a compliance-oriented culture whereby all AWS resources obey approved policies. Custom AWS Config Rules enable companies to effectively manage their regulatory needs, enhance their cloud security, and apply AWS solutions to stimulate innovation and growth[37], [38].

REFERENCES

[1] B. T. G. College, “Managing Deployed Containerized Web Application on AWS Using EKS on AWS Fargate by Bashair Abdullah M Algarni,” 2021.

[2] D. Aklamati, “Security Analysis of AWS-based Video Surveillance Systems,” no. October, pp. 27–28, 2021.

[3] B. Acharya, “Building Serverless Application with AWS Lambda,” no. May, 2020.

[4] S. A. Bello *et al.*, “Automation in Construction Cloud computing in construction industry : Use cases , benefits and challenges,” *Autom. Constr.*, vol. 122, p. 103441, 2021, doi: 10.1016/j.autcon.2020.103441.

[5] A. Bandaru, “Amazon web services,” no. December, 2020.

[6] S. Jagdishprasad and J. Tibrewala, “A COMPARATIVE STUDY ON GOOGLE APP ENGINE AMAZON WEB SERVICES AND MICROSOFT WINDOWS AZURE,” vol. 10, no. 1, pp. 54–60, 2019.

[7] I. Aljarah, N. Obeid, and O. Y. Adwan, “An Investigation of Microsoft Azure and Amazon Web Services from Users ’ Perspectives,” vol. 14, no. 10, pp. 217–241, 2019.

[8] J. Kharade and I. Technology, “Advance and Innovative Research,” no. August, 2022.

[9] A. S. S. K. Sreeharsha, S. M. Kesapragada, and S. P. Chalamalasetty, “Building Chatbot Using Amazon Lex and Integrating with A Chat Application,” *Interantional J. Sci. Res. Eng. Manag.*, vol. 06, no. 04, 2022, doi: 10.55041/ijsrem12145.

[10] T. Ahmad, U. Morelli, S. Ranise, and N. Zannone, “Extending access control in AWS IoT through event-driven functions: an experimental evaluation using a smart lock system,” *Int. J. Inf. Secur.*, vol. 21, no. 2, pp. 379–408, 2022, doi: 10.1007/s10207-021-00558-3.

[11] T. Van Ede, N. Khasuntsev, B. Steen, and A. Continella, “Detecting Anomalous Misconfigurations in AWS Identity and Access Management Policies,” *CCSW 2022 - Proc. 2022 Cloud Comput. Secur. Work. co-located with CCS 2022*, pp. 63–74, 2022, doi: 10.1145/3560810.3564264.

[12] J. Pedro, M. Rôla, and R. Morla, “FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO

PORTO Dynamic Security Testing," 2022.

[13] R. J. Podeschi and J. Debo, "Integrating AWS Cloud Practitioner Certification into a Systems Administration Course," vol. 20, no. December, pp. 17–26, 2022.

[14] N. Tissir, S. ElKafhali, and N. Aboutabit, *How Much Your Cloud Management Platform Is Secure? OpenStack Use Case*, vol. 183, no. February. Springer International Publishing, 2021. doi: 10.1007/978-3-030-66840-2_85.

[15] S. Bhatt, T. K. Pham, M. Gupta, J. Benson, J. Park, and R. Sandhu, "Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future," *IEEE Access*, vol. 9, pp. 107200–107223, 2021, doi: 10.1109/ACCESS.2021.3101218.

[16] X. Han, R. Schooley, D. MacKenzie, O. David, and W. J. Lloyd, "Characterizing Public Cloud Resource Contention to Support Virtual Machine Co-residency Prediction," *Proc. - 2020 IEEE Int. Conf. Cloud Eng. IC2E 2020*, pp. 162–172, 2020, doi: 10.1109/IC2E48712.2020.00024.

[17] D. Sokolowski, J. P. Lehr, C. Bischof, and G. Salvaneschi, "Leveraging Hybrid Cloud HPC with Multitier Reactive Programming," *Proc. SuperCompCloud 2020 3rd Work. Interoperability Supercomput. Cloud Technol. Held conjunction with SC 2020 Int. Conf. High Perform. Comput. Networking, Storage Anal.*, pp. 27–32, 2020, doi: 10.1109/SuperCompCloud51944.2020.00010.

[18] "How to set up a recurring Security Hub summary email | AWS Security Blog." https://aws.amazon.com/blogs/security/how-to-set-up-a-recurring-security-hub-summary-email/ (accessed Mar. 23, 2023).

[19] J. Backes *et al.*, "Reachability analysis for AWS-based networks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11562 LNCS, pp. 231–241, 2019, doi: 10.1007/978-3-030-25543-5_14.

[20] "Client-side Monitoring and Metering Service Level Agreements for Cloud Services A Thesis Presented By Eshetu Muleta Debe to School of Graduate Studies of St . Mary ' s University In Partial Fulfillment of the Requirements for the Degree of Master of Scien," no. June, 2019.

[21] S. Majumdar, T. Madi, Y. Jarraya, M. Pourzandi, L. Wang, and M. Debbabi, "Cloud Security Auditing: Major Approaches and Existing Challenges," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11358 LNCS, pp. 61–77, 2019, doi: 10.1007/978-3-030-18419-3_5.

[22] Karl Gilbert and Benjamin Caudill, "Hands-On AWS Penetration Testing with Kali Linux," pp. 140–160, 2019.

[23] L. Carvalho and M. Marden, "Fostering Business and Organizational Transformation to Generate Business Value with Amazon Web Services," *Idc*, pp. 1–14, 2018, [Online]. Available: https://d1.awsstatic.com/enterprise-marketing/cloud-economics/idc-fostering-business-and-organizational-transformation-to-generate-business-value-with-aws.pdf

[24] K. A. Torkura, M. I. H. Sukmana, F. Cheng, and C. Meinel, "CAVAS: Neutralizing application

and container security vulnerabilities in the cloud native era," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 254, no. June, pp. 471–490, 2018, doi: 10.1007/978-3-030-01701-9_26.

[25] Y. Rohinton, P. Publishing, Y. Wadia, and P. Publishing, "eBooks on Fault-tolerant System AWS Administration – The Definitive Guide AWS Administration - The Definitive Guide : Design , Build , and Manage Your Infrastructure on Amazon Web Services , 2nd Edition eBooks on Fault-tolerant System Design And Analysis ," 2018.

[26] B. S. Cole and J. H. Moore, "Eleven quick tips for architecting biomedical informatics workflows with cloud computing," *PLoS Comput. Biol.*, vol. 14, no. 3, pp. 1–11, 2018, doi: 10.1371/journal.pcbi.1005994.

[27] "Best Practices for Cloud Security Compliance| Softbinator Technologies." https://blog.softbinator.com/cloud-security-compliance/ (accessed Apr. 20, 2023).

[28] T. Hsu, "Hands-On Security in DevOps," p. 617, 2018.

[29] T. Madi, "Security Auditing and Multi-Tenancy Threat Evaluation in Public Cloud Infrastructures," no. November, 2018, [Online]. Available: https://spectrum.library.concordia.ca/id/eprint/985048/

[30] T. Vijayakumar, *Practical API architecture and development with azure and AWS: Design and implementation of APIs for the Cloud*. 2018. doi: 10.1007/978-1-4842-3555-3.

[31] J. Backes *et al.*, "Semantic-based Automated Reasoning for AWS Access Policies using SMT," *Proc. 18th Conf. Form. Methods Comput. Des. FMCAD 2018*, pp. 206–214, 2018, doi: 10.23919/FMCAD.2018.8602994.

[32] A. Pras, A. Sperotto, and S. Hungary, "Penetration testing of aws-based environments Master thesis R ´ eka SzabóSzab´Szabó P ´ eter Kiss," no. November, 2018.

[33] S. S. Heeney, "Building An Automated Ecosystem On AWS Implementing Robust Security Measures Using DCVS MSc Research Project Cloud Computing Ganesh Patil".

[34] Prof. Paolo Ernesto Prinetto, Dr. Matteo Fornero, and Dr. Nicoló Maunero, "POLITECNICO DI TORINO DEPARTMENT OF CONTROL AND COMPUTER ENGINEERING (DAUIN) Master Degree in Computer Engineering Custom cloud storage solutions based on Nextcloud: a case study implementation".

[35] R. Beuran, Z. Zhang, and Y. Tan, "AWS EC2 Public Cloud Cyber Range Deployment".

[36] R. M. Gebregergis, "Supply Chain Risks From Cloud Security Posture Management Services".

[37] Q. Jacquemart, A. B. Vitali, G. Urvoy-keller, Q. Jacquemart, A. B. Vitali, and G. U. Measuring, "Measuring the Amazon Web Services (AWS) WAN Infrastructure To cite this version : HAL Id : hal-02128052 Measuring the Amazon Web Services (AWS) WAN Infrastructure," 2019.

[38] B. Cook, *Formal Reasoning About the Security*, vol. 2. Springer International Publishing, 2018.

doi: 10.1007/978-3-319-96145-3.