Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2020, 7(2):77-82

Research Article ISSN: 2394 - 658X

Automating Cloud Security and Compliance at Scale Strategies and Best Practices

Rajashekar Reddy Yasani[1], Karthik Venkatesh Ratnam[2]

[1]Senior Security Engineer, Independent Security Researcher, Boston, MA
Cloud Security, Cloud Computing, Cyber Security
rajshekaryasani@gmail.com
[2]Cloud Engineer, Devsecops (cloud security)
Independent Security Researcher, Dallas, TX
karthikratnam1@gmail.com

ABSTRACT

Many rules, guidelines, and software controls have been developed by various agencies and standards bodies throughout the world to address data protection concerns, and they are all meant to be applied to data stored in the Cloud. Compliance obligations have so increased for service providers who store private information about their end users. It takes a lot of human work to follow these rules because they aren't in a machine-processable format. Providers often have to put in extra work to meet all of the regulations because numerous laws have similar requirements but don't mention each other. Every single data protection regulation that pertains to data stored in the cloud has been thoroughly researched by us. We have created a knowledge graph that incorporates all of these data compliance rules and is rich in semantic information. This encompasses both the data threats and the necessary security policies to lessen those risks. In this work, we showcase this knowledge graph and the evaluation system we built in great detail. We have checked our knowledge graph with the privacy policies of several cloud providers, including Rackspace, Amazon Web Services, Google Cloud, and IBM. Businesses may automate their compliance procedures and establish enterprise-level Cloud security rules with the help of this publicly-available knowledge graph.

Keywords: Cloud computing, cloud security, security domains, security compliance models, cloud security models.

INTRODUCTION

In the modern era of remote data and application hosting, cloud security automation has become an absolute necessity. Protecting private data and infrastructure is of utmost importance as more and more businesses move their activities to the cloud [1]. An effective and proactive method of real-time protection against several cyber threats is offered by cloud security automation, which is powered by cutting-edge technologies and sophisticated protocols. As we enter the era of cloud automation, this blog delves at the importance of cloud security automation and how it enables businesses to strengthen their digital defences while remaining agile and resilient [2]. Thanks to the cloud's adaptability, efficiency, and creativity, businesses in every sector have taken advantage of it. Despite this, a third of businesses have not reaped the benefits of cloud computing as anticipated, with 65% citing "security and compliance risks" as an important obstacle [3]. The most substantial barrier to cloud adoption is security process automation, even though the cloud presents new possibilities for transformation, modernisation, and innovation. Going cloud-less is already a daunting task, and the complexity of multi-cloud and hybrid setups just adds insult to injury [4].

Automating security workflows is commonly perceived as a major barrier to cloud adoption; yet, when properly implemented, it can also serve as a major enabler. Organisations may refocus their attention on innovation and growth when they automate the process of securing their cloud infrastructure. This allows them to obtain all the necessary information to secure their cloud environments [5].

Gartner predicts that worldwide spending on public cloud services will skyrocket in 2023, reaching an astounding USD 591.8 billion, thanks to a growth rate of 20.7%. According to Pingsafe, a major worry has emerged as a result of the cloud's meteoric rise in popularity: an alarming 80% of businesses experienced a cloud security infrastructure incident in the previous year, highlighting the increasing need for stringent security protocols in the cloud [6].

According to Strong DM, 54 percent of companies have strengthened their cloud defences by using cloud security automation products and services in response to this threat. According to Forrester's research [7], cloud security automation is becoming more commonplace. At 75%, configuration management is the top use case, followed by vulnerability scanning at 70%, patch management at 65%, and identity and access management at 60%. Cloud infrastructure security likewise relies heavily on log monitoring and analysis at 55%. With 80% of users reporting a better security posture, cloud security automation offers tremendous benefits, as demonstrated by Accenture. Not only that, but automation of cloud security is known to save costs by 75%, boost operational efficiency by 70%, lessen the likelihood of human error by 65%, and increase compliance by 60%. The importance of protecting assets stored in the cloud from cyber threats is rising, and these numbers show that cloud security automation is playing a key role in ensuring the safety of this trend [8]. A recent development in cloud security operations automation is the automation of security procedures that are typically built and implemented by hand. The greatest cloud security automation is difficult to deploy, nevertheless, for many businesses.

LITERATURE REVIEW

A. Cloud Data Compliance

Data protection standards are a collection of regulations and policies developed by groups tasked with ensuring the security of personal information [9]. Cloud computing security has been suggested to guarantee data protection and user privacy through the use of security and privacy compliance models such as ISO 27001, COBIT, etc. Based on the security controls that have been put in place, we have examined and classified all of the different Cloud compliance models. The policies and procedures put in place to safeguard data stored in the Cloud are the primary emphasis of cloud security [10]. Cloud service providers and end users alike are not immune to security breaches. Cloud service providers have a responsibility to make sure their customers know what to do to keep their data safe. Cloud providers use a variety of security controls—deterrent, preventative, detective, and corrective—to enforce security.

Security rules used to safeguard their environment are same across all three types of cloud services—SaaS, PaaS, and IaaS—despite the fact that these services and deployment patterns have been categorised differently. Security controls are the foundation upon which compliance models are deployed. To make sure the Cloud is secure enough, we need to align these models.

The IT compliance model is centred around the processing of electronic data, networks, and IT infrastructure. In order for all of IT's parts to function in tandem, the compliance model imposes certain norms and guidelines. On the basis of these compliance models, the security model is implemented. Our work in associating different security controls and compliance models is a major contribution. Users will have an easier time achieving data protection thanks to the transparency among the Cloud model, security control model, and compliance model.

Cloud services pose risks to users' data, so they should think carefully about all of them before signing up. Threats listed by CSA include unauthorised access to data, loss of data, account or service hijacking, unsecured APIs and interfaces, denial of service, malevolent insiders, misuse of cloud services, lack of due diligence, and weaknesses in shared technology. Many security measures have been put in place by cloud providers because they recognise the significance of these ongoing concerns. Amazon, Rackspace, and Google are just a few of the vendors who openly discuss the platform-wide security measures they've implemented. More than 800 cloud providers are accessible globally, as stated in [11]. The real issue is the number of them that are able to tackle such risks by utilising Cloud security standards.

The security concerns of various Cloud services are described in [12]. Service level agreements (SLAs) should also address security concerns, which cloud providers should do. This will provide customers with a clear understanding of the security concerns related to the Cloud. Cloud Control Matrix, Third Edition (CCM v3), issued by CSA in 2013, includes over 135 security rules and associated compliance models. There are 114 security controls spread over 14 categories in the ISO 27001:2013 standard. But it lacks safeguards like media protection and data encryption. There were 18 categories used to present the security controls in NIST 800-53. The Department of Defence (DoD) has recently released a document outlining eight controls and areas for information assurance. Our prototype system aims to accomplish just that—identify common security controls that customers can easily understand.

B. Semantic Web Ontology

Representing the World Wide Web, the semantic web mostly works with data rather than documents and offers standards to explain relationships between web content. It allows for the annotation of data with machine-understandable meta-data, which automates their retrieval and prevents them from being used in the wrong circumstances [13]. Tools for reasoning about ontology descriptions and languages for building ontologies are part

of the Semantic Web technologies. Examples of these languages are Resource Description Framework (RDF) and Web Ontology Language (OWL). To ensure that all agents with a basic understanding of Semantic Web technologies can communicate and utilise one other's data and Services effectively, these technologies can be utilised to establish uniform semantics of privacy information and regulations [14].

C. Text Extraction

Scientists have sifted through the massive text document corpus using the Natural Language Processing method to glean useful information. Researchers Rusu et al. [10] proposed a method to glean useful data and expressions by constructing subject-predicate-object triples. To do this, we first created Parse Trees from English sentences, and then we extracted triples from them [15]. The author of [16] created the KNOWITALL system as part of their research. It is scalable, domain-independent, and unsupervised, and it has helped automate the process of extracting large amounts of web-based data [17]. This problem was solved by the author by employing the strategy of Pattern Learning [17]. A different study found that "Noun Phrase Extraction" is an essential natural language processing method for data extraction from unstructured text [17]. Using 'Noun Phrases' retrieved from different part-of-speech taggers, the author [18] demonstrated the method of triplet creation. In order to extract the duties and authorisations from legal documents, many automated methods have been employed [19]. A number of writers have already investigated and used methods like text mining and semantic strategies [20]. A policy framework based on ontologies was suggested by the authors of [21] to represent policies and conversation specifications using permissions and obligations [22].

STEPS FOR SUCCESSFUL CLOUD SECURITY AUTOMATION

Fig 1: *Steps for successful cloud security automation*

Here are five best practices for the successful implementation of cloud security automation:

1) Automate Infrastructure Buildout

Engineers save a lot of time and effort by not having to manually configure things like security groups, networks, user access, firewalls, DNS domains, and log shipping thanks to infrastructure buildout automation. This makes it much less likely that developers will make security-related blunders. Also, security automation doesn't have to stress over best practices every time they launch a new instance because they can make modifications to the scripts and not the instances themselves.

2) Automate Script

An organization's system engineers would have to labour tirelessly to manually patch each server in the event of a zero-day vulnerability or other serious security workflow automation issue in traditional IT. But automating routines is as easy as changing one line in the manifests to point to the freshly released version. Instances, virtualised servers, or even bare metal servers can be automatically configured with the help of these declarative management tools—automatic script resources. These scripts prepare a newly launched instance for production by performing security configuration chores such as central authentication, intrusion detection agent installation, and multi-factor authentication.

3) Automate Deployments

An organization's security posture can be enhanced by automating deployments, which is a best practice in DevOps implementation. Deployment automation is crucial in a zero-day vulnerability because it guarantees that all instances or servers automatically receive any modifications made to the DevOps tool script. A single system engineer can now react swiftly to threats.

4) Set Up Recurring Security Checks

It is critical to be able to monitor the complete infrastructure through a single interface in the increasingly popular hybrid and multi-cloud setups that enable individual apps. It might be time-consuming and stressful to find and fix

the problem during automated security attacks and downtime.Engineers can better respond to threats and protect vital assets with the help of automated security monitoring.

5) Get Ready for the Future of Automation

Within the next several years, data balloons and hybrid environments will become commonplace, rendering the manual security method ineffective. That being said, building or contracting out an in-house automation team couldn't be timelier. It may take months or even years to achieve end-to-end process automation across hybrid environments, but the value will outweigh the time and effort spent educating staff to minimise human error.

STAGES OF CLOUD SECURITY AUTOMATION FRAMEWORK

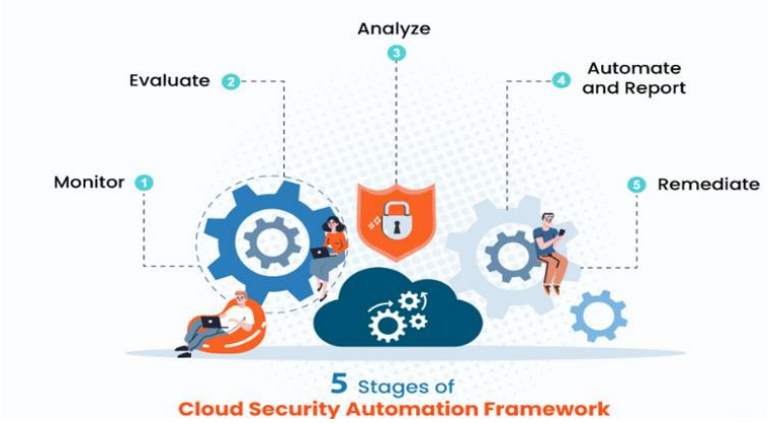

Fig 2: *5 Stages of Cloud Security Automation Framework*

Automation of cloud security involves a 5-step strategy as follows:

1) Monitor

To accommodate any and all operational demands, your cloud capacity may be easily scaled up or down. Therefore, it is crucial to keep an eye on the progress of each activity in your automated cloud security operations. You can learn the ins and outs of each workflow this way.

2) Evaluate

Identifying and ranking the activities to automate is an essential initial step in automating cloud security infrastructure. Routine chores, automated cloud installations, resource provisioning, and the creation of automation security rules are all examples of processes that could benefit from close monitoring in order to determine whether they could be automated.

3) Analyze

Sort the data by severity level: low, medium, or high, and then analyse it thoroughly. Automate low-risk processes before moving on to medium- and high-risk ones. You can investigate the effects on infrastructure and undertake controlled automation with the help of the thorough analysis.

4) Automate and Report

It is now possible to automate the workflows by pushing the results of the analysis to interconnected systems. The next step is to set up the automated processes so that they can produce reports that summarise the modifications either before or after.

5) Remediate

Whether you began automating basic or complicated procedures, you will now have a good understanding of cloud automation. As a result, you may improve the automation security posture as a whole and put corrective measures into action.

Automation in Cloud Security

Scripts, workflows, and technologies are used to automate security procedures and operations in the cloud. Automation is crucial in several important domains, such as:

Vulnerability Management: Rapid patching is possible in cloud systems because to automated vulnerability scanning techniques that find and rank issues.

Identity and Access Management (IAM): To make sure that no one other than authorised users may access sensitive information, automation can help implement policies like least privilege access.

Incident Response: In the event that a security incident is detected, automated incident detection and response systems can initiate predetermined measures to minimise harm.

Security Configuration Management: Security configurations can be kept consistent with best practices by automated inspections, which reduces the chance of misconfigurations.

DevSecOps in Cloud Security

With an emphasis on cooperation amongst development, operations, and security teams, DevSecOps incorporates security into the DevOps process. That security is built into the software development and deployment lifecycle from the start, rather than being an afterthought, is what it guarantees. The following are important parts of DevSecOps for cloud security:

Shift-Left Security: Integrating security considerations from the beginning of program development helps reduce vulnerabilities and minimises the need for patches after launch.

Continuous Integration/Continuous Deployment (CI/CD): By automating and integrating security testing into CI/CD pipelines, quick development can be achieved without sacrificing security.

Collaborative Culture: With DevSecOps, development, operations, and security teams work together in an atmosphere of mutual respect and accountability, making sure that security is a top priority for all parties involved.

Security-as-Code

The term "security-as-code" refers to the method of encoding configuration and policy details for system security. Consistency, version control, and automatability of security measures are guaranteed by this method. For cloud security, Security-as-Code offers several important advantages, such as:

Policy Enforcement: The definition of security policies in code guarantees that policies are consistently and auditably enforced throughout the cloud environment.

Scalability: Cloud environments can easily replicate security setups and rules with Security-as-Code, which is very useful for scaling them.

Change Management: By utilising version control systems, security policy changes may be monitored, tested, and deployed with less chance of configuration errors.

Cloud security process automation improves overall cloud environment security, speeds response times to security threats, lowers the likelihood of human mistake, and guarantees compliance with industry laws. Also, instead of doing mundane, repetitive security chores, teams can concentrate on more strategic endeavours like proactive threat hunting.

CONCLUSION

Clients who are thinking about migrating their data to the cloud but aren't sure if it's safe since they don't know what compliance models are available can benefit from our Cloud security comparison system. We were also able to more accurately identify and quantify the Cloud security policies and controls thanks to this research. Ongoing efforts include researching and evaluating alternative IT compliance models with the goal of refining our prediction algorithm. Security controls and compliance models will be highlighted in the analysis, as we predicted. The prototype will also aid Cloud users in selecting Cloud service providers according to the security compliance approach. One of our future goals is to improve the recommendation system by factoring in the price of cloud providers. Considering the cost will help us find the best Cloud provider. Also, this model prototype is not limited to security-related IT compliance models. By integrating this technology with e-commerce suppliers, we may discover the best solution for B2B services.

REFERENCES

[1]. K. P. Joshi, Y. Yesha, and T. Finin, ‘‘Automating cloud services life cycle through semantic technologies,’’ IEEE Trans. Services Comput., vol. 7, no. 1, pp. 109–122, Jan. 2014.

[2]. C. S. Alliance, ‘‘Cloud security alliance warns providers of 'the notorious nine' cloud computing top threats in 2013,’’ Threats Working Group Notorious Nine Cloud Computing Threats, vol. 2013, p. 8, Oct. 2013.

[3]. Security at Scale: Governance in AWS, Amazon Web Services, Seattle, WA, USA, Nov. 2013.

[4]. Rackspace, Rackspace Security Management. Accessed: Jan. 12, 2018. [Online]. Available: https://www.rackspace.com/security/management/

[5]. Google Apps to Offer Additional Compliance Options For EU Data Protection. Accessed: Jun. 6, 2012. [Online]. Available: http://googleenterprise.blogspot.com/2012/06/google-apps-to-offer-additional.html

[6]. F. Liu, J. Tong, J. Mao, R. B. Bohn, and J. V. Messina, NIST Cloud Computing Reference Architecture, document LEAF P 15-16, Sep. 2011.

[7]. S. Watkins, An Introduction To Information Security and ISO. Cambridgeshire, U.K.: IT Governance, 2013.

[8]. The SSAE16 Auditing Standard. Accessed: Dec. 14, 2013. [Online]. Available: http://www.ssae-16.com/

[9]. FEDRAMP, About Fedramp. Accessed: Mar. 20, 2015. [Online]. Available: http://www.gsa.gov/portal/category/102375

[10]. D. Rusu, L. Dali, B. Fortuna, M. Grobelnik, and D. Mladenic, ‘‘Triplet extraction from sentences,’’ in Proc. 10th Int. Inf. Soc., 2007, pp. 8–12.

[11]. O. Etzioni, M. Cafarella, D. Downey, A. M. Popescu, T. Shaked, and S. Soderland, ‘‘Unsupervised named-entity extraction from the WEB: An experimental study,’’ Artif. Intell., vol. 165, no. 1, pp. 91–134, 2011.
[12]. A. Hendre, T. Finin, and A. K. P. Joshi. (Jul. 2014). Cloud Security and Compliance Ontology. [Online]. Available: http://ebiQ.org/r/361/
[13]. SPECIFICATION V1.1.0, DMTF, New York, NY, USA, 2010.
[14]. T. Metsch and A. Edmonds, ‘‘Open cloud computing interface infrastructure,’’ in Proc. OCCI, 2010, pp. 1–7.
[15]. CSA Security Guidance, CSA, New Delhi, India, Nov. 2014.
[16]. P. Mell and T. Grance, The NIST Definition Of Cloud Computing. Gaithersburg, MD, USA: National Institute Standards Technology, 2011.
[17]. K. Joshi and P. C. Pearce, ‘‘Automating cloud service level agreements using semantic technologies,’’ in Proc. IEEE Int. Conf. Cloud Eng., Tempe, AZ, USA, 2015, pp. 416–421, doi: 10.1109/IC2E.2015.63.
[18]. Application Security and Development STIG, document V3R7, Apr. 2014.
[19]. L. Kagal and T. Finin, ‘‘Modeling communicative behavior using permissions and obligations,’’ in Proc. Int. Workshop Agent Commun., New York, NY, USA, Jul. 2004, pp. 120–133.
[20]. (2001). Introduction. [Online]. Available: http://www.standards.bz/iso-27002.html