# Security Audit of Cloud Infrastructure for AWS

Ravipati Sai Pridhvi, Saranu Yeshasri.
Department of Computer Science & Engineering,
VFSTR University, Andhra Pradesh, India
pridhvi.sai@gmail.com,saranuyeshasri26@gmail.com

**Abstract:** Amazon Web Services (AWS) cloud platform has a problem of security of having more identity and access management (IAM) users in there AWS cloud infrastructure and IAM role is a commutation with in the API's to the cloud infrastructure giving more permissions to the IAM role cause problem to amazon cloud infrastructure and security group which gives inbound and outbound access to the elastic computing cloud to all the users to may be the problem to cloud infrastructure and amazon simple storage service (S3) is there data storage in this who all has access to read and write permissions to the S3 buckets and key pair is the public and private keys to use commutation between the AWS elastic computing cloud (EC2) machine and local machine. Giving more permissions may cause's problem, so that wise we use to do security audit on AWS cloud infrastructure to report all this problem to AWS cloud users.

**Keywords:** AWS Cloud, Security Group, IAM, Key Pair, S3

.

## I. INTRODUCTION

### 1. Prologue to Cloud Security review for AWS

Consider cloud security review for AWS, who conveys proactive operational bits of knowledge, executes dull IT undertakings and offers brilliant suggestions for enhancing cloud spend. It is a wise Operational stage for open cloud administrations. The Security Audit for cloud draftsmen, cloud architects and IT chiefs to give them an additional pair of eyes and ears, that work in the virtual universe of the general population mists. The item was worked after deliberately investigating regular issues confronted by clients amid cloud operations. It was seen that while clients would prefer not to be bothered with an excess of devices, despite everything they have to work around complex issues, whilst overseeing mission basic workloads. This need is vastly improved balance with a robotized, master framework that sees how to apply knowledge with security. While robotization makes for more brilliant, more productive operations, you will dependably require your trusty building group. Security Audit does not endeavour to supplant this centre capacity, but rather is attempting to help it as a virtual cloud engineer who turns into your additional pair of eyes and ears in a virtual setup. Failing to tire, prepared to act even amidst the night, Security Audit along these lines makes an extraordinary expansion to a current group of cloud specialists. Including Security Audit is an awesome expansion to a current cloud group. Security Audit is the savvy bot, who will make cloud operations more productive by helping cloud modellers, designers and entrepreneurs. It will streamline your life by lessening the time spent on your normal cloud errands and unsurprising treatment of monotonous work.

- Schedules day by day cloud review
- Identifies infringement and dangers
- Enforces cloud best practices
- Get day by day reports
- Get cautioned on issues
- Get to the main driver speedier with all the over, the proficiency of a Cloud Ops Engineers' productivity is expanded.
- Better situational mindfulness
- Build a superior cloud-based business
- Get alarmed on security edges
- Helps oversee security
- Enables speedier reaction from your group
- Keeps you educated through reports

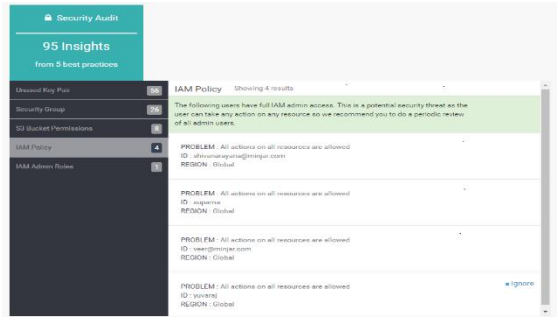
## II. METHODLOGY

Security Audit is the smart bot, who will make cloud operations more efficient by assisting cloud architects, engineers and business owners. It will simplify your life by reducing the time spent on your regular cloud tasks and predictable handling f repetitive work.

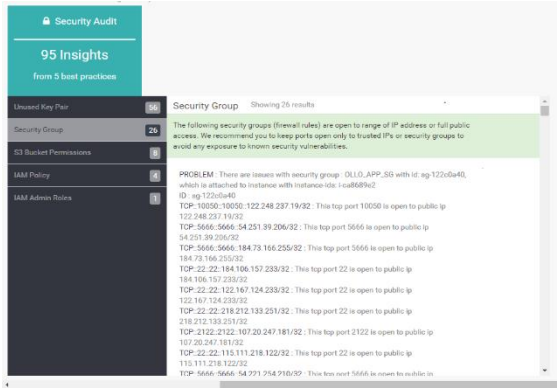
**IAM Role Access Controls:** AWS Identity and Access Management (IAM) having one unique IAM admin for your AWS account is risky. Instead, have one or more AWS IAM users, give them the permissions, and use these IAMs for everyday interaction with AWS. Also, try to use

temporary security credentials (IAM Roles) instead of long-term access keys.

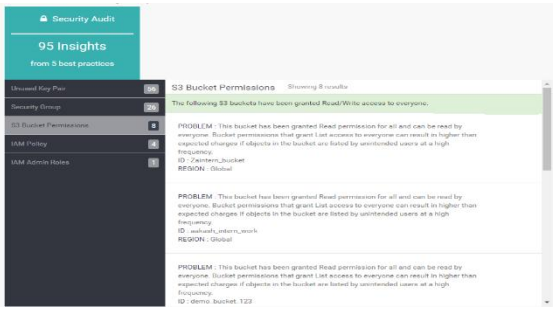
**IAM User:** Total number of admin accounts. If there are too many IAM admin accounts, this may lead to security issues. It is recommended not to have many IAM users with admin rights. You can grant different permissions to different people for different resources.EC2 instances the credentials that they need in order to access other AWS resources, like S3 buckets and RDS or Dynamo DB databases.



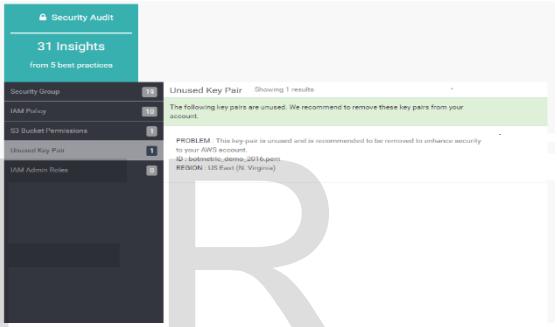

**Security Group:** A security group acts as a virtual firewall that controls the inbound and outbound traffic for one or more instances. You associate a security group with the launch of each instance. Since the data may have an open IP port or is open to public access, there are chances of data breach. In order to avoid exposure to security vulnerabilities, we recommend that only ports associated with relevant IP and security groups are kept open.




**S3 (Simple Storage Service)**: Amazon S3 default, all S3 bucket permissions are private and you need to give Read/Write access permissions to others by writing an access policy. Bucket permissions that grant List access to everyone can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency. Make sure you are granting limited access permissions.




**Key Pair:** EC2 Key Pairs are used for encrypting and decrypting login information: To log in to your instance, it is essential to generate a key pair, identify the name of that key pair when instance has to be launched, and provide the information about the private key when you connect to the instance.




To have your example of security Audit screen extra records, you should include a Security Audit part in the new record. Take after the guidelines above to make the new Security Audit part. The Trust Relationship approach ought to have the record ID of the record where the security Audit case is running.

## III. TECHNOLOGY USED

**Python and other Python Libraries:**
I have utilized Python 2.7 as a part of this venture as it is a simple to learn, capable programming dialect. It has proficient abnormal state information structures and a straightforward yet viable way to deal with item arranged programming. Python's rich linguistic structure and element writing, together with its deciphered nature, make it a perfect dialect for scripting and quick application improvement in numerous ranges on generally stages. The Python mediator and the broad standard library are unreservedly accessible in source or paired structure for every single real stage from the Python web webpage,

https://www.python.org/, and might be uninhibitedly dispersed. The same site likewise contains disseminations of and pointers to numerous free outsider Python modules, projects and instruments, and extra documentation. The Python translator is effectively stretched out with new capacities and information sorts executed in C or C++ (or different dialects callable from C). Python is additionally suitable as an augmentation dialect for adaptable applications. Different Python Libraries have been utilized. Boto is a Python bundle that gives interfaces to Amazon Web Services. At present, all elements work with Python 2.6 and 2.7.

**Boto Config:** There is a developing rundown of arrangement choices for the boto library. A number of these alternatives can be gone into the constructors for top-level questions, for example, associations. A few alternatives, for example, accreditations, can likewise be perused from environment variables (e.g. AWS_ACCESS_ KEY_ID,AWS_SECRET_ACCESS_KEY,AWS_ SECURITY_TOKENand AWS_PROFILE). It is likewise conceivable to deal with these alternatives in a focal spot using boto config documents.

**Django :** Django is an abnormal state Python Web system that supports fast advancement and perfect, down to earth plan. Worked by experienced designers, it deals with a great part of the bother of Web improvement, so you can concentrate on composing your application without expecting to re-examine the wheel. It's free and open source.

➢Ridiculously Fast

➢Fully Loaded

➢Reassuringly secure

➢Exceedingly adaptable

➢Incredibly flexible

## IV. RESULT

With the increase in cloud computing in the industry, many threats are being faced by large companies. They need to restrict the access to their resources on cloud, and only want them to be accessed from their trusted locations. Moreover, with the up-scaling of different resources, relationships between resources constantly keeps on changing and with the large amount of users in a large organization tracking which user has what access rights and what changes a particular user has made to resources and their relationships with other on-cloud resources. Also, there is a need to track all the activities and events and user who has performed those activities. For solving the above mentioned problem, I have created 5 different submodules which can be used separately for solving different purposes. This sub-module fetches the information related to all the IAM Roles form Amazon IAM service. This checks the permissions that they have related to Amazon EC2, Amazon S3 and Amazon RDS. All the unused permissions are sent to user after auditing. The IAM User form Amazon IAM service. This checks the permissions that they have related to Amazon EC2, Amazon S3 and Amazon RDS. All the unused permissions are sent to user after auditing. The security group acts as a virtual firewall that controls the inbound and outbound traffic for one or more instances, since the data may have an open IP port or is open to public access. After auditing we recommend that only ports associated with relevant IP and security groups are kept open the S3 bucket permissions you have to give Read/Write access permissions to others by writing an access policy has granted to everyone. All the unused permissions are sent to user after auditing all the unused access keys for last 8 weeks and alerts the user to disable these access keys as these may be a potential threat in future because if someone else got those credentials, it can be potential threat.

## V.CONCLUSION

During the span of this project, I learned various new technologies and various industry practices. I got familiar with the Amazon Web Services (AWS) Cloud Platform and various products and services offered by them. Security audit and provided users with the useful information regarding security resource changes and events in their amazon account, which may result in potential security threat.

## VI.REFERENCES

[1] A. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[2] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3350.

[3] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[4] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[5] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[6] Pring et al., "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.

[7] Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-39614.

[8] B. R. Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

[9] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing," TheWorldPrivacyForum,2009.http://www.worldprivacyforum.org/pdf/WPF_Cloud_ Privacy_Report.pdf.

[10] Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O' Reilly Media, USA, 2009.

[11] Ronald L. Kurtz, Russell Dean Vines "Cloud Security A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc., 2010

[12] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.