iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3063

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

IAM Services in Cloud Computing: Project Management for Enterprises

Sahil Pawar[1], Monika Singh[2]
[1, 2]*SICSR*

Abstract: ***Cloud computing is one of the most emerging technologies in today's scenario which aims to provide on-demand scalable access to computing resources over the internet via cloud vendors to multi-tenant organizations. Cloud computing provides a way through which an organization can increase their computing capabilities and infrastructure facilities dynamically as and when required. While cost and On-demand availability are the top two benefits of cloud, but various trust and security issues are becoming the top concerns for the cloud computing users. In federated identity management environment, federated identity as a useful feature for Single Sign-on (SSO) and user management has become an important part. Some of the problems in federated identity management environment are platform trustworthiness, management of multiple digital identities, identity theft. Security assertion markup language (SAML), OAuth, OpenID is the main concepts in cloud authentication and federated environment. This paper addresses the issue of Identity and Access Management (IAM) on various cloud platforms and their comparisons.***

Keywords: Cloud Computing, SSO, OpenID, Oauth, Identity federation, IAM, provisioning, Identity federation standards

I. INTRODUCTION

Cloud Computing is a technology which aims to provide on-demand scalable services over the Internet via Cloud vendors to multi-tenant organizations. Cloud Computing is defined by the National Institute of Standards and Technology (NIST) as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. An identity is a set of unique characteristics of a user. An Identity Management System (IDM) supports the management of multiple digital identities, their authentication, authorization, roles, and privileges within or across system. It also decides how to disclose personally identifiable information (PII) and service specific user credentials of any user. IDM has various components such as: Directory services, Access management, Password administration including single sign-on, Identity authentication, User provisioning, Roles management and Federated identities, which enables the creation of virtual communities of customers and partners that can conduct business on different websites with a single log-in.

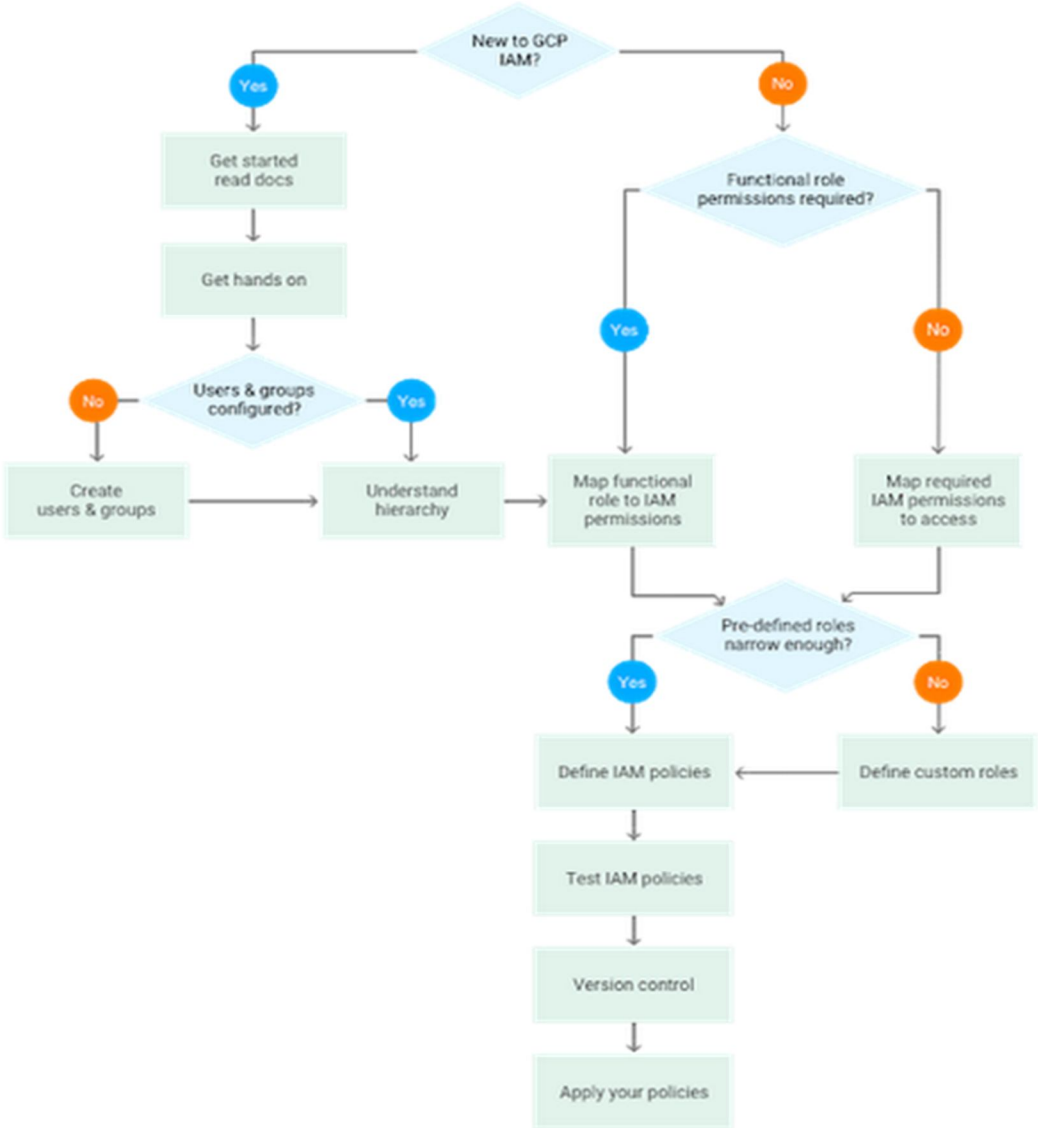
II. IMPORTANCE OF IDENTITY MANAGEMENT IN CLOUD

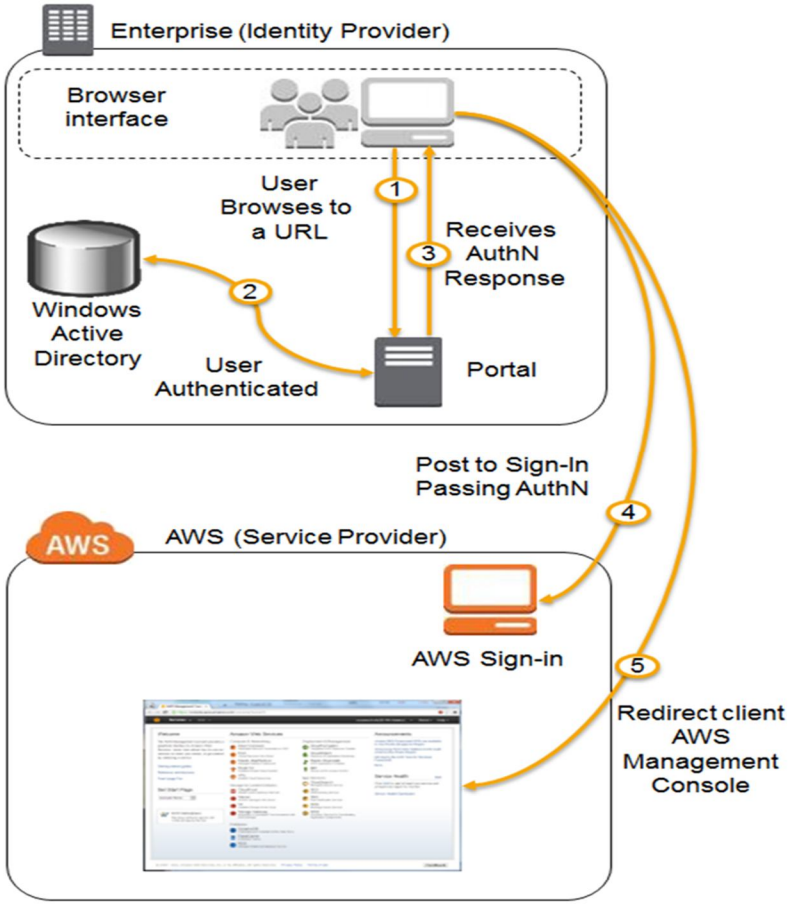
With the technological growth of cloud computing, web applications have migrated towards clouds and have raised the concerns for privacy and security of user specific sensitive data, like how can an end user or consumers verify that a service provider conform to the privacy laws and protect consumer's digital identity. Most of the service providers (e.g., Gmail and Google Maps are offered by Google) require the username/password security token to authenticate consumers but that leaves the consumer vulnerable to phishing attacks. To address this problem Identity Management (IDM) System can be used to provide the solution. IDM solution should help any user in making a suitable choice about how and what personal information user disclose, manage and control how user information can be used, cancel user subscription to any service, and keep tracking to verify that a service provider applies essential privacy policies. Most of the emphasis has been laid down on how to enable a more secure authentication event through the mechanisms like Active Directory or Shibboleth, which is a key component of securing the transaction between Identity Providers(IdP) and Service Providers (SP) IDM in cloud computing environment is an essential activity as large number of consumers and services are used. Many cloud consumers are accessing and using the cloud based services on a large scale, which comes up with security concerns of user data. Therefore, monitoring, storing, managing and controlling user identities is very crucial security concerns and requires a trust based solution. In an effort to understand the failures (and limited successes) of preceding identity management systems, Kim Cameron proposed seven laws of identity that he claims are essential for successful identity management systems. They are:

1) User Control and Consent: An IDM system must obtain a user's permission to discover information that identifies the user.

2) Minimal Disclosure for a Constrained Use: An IDM system that exposes less identifying information and inforces more limits on its use is preferred.
3) Justifiable Parties: An IDM system must be designed so that identifying information is revealed only to parties having a essential and justifiable need.
4) Directed Identity: An IDM system must sustain global identifiers for use by public entities and local identifiers for use by private entities.
5) Pluralism of Operators and Technologies: An IDM system must sustain interoperability of multiple identity technologies executed by different identity providers.
6) Human Integration: An IDM system must employ unambiguous human-machine interaction mechanisms that forbid identity-based attacks (example: phishing and impersonation).
7) Consistent Experience across Contexts: An IDM system must provide a simple, uniform experience to users while supporting multiple operators and technologies.

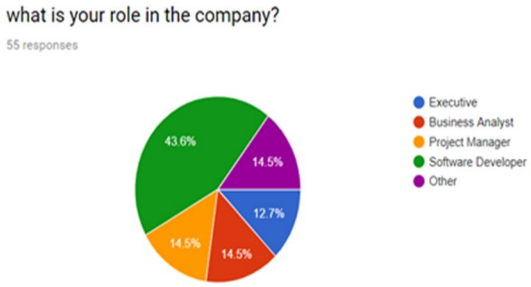
III. Flow OF IAM



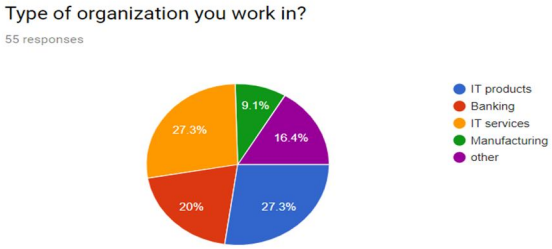


IV. METHODOLOGY

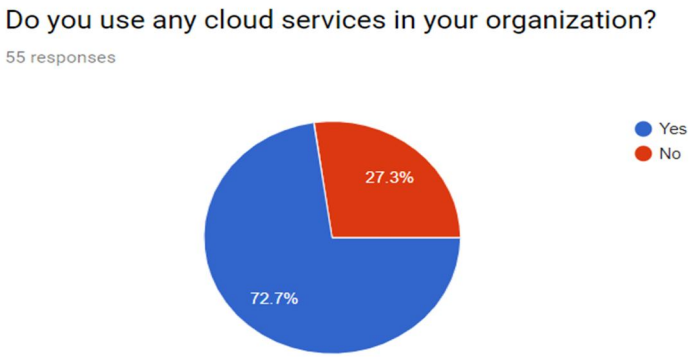
For getting to know more about IAM, we have conducted a survey where we asked professionals some questions



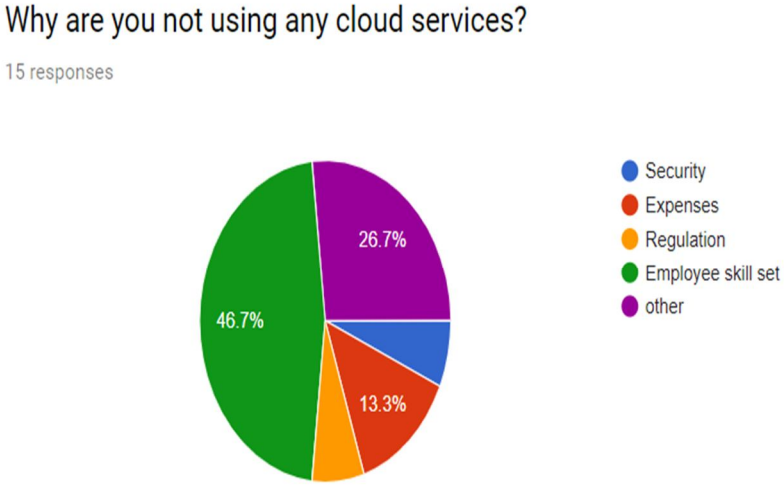
A. Mostly, to the people that we asked question about their profession, most of them were software developers.



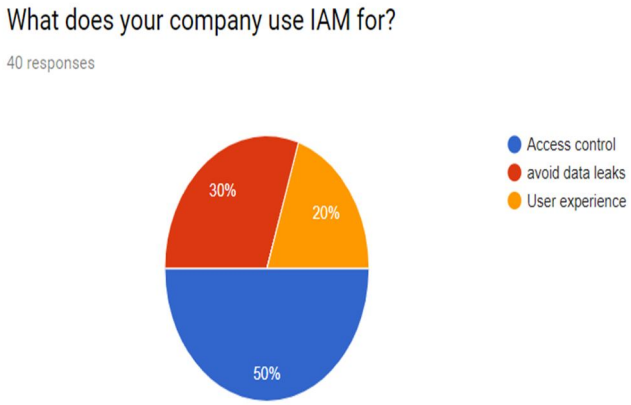
B. In general, these professionals work in the industry of IT products and IT services.



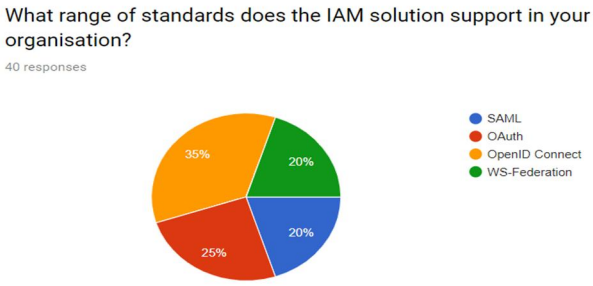
C. Most companies or organisations have or use cloud services for their work. It makes the work more reliable.



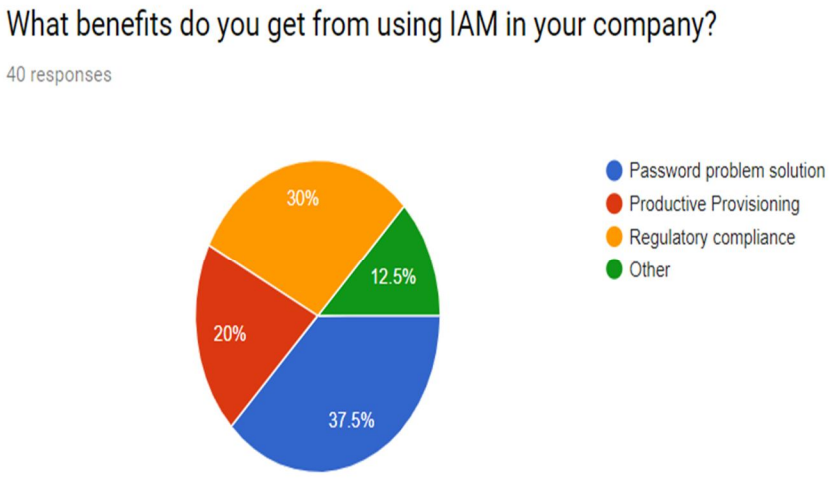
D. Organisations which do not use cloud services are mostly due to lack of employee skill sets. Employees do not have the ability to work on cloud platforms.



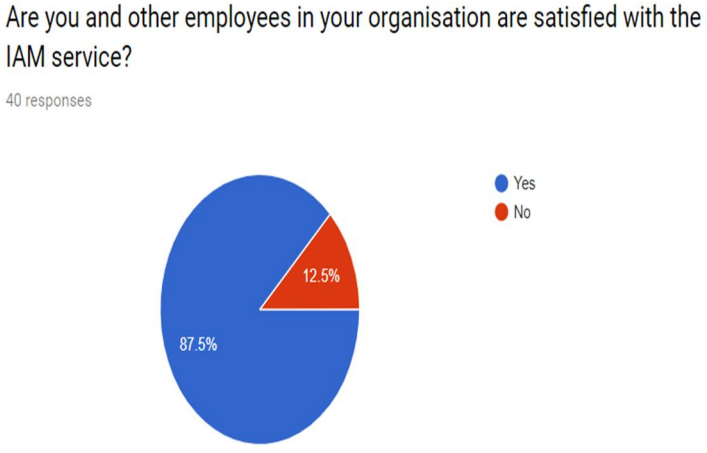
E. In most organisations, where they use IAM service, they use it for access control maximally.



F. OpenID Connect range of standards is mostly supported by the organisations. Other standards such as SAML, OAuth are less used.



G. Password problem solution is the main purpose of using IAM in organisations. Causes like regulatory compliance, productive provisioning is also the reason companies use it.



H. Professionals are mostly satisfied with the use of IAM service in their organisations.

V. COMPARISON

Concept	AWS	GCP
Users and Groups	Create individual users and add users to a group in AWS. The users do not need an email ID and are authorized to access various AWS resources.	Create members but they must have a Google account, or Create a Google Group and add the members' email addresses to it. The users can be outside of GCP.
Policy	A document that explicitly lists permissions. A policy is attached to a user or a group	A list of bindings that binds a list of members to a role. A policy is attached to a resource
Custom Policy	You can define a custom policy using JSON language.	You can only create a custom policy from existing list permissions.
Policy Versions	Versioning of policies is available.	Versioning is not available.
Programmatic Access	Access is possible by attaching an IAM role to an instance, or through AWS CLI.	You will require an IAM service account specially for programmatic access.
Environments	You create different accounts and link them using Account Access.	You can create projects where the resources of each project are totally isolated from the other projects in the same account
API	AWS provides SDKs to be able to connect with IAM API.	GCP provides a URI where you can send different types of HTTP requests to manage the IAM service.
Role Stages	There are no role launch stages available in AWS.	GCP provides different stages to create roles such as Alpha early development stage. Beta tested before rollout General Availability Ready for production..

VI. CONCLUSION

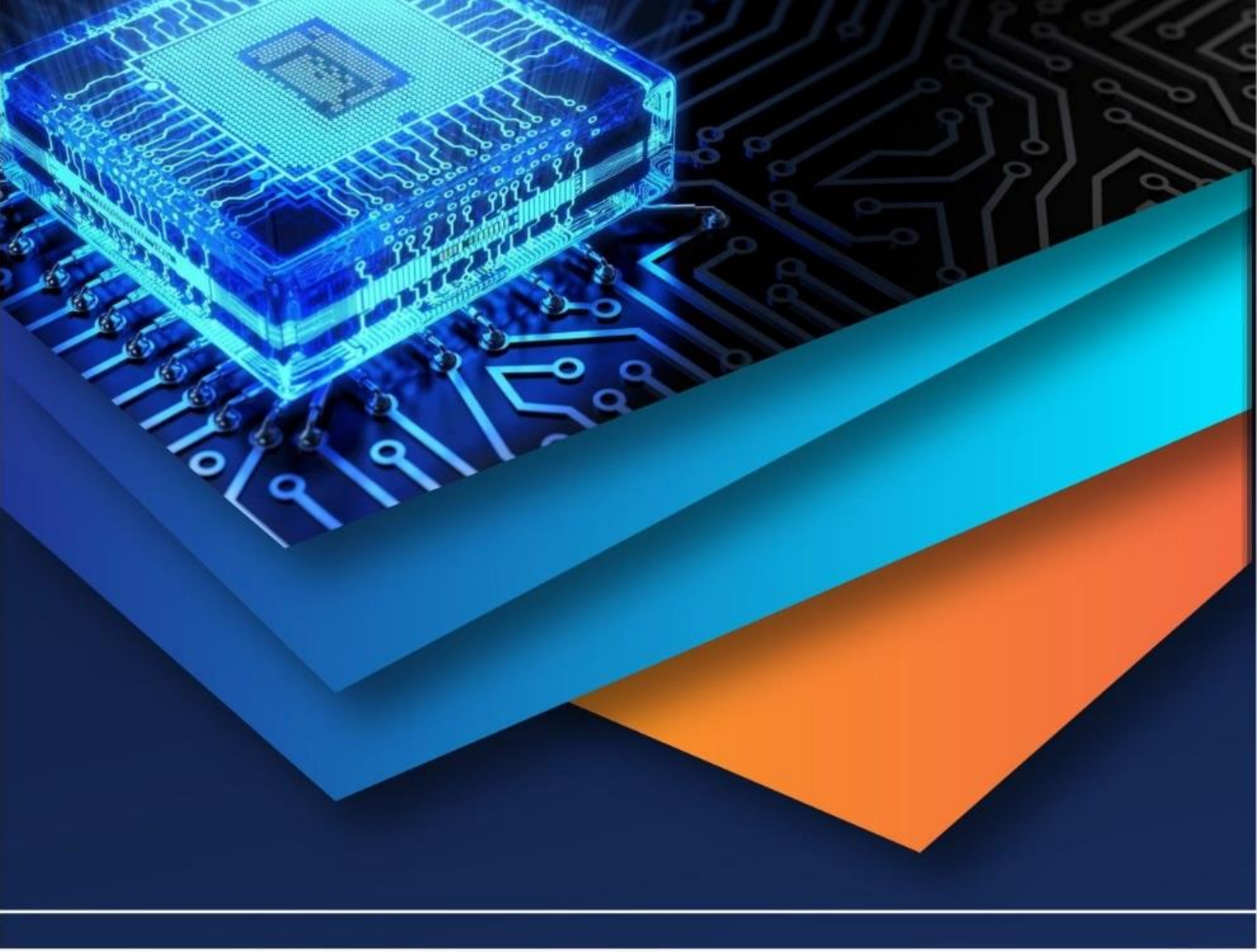
Cloud Identity and Access Management (Cloud IAM) enables you to create and manage permissions for Google Cloud Platform resources. Cloud IAM unifies access control for Cloud Platform services into a single system and presents a consistent set of operations. From this paper, we can conclude that AWS is better in terms of policy versioning, customization of policies and user groups but AWS is costly. However GCP is better in terms of role stages. By comparing all the parameters AWS is better option provided that it fits into budget of the organisation.

VII. ACKNOWLEDGEMENT

We are extremely grateful to Mr. Supratik Ghatak for his valuable guidance in the making of this reasearch paper. We are also thankful to Symbiosis Institute of Computer Studies and Research for providing us the infrastructure to carry out the study.

REFERENCES

[1] A Survey on Identity and Access Management in Cloud Computing Nida1, Pinki2, Harsh Dhiman3, Shahnawaz Hussain41, 2, 3,4M.tech(CSE), School of Computing Science and Engineering, Galgotias University, Greater Noida, Indi
[2] Angin, P., Bhargava, B., Ranchal, R., Singh, N., Linderman, M., Othmane, L. Ben and Lilien, L. 2010. An entity-centric approach for privacy and identity management in Cloud computing. In Proceedings of the 29th IEEE Symposium on. IEEE in Reliable Distributed System.
[3] Rizwana Shaikh, M. Sasikumar, "Identity Management in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 63-No.11, February 2013.
[4] https://www.cs.purdue.edu/homes/bb/IDM-final.ppt.
[5] https://www.stratoscale.com/blog/compute/comparing-google-iam-aws-iam/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY