1. Introduction

In recent era, due to its affordability, scalability, and flexibility, cloud computing has emerged as the preferred technology for many businesses. Instead of owning and maintaining own infrastructure, businesses can access a variety of computer resources, such as databases, storage, and applications, through the internet. The two most well-known suppliers of cloud computing services are Google Cloud Platform (GCP) and Amazon Web Services (AWS). Cloud-based services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are all offered by both AWS and GCP (Mell, 2011). This paper compares and evaluates AWS and GCP in three areas: Identity and Access Management (IAM) and Identity Aware Proxy (IAP), Endpoints, and Web Service Support. IAM and IAP enable businesses to securely manage user access to cloud resources. Endpoints allow us to expose Google Cloud and AWS services to the internet. Developers can use Web Service Support to create and deploy web apps on cloud platforms (Rehman 2017).

IAM is a service that gives businesses the ability to securely manage access to cloud resources. Identity-based access control is offered by AWS IAM for AWS services and resources. Businesses can utilize a web interface or programmatically to manage users and their access to AWS services and resources. Cloud Identity and Access Management, a similar service offered by GCP, enables businesses to control who has access to which cloud resources for users, groups, and service accounts (Zhang, 2016). IAP, on the other hand, is a solution that enables businesses to manage access to apps that are hosted on GCP and AWS. Similar services are offered by AWS under the names AWS WAF and AWS Identity and Access Management. For applications running on GCP, IAP interfaces with Cloud IAM to offer a centralized policy enforcement point.

Endpoints allow us to expose GCP and AWS services to the internet (Soltys, 2021). Amazon API Gateway is a service provided by AWS that allows businesses to establish, manage, and protect APIs at any size. RESTful APIs and WebSocket APIs are supported by Amazon API Gateway. GCP offers Cloud Endpoints, which let businesses to design, deploy, and manage APIs that adhere to the OpenAPI definition. Cloud Endpoints supports gRPC APIs, which are a high-performance, open-source platform for developing RPC APIs. Web Service Support, on the other hand, enables developers to create and deploy web applications on cloud platforms. Elastic Beanstalk is an AWS service that allows developers to deploy and manage web applications written in a range of programming languages, including Java,.NET, PHP, Node.js, Python, Ruby, and Go (Varia, 2014). The deployment specifics, such as resource provisioning, scalability, and monitoring, are handled by Elastic Beanstalk. With the help of GCP's App Engine, programmers may create and publish web applications and APIs in a number of different programming languages, including Java, Python, PHP, Node.js, Go, and Ruby. Scaling, load balancing, and other deployment-related concerns are handled by App Engine (Sony, 2014).

On the basis of three technologies—IAM and IAP, Endpoints, and Web Service Support—In this report, I have contrasted and critically evaluated AWS and GCP. Similar IAM and IAP, Endpoints, and Web Service Support capabilities are offered by both AWS and GCP. Nevertheless, GCP offers App Engine, which supports a number of programming languages, including Python, Node.js, and Go, and Cloud Endpoints, which supports gRPC APIs. Elastic Beanstalk, a feature of AWS, supports a number of programming languages, including Java,.NET, PHP, Node.js, Python, Ruby, and Go, and Amazon API Gateway offers support for RESTful and WebSocket APIs (Sony, 2014). Table 1 provides critical comparison of Google Cloud and AWS.

Table 1. Critical comparison of Google Cloud and AWS

Category	***Google Cloud***	***AWS***
Compute Services	Google Compute Engine, Google Kubernetes Engine, Cloud Run, Cloud Functions	Amazon EC2, Amazon Lightsail, AWS Lambda, Amazon ECS, Amazon EKS
Storage Services	Google Cloud Storage, Google Cloud SQL, Google Cloud Spanner, Google Cloud Bigtable	Amazon S3, Amazon EBS, Amazon EFS, Amazon Glacier
Database Services	Google Cloud SQL, Google Cloud Spanner, Google Cloud Bigtable, Google Cloud Datastore	Amazon RDS, Amazon DynamoDB, Amazon Redshift, Amazon Aurora
Networking Services	Google VPC, Google Cloud Load Balancing, Cloud CDN, Cloud Interconnect	Amazon VPC, Amazon Route 53, Amazon API Gateway, Amazon Direct Connect
Identity and Access Management	Google Cloud IAM, Google Cloud Identity, Google Cloud OAuth	AWS IAM, AWS Cognito, AWS Single Sign-On
Security and Compliance	Google Cloud Security Command Center, Google Cloud Armor, Google Cloud Identity-Aware Proxy, Google Cloud Key Management Service, Google Cloud SSL Certificates	AWS Security Hub, AWS Shield, AWS WAF, AWS Key Management Service, AWS Certificate Manager
Analytics Services	Google Cloud Dataproc, Google Cloud Dataflow, Google BigQuery, Google Data Studio	Amazon EMR, Amazon Kinesis, Amazon Athena, Amazon QuickSight
AI and Machine Learning Services	Google Cloud AI Platform, Google Cloud Vision API, Google Cloud Text-to-Speech, Google Cloud Natural Language API	Amazon SageMaker, Amazon Rekognition, Amazon Polly, Amazon Lex
Internet of Things Services	Google Cloud IoT Core, Google Cloud IoT Edge	AWS IoT, AWS Greengrass
Developer Tools	Google Cloud Deployment Manager, Google Cloud Source Repositories, Google Cloud Build, Google Cloud Code, Google Cloud Debugger	AWS CloudFormation, AWS CloudTrail, AWS CodeStar, AWS CodeCommit, AWS CodePipeline

2. IAM and IAP

Identity Aware Proxy (IAP) and Identity and Access Management (IAM) are two essential technologies that let businesses secure their cloud resources. The two most well-known cloud service providers, Google Cloud Platform (GCP) and Amazon Web Services (AWS), both offer IAM and IAP solutions. This comparative analysis compares the features, capabilities, and limits of the IAM and IAP services provided by AWS and GCP in order to critically evaluate them (Fedorov, 2020).

Organizations can control who has access to AWS resources with the use of the solution known as AWS Identity and Access Management (IAM). Companies may establish and manage AWS users and groups and grant them access to AWS resources thanks to IAM. IAM offers a centralized access control solution for AWS resources, which can be administered programmatically using APIs or using a web interface. Role-based access control (RBAC), multi-factor authentication (MFA), and identity federation are all supported by AWS IAM. Meanwhile, AWS Identity Aware Proxy (IAP), a service, gives businesses the ability to manage access to apps that are hosted on AWS (Li, 2020). IAP interacts with AWS IAM to give applications running on AWS a centralized policy enforcement point. IAP complies with the user authentication and authorization protocols set forth by OAuth 2.0 and OpenID Connect (OIDC). Businesses can set specific access controls based on user identity, group membership, and the security posture of the device thanks to IAP. IAP gives organizations the ability to monitor and log access attempts in real-time, allowing them to identify and address any security issues (Panigrahi, 2020).

Contrarily, Google Cloud Identity and Access Management (Cloud IAM) is a service that gives businesses the ability to control who has access to Google Cloud services. For Google Cloud resources, Cloud IAM offers a centralized access control solution that can be operated manually or programmatically using APIs (Mohammed, 2019). Companies may establish and manage Google Cloud users and groups thanks to Cloud IAM, which supports RBAC. Identity federation and MFA are also supported by Cloud IAM. Furthermore, A service called Google Cloud Identity Aware Proxy (Cloud IAP) enables businesses to manage access to GCP-based apps. When Cloud IAP and Cloud IAM are combined, a centralized policy enforcement point for apps operating on GCP is made available. OIDC and OAuth 2.0 standards for user authentication and authorization are supported by Cloud IAP (Roy, 2021). Businesses may create customized access controls based on user identity, group membership, and the security posture of the device thanks to cloud IAP. Organizations are able to recognize and respond to possible security issues thanks to the real-time monitoring and tracking capabilities offered by cloud IAP for access attempts.

Similar features and capabilities can be found in the IAM and IAP services provided by AWS and GCP. Both services support RBAC, identity federation, and MFA while offering centralized access control solutions for cloud resources. Both systems also support widely used user authentication and authorization protocols, including OAuth 2.0 and

OIDC (Roy, 2021). But there are certain distinctions between GCP Cloud IAM/IAP and AWS IAM/IAP. One noticeable distinction is that GCP Cloud IAM/IAP and Google Workspace have stronger interoperability, enabling businesses to control access to Google Workspace services from a single interface. Another distinction is that AWS IAP supports AWS WAF, allowing businesses to build unique rules to prevent typical attack patterns (Soliven, 2020).

For the purpose of protecting cloud resources, IAM and IAP are essential technologies, and both AWS and GCP offer reliable IAM and IAP solutions. Although there are significant differences in the support for custom rules and integration with other services, AWS IAM/IAP and GCP Cloud IAM/IAP have comparable capabilities and features. When deciding between AWS and GCP for their IAM and IAP solutions, organizations should carefully consider their unique needs and requirements.

Table 2. Comparison of IAM and IAP in Google Cloud and AWS

Feature	***AWS IAM***	***AWS IAP***	***GCP Cloud IAM***	***GCP Cloud IAP***
Centralized Access Control	Yes	Yes	Yes	Yes
User and Group Management	Yes	No	Yes	No
Permission Assignment	Yes	No	Yes	No
Multi-factor Authentication	Yes	No	Yes	No
Role-based Access Control	Yes	No	Yes	No
Identity Federation	Yes	No	Yes	No
Integration with Other Services	Yes (AWS IAP)	Yes	Yes (Google Workspace)	No
Support for Custom Rules	No	Yes	No	Yes
Standard Protocols Supported	OAuth 2.0, OIDC	OAuth 2.0, OIDC	OAuth 2.0, OIDC	OAuth 2.0, OIDC
Real-time Monitoring and Logging	No	Yes	No	Yes

3. Endpoints and Web Service support

Endpoints are essential parts of any contemporary programme because they give users a method to communicate with it. Amazon API Gateway, which offers a scalable and secure solution to create, publish, and manage APIs, can be used in AWS to construct endpoints (Patterson, 2019). REST, WebSocket, and HTTP are just a few of the protocols that Amazon API Gateway is compatible with. To build serverless applications, developers may simply combine their APIs with other AWS services like AWS Lambda (Stigler, 2018). To enhance disperse incoming traffic among various targets, such as EC2

instances, containers, and Lambda functions, AWS now provides Amazon Elastic Load Balancing (ELB). Endpoints are produced on Google Cloud using Cloud Endpoints, a fully managed service that lets programmers create, distribute, and maintain APIs. Cloud Endpoints offers a straightforward and user-friendly interface for developers and supports a variety of protocols, including gRPC and REST. Similar to AWS, Google Cloud provides a load balancing service called Google Cloud Load Balancing that may be used to split traffic between a number of instances or endpoints.

Both AWS and Google Cloud provide a variety of services that enable developers to deploy and maintain their web applications when it comes to web service support. Without worrying about the underlying infrastructure, developers using AWS can easily launch and maintain web apps with AWS Elastic Beanstalk. Numerous programming languages, including Java,.NET, and Node.js, are supported by Elastic Beanstalk. AWS Lambda enables developers to build serverless web apps that scalably grow in response to incoming traffic (Sendor, 2014). Utilizing App Engine, a fully managed platform that frees developers to concentrate on creating their apps without worrying about the supporting infrastructure, web applications may be launched and managed in Google Cloud. Python, Java, and Go are just a few of the programming languages supported by App Engine. Additionally, Cloud Functions, a serverless computing service that enables developers to run code in response to events like HTTP requests, is another service provided by Google Cloud.

Both AWS and Google Cloud provide strong support for web services and endpoints, as well as a variety of services that let developers launch and maintain their applications with ease and speed. AWS provides support for web services using AWS Elastic Beanstalk, AWS Lambda, and Amazon API Gateway for endpoints (Quadri, 2017). As an alternative, Google Cloud provides support for web services with App Engine and Cloud Functions as well as Cloud Endpoints and Google Cloud Load Balancing for endpoints. Developers should select the cloud provider that best satisfies their demands while deciding between the two options by taking into account their unique wants and requirements. In this regards, Table 3 provides a comprehensive comparison on the basis of endpoints and web service supports.

Table 3. Comparison of Endpoints and Web Services in context of AWS and Google Cloud

Feature	***AWS***	***Google Cloud***
Endpoints	Amazon API Gateway, Amazon ELB	Cloud Endpoints, Google Cloud Load Balancing
Supported Protocols	REST, WebSocket, HTTP	gRPC, REST
Web Service Support	AWS Elastic Beanstalk, AWS Lambda	App Engine, Cloud Functions
Programming Languages	Java, .NET, Node.js, and more	Python, Java, Go, and more
Managed Platform	No	App Engine
Serverless Compute Service	AWS Lambda	Cloud Functions
Integration with Other AWS	Yes	No

4. Conclusion

In this report, three essential technologies of Identity and Access Management (IAM) and Identity Aware Proxy (IAP), Endpoints, and Web Service Support have been thoroughly compared and evaluated in this report with respect to Google Cloud and Amazon Web Services (AWS). Both AWS and Google Cloud provide reliable IAM and IAP technologies for controlling user authentication and authorization. Google Cloud IAM enables more granular access control and easier integration with Google Cloud services, despite AWS IAM being more well-known and in usage. AWS necessitates the usage of extra technologies like Amazon Cognito and Amazon API Gateway, whereas Google Cloud's IAP offers a simpler solution for app security. Proceeding towards Endpoints, both Google Cloud and AWS provide tools for building and administering APIs. While Google Cloud offers Cloud Endpoints and Google Cloud Load Balancing, AWS offers Amazon API Gateway and Amazon Elastic Load Balancing. While the two services have similar features, Google Cloud supports the gRPC protocol, and Google Cloud Load Balancing has the ability to manage traffic globally, making it a more appealing choice for developers. I have compared the Web Service Support provided by AWS and Google Cloud, and that's all. While Google Cloud offers App Engine and Cloud Functions, AWS Elastic Beanstalk and AWS Lambda provide versatile and scalable alternatives for delivering web apps. AWS has an advantage in that it integrates with other AWS services and supports a larger variety of programming languages, but Google Cloud's App Engine offers a fully managed platform for the development of web applications. Overall, for managing identities, building APIs, and deploying web apps, both AWS and Google Cloud provide solid solutions. However, developers should take into account the distinct strengths and disadvantages of each platform when selecting a cloud provider. While Google Cloud offers easier and more streamlined options for managing identities and safeguarding applications, AWS is a more well-established platform with a wider selection of services and better interoperability with other AWS services. Both AWS and Google Cloud provide versatile and scalable web service support, with AWS supporting a greater variety of programming languages and Google Cloud offering a fully managed platform for the deployment of web applications.

5. References

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6), 50.

Rehman, S. U., & Wahab, M. A. (2017). Comparison between Amazon Web Services and Google Cloud Platform. International Journal of Computer Science and Network Security, 17(8), 81-91.

Zhang, Y., & Zhang, Z. (2016). A comparison study on cloud computing service providers: Amazon Web Services and Google Cloud Platform. In 2016 13th IEEE International Conference on e-Business Engineering (ICEBE) (pp. 155-160). IEEE.

Soltys, M., 2021, October. Cloudifying the Curriculum with AWS. In 2021 IEEE Frontiers in Education Conference (FIE) (pp. 1-7). IEEE.

Varia, J. and Mathew, S., 2014. Overview of amazon web services. Amazon Web Services, 105.

Soni, R.K., Soni, N., Soni, R.K. and Soni, N., 2021. Deploy a Spring Boot Application as a REST API in AWS. Spring Boot with React and AWS: Learn to Deploy a Full Stack Spring Boot React Application to AWS, pp.41-75.

Fedorov, V. (2020). Identity and Access Management (IAM) on AWS vs Google Cloud. Medium. https://medium.com/@vfedorov/identity-and-access-management-iam-on-aws-vs-google-cloud-cc7c9f5a70d3

Li, X. (2020). AWS vs Google Cloud: Which offers better Identity and Access Management? InformationWeek. https://www.informationweek.com/cloud/aws-vs-google-cloud-which-offers-better-identity-and-access-management/a/d-id/1337628

Panigrahi, P. (2020). AWS IAM Vs Google Cloud IAM: Comparison of IAM Services. Srijan Technologies. https://www.srijan.net/blog/aws-iam-vs-google-cloud-iam-comparison-iam-services

Mohammed, I.A., 2019. Cloud identity and access management–a model proposal. International Journal of Innovations in Engineering Research and Technology, 6(10), pp.1-8.

Roy, A., Banerjee, A. and Bhardwaj, N., 2021. A Study on Google Cloud Platform (GCP) and Its Security. Machine Learning Techniques and Analytics for Cloud Security, pp.313-338.

Soliven, K.A., 2020. Hybrid Cloud Architecture Design, Deployment and Analysis.

Patterson, S., 2019. Learn AWS Serverless Computing: A Beginner's Guide to Using AWS Lambda, Amazon API Gateway, and Services from Amazon Web Services. Packt Publishing Ltd.

Stigler, M. and Stigler, M., 2018. Amazon Web Services. Beginning Serverless Computing: Developing with Amazon Web Services, Microsoft Azure, and Google Cloud, pp.41-81.

Sendor, J., Lehmann, Y., Serme, G. and de Oliveira, A.S., 2014, March. Platform-level support for authorization in cloud services with OAuth 2. In 2014 IEEE International Conference on Cloud Engineering (pp. 458-465). IEEE.

Quadri, S.A., 2017. Cloud Computing: Migrating to the Cloud, Amazon Web Services, and Google Cloud Platform.

References used in Table 1, 2 and 3

Amazon Web Services. (2023). Amazon API Gateway. Retrieved from https://aws.amazon.com/api-gateway/

Amazon Web Services. (2023). AWS Identity and Access Management. Retrieved from https://aws.amazon.com/iam/

Amazon Web Services. (2023). AWS WAF. Retrieved from https://aws.amazon.com/waf/

Amazon Web Services. (2023). Elastic Beanstalk. Retrieved from https://aws.amazon.com/elasticbeanstalk/

Google Cloud. (2023). Cloud Endpoints. Retrieved from https://cloud.google.com/endpoints

Google Cloud. (2023). Cloud Identity and Access Management. Retrieved from https://cloud.google.com/iam

Google Cloud. (2023). Google Cloud Platform. Retrieved from https://cloud.google.com/

Google Cloud. (2023). App Engine. Retrieved from https://cloud.google.com/appengine

AWS Identity and Access Management (IAM). (2023). AWS. https://aws.amazon.com/iam/

AWS Identity and Access Management (IAM) – AWS Identity and Access Management. (2023). AWS. https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

AWS Identity Aware Proxy (IAP). (2023). AWS. https://aws.amazon.com/iap/

Cloud Identity and Access Management (Cloud IAM). (2023). Google Cloud. https://cloud.google.com/iam

Google Cloud Identity Aware Proxy (Cloud IAP). (2023). Google Cloud. https://cloud.google.com/iap

Cloud Identity and Access Management (IAM). (2023). Google Cloud. https://cloud.google.com/iam/docs/overview