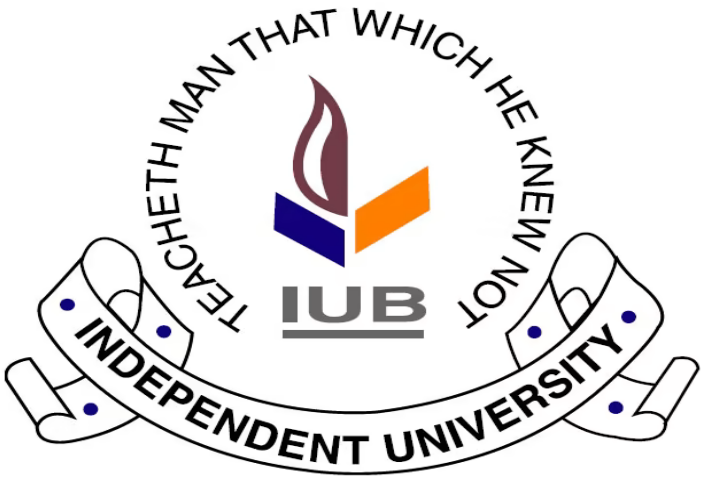


COURSE CODE: CSC 472

COURSE NAME: CLOUD COMPUTING

SECTION: 01

GROUP: B1

PROJECT TOPIC:

Creating Google Cloud Infrastructure Dhaka Metro Rail Ticketing System

SUBMITTED BY:

Tanvir Ahmed Aadeef

Mohsina Tabassum

Abu Ahamed Rafi

Aniqa Tabassum

Fahim Faisal Rhythm

SUBMITTED TO:

DR. RUBAIYET ISLAM

PROJECT NAME:

Creating Google Cloud Infrastructure Dhaka Metro Rail Ticketing System

Introduction:

This report outlines the design and implementation of a Google Cloud infrastructure for the Dhaka Metro Rail Ticketing System. To support the functioning of the ticketing system, the infrastructure makes use of a variety of elements, including Virtual Machines (VMs), Buckets, Virtual Private Clouds (VPCs), Subnets, VPC peering, and a SQL instance. The city's public transportation system must include the Dhaka Metro Rail Ticketing System. A reliable and scalable cloud infrastructure is required to manage ticket sales, revenue, and passenger information effectively. The design and deployment of a Google Cloud infrastructure for the Dhaka Metro Rail Ticketing System are presented in this study.

Project Goal and Objectives:

The main objective of this project is to create a digital system for booking tickets that will serve the people of Dhaka and allow them to purchase tickets for the Metrorail Mass Rapid Transit (MRT) starting with the current MRT Line 6 and onward. The major objective is to integrate this system with Google Cloud to ensure minimal downtime and public availability under a widely recognized and secure domain that is reachable to people throughout Dhaka.

The main objective is to design such a system using software to make ticket acquisition a smooth and efficient process. Conditions to be met in the designing phase include:

- Enabling Log-in Info for commuters

- The ability to book tickets anytime through the internet.
- To create a database of tickets issued and passenger information which are scanned physically at turnstiles.
- Ensure high availability and fault tolerance for the ticketing system.
- Provide secure and scalable storage for ticketing data.
- Establish a network architecture that enables seamless communication between system components.
- Implement robust security measures to protect sensitive data.
- Monitor and manage the infrastructure effectively.

Opportunities:

The system can be enhanced in the future to dynamically change features and offer more data on the transport like:

1. Carriage seat allocation
2. Train timing
3. Point-to-Point route subsystem
4. General feedback on how to improve the system
5. Use feedback to decrease maintenance time
6. Discount for off-time tickets in advance

Infrastructure Overview:

The infrastructure for the Dhaka Metro Rail Ticketing System comprises the following components:

a) Two virtual machines (VMs): Virtual machines offer the processing power required to run applications and services. The ticketing system is supported by two virtual machines (VMs), which provide scalability and fault tolerance.

b) Google Cloud Storage, Two Buckets For the ticketing system, data, files, and media are stored and managed in buckets. For convenient access and safe storage, two buckets are made.

c) Two VPCs: With the help of virtual private clouds, isolated network environments can be built. To improve security and separate various elements of the ticketing system, two VPCs are constructed.

d) Two Subnets: Subnets separate a VPC's IP address range into more manageable chunks. To further separate the infrastructure and effectively control network traffic, each VPC contains two subnets.

f) VPC Peering: To enable secure communication and data exchange between the two VPCs, VPC peering is established between them. It enables easy communication between the VMs and other components in various VPCs.

f) One SQL Instance: The relational database for the ticketing system is stored and managed by a single SQL instance. It offers a dependable and expandable data storage and retrieval solution.

Design and Implementation:

a) Virtual machines: To handle the workload of the ticketing system, two VMs are provisioned with the necessary characteristics. Because these VMs are deployed in different VPCs, redundancy and fault tolerance are guaranteed. The necessary operating system and software stack are installed on the virtual machines.

b) Buckets: To store static files, media assets, and other information related to the ticketing system, two Google Cloud Storage Buckets are created. To ensure data security, the buckets are configured with the proper access permissions.

c) VPCs and Subnets: Two VPCs with a total of four subnets each are created. In order to avoid IP conflicts, the VPCs are set up with specific IP address ranges. To ensure effective network management, subnets are made and IP address ranges are assigned within each VPC.

d) VPC Peering: To enable secure communication between the two VPCs, VPC peering is established between them. This enables communication between VMs and other components utilizing private IP addresses between those in one VPC and those in the other.

e) SQL Instance: The relational database for the ticketing system is provided as a managed SQL instance. It is set up with the proper amount of storage, performance options, and security safeguards. The SQL instance offers dependable data backup, scalability, and storage.

Product Summary:

The major objective is to create a website and a database that will be kept up to date with information on commuters and ticket information and make it simple for anyone who wants to buy a ticket to do so online.

System Stakeholders:

- Commuters
- System Maintenance Personnel
- Station Staff
- DMTCL Administration

Security and Access Control:

a) Network security: To regulate inbound and outbound traffic, network security rules and firewall regulations are put into place. Access control lists (ACLs) are set up to limit access to particular ports and IP ranges.

b) Data Security: Both at rest and in transit, data stored in the Buckets and SQL instance is secured by encryption. To ensure that only authorized individuals can access sensitive data, access controls and authentication measures are put in place.

c) Identity and Access Management: To control user access and permissions, Google Cloud Identity and Access Management (IAM) is used. Based on roles and responsibilities, fine-grained access control is developed to limit access to resources.

Monitoring and Management:

1. Logging and Monitoring:

To keep track of the functionality and health of the Dhaka Metrorail Ticketing System infrastructure, Google Cloud Logging and Monitoring services are crucial. Administrators can learn more about the behavior of the system, spot problems, and take preventative action by configuring logs and analytics. Following are important monitoring and management techniques:

Logging: The SQL instance, as well as pertinent logs from VMs, Buckets, VPCs, Subnets, and the Google Cloud Logging service, are gathered and stored there. To follow system activity, spot mistakes, and solve problems, log data can be analyzed, filtered, and visualized.

Metrics Monitoring: Google Cloud Monitoring is used to keep track of the performance metrics for VMs, VPCs, and SQL instances. This enables administrators to monitor resource usage, spot bottlenecks, and guarantee the best possible system performance.

Alerting: Depending on specified thresholds, customized notifications can be set up to inform administrators of key events like high CPU consumption, storage capacity restrictions, or security breaches. This makes it possible to take quick action to keep the system stable.

2. Scalability and Performance Optimization:

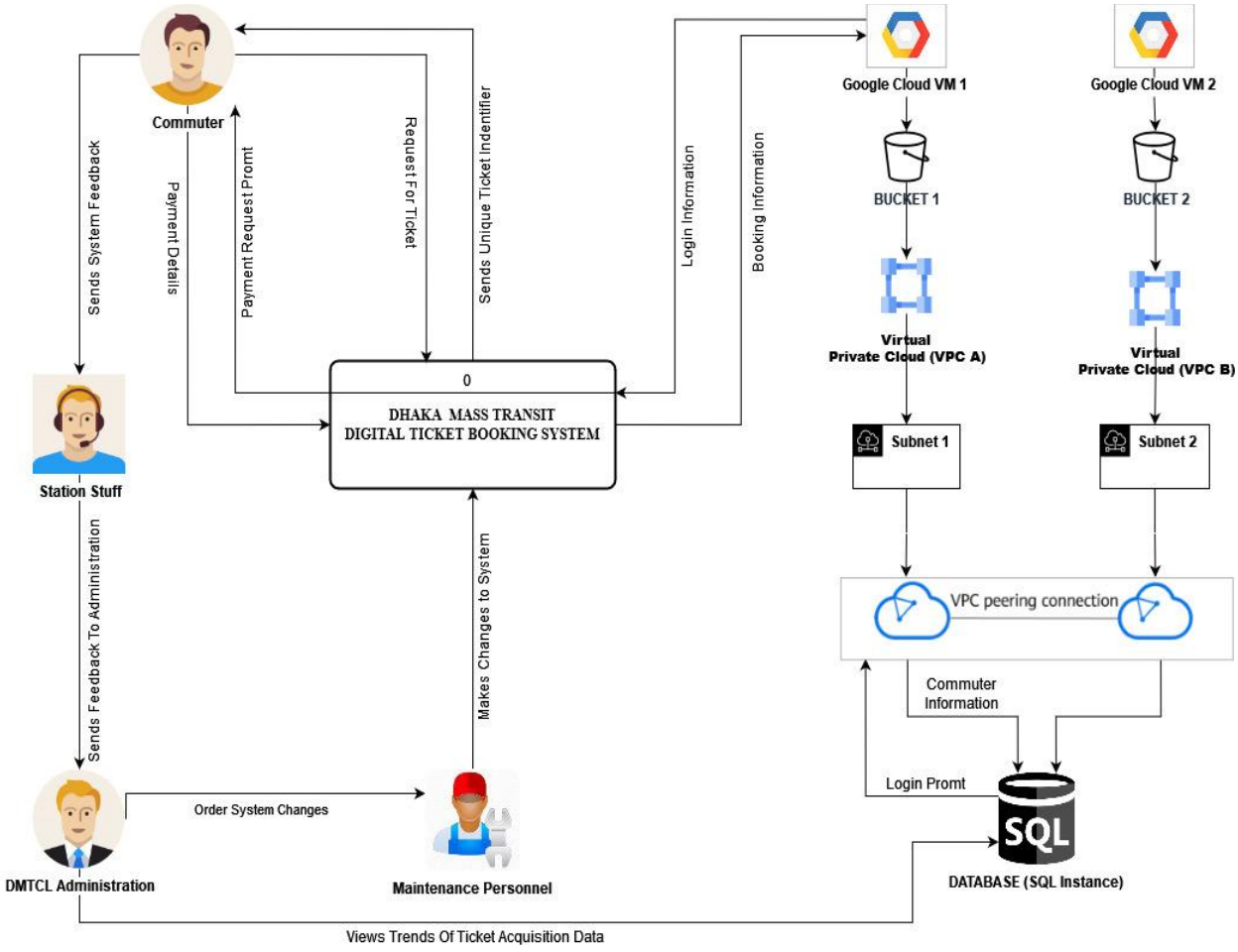
The following procedures are used to make sure the Dhaka Metro Rail Ticketing System can manage rising demand and keep up high performance:

The number of VM instances can be automatically adjusted based on predetermined criteria, such as CPU utilization or request rate, using Google Cloud Autoscaler. This makes it possible for the infrastructure to scale up or down dynamically, maximizing efficiency and reducing resource waste.

In order to improve speed and availability, Google Cloud Load Balancing divides incoming traffic among several VM instances. It ensures that no individual instances are overloaded and that the ticketing system runs efficiently.

Performance Monitoring: To locate performance bottlenecks and optimize resource allocation, ongoing performance monitoring is carried out. Monitoring data can be utilized to optimize database queries, tweak VM settings, and boost system performance as a whole.

Rich Picture:



Cost Calculation:

Bucket pricing

The monthly estimated cost of 1 bucket in our uses based on current google pricing is.

Storage: $0.02 per GB-month x 10 GB = $0.2

Network egress: $0.12 per GB x 10 GB = $1.22

Total monthly cost: $1.42/month

we used 2 buckets so total price will be $1.42*2= $2.84/month

SQL pricing

For the SQL substances we use the estimated monthly cost would be

Compute Engine instance cost: $24.61/month (e2-standard-1 instance in Montreal)

MySQL database cost: $0.0474/hour x 730 hours/month = $34.60/month (using Google Cloud SQL)

Persistent disk cost: $0.040/GB/month x 10GB = $0.40/month

Network egress cost: 0.12$/GB x 2 GB = $0.24/month (assuming you use the maximum network throughput)

Backup storage cost: $0.026/GB/month x 10GB = $0.26/month (assuming the backup size is the same as the persistent disk)

Total estimated monthly cost: $60.11/month

VM pricing

For VM's the estimated monthly cost would be

Compute Engine instance cost: $26.93/month (e2-medium instance in US regions)

Persistent disk cost: $0.11/GB/month x 10GB = $1.10/month (using balanced persistent disk)

Total estimated monthly cost: $28.03/month

As we used two VM's the total price will be: $28.03*2= $56.06/month

Therefore:

The total price = $(2.84 + 60.11 + 56.06) / month = $119.01/month

Challenges and Solutions to GCP:

Using free tiers in cloud computing can be a great way to get started with the platform and experiment with its features. However, there are some challenges that you might face when using free tires. Firstly, there is Limited resources. Free tiers usually come with limited resources such as CPU, memory, storage, and network bandwidth. This can be a challenge if you need to run resource-intensive workloads or host large-scale applications. Then Limited services issue, some cloud services might not be available in the free tier or have limited functionality. This can limit your ability to use advanced features and services that might be critical for your application. After that comes the limited time access issue. Most free tiers are available for a limited time, usually ranging from 12 months to 90 days. Once the free tier expires, you might need to upgrade to a paid plan or migrate to another cloud provider.

Managing IaaS security and updates in Google Cloud can be a complex task that requires careful planning and implementation. Security in Google Cloud offers several security features to help you secure your IaaS environment. Some of these features include Identity and Access Management (IAM), Cloud Security Command Center, and Google Cloud Armor. You can use these features to set up access controls, monitor your infrastructure for security threats, and protect your applications from attacks. And for Updates, Google Cloud offers several tools to

help you manage updates in your IaaS environment. For example, you can use Cloud Deployment Manager to automate the deployment and management of your infrastructure, including updates. You can also use Google Kubernetes Engine to manage containerized applications and update them without downtime. Additionally, Google Cloud offers a range of managed services such as Cloud SQL and Cloud Spanner, which are automatically updated and patched by Google.

We can also talk about the on-premises cloud services with online cloud services issues, there are several issues that a company might face like,

Infrastructure Costs: One of the biggest challenges of on-premises cloud services is the infrastructure cost. The company needs to purchase and maintain the hardware, software, and networking equipment. This can be a significant upfront investment, and ongoing maintenance costs can also add up quickly.

Scalability: Online cloud services are designed to be highly scalable, which means that they can quickly and easily add resources as needed to support growing demand. With on-premises cloud services, however, scaling up can be more challenging and may require additional investment in hardware and other resources.

Maintenance and Updates: With online cloud services, the provider is responsible for maintaining the infrastructure and ensuring that updates and patches are applied as needed. With on-premises cloud services, however, the company is responsible for performing these tasks, which can be time-consuming and resource-intensive.

Security: While on-premises cloud services give the company more control over security, it also means that they are responsible for ensuring that security measures are in place and

up-to-date. Online cloud services typically have more resources to invest in security, which can be an advantage.

Disaster Recovery: Online cloud services typically have built-in disaster recovery capabilities, which means that data can be quickly and easily recovered in the event of a disaster. With on-premises cloud services, however, disaster recovery can be more challenging and may require additional investment in backup and recovery solutions.

Technical Expertise: On-premises cloud services require technical expertise to manage and maintain the infrastructure, which can be a challenge for companies with limited IT resources. Online cloud services, on the other hand, typically have a team of experts who can provide support and assistance as needed.

Overall, the decision to use on-premises or online cloud services depends on the specific needs and resources of the company. While on-premises cloud services give the company more control over infrastructure and security, online cloud services can offer scalability, flexibility, and cost savings. But, If the company is not okay with the costs and issues of maintaining an on premises cloud service online services are highly recommended.

Advantages of Google Cloud Platform:

Scalability: Google Cloud Platform offers highly scalable resources that can easily grow to meet your needs. This allows you to quickly adjust your infrastructure as your business grows and your needs change.

Global Reach: Google Cloud Platform has a large number of data centers located around the world, which allows you to choose the location that is closest to your customers, reducing latency and improving performance.

Security: Google has invested heavily in security measures to ensure that its cloud platform is secure. It also offers a variety of security features, including data encryption, identity and access management, and security monitoring.

Big Data Analytics: Google Cloud Platform provides a variety of tools and services for big data analytics, including BigQuery, Dataflow, and Dataproc, which allow you to process and analyze large amounts of data quickly and efficiently.

Machine Learning: Google Cloud Platform has a variety of machine learning tools and services, including TensorFlow, Cloud AutoML, and Cloud ML Engine, which allow you to build and deploy machine learning models easily.

Disadvantages of Google Cloud Platform:

Complexity: Google Cloud Platform can be complex to set up and configure, especially for companies without a lot of experience with cloud-based services.

Cost: While Google Cloud Platform can be cost-effective for smaller businesses, it can be expensive for larger enterprises, especially if you require a lot of storage or computing power.

Limited Support: While Google Cloud Platform does offer support, it may not be as comprehensive as other cloud-based services, which could be an issue for companies that require a high level of support.

Limited Availability of Third-Party Applications: While Google Cloud Platform has a large number of third-party applications available, it may not have as many as other cloud-based services, which could limit your options when it comes to integrating with other software tools.

Learning Curve: Google Cloud Platform requires a certain level of technical expertise, which could be a challenge for companies without an experienced IT team.

Cloud Documentation:

There are many reasons why businesses and individuals choose Google Cloud as their cloud computing platform. Some of the main reasons include:

- Scalability: Google Cloud provides a highly scalable infrastructure that can quickly adapt to changing business needs.
- Reliability: Google Cloud has a highly reliable infrastructure that ensures high uptime and availability.
- Security: Google Cloud has many built-in security features and protocols to ensure that your data is safe and secure.
- Flexibility: Google Cloud supports a wide range of programming languages, frameworks, and tools, giving developers the flexibility to choose the tools that work best for their projects.
- Cost-effectiveness: Google Cloud offers a pay-as-you-go pricing model, which can help businesses save money on their cloud computing costs.

Security Features:

Google Cloud has many built-in security features and protocols to ensure that your data is safe and secure. Some of the key security features include:

- Identity and Access Management (IAM): IAM allows you to control who can access your resources and what they can do with them.
- Encryption: Google Cloud uses encryption to protect your data both at rest and in transit.
- DDoS protection: Google Cloud has built-in protection against Distributed Denial of Service (DDoS) attacks.
- Security Key Enforcement: Google Cloud allows you to enforce the use of security keys for user authentication, which can help prevent unauthorized access to your resources.
- Compliance: Google Cloud is certified to comply with many industry standards and regulations, including HIPAA, PCI DSS, and ISO 27001.

Google Cloud Firewall:

- Cloud Security Command Center: This is a centralized dashboard that provides visibility into your Google Cloud environment. It allows you to monitor your security posture, detect and respond to threats, and manage compliance.
- Google Cloud Armor: This is a web application firewall (WAF) that helps protect your web applications from malicious traffic. It provides customizable security policies that can be tailored to your specific needs.
- Data Loss Prevention (DLP): Google Cloud's DLP technology helps prevent the accidental or intentional exposure of sensitive data. It allows you to classify, mask, or redact sensitive data in real-time, as it moves through your systems.

- VPC Service Controls: This is a security perimeter that enables you to control access to your Google Cloud resources. It allows you to set up a secure boundary around your resources and control what traffic is allowed in and out.
- Identity-Aware Proxy (IAP): This is a security layer that controls access to your web applications running on Google Cloud. It provides a centralized authentication and authorization mechanism, allowing you to control who can access your applications.
- Cloud Audit Logs: This is a service that provides a record of all actions taken on your Google Cloud resources. It allows you to monitor and track activity across your entire cloud environment.
- Titan Security Key: This is a physical security key that provides an additional layer of protection against phishing and account takeover attacks. It helps ensure that only authorized users can access your Google Cloud resources.

Google Cloud Technical features:

There is no limit to the number of virtual machines (VMs) that you can create in Google Cloud. The number of VMs that you can create depends on the type of account you have, the resources available in your project, and the budget you have allocated for your project. Google Cloud provides a variety of compute services, including Compute Engine, Kubernetes Engine, and App Engine. Each of these services has different limitations on the number of VMs that can be created. For our purpose we would need to make 1 virtual machine to host our WebApp that will be available for everyone in Bangladesh.

There are a few factors to consider when selecting VMs for a metro rail project:

- Compute Power: The VMs should have enough computing power to handle the expected traffic and workload. For a metro rail project, this may include processing real-time data from sensors and devices and performing complex data analytics.
- Storage: The VMs should have enough storage capacity to store the data generated by the metro rail project. This may include storing data from ticketing systems, passenger information systems, and other sources.
- Network Connectivity: The VMs should have sufficient network bandwidth to handle the expected traffic and ensure fast and reliable data transfers. This is particularly important for real-time data processing and communication with other systems.
- Availability and Resilience: The VMs should be highly available and resilient, with automatic failover and redundancy features to ensure uninterrupted service. This is important for mission-critical systems such as those used in the metro rail industry.

Based on these factors, some suitable VM options for a metro rail project on Google Cloud cloud include:

- Compute Engine: Offers a wide range of VM options with customizable CPU, memory, and storage configurations to meet specific project requirements.
- Kubernetes Engine: Provides a managed environment for deploying containerized applications, with features such as automatic scaling and load balancing.
- App Engine: A fully managed platform for building and deploying web applications, with features such as automatic scaling and built-in security.

Google Cloud offers a free trial that provides $300 in credits to use within 90 days. During the free trial, we can create and use virtual machines (VMs) and other Google Cloud services without being charged, up to the limit of the $300 credit.

Comparison between Google Cloud Platform (GCP), Microsoft Azure, and Amazon Web Services (AWS):

Compute Services:

AWS offers Elastic Compute Cloud (EC2) instances, Amazon Lightsail, and AWS Lambda for compute services.

Azure offers Virtual Machines, Azure Functions, and Azure Batch for compute services.

GCP offers Compute Engine, Google Kubernetes Engine (GKE), and Cloud Functions for compute services.

Storage Services:

AWS offers Amazon Simple Storage Service (S3), Amazon Elastic Block Store (EBS), and Amazon Glacier for storage services.

Azure offers Azure Blob Storage, Azure File Storage, and Azure Table Storage for storage services.

GCP offers Cloud Storage, Cloud SQL, and Cloud Bigtable for storage services.

Database Services:

AWS offers Amazon Relational Database Service (RDS), Amazon DynamoDB, and Amazon ElastiCache for database services.

Azure offers Azure SQL Database, Azure Cosmos DB, and Azure Cache for Redis for database services.

GCP offers Cloud SQL, Cloud Spanner, and Cloud Bigtable for database services.

Networking Services:

AWS offers Amazon Virtual Private Cloud (VPC), Elastic Load Balancing, and AWS Direct Connect for networking services.

Azure offers Virtual Network, Azure Load Balancer, and Azure ExpressRoute for networking services.

GCP offers Virtual Private Cloud (VPC), Cloud Load Balancing, and Cloud Interconnect for networking services.

Machine Learning Services:

AWS offers Amazon SageMaker, Amazon Rekognition, and Amazon Comprehend for machine learning services.

Azure offers Azure Machine Learning, Azure Cognitive Services, and Azure Databricks for machine learning services.

GCP offers Cloud AutoML, Cloud ML Engine, and Cloud Vision API for machine learning services.

Serverless Services:

AWS offers AWS Lambda, Amazon API Gateway, and AWS Step Functions for serverless services.

Azure offers Azure Functions, Azure Logic Apps, and Azure Event Grid for serverless services.

GCP offers Cloud Functions, Cloud Pub/Sub, and Cloud Dataflow for serverless services.

Security and Identity Services:

AWS offers AWS Identity and Access Management (IAM), Amazon Cognito, and AWS Key Management Service (KMS) for security and identity services.

Azure offers Azure Active Directory, Azure Security Center, and Azure Key Vault for security and identity services.

GCP offers Cloud Identity and Access Management (IAM), Cloud Security Command Center, and Cloud Key Management Service (KMS) for security and identity services.

Pricing and Cost:

AWS offers a pay-as-you-go pricing model, as well as various pricing plans based on usage and volume.

Azure offers a pay-as-you-go pricing model, as well as various pricing plans based on usage and volume.

GCP offers a pay-as-you-go pricing model, as well as various pricing plans based on usage and volume.

Support and Documentation:

AWS offers various levels of support plans, as well as extensive documentation and community forums.

Azure offers various levels of support plans, as well as extensive documentation and community forums.

GCP offers various levels of support plans, as well as extensive documentation and community forums.

Conclusion:

A reliable and scalable solution for ticket sales and management is provided by the construction of a Google Cloud architecture for the Dhaka Metrorail Ticketing System using 2 VMs, 2 Buckets, 2 VPCs, 2 Subnets connected via VPC peering, and 1 SQL instance. High availability, fault tolerance, and effective network connectivity are all provided by the infrastructure's design. The required computing power is provided through the utilization of VMs, and Buckets enable safe and convenient data storage. With VPC peering, seamless communication between various components is made possible. The VPCs and Subnets provide isolation and effective network administration.

For storing and managing ticketing data, the SQL instance serves as a dependable and expandable database. Strong security measures, such as network security, data encryption, and access controls, guarantee the preservation of important information.

Monitoring and management practices, including logging, metrics monitoring, and scalability optimization, contribute to maintaining system health, identifying issues, and ensuring optimal performance.

By leveraging the power of Google Cloud, the Dhaka Metrorail Ticketing System infrastructure is well-equipped to handle the demands of ticket sales and management, contributing to the efficiency and convenience of the city's public transportation system.