THE UNIVERSITY OF TEXAS AT DALLAS

MIS 6363.S01

Cloud Computing Fundamentals

Spring 2025

Project Proposal

AI-Powered Supply Chain Optimization Amid Tariff and Trade Volatility

Submitted by

Team 6

Sri Harshanadh Reddy Chinthala | SXC23OO19

Vivek Vaddineni| vxv230008

Megha Chandrasekharan Nair | mxc220113

Table of Contents

Abstract

Geopolitical uncertainties, trade regulations, and tariff fluctuations increasingly impact the global supply chain, resulting in higher costs, interrupted shipping routes, and unpredictable delivery times. These challenges are further amplified during peak sales periods when businesses experience surges in demand.

With the help of real-time trade impact assessment, predictive analytics, and a self-healing mechanism, this project suggests a cloud-based, AI-driven supply chain optimization system that can reduce tariff risks, maximize supplier selection, and boost delivery effectiveness. This solution guarantees adaptive route planning, cost-effective procurement, and smooth logistics management despite trade volatility by integrating AWS cloud services.

Domain Description

A Story of Global Trade Uncertainty

What is a Supply Chain?

Think about a simple cup of coffee. A complicated worldwide supply chain is involved in every sip, even though one might think it is just a quick purchase from one's favorite cafe. The beans may come from Colombia, the packaging from China, and the machinery from Germany—all coordinated through a network of producers, suppliers, logistics providers, and retailers.

"Supply Chain" refers to the entire production, transportation, storage, and delivery process from raw materials to the end consumer. There are several important players involved, including:

- Manufacturers that manufacture products.
- Suppliers that provide raw materials or components.
- Logistics providers that transport the products.
- Warehouses and distribution centers that store inventory.
- Retailers and e-commerce platforms that sell to consumers.

Consumers and businesses benefit from stable prices and quick, effective deliveries when this network runs smoothly. Nevertheless, external factors such as trade tariffs, rising fuel prices, or global crises can make the supply chain unstable, costly, and ineffectual.

Common Issues in Supply Chain Management:

1. **Delivery Delays and Bottlenecks**
   - Congestion at major shipping ports leads to longer wait times.
   - Delays in customs clearance create uncertainty.
   - Labor shortages and strikes can impede the flow of products.

   Example: During the COVID-19 pandemic, worldwide shipping experienced severe disruptions, with port congestion in Los Angeles and Shanghai resulting in months-long delays for consumer goods.

   Rising Costs Due to Tariffs and Trade Wars

   - Import/export tariffs increase the cost of goods.
   - Trade agreements are frequently changed, causing supply chain planning uncertainty.
   - Businesses struggle to maintain stable pricing for consumers.

2. **Supply Chain Disruptions from Geopolitical Instability**
   - Wars, conflicts, and diplomatic disputes can restrict the movement of goods.
   - Economic sanctions can cut off supply routes and key trade partners.
   - Political instability creates a risk for long-term planning.

   Example: The Russia-Ukraine conflict disrupted the supply of wheat and energy supplies, causing shortages and price hikes across Europe.

3. **Unoptimized Inventory and Poor Demand Forecasting**
   - Some businesses overstock products, resulting in higher storage costs.
   - Some underestimate demand, resulting in stockouts and lost revenues.
   - Poor forecasting causes waste, inefficiencies, and financial losses.

   Example: During Black Friday and holiday sales, many businesses overstocked inventory in anticipation of demand, but owing to fluctuations in consumer spending, enormous quantities of unsold items lingered in warehouses, resulting in revenue losses.

Business Requirement

AI-Powered Supply Chain Optimization for Maersk in a Volatile Trade Environment

Understanding Maersk: A Global Supply Chain Giant

Few names are as influential as Maersk when we think of global trade and logistics. Founded in 1904, Maersk has grown into the world's largest shipping and logistics company, moving goods across 130+ countries with a fleet of over 700 container ships. Whether it's consumer goods, automotive parts, food products, or industrial machinery, Maersk ensures that businesses worldwide receive their shipments on time.

What Does Maersk Do?

Maersk operates a highly integrated global supply chain, offering services such as:

- **Container Shipping:** Transporting millions of containers across oceans every year.
- **Logistics and Freight Forwarding:** Managing complicated freight operations for multinational companies.
- **Warehousing and Inventory Management:** Storing goods in distribution hubs to optimize supply chains.
- **Customs Brokerage and Trade Compliance:** Helps businesses navigate import and export regulations.

- **Digital Supply Chain Solutions:** Using IoT, blockchain, and AI to track and improve shipments.

In essence, Maersk doesn't just move goods—it moves economies. Its ability to efficiently transport products across borders is vital to industries ranging from retail and e-commerce to energy and manufacturing.

Maersk plays a critical role in global trade, but rising tariffs, trade wars, and geopolitical uncertainties have made international shipping more complex and costly than ever before.

Why Unpredictable Trade Policies and Tariff Fluctuations Are a Major Issue for Maersk and Its Clients?

Maersk operates in a world where tariffs and trade policies change overnight, leading to:

- Slower global freight transport demand.
- Unpredictable customs delay due to new trade restrictions.
- Inefficient shipping routes as companies scramble to avoid costly regions.
- Supplier and inventory disruptions as businesses adjust to new trade realities.

Example: In 2019, the U.S. threatened to impose 25% tariffs on Mexican imports, causing panic among American businesses that relied on Mexican manufacturers.

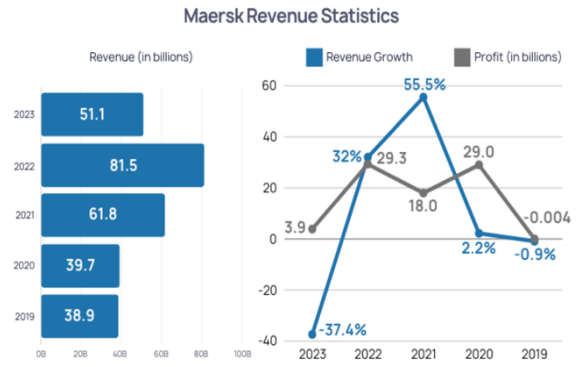
- Many businesses rushed to find alternative suppliers, disrupting the supply chain.
- Warehouse inventory surged as companies stockpiled goods before tariffs took effect

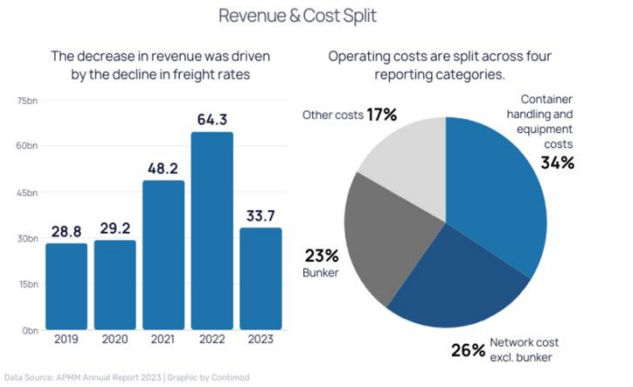
Impact of Global Disruptions on Maersk's Revenue (2019–2023)

From 2019 to 2023, Maersk's revenue has seen dramatic shifts influenced by volatile trade conditions, global tariffs, port congestion, extreme weather events, and fluctuating fuel prices—challenges that directly relate to the core problems addressed by our AI-powered AWS solution.

- In year 2019, Trade tensions and rising tariffs e.g., U.S.–China created uncertainty in routing and increased operational complexity.
- In year 2020, COVID-19 caused global disruptions. Port delays and fuel logistics issues exposed the need for real-time visibility and smarter forecasting.
- In year 2021, post-pandemic demand surged. Severe port congestion, weather disruptions, and fuel hikes pushed freight rates up, stressing manual systems.
- In year 2022, Peak revenue due to high shipping demand and global instability. Tariff regulations and compliance complexity made AI-driven solutions essential.

- In year 2023, Revenue dropped as trade stabilized, but volatility continued from new carbon tariffs, fuel price shifts, and climate-related disruptions.





Years	Revenue (in billions)	Revenue Growth	Profit (in billions)
2023	51.1	-37.4%	3.9
2022	81.5	32.0%	29.3
2021	61.8	55.5%	18.0
2020	39.7	2.2%	29.0
2019	38.9	-0.9%	-0.004

Maersk leverages cutting-edge digital technologies to provide real-time visibility, automation, and predictive analytics across its vast global supply chain. Their current solutions encompass the Internet of Things (IoT), blockchain, artificial intelligence (AI), big data analytics, and cloud computing.

While Maersk employs advanced technologies across its global operations, it currently lacks a **fully integrated, AWS-based architecture offers a complementary, API-driven system that adds AI-enhanced tariff intelligence, dynamic trade risk modeling, and cross-modal (ocean + inland) routing coordination — capabilities not currently emphasized in their Azure stack**. Although **Maersk is not directly liable for tariff payments, changes in trade policies significantly influence customer demand patterns, preferred shipping routes, and delivery schedules—adding complexity to operational planning.**
Rerouting vessels in response to geopolitical tensions, port closures, or cost pressures is often constrained by fixed schedules, infrastructure limitations, and high fuel costs, making real-time adjustments difficult. In contrast, **rerouting within inland logistics—across trucking, rail, and barge networks—is comparatively more flexible and can help absorb upstream disruptions. Additionally, aligning vessel deployment with inland network capacity requires better**

predictive coordination.

This project aims to complement and extend Maersk's existing digital capabilities through AWS-powered AI solutions that go beyond vessel-level insights. By integrating real-time tariff data, port congestion indicators, and inland transport availability, the solution enables intelligent forecasting of trade disruptions, dynamic risk assessment, and adaptive coordination between ocean and inland logistics. These capabilities enhance Maersk's responsiveness, empower data-driven decision-making, and strengthen operational resilience in the face of complex and volatile global trade conditions—while offering modular and scalable architecture that can be deployed alongside existing systems.

Stakeholders Involved in Addressing Trade Disruptions and AI-Powered Supply Chain Optimization for Maersk

1. **Maersk (Shipping and Logistics Provider)**
    - Manages global trade channels and operations.
    - Optimizes transportation efficiency and adapts to changing trade policies.
    - Implements AI for cost reduction and supply chain resilience.
2. **Government and Regulatory Agencies**
    - Establish trade policies, tariffs, and regulatory frameworks that impact global trade.
    - Influence compliance requirements and customs clearance procedures.
3. **Suppliers and Manufacturers**
    - Face disruptions due to changing trade agreements and tariffs.
    - Need reliable shipping and logistics support to mitigate risks.
4. **Retailers and Distributors**
    - Require stable supply chains to meet consumer demand.
    - Adjust sourcing strategies based on shifting trade dynamics.
5. **Customers and End Consumers**
    - Experience price fluctuations due to trade disruptions.
    - Demand transparency and reliability in product availability.
6. **Technology and Cloud Service Providers (e.g., AWS, Microsoft Azure, IBM Cloud)**
    - Provide AI, cloud computing, and data analytics solutions for real-time supply chain visibility.
    - Support automation and predictive analytics to optimize trade operations.

7. **Financial Institutions and Trade Insurers**
    - Manage financial risks associated with global trade disruptions.
    - Provide trade finance solutions, risk assessments, and insurance coverage for supply chain disruptions.

8. **Third-Party Logistics (3PL) and Freight Forwarders**
    - Assist businesses in adapting to new trade routes and compliance requirements.
    - Use digital solutions to optimize shipping and warehousing strategies.

9. **Data and AI Specialists**
    - Develop AI-driven risk assessment and route optimization solutions.
    - Implement machine learning models for real-time tariff intelligence and trade impact predictions.

10. **Industry Associations and Trade Bodies**
    - Advocate for favorable trade policies and industry-wide supply chain improvements.
    - Guide adapting to new trade realities.

User Requirements

Before implementing the system, we must identify key users and their needs to understand if the system will be useful.

1. Logistics Providers
- Require real-time tariff updates to adjust shipping routes.
- Require automated risk assessments to prevent shipment delays.
- Need alternative supplier and shipping recommendations when tariffs change.

2. Retailers and Manufacturers
- Require recommendations for supplier selection to avoid expensive trade routes.
- Require real-time trade risk alerts to make practical procurement decisions.
- Need smooth integration with existing inventory and logistics systems.

3. Trade Compliance Officers
- Need automated compliance checks against changing trade regulations.
- Require alerts on upcoming trade restrictions to prepare emergency plans.

4. Government and Regulatory Agencies
- Need a centralized dashboard for monitoring global trade trends.
- Require customs clearance optimization to improve shipment flow.

Solution requirements:

Our AI-powered trade impact assessment and logistics optimization system must fulfill the

following functional requirements to ensure smooth, cost-effective, and automated supply chain management for Maersk.

Functional Requirements:

1. **Business Rules**

- The system shall automatically assess and apply trade regulations based on real-time tariffs and customs updates.
- The system should prioritize cost-effective shipping routes based on dynamic trade conditions.
- The system shall suggest supplier reallocation when trade restrictions impact supply chains.
- The system shall enforce business logic for compliance monitoring, preventing high-risk shipments.

2. **Transaction Corrections, Adjustments, and Cancellations**

- The system shall allow automatic recalculation of shipping costs when tariffs or fees change after shipment initiation.
- The system shall support manual and AI-driven modifications to trade routes when better alternatives arise.
- The system shall process automated cancellations or order diversions in response to trade sanctions.

3. **Administrative Function**

- The system shall provide role-based access controls (RBAC) for administrators, supply chain managers, and compliance officers.
- The system shall allow administrators to override AI-based recommendations with manual input.

4. **Authentication and Authorization Levels**

- The system shall implement multi-factor authentication (MFA) via AWS Cognito for all users.
- The system shall support role-based access control (RBAC) for different levels of users:
    - Logistics managers: View trade analytics and approve route changes.
    - Compliance officers: Monitor tariff updates and verify legal compliance.
    - Business analysts: Generate cost-reduction reports.
    - System administrators: Manage users, predictive and AI models, and infrastructure.

5. **Audit Tracking**

- The system shall log all trade compliance checks, route changes, and supplier optimizations for auditing purposes.
- The system shall provide audit trails for regulatory reviews, including timestamps and responsible users.

6. **External Interfaces**

- The system shall integrate with:
    - Global trade databases for real-time tariff updates.
    - Maersk's existing APIs for shipment tracking and warehouse inventory.
    - Third-party logistics providers for seamless trade route adjustments.
    - AWS Data Exchange for real-time fuel price fluctuations and port congestion data.

7. Certification Requirements

- The system shall comply with ISO 27001 and GDPR for secure data handling.
- The system shall ensure that trade documentation meets customs regulations for each shipping route.

8. Reporting Requirements

- The system shall generate real-time reports on the following:
    - Trade impact analysis (tariff fluctuations, trade barriers).
    - Cost savings through AI-based routing and supplier optimizations.
    - Customs clearance, delays, and estimated delivery impact.
- Reports shall be exportable to CSV, PDF, and Excel formats.

9. Historical Data

- The system shall store historical trade data for at least 5 years for predictive analysis.
- AI models shall leverage historical tariff trends and shipment costs to improve future decision-making.

10. Legal or Regulatory Requirements

- The system shall ensure compliance with international trade laws, including:
    - WTO regulations for cross-border shipments.
    - USMCA, EU trade agreements, and China import/export laws.
- The system shall automatically flag shipments at risk of violating trade sanctions.

Non-Functional Requirements

To ensure high performance, scalability, and security, the system must meet the following non-functional requirements.

Performance

- The system shall process real-time trade updates within seconds of receiving data.
- AI-driven cost forecasting and route optimization must be completed quickly(within seconds) for seamless decision-making.

Scalability

- The system shall auto-scale based on trade data volume, handling millions of daily transactions.
- AWS Auto Scaling and Lambda will be used to adjust computing power dynamically.

Capacity

- The system shall support real-time analysis of at least 100,000 shipments per day.
- AI models must process trade policy updates from 50+ global sources concurrently.

Availability

- The system shall maintain 99.99% uptime with AWS multi-region deployment.
- Failover mechanisms should be in place to prevent service interruptions.

Reliability

- AWS CloudWatch and Step Functions shall monitor system performance and trigger auto-recovery mechanisms.
- AI-driven route optimizations must maintain a 95% accuracy rate in reducing costs.

Maintainability

- System updates shall be deployed via AWS Code Pipeline with zero-downtime rolling updates.
- Regular AI model retraining shall occur weekly to ensure optimal performance.

Serviceability

- The system shall include automated self-healing mechanisms that detect and resolve failures.
- Admin dashboards shall allow real-time monitoring of trade compliance and logistics performance.

Security

- The system shall use AWS IAM roles, KMS encryption, and AWS WAF for secure access control.
- All trade-sensitive data shall be encrypted at rest and in transit using AES-256 encryption.

Regulatory Compliance

- The system must be GDPR and CCPA compliant for data privacy.
- All transactions must be logged and auditable for regulatory compliance.

Manageability

- The system shall provide role-based access management, allowing businesses to define user permissions.
- Centralized dashboards shall allow administrators to monitor system health, trade risk assessments, and cost savings metrics.

Environmental Sustainability

- The system shall use AWS sustainability best practices, to optimize server power consumption.
- Carbon footprint tracking shall be included to promote eco-friendly logistics decisions.

Data Integrity

- The system shall implement checksums and validation mechanisms to prevent trade data corruption.
- AI models must undergo monthly quality assurance (QA) checks for accuracy.

Usability

- The system shall offer a user-friendly interface with:
    - Custom dashboards for different user roles.
    - API documentation for developers.

- Guided workflows for logistics managers and compliance officers.

Interoperability

- The system shall support integration with:
  - Existing Maersk tracking APIs.
  - AWS Data Exchange for real-time trade impact analysis.
  - Enterprise Resource Planning (ERP) systems used by Maersk and partners.

Implementation Phases

Step 1: Network Architecture and Access Management Setup

To begin implementing our AI-powered supply chain optimization system for **Maersk**, we first established a robust and secure cloud infrastructure using AWS. The goal of this step is to create isolated and well-managed environments for each core layer of the system, while ensuring strict access control across services.

Created Four Dedicated Virtual Private Clouds (VPCs):

- Each VPC corresponds to a specific layer of the architecture:
  - **Data Ingestion Layer** – for collecting external and internal data.
  - **Model Training Layer** – for building and deploying machine learning models.
  - **GPS Dashboards Layer** – for visualizing real-time supply chain data.
  - **Compliance Layer** – for auditing, monitoring, and enforcing governance.
- This segregation enhances security, simplifies maintenance, and allows each layer to scale independently.

Set Up IAM (Identity and Access Management):

- **Purpose:** To manage permissions and control access to AWS services across layers.
- Defined IAM roles and policies tailored to the specific needs of each layer (e.g., Lambda functions in the ingestion layer, SageMaker in model training).
- Ensured secure communication between services like Lambda, S3, SageMaker, and API Gateway by assigning appropriate IAM roles.
- Implemented the principle of least privilege to minimize security risks.

Step 2: Implementing Data Ingestion Layer – Integrating Real-Time Trade & Logistics Data

The second step of the implementation process enhances the existing ingestion layer by adding network security and internet accessibility improvements, allowing Maersk's supply chain system to safely access real-time APIs from external sources. This

design introduces a segregated network using public and private subnets, along with a NAT Gateway for outbound traffic, while all data services remain securely confined within the VPC.

1. Internet Gateway and NAT Gateway Setup: Enabling Controlled Internet Access

To securely retrieve data from external APIs:

- An Internet Gateway is configured outside the Availability Zone and linked to the VPC, allowing third-party APIs to access the cloud environment.
- A NAT Gateway is placed in a Public Subnet and serves as the secure conduit for outbound internet access, enabling internal resources like Lambda to connect with APIs when triggered—without being exposed to the public internet.
- This setup ensures that the system maintains security and isolation while preserving real-time connectivity with data sources.

2. Set Up External API Endpoints (Routed Through Internet Gateway)

We integrated third-party and sensor-based APIs providing critical real-time data, including:

- Port Congestion API – Tracks delays and queue times at international ports.
- 3PL APIs – Supplies logistics data from external warehouse and shipping partners.
- Marine Traffic / AIS API - Provides real-time vessel location, capacity, and ETAs
- WTO, Tariff, Customs APIs – Monitors real-time tariff policies and trade rules.
- Fuel Rate API – Provides live fuel pricing that influences shipping costs.
- Weather & Location APIs – Powered by IoT devices for live tracking and environmental monitoring.

These APIs are accessed through the Internet Gateway and securely routed into AWS for downstream processing.

3. Data Transfer Layer – Monitoring and Compliance

- Data from APIs is passed through a Data Transfer Service, serving as the secure ingestion point.
- Amazon CloudWatch, placed outside subnets but within the VPC, is integrated at this layer to:
    - Monitor all API calls and data flow.
    - Track failures, anomalies, and throughput.
    - Ensure data integrity, compliance, and traceability across ingestion points.

4. API Gateway – Managed RESTful Entry

- Amazon API Gateway is implemented to manage API communication.
- Positioned alongside CloudWatch outside the subnet, it:
  - Accepts and authenticates external API calls.
  - Routes requests to internal processors.
  - Supports rate-limiting, token-based access, and usage plans to regulate load and ensure fair API usage.

5. Lambda ("Data Processor") for Real-Time Processing

- A Lambda function is placed in the Private Subnet, triggered by API Gateway.
- It performs core data transformations:
  - Parses JSON/XML responses.
  - Cleans and normalizes data formats (e.g., currency conversion, timestamp formatting).
  - Enriches data with logic-based tagging (e.g., congestion severity, tariff impact).
  - Applies validation rules to enforce schema compliance.
- Through the NAT Gateway, this Lambda function securely accesses external APIs when needed, while internal access is locked down.

6. Data Storage – DynamoDB and Amazon S3

- Amazon DynamoDB stores structured, real-time data such as shipment logs, tariff updates, and compliance flags.
- Amazon S3 holds semi-structured/unstructured data, such as port congestion heatmaps, customs PDFs, and fuel rate history.
- Both storage solutions are placed inside the Private Subnet, ensuring that no external system can access data directly.
- The Lambda processor writes to these databases in real-time.

7. IAM – Role-Based Security and Service Access Control

- AWS IAM Roles and Policies enforce least-privilege access across the ingestion layer:
  - API Gateway → Lambda: Limited to invoking functions only.
  - Lambda → S3/DynamoDB: Granted specific write permissions.
  - CloudWatch → All components: Monitors events across the ingestion flow.
- IAM guarantees encrypted, logged, and policy-controlled interaction between services, enhancing security and accountability.

How API Endpoints Are Structured:

- Each API is encapsulated in its own microservice-style endpoint.
- API Gateway defines resources such as:
- /logistics/3pl → for 3rd-party logistics data
- /tariffs/wto → for World Trade Organization tariff info
- /fuel/current → for current fuel prices
- /weather/deviceID/location → for weather info related to a specific device and location
- These endpoints support GET requests (for data fetching) and optionally POST (for IoT updates or secure handshakes).
- Each is governed by usage plans, rate limits, and authentication tokens.

Regulatory Considerations:

Yes, integrating third-party APIs—especially across borders—does raise regulatory concerns, particularly related to:

- **Data Residency Laws** (e.g., GDPR, India's Data Protection Bill): Must ensure data storage and usage complies with regional laws.
- **Trade Regulations**: Customs and tariff data must reflect real-time official sources to avoid legal penalties.
- **Security & Audit**: Every API call and data transaction is logged via **CloudWatch** to enable traceability.

To address these:

- IAM ensures no unauthorized data access.
- All incoming data is encrypted.
- Logs and audit trails are automatically maintained.
- CloudWatch alerts notify of suspicious or non-compliant behavior.

Step 3: Model Training and Optimization Layer

The third phase of the implementation focuses on the Model Training Layer, where machine learning models are trained, deployed, and orchestrated to deliver intelligent insights to Maersk's global supply chain. This layer not only performs advanced forecasting and route optimization but also integrates cost analysis, real-time decision-making, and automated retraining mechanisms.

Purpose of This Layer

To enable Maersk to:

- Predict delivery delays, trade disruptions, and fuel-based cost fluctuations.
- Automatically reroute shipments based on risk and cost forecasts.
- Monitor and optimize AI infrastructure and logistics workflows.
- Automate retraining cycles to ensure models evolve with changing data.

Core AWS Services Used

Component	Purpose
Amazon SageMaker	Trains and deploys ML models on trade, tariff, and fuel data
Amazon Forecast	Time series prediction of weather delays and fuel-driven cost changes
AWS Lambda	Executes real-time route optimization logic
Amazon EC2	Hosts trade update processors for tariff and policy monitoring
AWS Fargate	Serverless container execution for logistics task automation
AWS Compute Optimizer	Analyzes resource efficiency of compute workloads
AWS Cost Explorer	Tracks and monitors AI infrastructure spending
AWS Step Functions	Automates AI model retraining pipelines
AWS Incident Manager	Handles trade disruption alerts and coordinates responses
Amazon CloudWatch	Provides a real-time global trade monitoring dashboard

1. Connected Core Data Services to the Model Layer

- **Amazon SageMaker** is at the heart of this layer, acting as the primary machine learning engine.
- SageMaker is securely connected to:
    - **Trade Data Lake (Amazon S3)** – for historical trade and logistics datasets.
    - **Trade Data Storage (Amazon DynamoDB)** – for real-time tariff, fuel, and port status data.
    - **IAM** manages access between these services, ensuring strict role-based control and compliance.

2. Forecasting and Route Optimization Workflows

Risk/Cost Prediction Engine:

- SageMaker feeds structured data into Amazon Forecast, which is used to predict:

- Delivery delays due to weather or port congestion.
- Transportation cost surges due to fluctuating fuel prices.

AI Route Optimizer:

- Forecast outputs are passed to a Lambda function serving as the AI Route Optimizer.
- This function evaluates current trade routes and proposes optimized alternatives, considering predicted risks and costs.
- If a threshold is breached (e.g., route becomes 20% costlier), the system sends automatic notifications for rerouting decisions.

Business Value for Maersk: Enables proactive route management and cost control before disruptions occur.

3. Advanced Trade Analysis and Processing Pipeline

Trade Update Processor (EC2):

- **Amazon EC2** instances host the **Trade Update Processor**, which:
  - Analyzes incoming tariff updates.
  - Identifies region-specific trade policy shifts.
  - Detects anomalies in customs data.

- Processed data from EC2 is passed to AWS Fargate, which runs containerized workloads that:
  - Perform further event-based logistics analysis.
  - Act on complex rule sets (e.g., embargo zones, redirection logic).

Cost Efficiency Analyzer (Compute Optimizer):

- Fargate outputs are evaluated using AWS Compute Optimizer to ensure that workloads are running at optimal cost-performance ratios.
- Helps identify underutilized compute resources and suggests improvements.

Cloud Cost Monitoring (Cost Explorer):

- **AWS Cost Explorer** is integrated to monitor cloud spending trends for the model training pipeline.
- Tracks compute hours, data processing costs, and storage charges.

Business Value for Maersk: Provides full visibility into cost drivers and empowers cost-efficient AI infrastructure management.

4. Automated Model Maintenance and Monitoring

Automated AI Retraining (Step Functions):

- **AWS Step Functions** are used to orchestrate automated model retraining workflows triggered by:
  - Cost thresholds,
  - Trade disruptions,
  - Seasonal data spikes.

Real-Time Trade Disruption Handler (Incident Manager):

- **AWS Incident Manager** is triggered by Step Functions when major changes are detected (e.g., a country introduces a sudden import ban).
- Ensures timely response, coordination, and decision-making across stakeholders.

Business Value for Maersk: Keeps the system continuously learning and adapting to global trade dynamics.

5. Real-Time Global Trade Monitoring

Global Trade Monitoring Dashboard (CloudWatch):

- Centralized dashboards built in Amazon CloudWatch visualize:
  - Model performance,
  - Trade cost metrics,
  - Processing pipelines,
  - Regional disruptions.
- Two critical feedback loops:
  - EC2 → CloudWatch: Sends trade policy insights to visualize shifting patterns.
  - Cost Explorer → CloudWatch: Adds cost efficiency KPIs to trade dashboards.
  - CloudWatch → AI Route Optimizer (Lambda): Triggers route adjustments based on visualized disruptions.

Business Value for Maersk: Empowers real-time awareness of global operations with actionable dashboards.

Security and Governance

- **IAM** roles strictly govern access to SageMaker, Lambda, EC2, Fargate, and Step Functions.
- **CloudWatch** logs all model accesses, parameter changes, and retraining triggers.

- All data flows are encrypted, and audit trails ensure full regulatory compliance.

Step 4: GPS Dashboard Layer – Real-Time Shipment Tracking and Blockchain-Backed Visibility

The fourth implementation step focuses on building a real-time GPS tracking and dashboarding layer**,** which brings visibility, transparency, and automation to Maersk's global trade operations. This layer integrates IoT-based location tracking, blockchain-led trade verification, and centralized compliance dashboards to provide real-time insights into the movement and status of shipments across borders.

Purpose of This Layer

To enable Maersk to:

- Track shipments and container movements in real time using IoT.
- Automate and verify trade events via smart contracts and blockchain.
- Visualize contract statuses, GPS trails, and compliance metrics in live dashboards.

Core AWS Services Used

Service	**Purpose**
Amazon S3 (Trade Data Lake)	Stores historical trade, contract, and tracking data
AWS IoT Core	Captures GPS data from connected shipping containers and vehicles
AWS Lambda	Processes IoT events and triggers blockchain updates
Amazon Managed Blockchain	Records verified trade events to an immutable ledger
Amazon QuickSight	Provides real-time dashboards for compliance, shipment status, and trade traceability

1. Connecting S3 to IoT Core for Tracking Reference

- The Trade Data Lake in Amazon S3 contains contextual metadata such as:
  - Shipment ID
  - Expected delivery timelines
  - Origin and destination ports
  - Pre-assigned route and carrier
- This metadata is used by AWS IoT Core to validate and match live GPS signals from sensors embedded in shipping containers and freight vehicles.

Why It Matters: Ensures that only authorized, recognized assets are tracked and reported in the system.

2. Real-Time GPS Tracking via AWS IoT Core

- **AWS IoT Core** receives location updates from GPS-enabled IoT devices every few seconds.
- Devices send data such as:
  - Current latitude/longitude
  - Speed and direction
  - Temperature (for sensitive cargo)
  - Container ID and timestamp
- These messages are received through **HTTPS** protocols and routed to the cloud in real time.

3. Triggering Smart Contracts via Lambda

- Every message received by IoT Core triggers a Lambda function known as the Smart Contract Processor.
- Lambda checks:
  - Has the container reached a customs zone?
  - Was there a delivery or loading event?
  - Is there a deviation from the expected route?
- When an event matches predefined rules, Lambda logs the result as a contract event.

Example Events:

- "Shipment arrived at Port of Singapore"
- "Cold chain breach detected – initiate refund protocol"

4. Writing Verified Trade Events to Blockchain

- Lambda writes the contract event to Amazon Managed Blockchain, where:
  - It is cryptographically hashed and stored.
  - Each event is linked to prior records, creating an immutable chain of custody for trade compliance.
- Smart contracts ensure:
  - Automatic validations,
  - No tampering,
  - Full auditability of events across the supply chain.

Why Blockchain? Maersk deals with cross-border shipments where trust, verification, and auditability are critical. Blockchain ensures no stakeholder can alter shipment records without traceability.

5. Visualizing Insights with QuickSight Dashboards

- **Amazon QuickSight** is connected to the Blockchain Trade Ledger and S3 Data Lake.
- Dashboards show:
  - Real-time shipment paths with GPS coordinates
  - Smart contract status (e.g., "Delivered", "Customs Cleared", "Violation Detected")
  - Compliance scorecards based on adherence to contractual terms
- QuickSight dashboards are refreshed automatically as new events are logged to the blockchain.

Step 5: Compliance & Continuous Optimization Layer

The final layer of our implementation ensures that Maersk's AI-powered supply chain system remains secure, high-performing, and continually improving. This Compliance & Optimization Layer is responsible for monitoring operational health, performing ongoing security checks, and automating model retraining and updates based on performance insights and system activity.

Purpose of This Layer

To enable Maersk to:

- Monitor the real-time health of trade, tracking, and AI systems.
- Continuously scan for potential security risks or configuration vulnerabilities.
- Automatically retrain and redeploy AI models when performance thresholds or security conditions demand it.
- Maintain compliance with global IT security standards and operational SLAs.

Core AWS Services Used

Service	Purpose
AWS CloudWatch	Monitors system performance, latency, error rates, and data pipeline health
Amazon Inspector	Conducts continuous security auditing and vulnerability scanning
AWS Step Functions	Orchestrates automated workflows for retraining, testing, and redeploying AI models

Service	Purpose
IAM	Manages access and policy enforcement across monitoring and automation services

1. Real-Time System Monitoring (CloudWatch)

- **CloudWatch** is used to continuously monitor the performance and health of:
  - **Lambda (Data Processor)**: Monitors latency, invocation failures, and throttling issues during trade data ingestion and transformation.
  - **IoT Core (GPS Tracking)**: Tracks message delivery success, device health, and GPS update delays.
  - **SageMaker (AI Model)**: Captures training job durations, endpoint health, and model inference response times.
- CloudWatch dashboards are configured to provide centralized visibility into:
  - Shipment tracking activity
  - AI prediction reliability
  - System utilization and anomalies
- **Alarms and triggers** are set up to flag when performance deviates from expected ranges (e.g., increased error rates or dropped messages).

2. Continuous Security Auditing (Amazon Inspector)

- **Amazon Inspector** is connected to all relevant services and EC2-based components (such as the Trade Update Processor in earlier layers).
- It regularly scans for:
  - Unpatched software or libraries
  - Network exposure risks
  - Misconfigured access policies
  - CVEs (Common Vulnerabilities & Exposures)
- **Trigger Flow**:
  - When CloudWatch detects potential issues or abnormal usage patterns, it notifies Inspector to initiate deeper security scans.
  - These scans are automated and generate security findings in near real-time.

Why This Matters: Maersk operates in a high-compliance industry; proactive security scanning reduces the risk of data breaches, compliance failures, or supply chain disruption due to system vulnerabilities.

3. Automated AI Lifecycle Management (Step Functions)

- Based on performance or security scan results, **AWS Step Functions** are triggered

to:

  - Initiate **retraining of AI models** in SageMaker.
  - Deploy updated model versions.
  - Perform post-deployment testing.
  - Log all actions for compliance review.
- These workflows are rule-based and tied to real-world conditions such as:
  - Drop in prediction accuracy
  - Increased processing delays
  - New trade regulations or system patches applied
- Step Functions also integrate with **Incident Manager** (from earlier steps) if retraining is triggered by a trade disruption or model drift.

Why It's Critical: AI models are only as good as the data they learn from. This system ensures that Maersk's models stay fresh, relevant, and performance-optimized — without manual intervention.

Security & Governance Overview

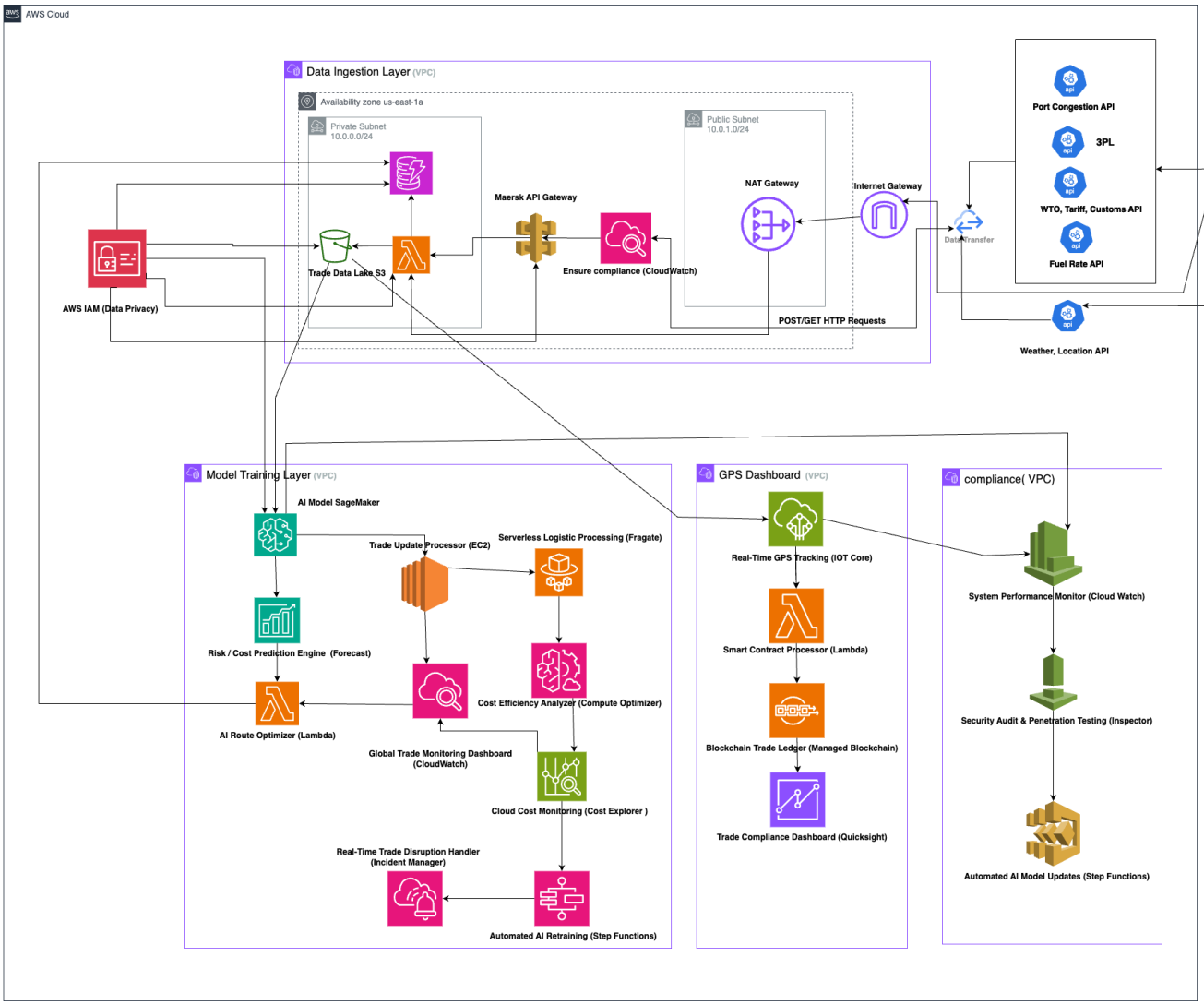
To ensure the enhanced Data Ingestion Layer remains secure, auditable, and compliant, we implemented a multi-layered security and governance strategy aligned with AWS best practices. This updated configuration prioritizes network isolation, service-level permissions, and full traceability, while preserving the system's ability to ingest real-time external data.

- **Network Isolation & Access Control:** All critical services, including Lambda, S3, and DynamoDB, are placed within a private subnet, inaccessible from the public internet. Only the NAT Gateway (in a public subnet) allows outbound traffic, ensuring internal services can fetch API data without being exposed to external threats. The Internet Gateway is positioned outside the Availability Zone and solely enables external APIs to route requests into the system.
- **IAM-Based Role Enforcement**: Each component within the Data Ingestion Layer is assigned strict IAM roles and policies that follow the principle of least privilege. These roles define service-to-service interaction boundaries, such as:
  - API Gateway → Lambda (execution-only)
  - Lambda → DynamoDB & S3 (write-only, scoped access)
  - CloudWatch → All ingestion events (read and alert configuration)
- **Real-Time Monitoring and Logging:** Amazon CloudWatch is deeply integrated to monitor every stage of data flow. It logs API usage, Lambda invocations, NAT activity, and storage interactions. All metrics, error logs, and anomaly events are automatically collected and stored for audit and compliance review.

- Audit Trail and Regulatory Compliance: AWS CloudTrail is enabled to record all IAM role assumptions, API calls, data modifications, and system-level changes across the ingestion pipeline. This ensures that every access point and action is fully traceable and meets international compliance frameworks like GDPR, ISO 27001, and CCPA.
- **Alerting and Threat Detection:** Custom CloudWatch Alarms are set to detect unusual activity (e.g., excessive API requests, malformed payloads, NAT connection spikes). These alerts are routed to system administrators and logged for historical analysis.
- **Encryption and Data Integrity:** All data in transit between services is encrypted using TLS, while data at rest in S3 and DynamoDB is secured via AES-256 encryption. Access to stored data is strictly governed by IAM roles, and checksum validation mechanisms are applied during data ingestion to ensure integrity.

By combining network security, strict access controls, continuous monitoring, and comprehensive logging, this updated ingestion layer provides Maersk with a resilient, compliant, and auditable data pipeline—capable of supporting secure real-time trade intelligence operations across the globe.

Architecture Diagram:



Simulation Scenario: Tariff Spike on Chinese Imports

In response to rising geopolitical tensions, the U.S. announces a sudden 245% tariff hike on a wide range of imports from China, including electronics and industrial parts. Several Maersk shipments are already enroute from ports like Shanghai, raising urgent questions: How can we minimize loss, ensure compliance, and reroute quickly?

Thanks to our AI-powered, AWS-native architecture, Maersk is equipped to respond instantly, securely, and autonomously. While mid-voyage ship rerouting is limited, the system identifies containers at risk and recommends downstream actions—such as adjusting inland routes, redirecting transshipment paths, or allocating future shipments through alternate sourcing locations like Taiwan or Vietnam.

Step 1: Instant Tariff Detection

- A trusted WTO tariff API detects and publishes the hike.
- The data is ingested through an Internet Gateway, handled by API Gateway, and

processed securely via Lambda in a Private Subnet using a NAT Gateway.

- Lambda cleans and normalizes the data, storing it in DynamoDB and S3, while CloudWatch logs the event and raises an alert: “New tariff detected: 245% hike on China-origin goods.”

Step 2: Rapid Impact Analysis

- Alert triggers Amazon SageMaker, which analyzes:
    - Affected SKUs and shipping routes
    - Potential alternative sourcing that clients look for (e.g., Taiwan, Vietnam)
    - Estimated tariff exposure
- Amazon Forecast models:
    - Predicted delay and rerouting timelines
    - Supplier substitution impact
- A secondary Lambda generates re-routing, future vessel deployment and sourcing alternatives for the clients with cost projections.

Step 3: Automated Action via AI Workflow

- Step Functions orchestrate the response:
    - Retrain ML models with new tariff data
    - Validate routing and supplier predictions
    - Update internal logic for optimal logistics paths
- Amazon Inspector ensures security compliance.
- AWS Cost Explorer alerts finance on updated cost exposure.

Step 4: Real-Time Logistics & Compliance Visibility

- IoT Core continues tracking every Maersk container globally.
- Any reroute, delay, or customs flag is logged in real time via Lambda smart contracts to Amazon Managed Blockchain.
- QuickSight Dashboard shows:
    - Updated ETAs and routes
    - Cost impact
    - Compliance status
    - Live container movement

Step 5: Empowered Decision Support

- Maersk’s operations team monitors the situation live—without disruption.
- Real-time dashboards show:
    - Optimized AI-driven alternatives
    - Verified audit trails
    - Predictive alerts
- Business continuity is maintained, with zero downtime and full compliance visibility.

Simulation Outcome Summary

Metric	Before Tariff Hike	After Solution Response
Tariff Cost Impact	5–15%	Detected spike to 35%; prepared for future with appropriate rerouting and fleet deployment.
Delivery Route	Shanghai → Los Angeles	Optimized for future: Taiwan → Seattle
Model Retraining	Manual & Delayed	Auto-triggered via Step Functions
Event Logging	No audit trail	Verified via Amazon Managed Blockchain
Compliance Visibility	Partial	Real-time tracking via CloudWatch & QuickSight

Why our Architecture wins?

Feature	Our AWS Architecture	Azure / GCP / Others
Real-Time Tracking	Built with IoT Core + Lambda for live updates	Azure/GCP need more manual setup; GCP IoT Core retiring
Blockchain Auditability	Native Blockchain for verified trade events	Azure Blockchain retired-MAERSK forced to no longer use Blockchain; GCP requires third-party tools
Security & Compliance	Full-stack IAM, Inspector, CloudTrail, private subnets	Azure and GCP strong, but need more custom policies
Service Integration	Tight integration from ingestion to AI to dashboards	Azure/GCP require more orchestration across services
Supply Chain	AWS powers global	Azure stronger in finance; GCP stronger

Feature	Our AWS Architecture	Azure / GCP / Others
Expertise	logistics (e.g., Amazon, BMW)	in retail/tech

Cost Breakdown and Cost-Benefit Analysis

Our proposed AWS cloud solution offers Maersk a future-ready digital transformation at a fraction of the cost of continuing with traditional ERP and on-premises AI systems. It delivers scalability, automation, cost efficiency, and global reach, enabling Maersk to operate a truly intelligent supply chain in real time all while saving $400,000 or more per year and dramatically improving agility, security, and compliance.

Monthly Cost Estimate by Core AWS Services

Below is a breakdown of costs for each core AWS service used in our solution, estimated under three usage scenarios:

AWS Service	Pricing Model	Unit Price	Low Load	Medium Load	High Load
AWS Lambda	$0.20 per 1M requests + $0.00001667 per GB-secor	128MB, 1 sec = $0.000002084	$1.50 (1M invoc)	$15 (10M)	$150 (100M)
Amazon S3 (Standard)	$0.023 per GB-month	$0.023/GB	200 GB → $4.60	1 TB → $23	5 TB → $115
S3 Requests (PUT, GET)	$0.005 per 1,000 PUT	Mixed 100K/200K	~$0.50	~$2	~$10
	$0.0004 per 1,000 GET				
Amazon SageMaker	ml.m5.xlarge: $0.25/hr	Per hour	100 hrs training + 50 hrs endpoint → $35	400 hrs + 200 hrs → $130	1,000 hrs + 800 hrs → $330
	Endpoint: $0.10/hr				
Amazon Forecast	Import: $0.24/1K items	Based on 50K items	$20	$75	$250
	Forecast: $0.60/1K				
	Query: $0.05/1K				
Amazon EC2 (t3.medium)	$0.0416 per hour	Per hour	200 hrs → $8.32	500 hrs → $20.80	1,000 hrs → $41.60
AWS Fargate	$0.04048 per vCPU-sec	0.5 vCPU, 1GB, 15 sec task	10K tasks → $5.37	50K → $26.85	200K → $107.40
	$0.004445 per GB-sec				
Amazon Managed Blockchain	$0.29 per node-hour (Hyperledger Fabric)	~1 peer node, 24/7	$209.28	2 nodes → $418.56	3 nodes → $627.84
Amazon QuickSight	$18/user/month (Reader)	1 Author + 5 Readers	$114	$114	$114
	$24/month (Author)				
AWS IoT Core	$1 per million messages	Based on devices	1M → $1	5M → $5	25M → $25
AWS Step Functions	$0.025 per 1K state transitions	Based on executions	20K transitions → $0.50	100K → $2.50	500K → $12.50
Amazon Inspector	$0.30 per EC2 scan + $0.0005 per Lambda scan	10 scans/month	$3	$10	$25
Amazon CloudWatch	Logs: $0.50/GB ingest	10 GB logs/month	$5.30	50 GB → $26.50	100 GB → $53
	$0.03/GB-month storage				
AWS Cost Explorer	Free	—	Free	Free	Free
IAM / CloudTrail	$2 per 100K events/month (beyond free tier)	500K events	$0 (under free)	$0	$2
NAT Gateway	$0.045/hr + $0.045/GB	~720 hrs + data out	$30	$35	$40

Total Monthly Cost Estimates

Usage Tier	Monthly Estimate (Roughly)
Low Load (Prototype or PoC)	$562.37
Medium Load (Regional Maersk Operation)	$923.21
High Load (Global Rollout)	$1,883.34

AWS Cloud Solution vs Traditional ERP and On-Prem Systems

As part of this project, we conducted a cost-benefit analysis to evaluate the financial and operational impact of replacing Maersk's existing on-premises systems and traditional ERP-based processes with the proposed cloud-native solution built entirely on AWS. This analysis considers both direct costs (infrastructure, licensing, maintenance) and indirect costs (downtime, inflexibility, human resource demands).

Traditional ERP / On-Prem AI Pipelines: Current State at Maersk

Maersk's legacy systems largely rely on a mix of:

- On-premises servers for data storage and AI model processing.
- Traditional ERP software (e.g., SAP, Oracle) for logistics workflows and trade reporting.
- Manual or semi-automated processes for data ingestion, compliance, and Performance monitoring.

Key Cost Challenges:

Area	**Cost Implication**
CapEx	$200,000+ initial investment for hardware, licensing, and setup
ERP Licenses	$20,000–$50,000/user/year for logistics & analytics modules
AI Model Infrastructure	High GPU/CPU infrastructure costs for training and inference
Scalability	Requires manual hardware expansion (~$10K+/server)
Maintenance	Dedicated IT teams and system administrators (~$150K+/year)
Integration Overhead	Difficult to integrate with modern IoT and external APIs
Deployment Speed	Weeks/months per update or feature rollout
Automation Limits	Minimal support for AI-driven automation or smart contracts

Our AWS Cloud-Based Architecture: Proposed Solution

Our system is a fully serverless, scalable, and intelligent cloud infrastructure hosted on AWS. It includes:

- Real-time data ingestion using API Gateway, Lambda, and IoT Core
- AI/ML automation using SageMaker, Forecast, and Step Functions
- Immutable event tracking using Managed Blockchain
- Monitoring and security using CloudWatch, Inspector, IAM, and Cost Explorer

Key Benefits & Cost Efficiencies:

Area	AWS Cloud Cost (Monthly Avg)	Savings vs On-Prem
Infrastructure Setup	$0 upfront (pay-as-you-go)	Saves $200,000+ in CapEx
AI Training & Inference (SageMaker)	~$300–$2,000/month	60–80% lower than GPU server hosting
Real-Time Ingestion & APIs	~$50–$150/month	No need for custom-built connectors or middleware
Monitoring & Compliance	Included with CloudWatch + Inspector	Saves IT monitoring labor costs (~$40K/year)
Blockchain & Smart Contracts	~$200–$600/month	Replaces expensive middleware for auditing
Maintenance & Admin	Minimal (fully managed)	Reduces IT workforce dependency
Scalability	Auto-scaled on demand	No hardware expansion cost
Deployment Speed	Minutes to hours	Saves months in change rollouts

Long-Term Financial Comparison: 1-Year TCO:

Cost Category	Traditional ERP / On-Prem	AWS Cloud Solution
Initial Investment	~$250,000	$0
Annual Software & Licensing	~$100,000+	Included in usage cost
AI Model Infrastructure	~$50,000	~$10,000–$20,000
IT Team & Maintenance	~$150,000/year	Minimal
Total 1-Year Cost	~$500,000+	~$30,000–$70,000
Estimated Savings	—	$400,000+ annually

Executive Summary

This AI-powered AWS implementation introduces a significant enhancement to Maersk's hybrid logistics environment. This solution brings in real-time intelligence by integrating data from tariffs, port congestion, fuel rates, weather, and inland transport APIs—enabling faster, smarter responses to evolving trade and logistics conditions. Automated regulatory compliance and trade policy monitoring reduces manual intervention and ensures adherence to international standards. With AWS-native services like SageMaker, Lambda, and CloudWatch, the system supports scalable, event-driven analytics while maintaining cost and resource efficiency. Blockchain-backed auditing and centralized logging offer traceability and

transparency across the data lifecycle. Critically, this architecture is designed to integrate seamlessly with Maersk's physical operations, enhancing coordination between cloud-based analytics and on-the-ground execution. By bridging the gap between digital insight and operational action, Maersk can improve agility, reduce risk, and strengthen its global supply chain resilience.

References:

1. ResearchGate. (n.d.). *Supply Chain Management*. Retrieved from https://www.researchgate.net/publication/304194361_Supply_Chain_Management
2. ScienceDirect. (2022). *Article on Supply Chain Management*. *Transportation Research Part E: Logistics and Transportation Review*. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S1366554522000709
3. Gereffi, G. (2022). *Resilience decoded: The role of firms, global value chains, and the state in COVID-19 medical supplies*. *Columbia Center on Sustainable Investment (CCSI)*. Retrieved from https://ccsi.columbia.edu/sites/default/files/content/docs/fdi%20perspectives/No%20348%20-%20Gereffi%20-%20FINAL.pdf
4. INFORMS. (2019). *Impact of Tariffs on Global Supply Chain Network Configuration: Models, Predictions, and Future Research*. *Manufacturing & Service Operations Management*. Retrieved from https://pubsonline.informs.org/doi/epdf/10.1287/msom.2019.0802
5. Acropolium. (2024). *Cloud Computing in Logistics and Supply Chain*. Retrieved from https://acropolium.com/blog/cloud-computing-in-logistics-and-supply-chain/
6. Maersk. (2024). *How Can Generative AI Drive Logistics Transformation?*. Retrieved from https://www.maersk.com/insights/digitalisation/2024/01/03/how-can-generative-ai-drive-logistics-transformation
7. Cost Benefit Analysis of Dynamic Route Planning at Sea. Retrieved From https://www.sciencedirect.com/science/article/pii/S2352146516300552
8. Global tariffs impacting supply chains. Retrieved From: https://www.maersk.com/news/articles/2025/03/13/global-tariffs-impacting-supply-chains
9. International Monetary Fund (IMF). (2021). *Longer Delivery Times Reflect Supply Chain Disruptions*. Retrieved from https://www.imf.org/en/Blogs/Articles/2021/10/25/longer-delivery-times-reflect-supply-chain-disruptions
10. New York Post. (2025). *Lindt Moving Some Chocolate Production From US Over Canada's Tariffs*. Retrieved from https://nypost.com/2025/03/04/business/lindt-moving-some-chocolate-production-from-us-over-canadas-tariffs/