**PRD**

**This PRD has been formatted so that it doesn’t contain any sensitive, IP information/data**

**Objective:**  
Migrate IOT App from legacy on prem middleware platform to one of the following public cloud provider, AWS, Azure, GCP. The migration aims to improve scalability, reduce costs, and enhance operational efficiency.

**Scope:**  
This PRD covers the requirements for migrating IOT application servers, databases, storage, etc.

Elastic Load Balancers to auto-scale during peak and off peak hours

RDS Database to store customer data

Integrate cloudwatch to measure latency and collect metrics on user logins, time to resolve issues by support engineers etc.

Use AI/ML Models to predict if support time can be improved by using supervised and labelled data of customers with whom the support engineers are interacting

Train data sets to provide information on the dependent variables

Work with data scientists to choose the right AI model

**Out of scope for this project are:**

Support on mobile devices and other platforms.

**Success Metrics:**

* Reduce operational costs by 90%.
* Achieve availability target 99.9% uptime post-migration.
* Decrease deployment times by 50% or more
* Improve application performance by: e.g., response time by 20%.

**2. Key Goals and Requirements**

**2.1 Business Goals**

* Enable flexible scaling to support fluctuating workloads.
* Simplify infrastructure management and reduce time for upgrades.

**2.2 Functional Requirements**

* **Compute Resources:** Provision virtual machines or serverless functions as required to support current application workloads.
* **Data Storage:** Migrate existing databases to cloud-native storage solutions-Amazon RDS and ensure data consistency.
* **Networking:** Implement secure network configurations to control access (e.g., VPC setup, firewalls).
* **Disaster Recovery & Backup:** Establish automated backups and disaster recovery plans, with recovery time objective, RTO of 4 hours

**2.3 Non-Functional Requirements**

* **Scalability:** Support auto-scaling to handle increased load without manual intervention.
* **Security:** Ensure encryption at rest and in transit, and set up identity and access management (IAM) policies.
* **Performance:** Application should have no more than a specific latency target, 100ms increase in response times as mentioned in the AWS documentation

**3. Assumptions and Dependencies**

* **Assumptions:**
  + The application codebase is compatible with the target cloud environment.
  + The current infrastructure is fully documented for a smooth migration process.
* **Dependencies:**
  + Required cloud infrastructure (e.g., VPCs, IAM) will be provisioned by the cloud provider’s setup team.
  + Collaboration with [IT team, DevOps, security team] is necessary to meet compliance and security requirements.

**4. User Stories**

1. **As a systems administrator,** I want to monitor cloud resources in real time so that I can respond promptly to any performance issues.
2. **As a security engineer,** I want all sensitive data to be encrypted to meet industry standards and regulatory requirements.
3. **As a developer,** I want to deploy updates to the application without service interruption, so users experience continuous availability.

**5. Technical Requirements**

**5.1 Cloud Service Setup**

* **Compute:** Define instance types and sizing based on current workloads.
* **Storage:** Select appropriate storage classes and configure backup policies.
* **Networking:** Configure VPN or direct connection for secure, low-latency access.

**5.2 Migration Process**

* **Data Transfer:** Use data migration tool, AWS Database Migration Service to move data.
* **Testing:** Conduct pre- and post-migration testing to verify functionality and performance.
* **Cutover Plan:** Outline steps for final cutover to ensure minimal downtime.

**5.3 Post-Migration Monitoring and Maintenance**

* **Monitoring Tools:** Configure monitoring tool, e.g., CloudWatch for continuous monitoring.
* **Incident Management:** Establish a procedure for incident response in case of outages or service degradation.
* **Optimization:** Regularly review and optimize resources for cost efficiency and performance.

**6. Risks and Mitigations**

| **Risk** | **Impact Level** | **Mitigation Strategy** |
| --- | --- | --- |
| Data loss during migration | High | Implement regular backups before and during migration. |
| Application compatibility issues | Medium | Conduct thorough testing and set up a staging environment. |
| Security vulnerabilities | High | Conduct a security audit and enforce strict IAM policies. |

**7. Timeline and Milestones**

1. **Preparation Phase:**2-3 weeks- Set up the cloud environment, configure networks, and establish IAM roles.
2. **Data Migration:** 2-3 weeks - Migrate databases, conduct data validation.
3. **Application Migration:** 3 weeks- Deploy application components and test integrations.
4. **Testing Phase:** 1 week- Perform load testing, security testing, and UAT.
5. **Go-Live:** 3 days- Final cutover to cloud, verify performance.
6. **Post-Migration Review:** **ongoing-** Optimize configurations, finalize documentation.

**8. Acceptance Criteria**

* All migrated services meet predefined performance benchmarks.
* Security configurations comply with legal and security teams
* Downtime during migration does not exceed 30 minutes.
* Successfully documented all procedures and provided training for ongoing maintenance.