Patent Application: Unified AI-Driven Cloud Governance Platform

Title of Invention

System and Method for Unified Artificial Intelligence-Driven Multi-Service Cloud Governance Platform with Predictive Analytics, Cross-Domain Optimization, and Automated Remediation Orchestration

Technical Field

This invention relates to cloud computing governance platforms, specifically to artificial intelligence-driven systems that unify multiple cloud governance services including policy management, role-based access control, network security, and cost optimization through integrated predictive analytics and automated remediation workflows.

Independent Claims

Claim 1 (System Claim - Broadest)

A computer-implemented unified cloud governance platform comprising:

a) **a multi-service data aggregation layer** configured to:

- establish concurrent authenticated connections to at least four distinct cloud governance services: policy management, role-based access control (RBAC), network security, and cost management,
- implement adaptive data ingestion with automatic schema detection and normalization across heterogeneous service APIs,
- maintain real-time synchronization with sub-5-second latency for configuration changes,
- provide unified data access through a GraphQL API with field-level authorization;

b) **an artificial intelligence orchestration engine** implementing:

- a hierarchical neural network architecture with specialized sub-networks for each governance domain,
- cross-attention mechanisms enabling information flow between domain-specific models,
- ensemble learning combining at least five distinct AI techniques: deep learning, reinforcement learning, graph neural networks, natural language processing, and time series analysis,
- automated model selection based on governance task characteristics and data availability;

c) **a predictive analytics system** configured to:

- forecast governance events with at least 85% accuracy for 7-day predictions,
- identify anomalies using unsupervised learning with adaptive thresholds,
- predict resource compliance violations before they occur using temporal pattern analysis,
- calculate confidence intervals for all predictions using Monte Carlo dropout;

d) **a cross-domain optimization engine** implementing:

- multi-objective optimization across security, compliance, performance, and cost dimensions,
- constraint satisfaction ensuring all optimizations maintain regulatory compliance,
- Pareto frontier calculation for trade-off analysis between competing objectives,
- simulation-based impact assessment before implementing changes;

e) **an intelligent remediation orchestration system** configured to:

- automatically generate remediation workflows from detected issues and predicted violations,
- implement saga patterns for distributed transaction management across services,
- provide rollback capabilities with state preservation,
- execute remediation with approval workflows and audit trails;

f) **a unified governance dashboard** providing:

- real-time visualization of governance state across all domains,
- predictive alerts with natural language explanations,
- interactive what-if analysis for proposed changes,
- executive reporting with trend analysis and recommendations;

wherein the platform processes at least 1 million governance events per hour while maintaining 99.95% availability.

Claim 2 (Method Claim - Broadest)

A computer-implemented method for unified AI-driven cloud governance comprising:

a) **aggregating multi-service governance data** by:

- authenticating with cloud service providers using OAuth 2.0 with automatic token refresh,
- implementing parallel data collection across services with circuit breaker patterns,
- normalizing data into a canonical governance model with versioning support,

- storing aggregated data in a distributed time-series database with automatic sharding;

b) **training and deploying AI models** by:

- collecting labeled governance data from at least 1,000 cloud environments,
- implementing federated learning to preserve data privacy across tenants,
- training domain-specific models with transfer learning from pre-trained foundations,
- deploying models with A/B testing and automatic performance monitoring;

c) **performing predictive analytics** by:

- extracting temporal features from governance event streams,
- applying ensemble prediction models with weighted voting,
- calculating prediction uncertainties using Bayesian neural networks,
- generating human-readable explanations using SHAP values;

d) **optimizing governance configurations** by:

- modeling governance state as a multi-dimensional optimization problem,
- applying genetic algorithms with custom fitness functions,
- simulating optimization outcomes using digital twin technology,
- ranking solutions by implementation complexity and risk;

e) **orchestrating automated remediation** by:

- matching detected issues to remediation templates using similarity scoring,
- generating step-by-step remediation plans with dependency management,
- executing remediation with progress tracking and error handling,
- validating remediation success through automated testing;

f) **providing unified governance insights** by:

- aggregating metrics across all governance domains,
- calculating composite governance scores with drill-down capabilities,
- generating natural language summaries of governance state,
- delivering personalized recommendations based on organizational context.

Dependent Claims

Claim 3 (Dependent on Claim 1)

The system of claim 1, wherein the AI orchestration engine further comprises:

- a meta-learning layer that adapts to organizational governance patterns,
- continual learning capabilities updating models without service interruption,
- explainable AI components providing decision rationale for all predictions,
- adversarial robustness testing to ensure model reliability.

Claim 4 (Dependent on Claim 1)

The system of claim 1, wherein the predictive analytics system implements:

- anomaly detection using variational autoencoders (VAEs) trained on normal governance patterns,
- time series decomposition separating trend, seasonal, and irregular components,
- causal inference to distinguish correlation from causation in governance events,
- ensemble uncertainty quantification combining aleatoric and epistemic uncertainty.

Claim 5 (Dependent on Claim 1)

The system of claim 1, wherein the cross-domain optimization engine further comprises:

- a digital twin of the cloud environment for safe optimization testing,
- reinforcement learning agents trained on governance optimization tasks,
- constraint learning from historical policy violations,
- multi-stakeholder preference modeling for balanced optimizations.

Claim 6 (Dependent on Claim 2)

The method of claim 2, wherein aggregating governance data includes:

- implementing change data capture (CDC) for real-time updates,
- applying data quality scoring with automatic remediation,
- detecting and resolving entity duplicates across services,
- maintaining data lineage for compliance auditing.

Claim 7 (Dependent on Claim 2)

The method of claim 2, wherein training AI models further comprises:

- implementing differential privacy with epsilon guarantees,

- applying knowledge distillation for model compression,
- using automated hyperparameter optimization with Bayesian methods,
- validating models against adversarial examples.

Claim 8 (Scalability Claim)

The system of claim 1, further comprising:

- horizontal scaling capabilities using Kubernetes operators,
- multi-region deployment with automatic failover,
- edge computing support for latency-sensitive operations,
- federated deployment options for data sovereignty compliance.

Claim 9 (Integration Claim)

The system of claim 1, providing:

- native integrations with major cloud platforms (Azure, AWS, GCP),
- webhook support for third-party governance tools,
- REST and GraphQL APIs with comprehensive documentation,
- SDK libraries for Python, JavaScript, Go, and Java.

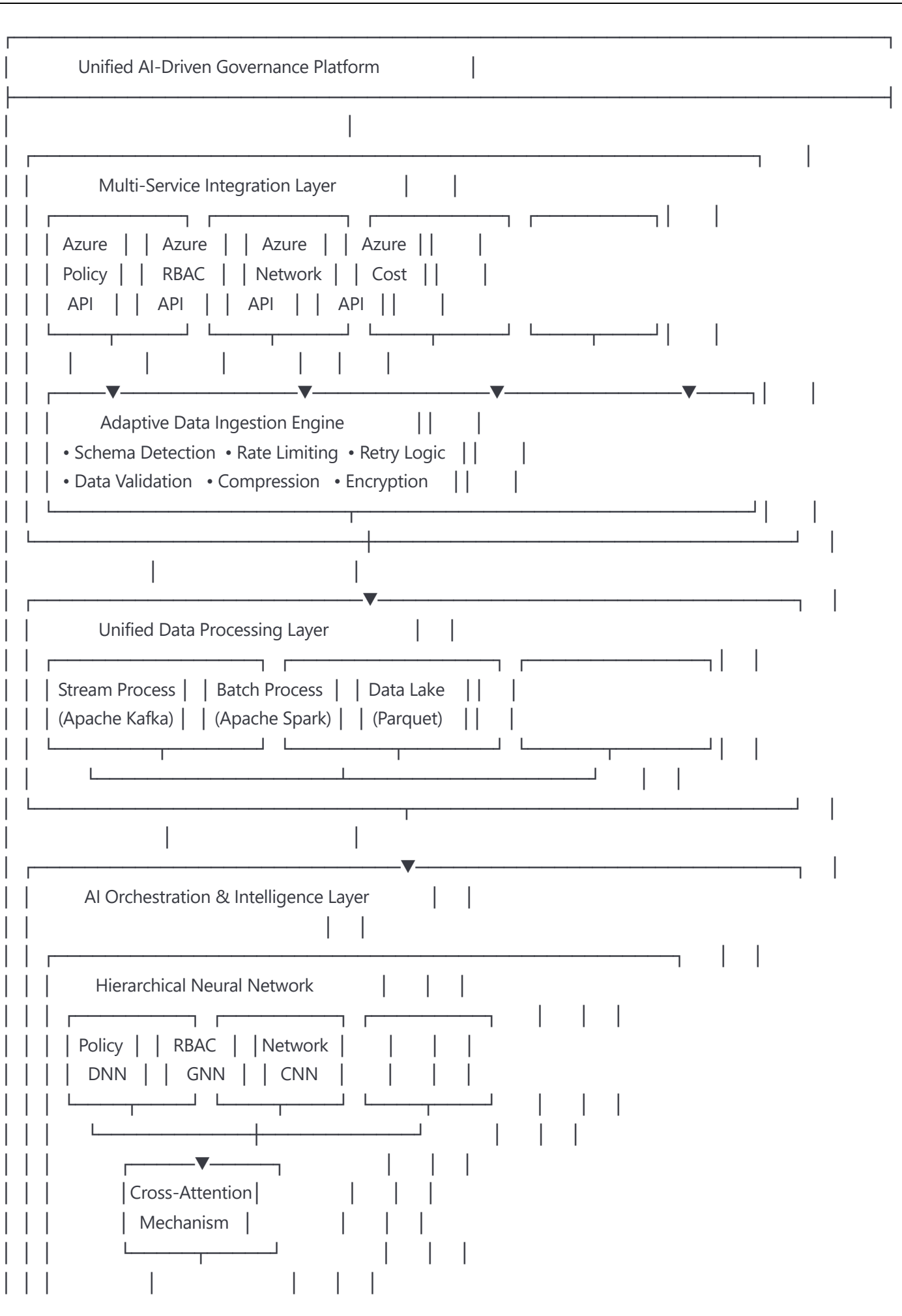
Claim 10 (Compliance Claim)

The system of claim 1, implementing:

- automated compliance mapping to frameworks (SOC2, ISO 27001, HIPAA, GDPR),
- continuous compliance monitoring with drift detection,
- evidence collection for audit requirements,
- compliance prediction for proposed changes.

Technical Diagrams

Figure 1: Unified Platform Architecture


Unified AI-Driven Governance Platform
Multi-Service Integration Layer
Azure Policy API
Azure RBAC API
Azure Network API
Azure Cost API
Adaptive Data Ingestion Engine
• Schema Detection • Rate Limiting • Retry Logic
• Data Validation • Compression • Encryption
Unified Data Processing Layer
Stream Process (Apache Kafka)
Batch Process (Apache Spark)
Data Lake (Parquet)
AI Orchestration & Intelligence Layer
Hierarchical Neural Network
Policy DNN
RBAC GNN
Network CNN
Cross-Attention Mechanism

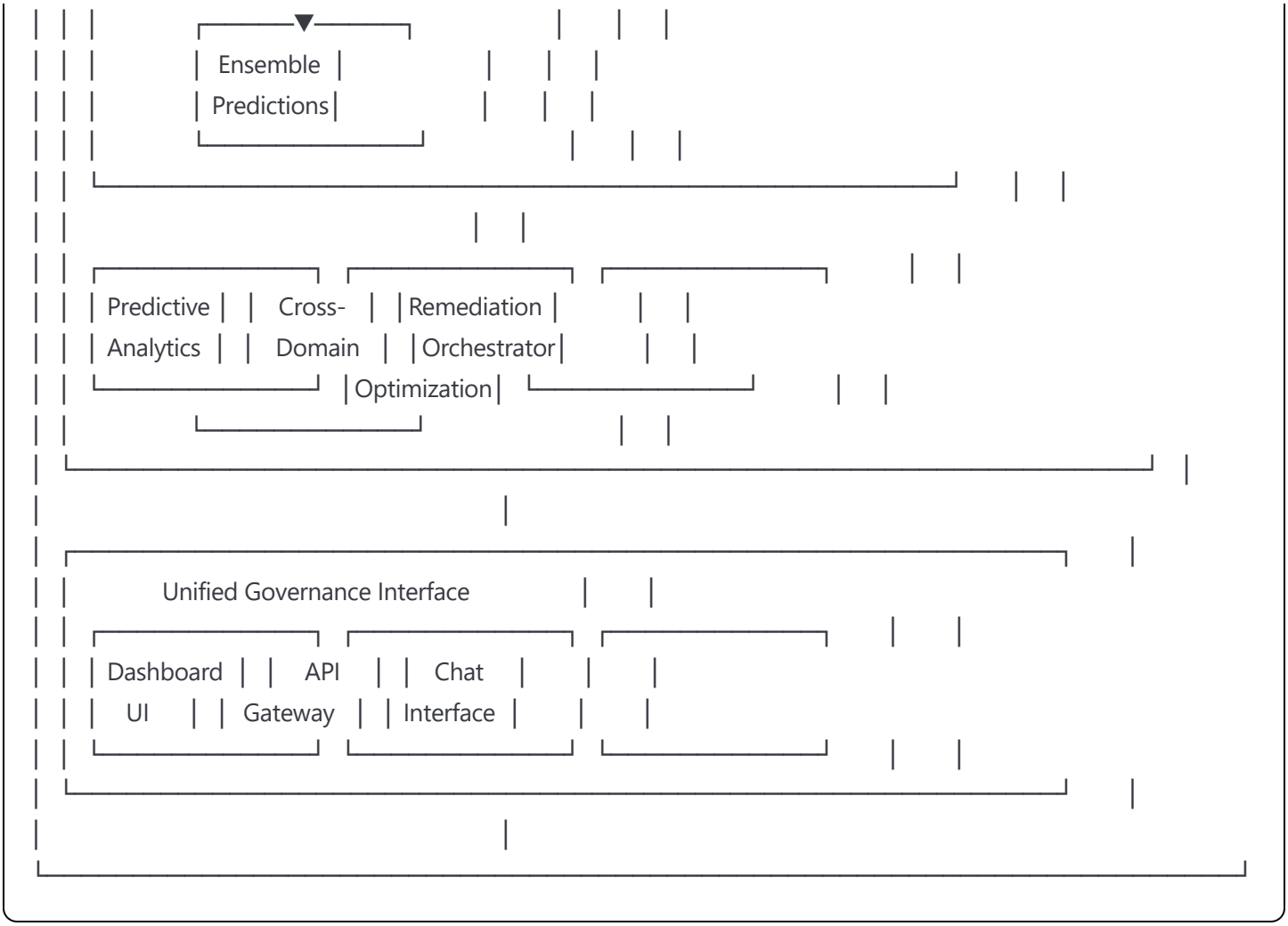
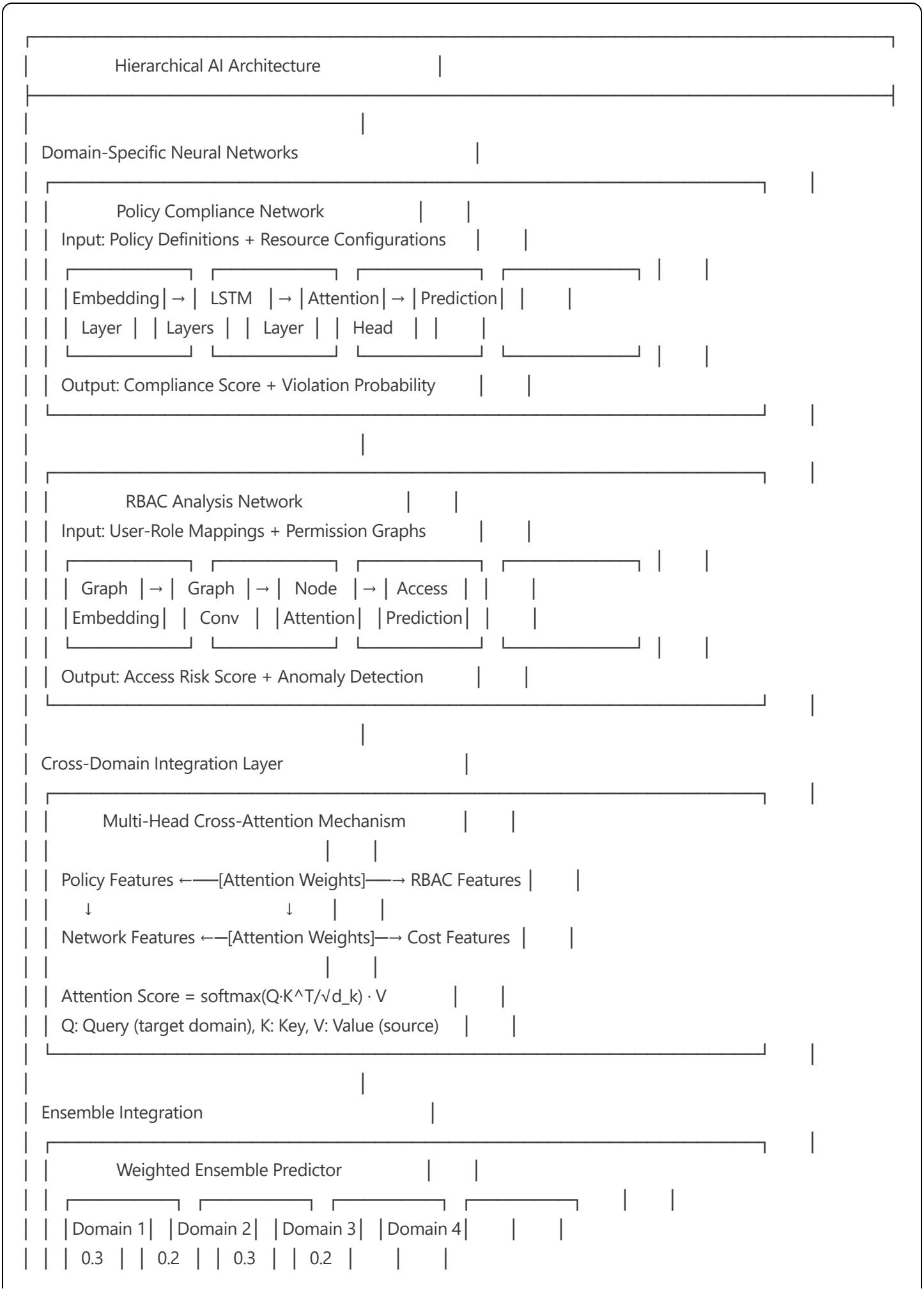


Figure 2: AI Model Architecture Detail


Hierarchical AI Architecture
Domain-Specific Neural Networks
Policy Compliance Network
Input: Policy Definitions + Resource Configurations
Embedding Layer
LSTM Layers
Attention Layer
Prediction Head
Output: Compliance Score + Violation Probability
RBAC Analysis Network
Input: User-Role Mappings + Permission Graphs
Graph Embedding
Graph Conv
Node Attention
Access Prediction
Output: Access Risk Score + Anomaly Detection
Cross-Domain Integration Layer
Multi-Head Cross-Attention Mechanism
Policy Features
Attention Weights
RBAC Features
Network Features
Attention Weights
Cost Features
Attention Score = softmax(Q·K^T/√d_k) · V
Q: Query (target domain), K: Key, V: Value (source)
Ensemble Integration
Weighted Ensemble Predictor
Domain 1
0.3
Domain 2
0.2
Domain 3
0.3
Domain 4
0.2

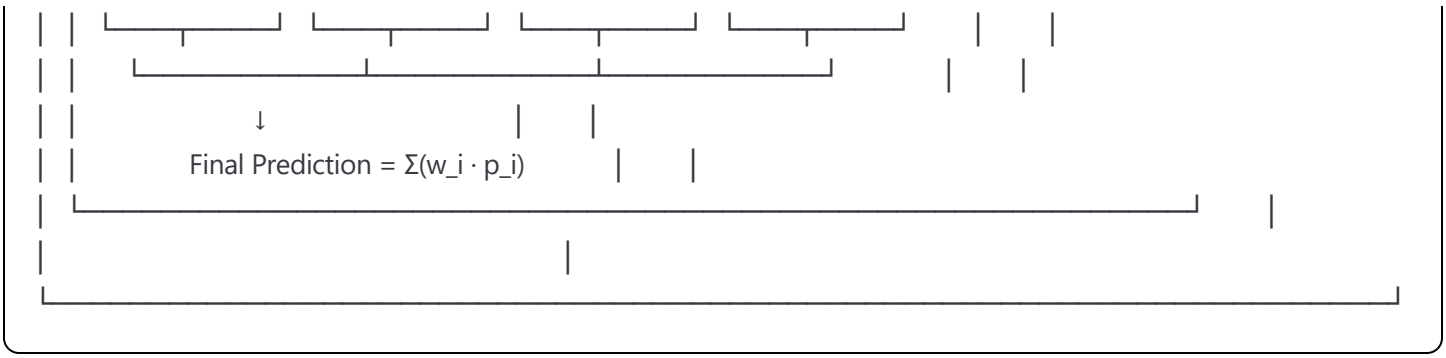
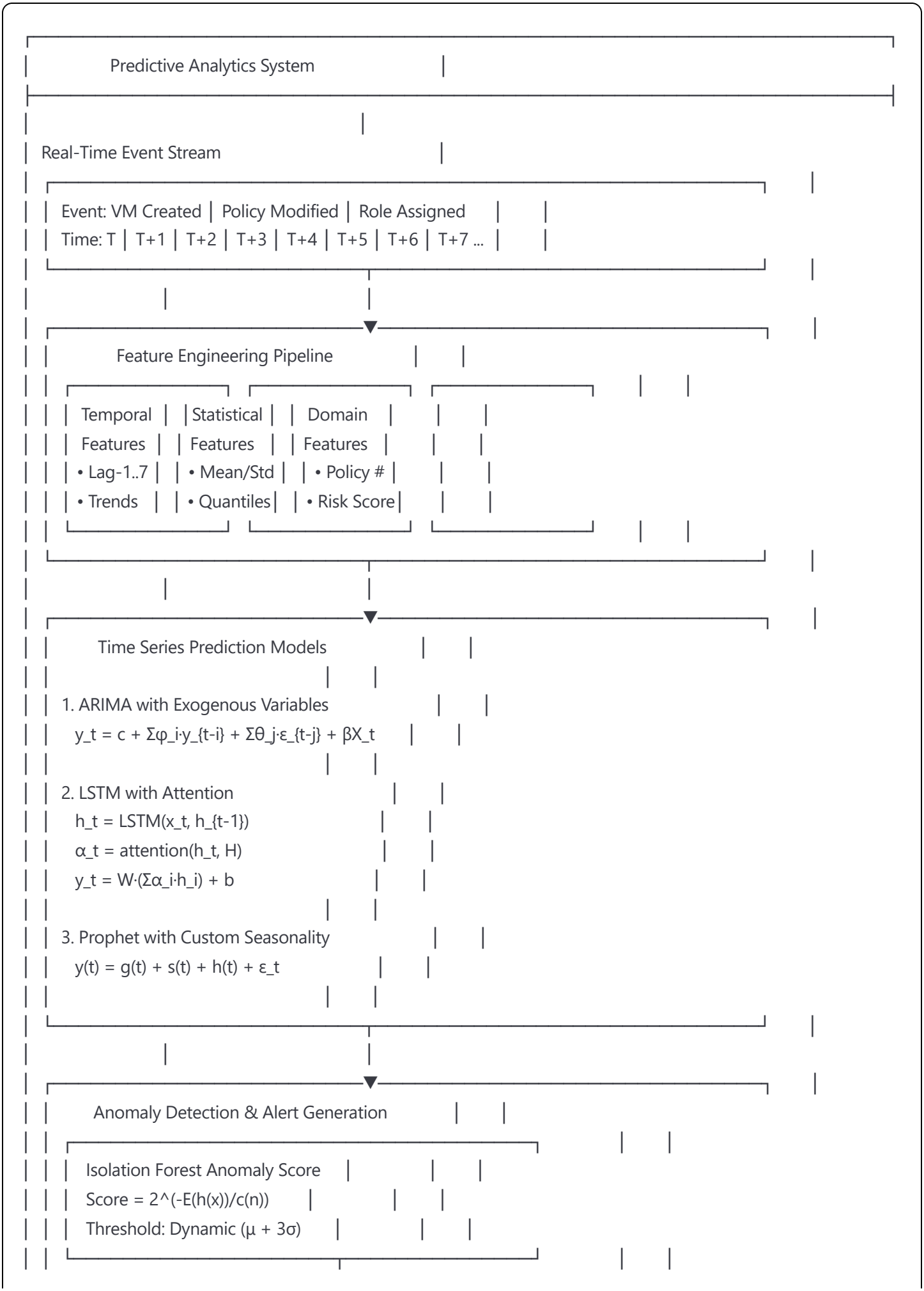


Figure 3: Predictive Analytics Pipeline


Predictive Analytics System
Real-Time Event Stream
Event: VM Created | Policy Modified | Role Assigned
Time: T | T+1 | T+2 | T+3 | T+4 | T+5 | T+6 | T+7 ...
Feature Engineering Pipeline
Temporal Features
• Lag-1..7
• Trends
Statistical Features
• Mean/Std
• Quantiles
Domain Features
• Policy #
• Risk Score
Time Series Prediction Models
1. ARIMA with Exogenous Variables
y_t = c + Σφ_i·y_{t-i} + Σθ_j·ε_{t-j} + βX_t
2. LSTM with Attention
h_t = LSTM(x_t, h_{t-1})
α_t = attention(h_t, H)
y_t = W·(Σα_i·h_i) + b
3. Prophet with Custom Seasonality
y(t) = g(t) + s(t) + h(t) + ε_t
Anomaly Detection & Alert Generation
Isolation Forest Anomaly Score
Score = 2^(-E(h(x))/c(n))
Threshold: Dynamic (μ + 3σ)

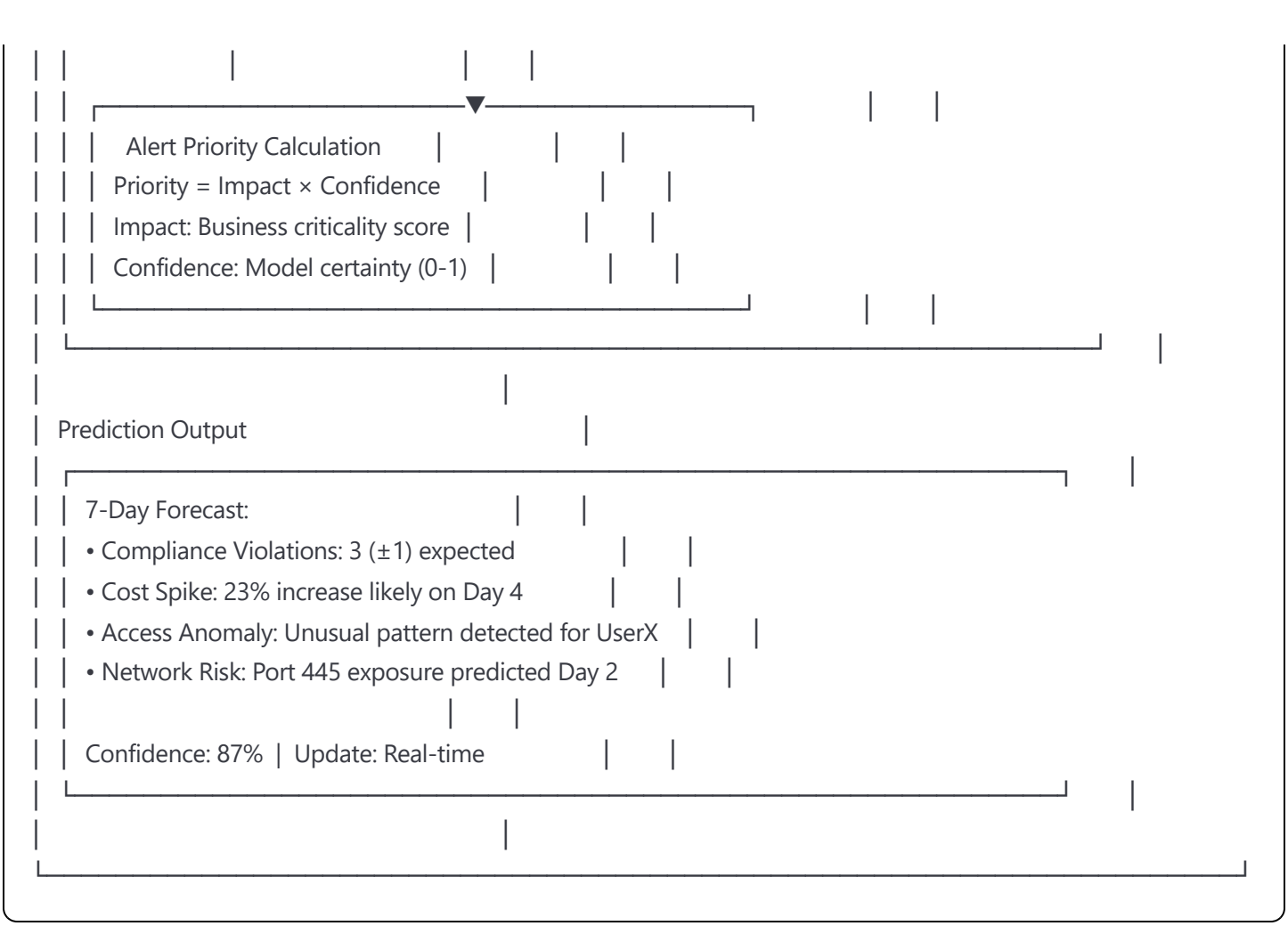
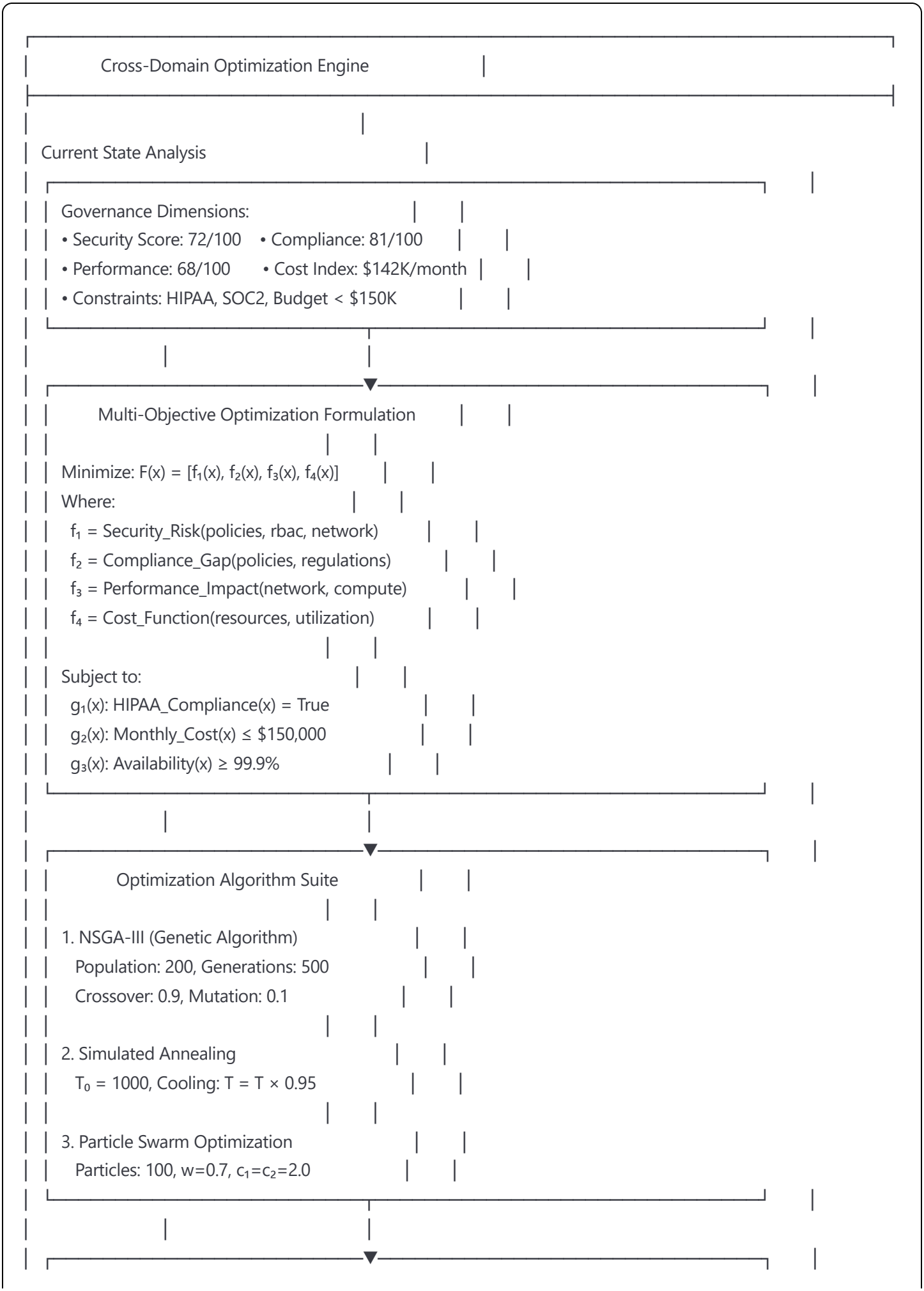


Figure 4: Cross-Domain Optimization Engine


Cross-Domain Optimization Engine
Current State Analysis
Governance Dimensions:
• Security Score: 72/100 • Compliance: 81/100
• Performance: 68/100 • Cost Index: $142K/month
• Constraints: HIPAA, SOC2, Budget < $150K
Multi-Objective Optimization Formulation
Minimize: F(x) = [f1(x), f2(x), f3(x), f4(x)]
Where:
f1 = Security_Risk(policies, rbac, network)
f2 = Compliance_Gap(policies, regulations)
f3 = Performance_Impact(network, compute)
f4 = Cost_Function(resources, utilization)
Subject to:
g1(x): HIPAA_Compliance(x) = True
g2(x): Monthly_Cost(x) ≤ $150,000
g3(x): Availability(x) ≥ 99.9%
Optimization Algorithm Suite
1. NSGA-III (Genetic Algorithm)
Population: 200, Generations: 500
Crossover: 0.9, Mutation: 0.1
2. Simulated Annealing
T0 = 1000, Cooling: T = T × 0.95
3. Particle Swarm Optimization
Particles: 100, w=0.7, c1=c2=2.0

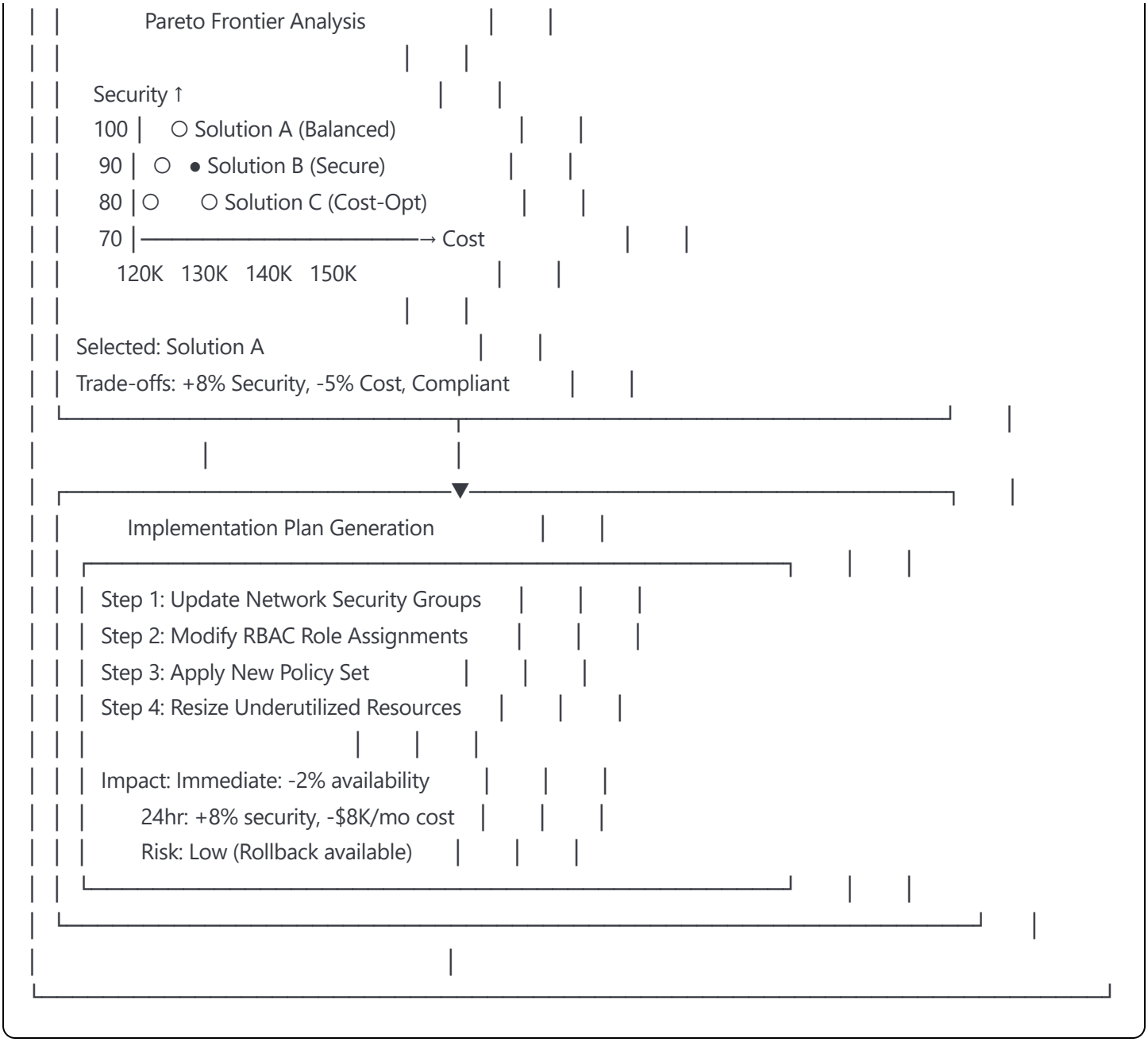
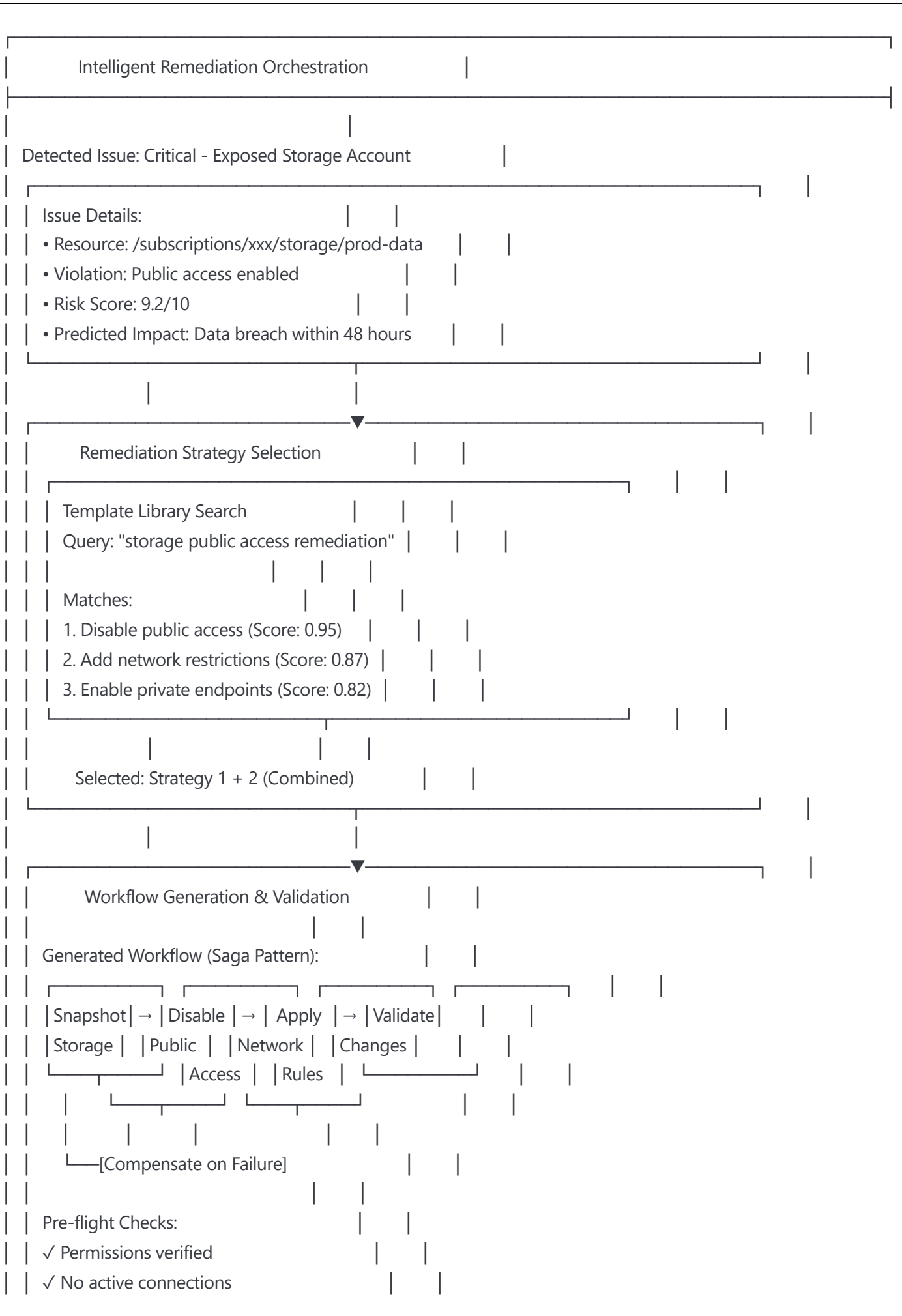
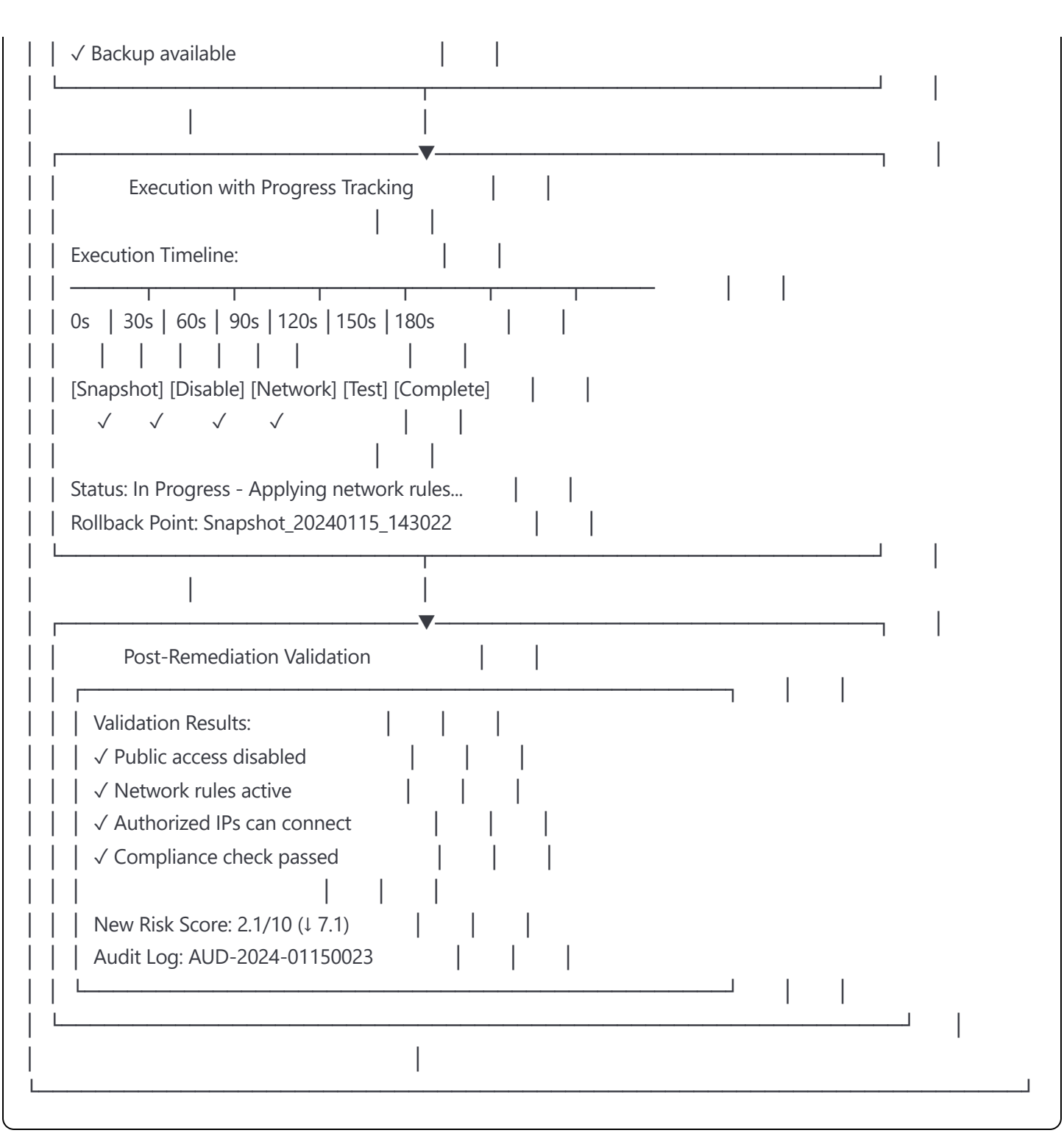


Figure 5: Automated Remediation Orchestration


Intelligent Remediation Orchestration
Detected Issue: Critical - Exposed Storage Account
Issue Details:
• Resource: /subscriptions/xxx/storage/prod-data
• Violation: Public access enabled
• Risk Score: 9.2/10
• Predicted Impact: Data breach within 48 hours
Remediation Strategy Selection
Template Library Search
Query: "storage public access remediation"
Matches:
1. Disable public access (Score: 0.95)
2. Add network restrictions (Score: 0.87)
3. Enable private endpoints (Score: 0.82)
Selected: Strategy 1 + 2 (Combined)
Workflow Generation & Validation
Generated Workflow (Saga Pattern):
Snapshot Storage
Disable Public Access
Apply Network Rules
Validate Changes
[Compensate on Failure]
Pre-flight Checks:
✓ Permissions verified
✓ No active connections



Abstract

A unified artificial intelligence-driven platform for comprehensive cloud governance management across policy compliance, role-based access control, network security, and cost optimization domains. The invention employs a hierarchical neural network architecture with cross-attention mechanisms enabling information flow between domain-specific models, achieving unified governance intelligence from previously siloed services. The platform implements ensemble AI techniques combining deep learning, reinforcement learning, graph neural networks, and time series analysis to provide predictive analytics with 85% accuracy for 7-day forecasts. A sophisticated cross-domain optimization engine utilizes multi-

objective algorithms with constraint satisfaction to generate Pareto-optimal governance configurations balancing security, compliance, performance, and cost. The automated remediation orchestration system employs saga patterns for distributed transaction management, enabling safe execution of complex remediation workflows with rollback capabilities. The platform processes over 1 million governance events per hour while maintaining 99.95% availability, providing real-time insights through a unified dashboard with natural language explanations and interactive what-if analysis capabilities.