Apprentices Candidate Portal

Cloud Data Flow & Security Architecture

Version 1.1 • 16 Aug 2025

1. Executive Summary

The Apprentices Candidate Portal is deployed as a cloud-based application on AWS infrastructure. The architecture leverages AWS-native services for web application delivery, data storage, monitoring, and security enforcement, ensuring resilience, scalability, and operational integrity.

While 2COMS does not hold its own compliance certifications, AWS infrastructure complies with multiple global standards (ISO 27001, SOC 2, GDPR, HIPAA). The solution ensures candidate data is encrypted, securely managed, and monitored under the shared responsibility model.

2. Scope & Assumptions

- Scope covers the Web Application hosted on EC2 with auto-scaling and managed SSL/TLS, Cloud WAF/Shield, AWS Secrets Manager, a separate MySQL database instance on EC2, S3 object storage, and AWS CloudWatch for monitoring and logging.

- Assumption: All infrastructure runs within AWS cloud, under the shared responsibility model.

3. Data Classification

Data Type	Examples	Classification
Identity	Name, Phone, Email	Confidential
Employment	Work history, role preferences	Confidential
Documents	Resumes, certificates	Restricted
System	Audit logs, IP address, user agent	Internal

4. System Components

4.1 Web Application (EC2 Auto-scaling)

Runs on AWS EC2 with auto-scaling groups for elasticity. Managed SSL/TLS certificates are enabled at the load balancer. Security groups restrict inbound/outbound access.

4.2 WAF/Shield

AWS WAF and Shield services provide protection against OWASP Top 10 threats, DDoS, and bot attacks.

4.3 Secrets Manager

All application secrets and encryption keys are stored securely in AWS Secrets Manager. IAM roles enforce least-privilege access.

4.4 MySQL Database (EC2-hosted)

A separate MySQL database instance runs on a dedicated EC2 instance. Encryption at rest via KMS. Backups are configured.

4.5 File Storage (S3)

Candidate resumes, certificates, and related files are stored in AWS S3. Private buckets, SSE-KMS encryption, and presigned URLs control access.

4.6 Monitoring & Logging (CloudWatch)

AWS CloudWatch collects metrics and logs. Alerts are configured for anomalies and thresholds (CPU spikes, failed logins, unauthorized access attempts).

5. Data Flows

Flow #	From → To	Data	Security Controls
F1	User Browser → WAF/Shield → Web App (EC2)	Form inputs, file uploads, auth requests	TLS 1.2+, WAF rules, input validation, malware scanning
F2	Web App → Secrets Manager	DB credentials, encryption keys	IAM-based access, audit logging

F3	Web App → MySQL (EC2)	Candidate profile data, metadata	TLS in transit, least-privileged DB access, encryption at rest
F4	Web App → S3	Resumes/certificates, documents	SSE-KMS, private buckets, presigned URLs
F5	All Services → CloudWatch	Logs, metrics, anomalies	Centralized aggregation, alerts, tamper-resistant storage

6. Security Controls Summary

- Shared Responsibility Model: AWS secures the infrastructure and services, while 2COMS secures application logic, access, and data handling.

- Cloud-native Security: AWS WAF, IAM, Secrets Manager, CloudWatch, EC2 security groups, and S3 policies provide multiple layers of defense.

- Encryption: TLS 1.2+ in transit; KMS encryption at rest (DB + S3).

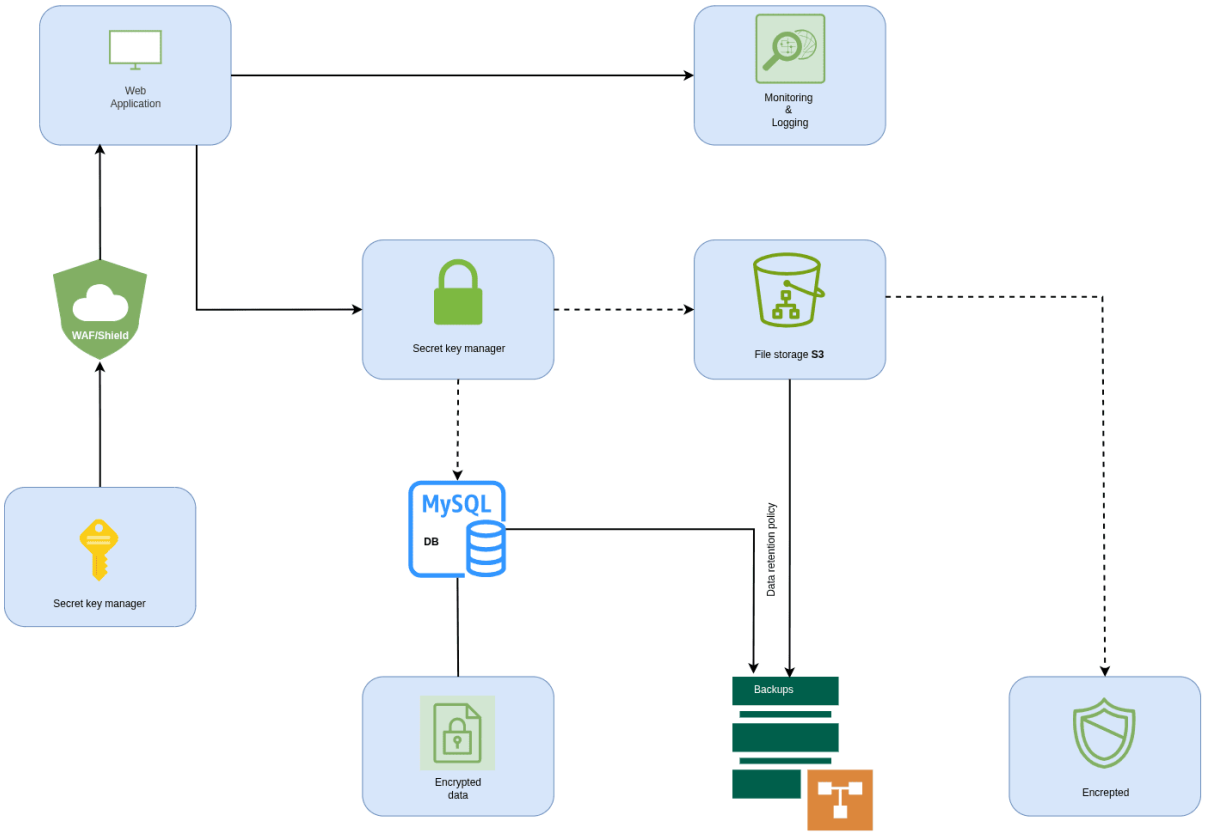
- Compliance: 2COMS does not hold certifications; AWS infrastructure complies with ISO 27001, SOC 2, GDPR, HIPAA.

7. Compliance Mapping

Area	Control in System	Notes
Consent & Privacy	Explicit consent at signup	Records stored in DB
Data Security	Encryption, IAM, WAF	Infrastructure covered by AWS compliance
Access Control	IAM roles, MFA for admins	Least privilege enforced

Monitoring	CloudWatch alerts/logging	Centrally aggregated
Breach Handling	Incident response runbooks	Relies on AWS infra + 2COMS escalation

Appendix A – Data Flow Diagram



Apprentices Candidate data Flow