FACT KEEP

Data Collection and Processing: Security Protocols – Ver. 2.6

Overview:

Data Collection and Security

We collect and transmit your data using secure, encrypted connections (HTTPS with TLS). Only authorized clients can access protected areas of our service, which requires an API key or access token. Incoming network traffic is filtered using industry-standard firewall controls to ensure only approved requests reach our systems.

Data Processing and Storage

Your data is stored in encrypted form within our databases. All processing occurs in a secure cloud environment where access is strictly limited based on job roles and least-privilege principles. Internal system-to-system communication is also encrypted. Access to data is governed through robust identity and access controls.

Data Collection Security Controls

- **Encrypted Transport:**

  All inbound and outbound data is transmitted using HTTPS with TLS 1.2+ enforcement at the CloudFront CDN and the FastAPI backend. This ensures end-to-end encryption from client to application layer.

  - Data is never transmitted in plaintext; interception would yield unreadable encrypted data.

- **Authentication Mechanisms:**

  Protected API routes require API key or token-based authentication. Keys are scoped, rotated periodically, and stored securely.

  - Only authenticated/approved parties can interact with sensitive operations.

- **Network Access Control:**

  AWS Security Groups restrict inbound and outbound traffic to approved ports, sources, and services. Unapproved traffic is blocked before reaching application layers.

  - Only specific, allowed traffic ever reaches the backend. Everything else is automatically blocked.

Data Processing & Storage Controls

- **Storage Encryption:**

  MongoDB storage volumes are encrypted at rest using AES-256 (via AWS-managed encryption). Backups and snapshots inherit the same encryption policy.

  - Stored data cannot be read by unauthorized parties, even if the hardware is compromised.

- **Compute Environment:**

  Application workloads run on hardened EC2 instances in a private subnet with no public IP exposure. IAM roles applied to instances follow least-privilege design patterns.

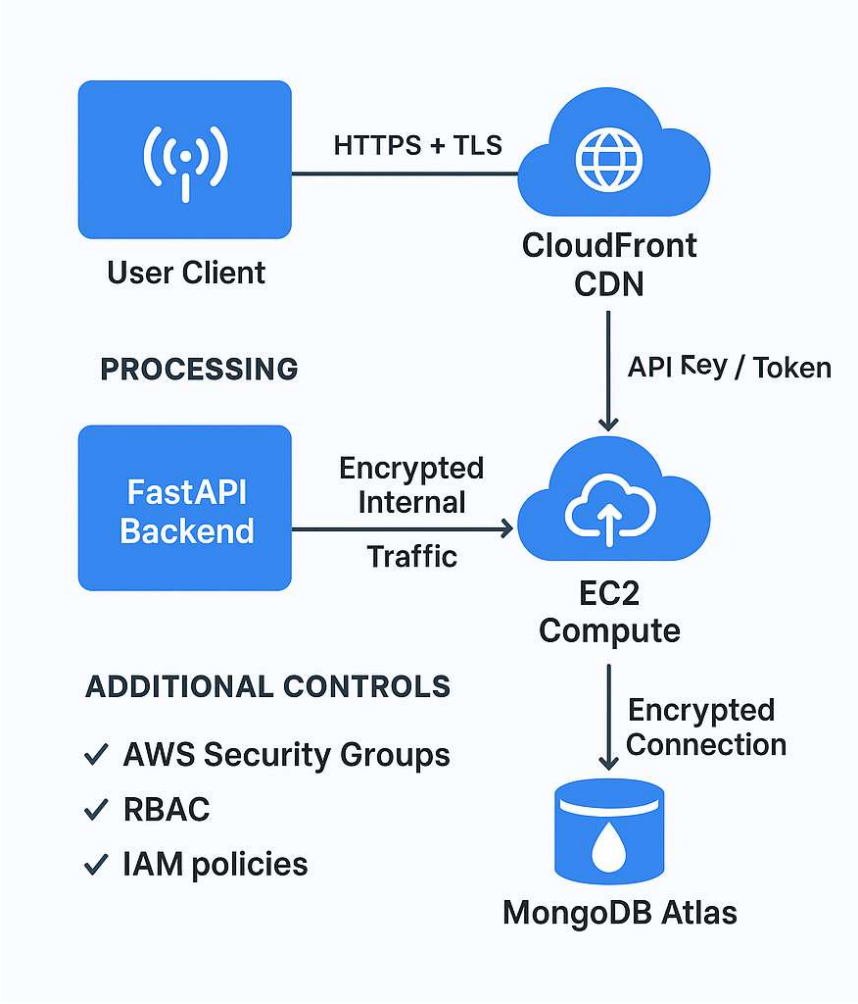
  - Internal components cannot touch data or systems they are not explicitly allowed to interact with.

- **Internal Traffic Protections:**

  All inter-service communication (application → database → internal APIs) is encrypted. Access between components is governed by IAM policies and application-level RBAC to ensure each system or user can only access allowed resources.

  - Internal traffic cannot be intercepted or read, and users/services inside the system only access what their role permits.

Data Flow Diagram



Compliance Considerations

This architecture aligns with SOC 2, ISO 27001, and general best practices for data security and privacy.

In Conclusion

Through encrypted transport, storage, and internal communication, combined with strong authentication, access control, and network security measures, this system ensures secure collection, processing, and storage of your sensitive data.