Securing Your Data: FactKeep's Comprehensive Security Architecture

Executive Summary

In an era where data breaches and security vulnerabilities pose significant risks to organizations, FactKeep has implemented a multi-layered security architecture designed to protect sensitive data throughout its entire lifecycle. This white paper outlines our comprehensive approach to data collection, processing, and storage security, demonstrating our commitment to maintaining the highest standards of data protection.

Our security framework employs encryption at every stage, robust authentication mechanisms, granular access controls, and network isolation to ensure that your data remains confidential, maintains integrity, and stays available only to authorized parties.

Introduction

The Challenge of Data Security

Organizations today face unprecedented challenges in protecting their data assets. Threats range from external attacks and unauthorized access attempts to insider threats and infrastructure vulnerabilities. A comprehensive security strategy must address protection at multiple levels: during transmission, while at rest, and throughout processing.

FactKeep's Security Philosophy

FactKeep's security architecture is built on three core principles:

Defense in Depth: Multiple layers of security controls ensure that if one layer is compromised, others continue to protect your data.

Least Privilege Access: Every user, service, and system component receives only the minimum permissions necessary to perform its designated function.

End-to-End Encryption: Data remains encrypted throughout its journey; from the moment it leaves your systems until it's securely stored and processed within our infrastructure.

Security Architecture Overview

Three-Tier Protection Model

FactKeep's security architecture operates across three critical tiers:

Data Collection Security protects information as it enters our systems through encrypted transport channels, authentication requirements, and network-level filtering.

Data Processing Security ensures that compute operations occur in isolated, hardened environments with strict access controls and role-based permissions.

Data Storage Security safeguards information at rest through encryption, secure backup procedures, and comprehensive access governance.

This layered approach ensures continuous protection regardless of where data resides within our infrastructure or what operations are being performed on it.

Data Collection Security

Encrypted Transport Layer

All data transmitted to and from FactKeep travels through encrypted channels using HTTPS with Transport Layer Security (TLS) version 1.2 or higher. This encryption is enforced at two critical points:

The CloudFront Content Delivery Network (CDN) serves as the first point of contact, ensuring that all incoming connections use strong encryption from the moment they reach our infrastructure.

The FastAPI backend maintains encryption standards throughout the application layer, creating an unbroken chain of protection from client to server.

This dual-layer enforcement means that data never exists in plaintext during transmission. Even if network traffic were intercepted, the encrypted payload would remain unreadable without the proper decryption keys.

Authentication and Authorization

Access to protected resources requires proper authentication through one of two mechanisms:

API Key Authentication provides programmatic access for automated systems and integrations. These keys are carefully scoped to limit their capabilities to specific operations and resources.

Token-Based Authentication enables secure session management for interactive users and applications, with tokens that expire and require renewal to maintain access.

Both authentication methods include security features such as periodic rotation schedules and secure storage practices to minimize the risk of unauthorized access through compromised credentials.

Network Access Control

Before traffic ever reaches application layers, it must pass through network security controls implemented via AWS Security Groups. These controls function as a virtual firewall, examining each connection request against a whitelist of approved sources, destinations, and ports.

Traffic that doesn't match approved patterns is automatically blocked at the network perimeter, preventing unauthorized connection attempts from consuming resources or probing for vulnerabilities. This creates a secure network boundary that only permits legitimate, expected traffic patterns.

Data Processing Security

Compute Environment Isolation

Application workloads execute on hardened Amazon EC2 instances specifically configured for security:

Private Subnet Deployment ensures compute instances have no direct exposure to the public internet. These instances cannot be reached from external networks, and they access external resources only through controlled channels.

Least Privilege IAM Roles govern what each compute instance can access within the AWS infrastructure. Roles are carefully crafted to grant only the specific permissions required for each instance's designated function.

This isolation strategy ensures that even if an application vulnerability were exploited, the attacker would find themselves in a severely restricted environment with limited ability to access sensitive data or move laterally through the infrastructure.

Role-Based Access Control

Within the application layer, access to data and operations is governed by comprehensive Role-Based Access Control (RBAC) policies. These policies define precisely what each user role, service account, and system component can access.

RBAC implementation ensures that developers cannot access production data, operational staff cannot modify application code, and automated systems can only touch the specific resources they need for their designated tasks. This granular control significantly reduces the attack surface and limits potential damage from compromised accounts.

Internal Communication Security

Communication between internal system components receives the same encryption treatment as external traffic. Traffic flowing from application servers to databases, between microservices, or to internal APIs travels through encrypted channels.

Combined with IAM policies and RBAC enforcement, this approach ensures that internal network access provides no advantage to attackers. Even if someone gained access to the internal network, they would encounter encrypted traffic and face authorization challenges at every system boundary.

Data Storage Security

Encryption at Rest

All data stored in MongoDB databases benefits from AES-256 encryption applied at the storage volume level. This encryption is managed through AWS's encryption services, providing:

Transparent Operation: Applications interact with data normally while encryption and decryption happen automatically at the storage layer.

Key Management Security: Encryption keys are stored and managed separately from the encrypted data, following best practices for key lifecycle management.

Backup Protection: All backups and snapshots automatically inherit the same encryption policy, ensuring that archived data receives identical protection to production data.

This storage encryption strategy means that physical access to storage hardware would not compromise data confidentiality. The data remains encrypted and unreadable without proper authorization through the application and its associated decryption keys.

Access Governance

Access to stored data is controlled through multiple mechanisms working in concert:

IAM policies define what AWS-level operations are permitted on storage resources.

Database-level permissions control which application components can query or modify specific data collections.

Application RBAC determines which users can trigger operations that ultimately access stored data.

This multi-layer governance ensures that access control failures at one level don't automatically compromise data security, as additional authorization checks occur at other layers.

Compliance and Standards Alignment

Industry Framework Compliance

FactKeep's security architecture aligns with requirements from multiple industry-standard frameworks:

SOC 2 Alignment: Our controls address the Trust Services Criteria for security, availability, and confidentiality that SOC 2 examinations evaluate.

ISO 27001 Principles: The architecture incorporates information security management best practices consistent with ISO 27001 standards for protecting information assets.

Privacy Best Practices: Our approach to data minimization, encryption, and access control reflects modern privacy-by-design principles.

This alignment demonstrates that our security measures meet expectations established by independent standards bodies and industry consensus around effective data protection.

Data Flow and Security Integration

End-to-End Protection

Consider how data flows through the FactKeep system with security at every stage:

A client application initiates a connection that must use HTTPS with TLS 1.2 or higher. The connection passes through CloudFront CDN where encryption is verified and network-level filtering occurs via Security Groups.

Upon reaching the FastAPI backend, the request undergoes authentication verification through API key or token validation. Authorization checks determine whether the authenticated party has permission for the requested operation.

If processing is required, the operation executes on isolated EC2 instances in private subnets, with IAM roles limiting what resources can be accessed. Communication with the MongoDB database occurs over encrypted internal channels.

Data stored in MongoDB resides in AES-256 encrypted volumes, remaining protected even if physical hardware is compromised.

Results return to the client through the same encrypted channels, maintaining confidentiality throughout the complete request-response cycle.

Continuous Security Posture

This integrated approach means security isn't dependent on any single control. Multiple independent security layers work together, ensuring that:

- Encryption protects data confidentiality during transit and at rest
- Authentication verifies the identity of parties requesting access
- Authorization ensures only permitted operations occur
- Network controls block unauthorized traffic at the perimeter
- Access governance limits what each identity can access
- Isolation restricts lateral movement and limits blast radius

Conclusion

FactKeep's security architecture demonstrates a comprehensive, defense-in-depth approach to protecting sensitive data throughout its lifecycle. By implementing encryption at every stage, enforcing strong authentication and authorization, isolating processing environments, and maintaining granular access controls, we create multiple layers of protection that work together to safeguard your data.

Our alignment with industry standards like SOC 2 and ISO 27001 principles provides assurance that our security measures meet established criteria for effective data protection. As threats evolve, our security architecture provides a robust foundation for adapting controls while maintaining the core principles of confidentiality, integrity, and availability.

Organizations can trust FactKeep to handle their sensitive data with the care and protection it deserves, backed by a security architecture designed to meet the challenges of today's threat landscape.

Document Version: Based on Security Protocols Ver. 2.6
For More Information: Contact FactKeep Security Team