LumiaX

Owner:
Reviewer:
Contributors:
Date Generated: Sat Nov 02 2024

Executive Summary

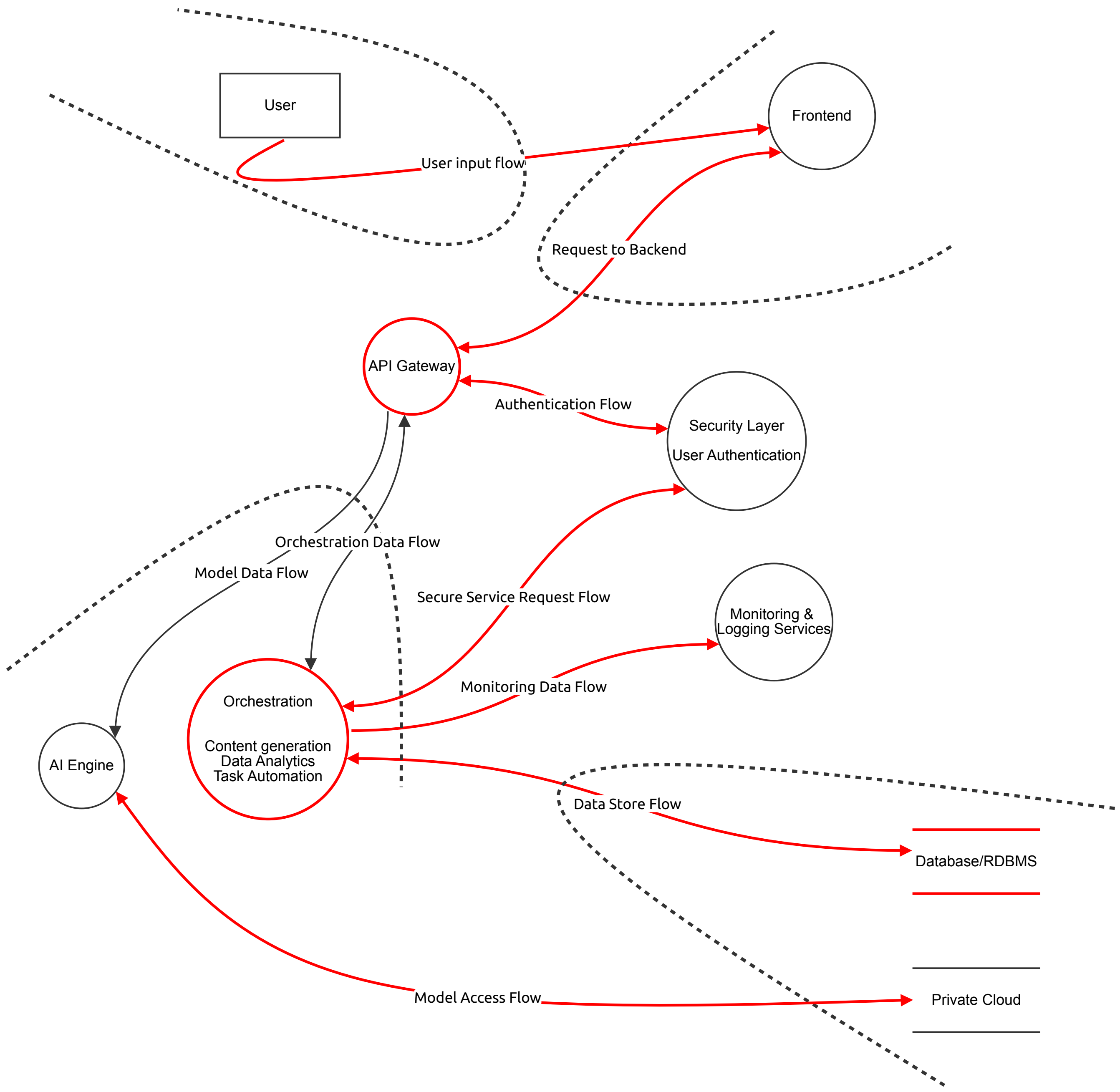
High level system description

Not provided

Summary

Total Threats	12
Total Mitigated	0
Not Mitigated	12
Open / High Priority	8
Open / Medium Priority	4
Open / Low Priority	0
Open / Unknown Priority	0

New STRIDE diagram



New STRIDE diagram

User (Actor)

The end-user interacting with the system through the graphical user interface (GUI)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Frontend (Process)

The web or mobile app handling requests from the user.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request to Backend (Data Flow)

sending requests to backend services

Number	Title	Type	Priority	Status	Score	Description	Mitigations
34	Tampering with Data in Transit	Tampering	High	Open		An attacker could attempt to alter data in transit between the Frontend and API Gateway. This could compromise the integrity of the data, potentially leading to unauthorized data modifications or injections.	Use AES-256-GCM encryption for data in transit, enforce HTTPS/TLS for all data flows to ensure secure communication channels, and validate message integrity with cryptographic signatures to detect tampering.

Data Store Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
43	Encryption Bypass	Information disclosure	Medium	Open		Given that sensitive data is a core part of LumiMind, we need to ensure that threats related to weak encryption in transit or at rest are covered, particularly around the RDBMS and Private Cloud.	Use strong encryption standards for data at rest (AES-256-GCM) and in transit (TLS). Regularly review encryption configurations to ensure they meet current standards.

Model Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Monitoring Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
37	Data Leakage via Monitoring Services	Information disclosure	High	Open		Sensitive information could be exposed through Monitoring & Logging Services if logs are improperly secured or sanitized, potentially allowing unauthorized users to access sensitive data contained within logs.	Apply access controls to restrict access to logs, encrypt sensitive data within logs, and sanitize logs to remove any personally identifiable information (PII) or other sensitive data before storage. Limit access to Monitoring & Logging Services to authorized personnel only.

Orchestration Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
42	Phishing, Accidental Data Breaches	Information disclosure	High	Open		Due to low cybersecurity awareness among employees there is a risk of employees unknowingly clicking on phishing emails or mishandling sensitive information, leading to data exposure.	Regular employee training on secure data handling, phishing awareness, and enforcing strong, unique passwords with multi-factor authentication.

User input flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
33	User Identity Spoofing	Tampering	High	Open		An attacker might impersonate a legitimate user by bypassing or tampering with authentication mechanisms, exploiting weaknesses in the User Input Flow or Authentication Flow. This could allow unauthorized access to the system, leading to potential misuse of resources or data theft.	Implement multi-factor authentication (MFA) to verify user identities, and enforce OAuth 2.0 with JWT tokens to secure and validate user sessions. Regularly audit authentication logs for suspicious activity.
35	Repudiation of User Actions	Information disclosure	Medium	Open		Users might deny having performed specific actions if proper logging and accountability mechanisms are not in place, particularly within the User Input Flow and Secure Service Request Flow. This can hinder incident investigations and accountability.	Implement detailed logging of all user actions with unique session identifiers and timestamps. Use JWT tokens to verify and log each user's actions, and store logs securely within Monitoring & Logging Services with restricted access to ensure integrity.

Secure Service Request Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
36	Repudiation of User Actions	Information disclosure	Medium	Open		Users might deny having performed specific actions if proper logging and accountability mechanisms are not in place, particularly within the User Input Flow and Secure Service Request Flow. This can hinder incident investigations and accountability.	Implement detailed logging of all user actions with unique session identifiers and timestamps. Use JWT tokens to verify and log each user's actions, and store logs securely within Monitoring & Logging Services with restricted access to ensure integrity.

Model Access Flow (Data Flow)

AI Engine retrieves or accesses models stored in the Private Cloud

Number	Title	Type	Priority	Status	Score	Description	Mitigations
44	Encryption Bypass	Information disclosure	Medium	Open		Given that sensitive data is a core part of LumiMind, we need to ensure that threats related to weak encryption in transit or at rest are covered, particularly around the RDBMS and Private Cloud.	Use strong encryption standards for data at rest (AES-256-GCM) and in transit (TLS). Regularly review encryption configurations to ensure they meet current standards.

API Gateway (Process)

Manages communication between the frontend and backend services

Number	Title	Type	Priority	Status	Score	Description	Mitigations
38	DoS Attack on API Gateway	Denial of service	High	Open		Attackers could attempt to overwhelm the API Gateway with a large volume of requests, potentially leading to service disruption and unavailability of backend services.	Implement rate limiting, IP-based throttling, and automated request filtering on the API Gateway to mitigate the effects of a DoS attack. Additionally, consider deploying a Web Application Firewall (WAF) to block malicious traffic patterns.

AI Engine (Process)

Where the TensorFlow Models and PyTorch Models are processed.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Orchestration

Content generation
Data Analytics
Task Automation (Process)

This process includes services like Content Generation, Data Analytics, Task Automation, and Authentication.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
39	Privilege Escalation via Orchestration Services	Elevation of privilege	High	Open		Unauthorized users could exploit vulnerabilities within the Orchestration Layer to gain elevated privileges, allowing access to backend services such as Content Generation, Data Analytics, and Task Automation. This could lead to unauthorized data access or system manipulation.	Enforce strict role-based access control (RBAC) within the Orchestration Layer to limit user permissions. Validate user roles and permissions for each request, and ensure the Security Layer policies are applied consistently across all services.

Security Layer

User Authentication (Process)

Contains the mechanisms that ensure security, such as AES-256-GCM encryption and OAuth 2.0 for authentication.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Database/RDBMS (Store)

This is where user data and other sensitive information are stored.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
40	Unencrypted Data in Database/RDBMS	Information disclosure	High	Open		Sensitive data stored in the Database/RDBMS may be exposed if it is not properly encrypted, allowing unauthorized users to access or retrieve sensitive information.	Apply database encryption (e.g., AES-256) to protect data at rest. Implement strict access controls to limit database access to only authorized users and services. Regularly monitor and audit database access logs for any suspicious activity.
41	Tampering with Data in Database/RDBMS	Tampering	High	Open		An attacker could attempt to modify or corrupt data stored in the Database/RDBMS, potentially leading to data integrity issues, inaccurate analytics, or incorrect application behavior	Enforce strict access controls to restrict write permissions to only authorized services or users. Implement data integrity checks, such as hashing or digital signatures, to verify data integrity. Regularly monitor the database for unauthorized modifications

Private Cloud (Store)

This contains the TensorFlow and PyTorch Models and other essential backend data.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Monitoring & Logging Services (Process)

Prometheus, Grafana, and ELK Stack to monitor system health and log data.

Number	Title	Type	Priority	Status	Score	Description	Mitigations