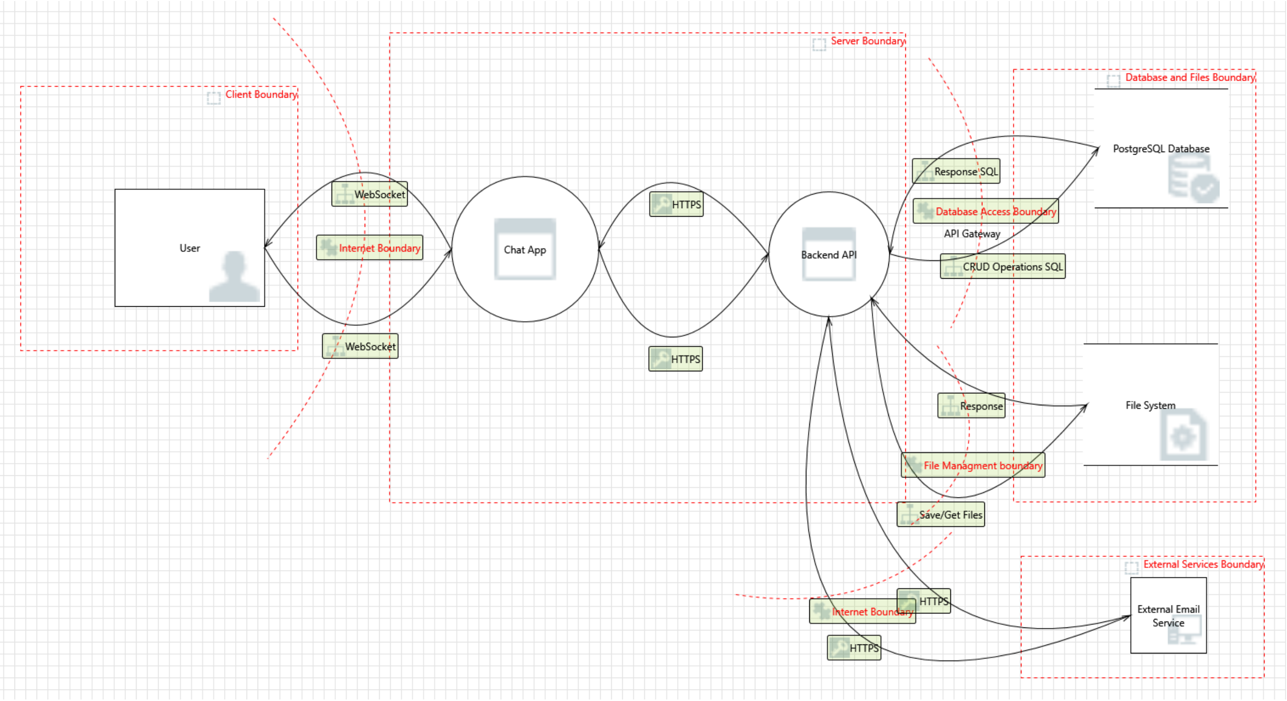
Security model



Title	Category	Interaction	Priority	Description	Mitigation Plan
Data Store Inaccessible	Denial Of Service	CRUD Operations SQL	High	An external agent prevents access to a data store on the other side of the trust boundary.	- Implement database replication and failover mechanisms - Use a DDoS protection service - Monitor database connection pools - Use rate limiting and timeouts for SQL queries
Weak Access Control for a Resource	Information Disclosure	Response SQL	High	Improper data protection of PostgreSQL Database can allow an attacker to read information not intended for disclosure. Review authorization settings.	- Enforce role-based access control (RBAC) - Encrypt data at rest and in transit - Conduct regular access audits - Implement database activity monitoring

Potential Excessive Resource Consumption	Denial Of Service	Save/Get Files	Medium	Does Backend API or File System take explicit steps to control resource consumption?	- Use rate limiting and quotas for file operations - Implement connection timeouts - Apply load balancing for file system operations - Monitor and alert on resource exhaustion
Potential Process Crash or Stop for Chat App	Denial Of Service	WebSocket	High	Chat App crashes, halts, stops, or runs slowly; in all cases violating an availability metric.	- Implement WebSocket connection health checks - Use automatic failover for Chat App - Deploy a circuit breaker pattern - Conduct load testing to simulate high traffic
Weak Access Control for a Resource	Information Disclosure	Response	High	Improper data protection of File System can allow an attacker to read information not intended for disclosure.	- Restrict access to file system operations - Encrypt sensitive files - Use intrusion detection for unauthorized file access - Regularly review and update file permissions
Data Store Inaccessible	Denial Of Service	Response	High	An external agent prevents access to a data store on the other side of the trust boundary.	- Enable database replication and backups - Use a Content Delivery Network (CDN) to cache data where possible - Apply rate limiting and IP blacklisting
Data Flow HTTPS Is Potentially Interrupted	Denial Of Service	HTTPS	High	An external agent interrupts data flowing across a trust boundary in either direction.	- Use TLS 1.3 for all HTTPS traffic - Implement mutual TLS authentication - Deploy a Web Application Firewall (WAF) - Use retry mechanisms and load balancers
Backend API Subject to Elevation of Privilege	Elevation Of Privilege	HTTPS	High	External Email Service may be able to remotely execute code for Backend API.	- Validate all incoming API requests - Apply input sanitization - Enforce strict authentication and authorization rules - Regularly patch and update the Backend API

PostgreSQL Database Data Store Could Be Corrupted	Tampering	CRUD Operations SQL	High	Data flowing across CRUD Operations SQL may be tampered with by an attacker, potentially corrupting the PostgreSQL Database.	- Encrypt data in transit using TLS - Validate SQL inputs to prevent injection - Implement database integrity checks - Log and audit all database write operations
Data Store Denies File System Potentially Writing Data	Repudiation	Save/Get Files	High	File System claims it did not write data received from an entity on the other side of the trust boundary.	- Implement secure and tamper-proof logging - Use digital signatures for file write operations - Enable audit trails for all file actions - Use timestamps to validate operation sequences