Dynamic Analysis Report

1. Analysis Environment

The analysis was conducted inside a Docker container under a no-network mode (--network=none),
using strace, inotify, ss, and ps tools to monitor system calls and runtime behavior.
Duration: 60 seconds. Entry file: node src/server.js. Environment: Node.js v20.19.5, Network: isolated (no outbound connections).

2. Runtime Behavior Overview

During initialization, the program displays startup messages indicating RSA-4096 key generation and server setup.
It automatically creates a 4096-bit RSA key pair, suggesting built-in encryption support.

The system then attempts to connect to MongoDB on localhost (127.0.0.1:27017 / ::1:27017), but receives ECONNREFUSED since no MongoDB service exists in the container.

The connection failure causes the process to terminate prematurely, and no network listeners are active.
The ss.txt file only contains headers, confirming no open ports.

3. System Call Analysis

strace logs reveal multiple connect() attempts to 127.0.0.1:27017, file reads of project and Node modules, and normal stdout writes.
No suspicious execve() or access to sensitive files was detected.

4. Summary Results

Check Item	Result	Explanation
External Connections	None	All connections target localhost

Listening Ports	None	No ports opened
File I/O	Normal	No sensitive file accessed
Process Behavior	Safe	No external command execution
Encryption	RSA-4096 generated	Normal key generation
Error Handling	Weak	Crashes on MongoDB failure

5. Security Evaluation and Recommendations

Category	Finding	Severity	Recommendation
Database Dependency	Relies on MongoDB; may attempt external connection if misconfigured	Medium	Restrict DB to local network
Error Handling	Uncaught exception on DB failure	Low–Medium	Add try-catch and retry limits
Key Management	RSA key generated dynamically	Info	Ensure keys not logged
Communication	Uses RSA encryption	Normal	Maintain encryption practice
Syscalls	No exec or file injection	Safe	Maintain current isolation

6. Conclusion

The dynamic analysis indicates that the chat system initializes an RSA-4096 key pair and attempts a local MongoDB connection, which fails due to no-network mode.
No external connections, file tampering, or command execution were observed. The primary issue is weak error handling and potential misconfiguration risk.
Overall risk rating: Moderate.