Department of Computing

MSc in Artificial Intelligence

Intelligent Agents - IA_PCOM7E January 2025

Development Team Project: Project Report

AI-Based Performance Monitoring and Fitness Data Analysis System

Group A:

Tala Anabtawi, Marwa Alkuwari, Noora Alboinin, Abdulhakim Bashir

Institution: University of Essex

2025

Table of Contents

1.0 Introduction

Wearable technology has enhanced fitness tracking (Migliaccio et al., 2024), yet existing systems often lack deep data processing advanced AI insights, and secure archival, limiting their effectiveness for comprehensive performance evaluation. This project proposes an AI-based performance monitoring and fitness data analysis system that applies digital forensics principles to enhance data retrieval, analysis, and storage. While digital forensics is often linked to criminal investigations, its core focus on structured data retrieval, anomaly detection, and traceable archival can be seen equally relevant in fitness data analysis for performance tracking and training optimization.

The system leverages a multi-agent system (MAS) for task specialization (Tomasino, 2025): a Data Retrieval Agent extracts Fitbit data, a Data Validation Agent ensures accuracy, an AI Analysis Agent detects anomalies, a Reporting Agent archives structured records, and a Security Agent manages encryption and data transmission. By employing edge computing for low-latency processing (Satyanarayanan, 2017) and a RESTful API for secure integration with third-party platforms, the system ensures scalable, structured data processing and supports retrospective evaluation.

2.0 System Requirements

The system integrates Fitbit wearables, AI-driven analysis, and secure performance data storage to ensure structured fitness data retrieval, processing, and archival.

2.1 Hardware Requirements

- **Fitbit Wearable Devices** for real-time biometric data retrieval. Fitbit was selected due to its extensive research validation making it a reliable choice for biometric data collection (Kasparian & Badawy, 2022).
- **Cloud Storage** (AWS S3, Firebase, Azure) with AES-256 encryption for forensic archival.
- **Computational Resources:**
    - **Edge Devices** (Raspberry Pi, NVIDIA Jetson) for local AI pre-processing
    - **Cloud ML Servers** (AWS Lambda, Google AI Platform) for scalable AI analysis and long-term data storage.

2.2 Software & Library Requirements

- **Languages:** Python (AI & data processing), JavaScript (React/Node.js) (dashboard visualization).
- **APIs & SDKs:** Fitbit Web API (OAuth 2.0 for secure data retrieval), MQTT **MQTT** (real-time data transfer for agent communication).
- **AI & Data Processing:** TensorFlow/Keras (biometric trend analysis), Pandas/Numpy (data structuring), OpenCV (anomaly detection).
- **Storage:** PostgreSQL (structured archival), Firebase Firestore (real-time data access)

These requirements ensure secure, scalable, and AI-driven fitness data processing, aligning with digital forensics principles in the context of structured performance monitoring and multi-agent system integration.

3.0 Design Decisions

The system is designed to deliver accurate, efficient, and secure performance analysis of Fitbit data. Each decision aligns with the project's focus on structured data handling, real-time insights, and retrospective evaluation, with critical evaluation of strengths, weaknesses, and mitigations.

3.1 AI-Driven Analysis

Decision: Implement Isolation Forest and One-Class SVM for anomaly detection.
Justification: These models effectively detect irregular patterns (Ravinder et al., 2024), aiding coaches in identifying performance issues and biometric anomalies.

- **Strengths:** Adapts to individual fitness patterns; automates insights.
- **Weaknesses:** Computationally demanding; models require regular updates.
- **Mitigation:** Use on-device pre-processing with cloud-based model updates to reduce strain on local resources.

3.2 Edge Computing for Real-Time Processing

Decision: Process Fitbit data locally to reduce latency and bandwidth use.
Justification: Edge computing ensures low-latency insights and improves data privacy by limiting cloud exposure (Karati & Das, 2022).

- **Strengths:** Faster response times; enables offline data continuity (Xu et al., 2019).
- **Weaknesses:** Limited processing power on edge devices. Risk of data exposure (George & Thampi, 2019).
- **Mitigation:** Defer complex processing to cloud servers post-session (Ullah et al., 2022). Implement AES-256 encryption for data in transit and at rest to minimize exposure risks.

3.3 RESTful API for Secure and Modular Integration

Decision: Develop a RESTful API for secure Fitbit data retrieval and integration with performance tracking tools.
Justification: Ensures scalable system growth and seamless integration with third-party platforms.

- **Strengths:** Promotes modular expansion; enables secure communication.
- **Weaknesses:** Requires frequent updates to align with Fitbit SDK changes.
- **Mitigation:** Use version control and ensure backward compatibility.

3.4 Multi-Agent System (MAS) Integration

The system's MAS structure ensures efficient task distribution and enhances data integrity, security, and scalability (Schwaiger & Stahmer, 2005). Each agent performs specialized roles to enhance system reliability and performance:

- **Data Retrieval Agent** – Captures Fitbit data and manages API rate limits.
- **Data Validation Agent** – Verifies data accuracy before analysis to ensure forensic reliability.
- **AI Analysis Agent** – Identifies trends and anomalies with cloud support for complex model updates.
- **Reporting Agent** – Archives structured performance records with timestamps for traceable review.
- **Security Agent** – Manages encryption, API token refresh, and secure data transmission.

4.0 Development Approach

The system will follow an iterative, agent-based approach guided by Agile methodology for continuous testing and refinement. Modular design ensures scalability, while Test-Driven Development (TDD) enhances data reliability. Continuous Integration (CI) minimizes integration issues. Tools like Python, Fitbit API, and MQTT optimize performance, scalability, and secure data handling, aligning with the system's focus on structured data retrieval and retrospective analysis.

5.0 System Architecture and Diagram

Figure 1 below demonstrates the system’s architecture which employs a multi-agent system (MAS) for efficient task distribution and data security. Specialized agents manage data collection, validation, analysis, and reporting, while the Security Agent ensures encrypted data flow. A shared AgentBase class enhances modularity, supporting scalability and forensic traceability.

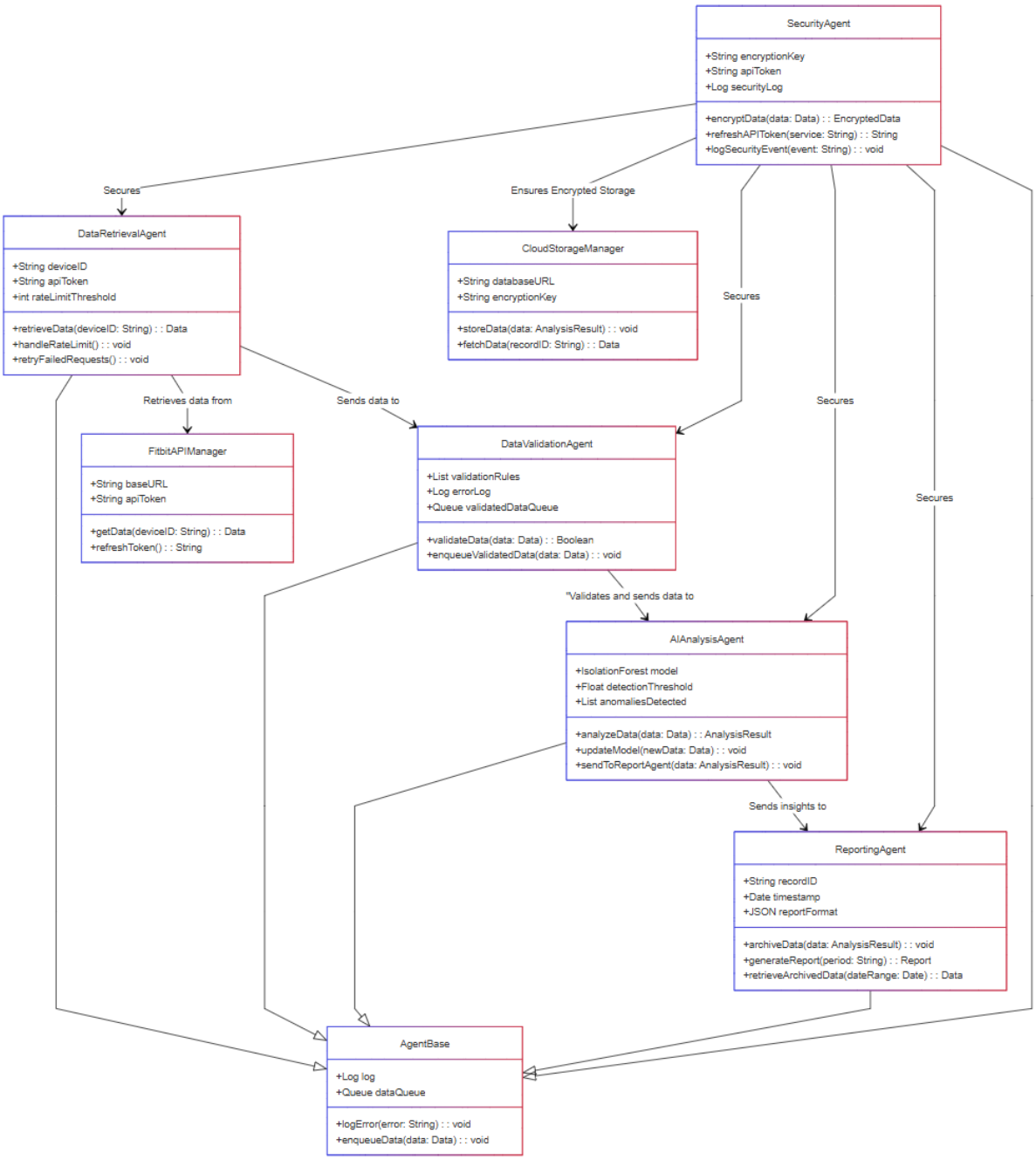

Figure 1: System Architecture — Class Diagram

Figure 2 illustrates the system's sequence flow, emphasizing secure data retrieval, validation, and archival. The Data Retrieval Agent requests Fitbit data, verified by the Security Agent for token validity. Invalid data triggers an alert and is rejected, while valid data is analyzed by the AI Analysis Agent for trends and anomalies. Results are encrypted by the Security Agent and archived in the Cloud Storage Manager. Upon request, data integrity is verified before generating a report, ensuring security, traceability, and compliance with forensic data management principles.

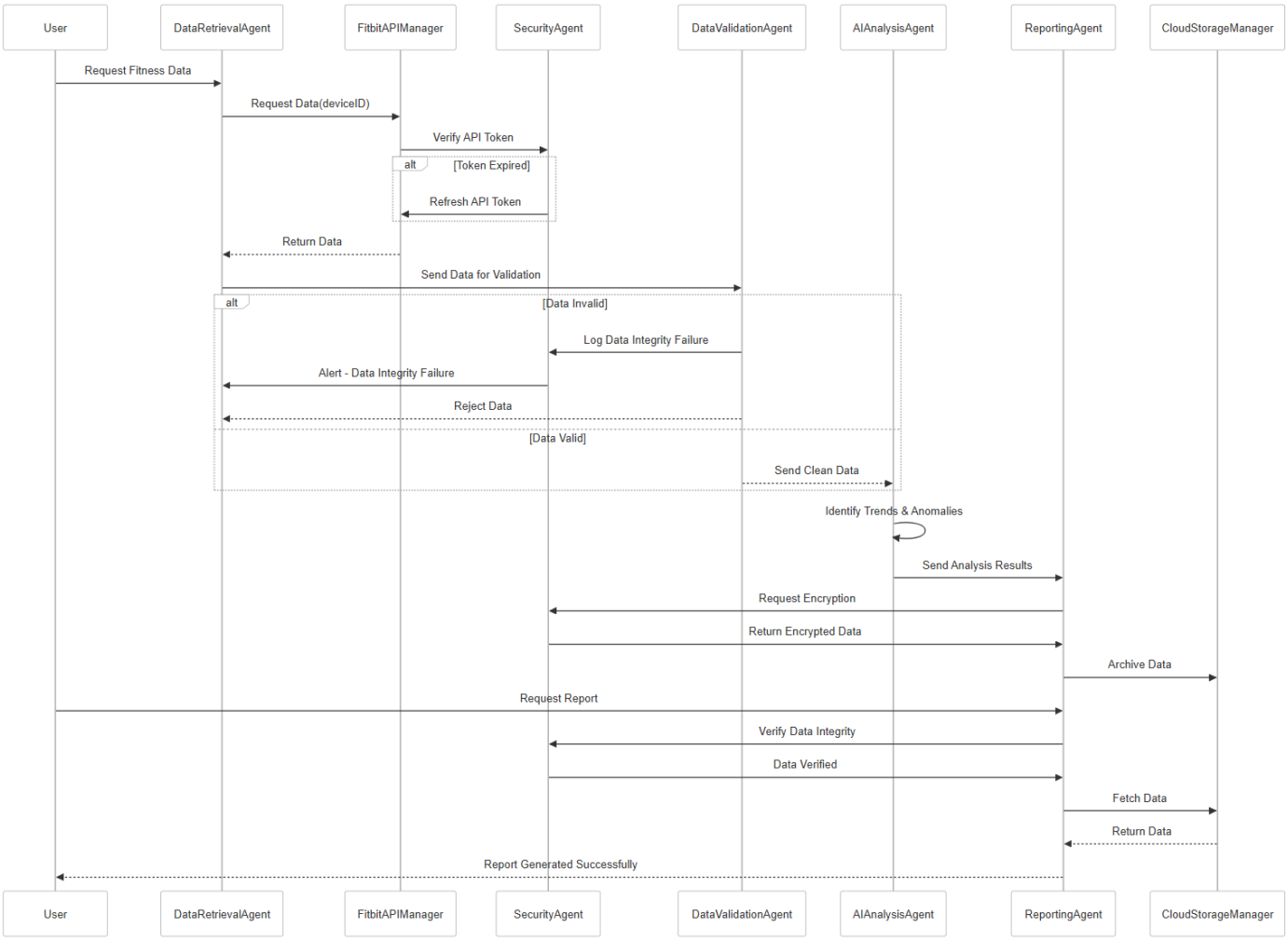

Figure 2: Sequence Diagram — Secure Data Flow and Forensic Traceability

6.0 Challenges & Mitigation Strategies

The system's design introduced key challenges that required strategic mitigation to ensure reliability, security, and efficiency.

6.1 Data Integrity Risks

Corrupted or incomplete Fitbit data risked skewed analysis. While the **Data Validation Agent** verifies data, reliance on automation risks false positives. To mitigate this, invalid data is logged for forensic review, ensuring traceability and correction.

6.2 API Token Expiry

Frequent Fitbit API token expiry risked data loss. The **Security Agent** mitigates this with proactive renewal, but a retry mechanism was added to prevent prolonged downtime.

6.3 Data Leakage Risks

Despite encryption by the **Security Agent**, cloud-stored data remains vulnerable to tampering. An integrity check before report generation mitigates this risk by flagging altered data.

6.4 Computational Overload

Local processing risks performance strain on edge devices. Offloading complex model updates to cloud servers minimizes this risk, ensuring efficient resource use.

7.0 Conclusion

This system effectively addresses data integrity, security, and performance risks through strategic design choices and mitigations. By integrating agent-based computing and forensic principles, it ensures robust, scalable, and secure fitness data analysis.

8.0 References

George, G. and Thampi, S.M., 2019. Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things. *Pervasive and Mobile Computing*, *59*, p.101068.

Karati, A. and Das, S.K., 2022, December. Federated secure data sharing by edge-cloud computing model. In *GLOBECOM 2022-2022 IEEE Global Communications Conference* (pp. 1362-1367). IEEE.

Kasparian, A.M. and Badawy, S.M., 2022. *Utility of Fitbit devices among children and adolescents with chronic health conditions: a scoping review. mHealth 8: 26* [online]

Migliaccio, G.M., Padulo, J. and Russo, L., 2024. The impact of wearable technologies on marginal gains in sports performance: An integrative overview on advances in sports, exercise, and health. *Applied Sciences*, *14*(15), p.6649.

Ravinder, M., Kulkarni, V., Shah, P.R., Shah, K. and Rao, A., 2024, June. Optimization of energy management and anomaly detection in smart grid analytics using deep learning. In *2024 International Conference on Integrated Circuits, Communication, and Computing Systems (ICIC3S)* (Vol. 1, pp. 1-6). IEEE.

Satyanarayanan, M., 2017. The emergence of edge computing. *Computer*, *50*(1), pp.30-39.

Schwaiger, A. and Stahmer, B., 2005, August. Probabilistic holons for efficient agent-based data mining and simulation. In *International Conference on Industrial Applications of Holonic and Multi-Agent Systems* (pp. 50-63). Berlin, Heidelberg: Springer Berlin Heidelberg.

Tomasino, A., 2025. Knowledge-Based Coordination in cyber-physical systems via distributed ledger technologies.

Ullah, F., Mohammed, I. and Babar, M.A., 2022. A framework for energy-aware evaluation of distributed data processing platforms in edge-cloud environment. *arXiv preprint arXiv:2201.01972*.

Xu, X., Tang, B., Jiang, G., Liu, X., Xue, Y. and Yuan, Y., 2019, July. Privacy-aware data offloading for mobile devices in edge computing. In *2019 International conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)* (pp. 170-175). IEEE.