future internet

MDPI

Article

A Novel Semantic IoT Middleware for Secure Data Management: Blockchain and AI-Driven Context Awareness

Mahmoud Elkhodr [1,*], Samiya Khan [2] and Ergun Gide [1]

[1] School of Engineering and Technology, Central Queensland University, Sydney, NSW 2000, Australia; e.gide1@cqu.edu.au

[2] School of Computing and Mathematical Sciences, University of Greenwich, London SE10 9LS, UK; samiya.khan@greenwich.ac.uk

* Correspondence: m.elkhodr@cqu.edu.au

Abstract: In the modern digital landscape of the Internet of Things (IoT), data interoperability and heterogeneity present critical challenges, particularly with the increasing complexity of IoT systems and networks. Addressing these challenges, while ensuring data security and user trust, is pivotal. This paper proposes a novel Semantic IoT Middleware (SIM) for healthcare. The architecture of this middleware comprises the following main processes: data generation, semantic annotation, security encryption, and semantic operations. The data generation module facilitates seamless data and event sourcing, while the Semantic Annotation Component assigns structured vocabulary for uniformity. SIM adopts blockchain technology to provide enhanced data security, and its layered approach ensures robust interoperability and intuitive user-centric operations for IoT systems. The security encryption module offers data protection, and the semantic operations module underpins data processing and integration. A distinctive feature of this middleware is its proficiency in service integration, leveraging semantic descriptions augmented by user feedback. Additionally, SIM integrates artificial intelligence (AI) feedback mechanisms to continuously refine and optimise the middleware's operational efficiency.

Keywords: Internet of Things (IoT); blockchain; artificial intelligence (AI); semantic annotation; data security; user-centric operations; healthcare

check for updates

Citation: Elkhodr, M.; Khan, S.; Gide, E. A Novel Semantic IoT Middleware for Secure Data Management: Blockchain and AI-Driven Context Awareness. *Future Internet* **2024**, *16*, 22. https://doi.org/10.3390/fi16010022

Academic Editor: Antonio Esposito

Received: 20 November 2023
Revised: 2 January 2024
Accepted: 5 January 2024
Published: 7 January 2024

1. Introduction

The advancement in technologies such as artificial intelligence, machine learning, and 5G has catalysed the evolution and adoption of the Internet of Things (IoT). Improved connectivity and reduced component costs have led to the large-scale adoption of IoT to support diverse applications in varied sectors ranging from healthcare, smart cars, agriculture, smart homes, and many others [1]. The backbone of the IoT infrastructure is a network of interconnected devices, which enable real-time data collection and analysis. By 2030, the number of IoT devices are forecast to reach 30 billion [2] worldwide, while the IoT market worth is expected to increase from USD 182 billion (2020) to USD 621 billion by 2030 [3].

As of 2023, the global spending on IoT has already surpassed its expected forecast [4]. This spending has linearly increased over the years despite the COVID-19 pandemic because of the exemplary role IoT plays in the development of systems that enable remote monitoring and control. The impact of IoT on healthcare extends beyond the pandemic. The healthcare IoT market is projected to exhibit an annual growth rate (CAGR) of 12.32% from 2023 to 2028 [5].

However, there are several challenges associated with the management and handling of medical data. A typical medical record contains a multitude of different types of information, such as medical history, treatment plans, lab test results, and demographics. Thus, the fundamental challenge is to store, manage and analyse these data. Another significant challenge includes maintaining data quality as the data are typically collected from multiple sources, which include information management systems and healthcare providers. The inconsistencies that may arise because of the integration of data from different sources result in unreliable analysis and decisionmaking.

Other challenges associated with medical data include privacy and security concerns. Regulations and laws securing patient privacy, such as the Health Insurance Portability and Accountability Act (HIPAA) [6] in the United States and General Data Protection Regulation (GDPR) [7] in the United Kingdom and European Union, impose strict requirements for storing, managing, handling, and sharing medical information. Any research including non-commercial and commercial projects involving patient data must adhere to these regulations.

To address some of the challenges in the IoT domain, our previous work introduced the Internet of Things Management Platform (IoT-MP) [8,9]. The IoT-MP was developed to tackle the complexities of managing an expansive IoT infrastructure, especially considering the constrained resources of typical IoT devices. This platform supports fundamental management functions necessary for optimal operation, monitoring, and communication.

Building on the foundational works of the IoT-MP, subsequent research [10] has introduced a framework for securely authenticating patients and facilitating the secure sharing of biomedical data through cloud computing technologies. Further advancements were achieved with [11], which seamlessly incorporated blockchain into the aforementioned framework. This evolution in our research culminated in the introduction of BioChainReward (BCR), a blockchain-based framework for secure and privacy-preserving biomedical data sharing [12]. BCR stands out by implementing an AI-enabled privacy-preservation sublayer, adapting its privacy measures depending on the data request's nature and purpose.

Despite the progress made with platforms like IoT-MP and BCR, there are still formidable challenges to be addressed. A paramount issue is the heterogeneity of medical data. Data from various sources like hospitals, clinics, and labs come in different formats, each employing unique coding systems and terminologies [13]. Such diversity complicates the task of data integration and analysis. For instance, patient outcome data sourced from various healthcare institutions might differ structurally, impeding meaningful comparisons. Another considerable obstacle lies in the realm of semantic annotations. Understanding medical measurements often demands domain-specific knowledge. For instance, a single data point like a heart rate exceeding 150 beats per minute can signify different health states depending on whether the person was at rest or running. Therefore, the data context is critical, and any misinterpretations can drastically skew diagnoses and treatment decisions.

Given the gaps left by solutions such as the IoT-MP and the challenges still at play, middleware remains a promising answer to these challenges. Serving as a buffer layer between IoT devices and data-utilising applications, middleware offers compatibility, interoperability, standardisation, and abstraction, fostering seamless data integration and inter-system communication. When combined with technologies like AI and blockchain, the potential will be further amplified. On one hand, AI's prowess lies in data analysis and insight generation, particularly from heterogeneous sources. On the other hand, blockchain provides a robust framework for secure data management and sharing in IoT systems. Thus, their amalgamation into a semantic middleware may reduce some of the challenges encountered.

To this end, this paper presents the Semantic IoT Middleware (SIM). This novel middleware is designed to address the challenges identified previously. SIM employs blockchain technology with artificial intelligence (AI) to enhance data security, providing an encompassing user-centric solution tailored for diverse IoT systems, especially in the healthcare area. SIM provisions semantic annotations and user feedback to ensure data security and integrity. Additionally, it facilitates service integration and improves operational efficiency. Thus, the primary contributions of this work are as follows:

1. A comprehensive proposal of the Semantic IoT Middleware (SIM), designed for broad IoT applications with a focus on healthcare, addressing challenges in data interoperability, heterogeneity, and system complexity.
2. The integration of blockchain technology within SIM for enhanced data security and integrity, coupled with an innovative AI Feedback and Analysis Module for continuous system improvement based on user feedback and data analysis.
3. Introduction of an innovative AI Feedback and Analysis Module, harnessing the power of artificial intelligence to continually refine and enhance system operations based on user feedback and real-time data analysis.
4. The introduction of detailed implementation algorithms as a blueprint for practical application and a proof of concept demonstrating the feasibility and adaptability of SIM in various scenarios.
5. An expanded discussion on user-centric operations in SIM, showcasing its application in diverse contexts beyond healthcare, emphasising its intuitive and accessible user interface.
6. A comparative assessment of the proposed middleware against existing methodologies, demonstrating its capabilities in terms of security, interoperability, and user-centric design.

The remainder of the paper is organised as follows: Section 2 delves into the background of IoT middleware and its application in healthcare. Section 3 presents the proposed middleware, detailing its architecture and modules. Section 4 presents a case study and scenario. The proof of concept is provided in Section 5. Section 6 focuses on the evaluation of the proposed system. Section 7 discusses the challenges encountered during this research. Section 8 offers the concluding remarks and summarises the contributions of this work.

2. Background and Related Work

The evolution of IoT has given birth to a range of smart devices. However, to develop a sustainable ecosystem, all IoT devices need to work together seamlessly regardless of their technology or manufacturer. As the world transitions towards a future that is expected to use IoT devices in greater capacity, it is crucial to find a solution to this problem of interoperability. On the other hand, the semantic web involves annotating data with semantic information to preserve the context and meaning and allow them to be machine-understandable [14].

Using the same concept, semantic annotations when used in IoT allow data from different devices to be understandable by different machines and frameworks, enabling efficient context-aware data exchange and integrated analysis. Thus, the concept of the semantic web can be borrowed to address the interoperability issues in IoT. In other words, a unified framework for data communication and representation can greatly impact the usefulness and efficiency of IoT systems. Nonetheless, the integration of semantic annotation suffers from several challenges, such as complexity, security, and performance, and, as IoT evolves, the evolution of an integrative use of these technologies is also expected for the development of sustainable IoT ecosystems.

IoT middleware is a software layer that enables communication among the diverse components of IoT ecosystems, which include network hardware, network stacks, operating systems, and applications [15]. Interoperability, self-adaptability, reliability, scalability, lightweight nature, and real-time capabilities are some of the key characteristics of IoT middleware [16]. However, the development of IoT middleware to maintain machine-to-machine communications and demonstrate the above-mentioned characteristics is a daunting task [17].

Various architectures for IoT middleware have been proposed over the years. Existing work [18] in this area classified these architectures into several categories, including application-specific, agent-based, VM-based, database-oriented, tuple spaces, service-oriented, and message-oriented architectures. Architectures of IoT middleware have evolved over the years to support and cater to the changing demands of IoT environments.

Table 1 provides an analysis of the benefits and shortcomings of the aforementioned architectures. The best-fit architecture for an IoT application is identified based on the specific requirements of the application, such as scalability, modularity, nature of devices, and need for real-time processing. With the ever-growing complexity and challenges associated with IoT systems, hybrid architectures [19] may also be employed to address specific challenges and cater to the diverse demands of the IoT system.

Table 1. Comparative analysis of advanced features in IoT middleware architectures.

Architecture	Use Cases	Pros	Cons
Application-specific	Tailored for particular use cases or industries [20,21]	High optimization, reduced overhead, fine-tuned performance	Lack of flexibility
Agent-based	Uses autonomous agents for decisionmaking [22–24]	Scalability, decentralised decisionmaking, fault tolerance	High complexity in managing agents
VM (Virtual Machine)-based	Abstracts hardware layer using VMs [25,26]	Hardware abstraction, ease of application deployment, scalability	Overheads and performance issues
Database-oriented	Centralises IoT data management [27–29]	Structured data storage, support for complex queries	Overheads, scalability issues, single points of failure
Tuple spaces	Distributed shared memory concept [30–32]	Flexibility, synchronous/asynchronous communication	High complexity and data redundancy
Service-oriented	Modular services for specific functions [33]	High modularity, service reuse, adaptability	Overheads, latency issues, complexity
Message-oriented	Message-based device communication [34,35]	Asynchronous communication, scalability	Overheads, message losses, sequencing issues
Semantic IoT Middleware (SIM)	Comprehensive IoT ecosystems, healthcare, smart homes, industrial automation	Semantic data processing, AI-driven feedback, blockchain security	Complexity in semantic processing, initial setup overheads

Several commercial-grade IoT middleware solutions are also available. Some of the popular solutions include AWS IoT Core [36], FIWARE-IoT-Agent [37], FIWARE-ORION [38], Linksmart [39], Microsoft Azure [40], OpenIoT [41], and Symbius IoT [42]. Table 2 provides a technical comparison of these commercial-grade solutions, which demonstrates an overarching trend in areas of future innovation. These solutions can benefit from the integration of improved security features, AI/ML, and edge computing capabilities [43–46]. In academia, research into IoT middleware continues apace as commercial-grade products, despite their merits, still possess limitations and scope for innovation. Moreover, the explosive growth regarding IoT devices and their diverse applications poses a plethora of challenges to the evolution of these products.

Table 2. Comparison of commercial-grade IoT middleware solutions.

Product	Key Features	Scope for Innovation
AWS IoT Core [43]	Device communication security, device authentication, rules engine for routing device data, and integration with other AWS services	Better edge computing capabilities, enhanced support for heterogeneous devices, more robust data analytics tools built in
FIWARE-IoT-Agent [44]	Combines IoT devices with the Orion Context Broker, supports multiple IoT protocols, provides service and device provisioning	Expands the set of supported protocols, tighter integration with non-FIWARE systems, enhanced security features

Table 2. *Cont.*

Product	Key Features	Scope for Innovation
FIWARE-ORION [44]	Publish/Subscribe Context Broker, allows for real-time context data management, also supports NGSI (Next Generation Service Interfaces)	More robust support for diverse data models, improved scalability, and enhanced data transformation capabilities
Linksmart [45]	Offers open-source tools for IoT, focus on semantic interoperability, provides features like service catalogue and distributed marketplace for data and services and user-friendly UI/UX enhancements, support for newer IoT protocols, built-in analytics tools	Scope for innovation and expansion given its open source nature.
Microsoft Azure (IoT Hub) [43]	Supports bi-directional communication between IoT applications and the devices it manage, supports a wide array of SDKs, built-in device authentication	Enhanced AI and ML capabilities, better integration with non-Azure systems, more comprehensive device management tools
OpenIoT [46]	Open-source, focuses on semantic interoperability for cloud-based IoT, offers utility-based sensing via virtual sensors	More user-friendly deployment options, enhanced real-time analytics, better security features.
Symbius IoT [42]	Offers a unified middleware solution, supports compatibility with major sensor manufacturers, streamlined data accessibility, reduced deployment complexities	Expanding compatibility, enhancing security, and offering richer data insights
IBM Watson IoT Platform [47]	Includes advanced AI capabilities for data analytics, anomaly detection, and predictive maintenance. Demonstrates high scalability, real-time data processing, easy integration with other products, and provides tools for data management.	AI capabilities can be enhanced to support automated decisionmaking. In addition to this, it can include enhanced support for blockchain and edge computing, with the addition of tools to facilitate development of custom solutions.
Google Cloud IoT Core [48]	Fully managed service that is scalable and allows seamless data integration. Moreover, it also provides efficient data management and robust security features.	Discontinued in August 2023 due to non-technical reasons.

As the IoT landscape diversifies with the introduction of new devices and protocols, it is imperative to evolve existing platforms to ensure seamless interoperability and integration. In this context, [49] presents an innovative multilayer IoT middleware rooted in the concepts of knowledge graph, effectively addressing the challenge of connecting a heterogeneous array of IoT devices employing various communication protocols. Another work, [50], was proposed in this area, with a prime focus on resolving privacy and security issues, specifically concentrated on the message queuing telemetry transport (MQTT) protocol.

Some of the recent works that have amalgamated the concept of semantic annotations in IoT middleware include GMSCA [51], S2NetM [52], and SEDIA [53]. GMSCA is a generic IoT middleware for smart city applications that targets to address challenges regarding heterogeneity, service management, and security. However, the paper acknowledges that security is still a challenge that needs to be addressed in future work. S2NetM introduces the concept of Semantic Social Network of Things Middleware, and the purpose of this study is to enhance semantic interoperability in Social Internet of Things (SIoT) systems by comprehending and using social relationships. The study acknowledges several challenges, such as security and standardisation in SIoT environments.

On the other hand, SEDIA is a platform for integrating IoT data with semantic enrichment. This work is focused on smart city applications and aims to address specific challenges such as integrating diverse data sources and incorporating geographical data.

A proof of concept is provided using air quality monitoring as a case study. This study is a significant step towards developing a generic and sustainable platform for IoT data management. Although no specific challenges have been identified by the study, the proposed platform uses MQTT, which has associated security and privacy challenges [54]. These challenges are particularly grave for healthcare applications, where identity and data protection are the highest priorities. Therefore, this paper proposes the use of a blockchain-based decentralised identity system that will facilitate the authentication of users and administrators.

Blockchain's potential for securing IoT devices and their usage is widely recognised in both academia and industry. Therefore, it is viewed as a technology that is all set to revolutionise how IoT devices are administered, operated, and, most importantly, secured. Recent research [55] introduced BPIIoT, a decentralised peer-to-peer Industrial Internet of Things platform underpinned by blockchain. This platform facilitates direct communication between peers in a trustless network without necessitating a central intermediary. Another significant contribution [56] integrated permissioned blockchain mechanisms into a privacy-conscious IoT middleware. This middleware functions without any central authority and does not intrinsically trust the IoT platform.

Despite significant advancements in both IoT and blockchain and the growing research on their integration into IoT middleware, a clear gap persists. While our previous works, including IoT-MP [8,9], the Biometric Authentication Framework [10], and BCR [12], made progress in certain areas, middleware solutions on the whole still often lack cohesive semantic translation or annotation capabilities. These solutions, although pioneering, underscore the broader challenge of fully integrating security, transparency, and other essential IoT features. This highlights the urgent need for a comprehensive solution that combines semantic annotation, heightened security, transparency, and core IoT functionalities. Such a solution would address the current system limitations while capitalising on their inherent strengths. In the following section, the architecture of the Semantic IoT Middleware (SIM), designed to fill this critical gap and meet the highlighted needs, will be presented.

3. The Proposed Semantic Internet of Things Middleware

The proposed Semantic IoT Middleware (SIM) seamlessly integrates semantic annotation capabilities, blockchain technology, and AI-powered feedback mechanisms. The middleware harnesses the security and decentralised advantages of blockchain to manage and store semantic annotations, ensuring data integrity and protection from unauthorised modifications. Additionally, the embedded AI Feedback and Analysis Module employs advanced artificial intelligence techniques, focusing on refining the quality and usability of semantic annotations through user feedback and system events. As a result, end users, applications, and third parties, such as health monitoring apps, emergency response teams, and healthcare data analytics providers, benefit from secure, transparent, and meaningful access to users' IoT devices. The architecture of the middleware is depicted in Figure 1 and detailed below:

1. **IoT Data and Event Generation Module**: Constitutes the data and event sources in the IoT system, which may be varied, i.e., diverse types, capabilities, protocols, formats, locations, and domains.
2. **Semantic Annotation Component**: Processes and attributes common vocabulary and structure to data and events sourced from the IoT module. It leverages a semantic annotation model for defining concepts, properties, and relationships pertinent to the IoT domain, with an annotation tool that either automatically or semi-automatically assigns semantic annotations.
3. **Data Security and Encryption Module**: This component, placed after the Semantic Annotation Component, ensures the secure transition of data to the blockchain network. It handles encryption and decryption of data and events, authentication and authorisation of users and applications, and digital signing and verification of semantic operations. It interacts with the Blockchain Component to secure the storage

and retrieval of semantic annotations. It also optimises lightweight and efficient security protocols and algorithms compatible with the IoT environment.

4. **Blockchain Component**: Stores and manages semantic annotations in a distributed, decentralised manner. It incorporates a blockchain network comprising multiple nodes that maintain a shared ledger of transactions, with each transaction containing a verified and validated semantic annotation. It ensures the security, integrity, and trustworthiness of the semantic annotations, mitigating unauthorised access and modification.
5. **Semantic Query Module**: Enables discovery and access of blockchain-stored semantic annotations, utilising a semantic query language for expressing user and application information needs based on concepts, properties, and relations defined in the semantic annotation model. It uses a semantic query engine to process and execute semantic queries over the blockchain network and return relevant results.
6. **Semantic Analysis and Inference Engine**: Analyses and infers from semantic annotations stored on the blockchain network, utilising logical rules and algorithms to derive new knowledge and insights from the semantic annotations. It employs AI and deep learning techniques to enhance reasoning capabilities and tackle complex and uncertain scenarios.
7. **Service Integration and Composition Module**: Facilitates integration and composition of IoT services and applications based on the semantic annotations in the blockchain network. It uses a semantic service model to define functionalities, inputs, outputs, and parameters of various IoT services and applications. It also uses a semantic service discovery and composition tool to automatically or semi-automatically find and combine suitable IoT services and applications according to their semantic descriptions and user requirements.
8. **Semantic Visualisation Component**: Provides graphical and interactive representations of semantic annotations, queries, reasoning, and services.
9. **AI Feedback and Analysis Module**: This module acts as a central entity in the middleware that harnesses the power of artificial intelligence and machine learning techniques to enhance the system's capabilities. It primarily focuses on gathering and analysing user feedback and system events, ensuring that all insights are accounted for to refine the quality and usability of semantic annotations, queries, reasoning, and services.

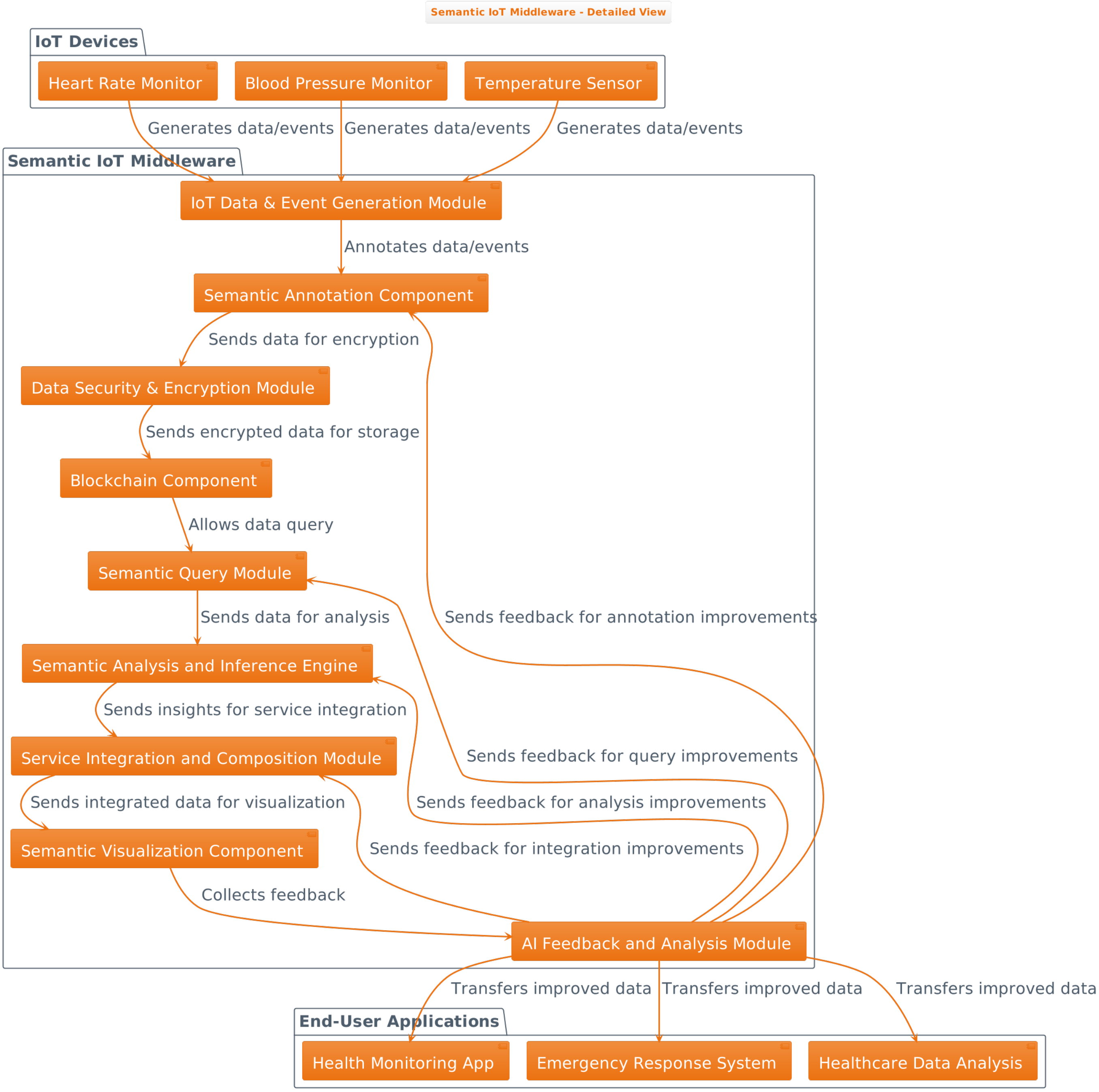
Semantic IoT Middleware - Detailed View
IoT Devices
Heart Rate Monitor
Blood Pressure Monitor
Temperature Sensor
Generates data/events
Generates data/events
Generates data/events
Semantic IoT Middleware
IoT Data & Event Generation Module
Annotates data/events
Semantic Annotation Component
Sends data for encryption
Data Security & Encryption Module
Sends encrypted data for storage
Blockchain Component
Allows data query
Semantic Query Module
Sends data for analysis
Sends feedback for annotation improvements
Semantic Analysis and Inference Engine
Sends insights for service integration
Sends feedback for query improvements
Service Integration and Composition Module
Sends integrated data for visualization
Sends feedback for analysis improvements
Semantic Visualization Component
Sends feedback for integration improvements
Collects feedback
AI Feedback and Analysis Module
Transfers improved data
Transfers improved data
Transfers improved data
End-User Applications
Health Monitoring App
Emergency Response System
Healthcare Data Analysis

Figure 1. SIM architecture showing all its modules and components.

Figure 2 presents additional insights into the Service Integration and Composition process within SIM. Using an example, it presents a step-by-step workflow of how user requirements lead to the discovery, assessment, selection, and integration of services.

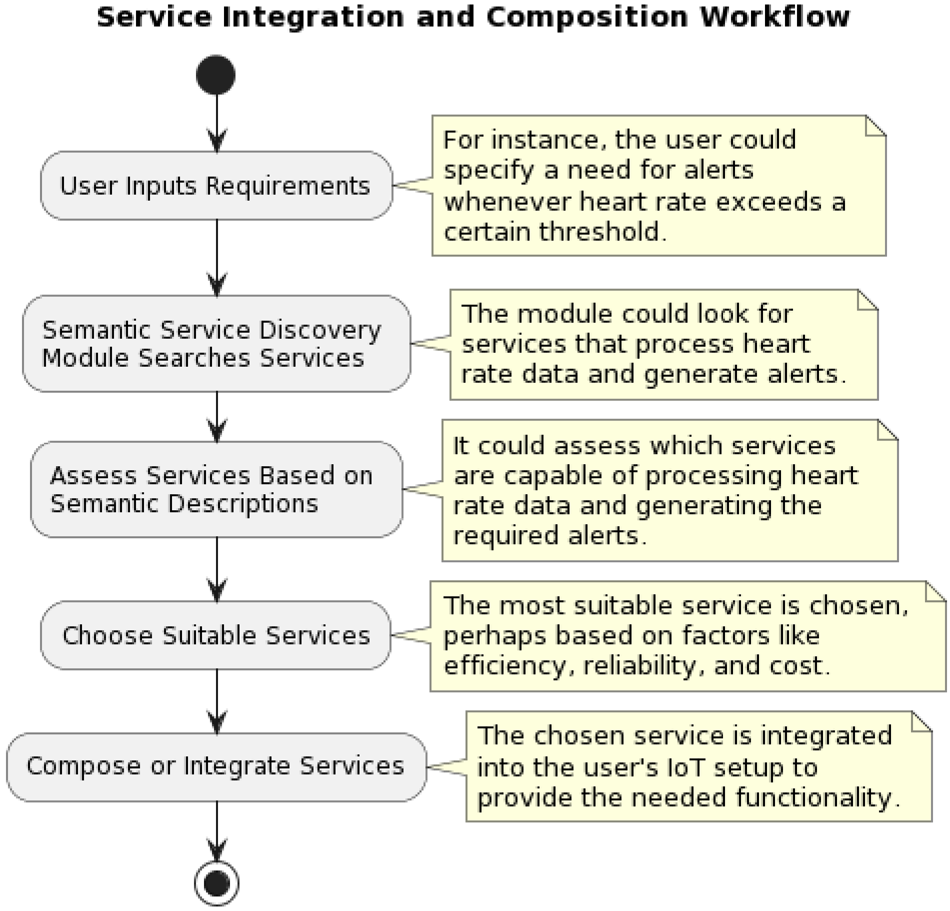
Service Integration and Composition Workflow
User Inputs Requirements
For instance, the user could specify a need for alerts whenever heart rate exceeds a certain threshold.
Semantic Service Discovery Module Searches Services
The module could look for services that process heart rate data and generate alerts.
Assess Services Based on Semantic Descriptions
It could assess which services are capable of processing heart rate data and generating the required alerts.
Choose Suitable Services
The most suitable service is chosen, perhaps based on factors like efficiency, reliability, and cost.
Compose or Integrate Services
The chosen service is integrated into the user's IoT setup to provide the needed functionality.

Figure 2. Service Integration and Composition workflow of SIM.

3.1. Design Decisions: Incorporating AI into the Middleware

The introduction of AI into the middleware represents a significant advancement in the domain of IoT and Health Informatics, and our approach required a great deal of thought and deliberation. We considered three options:

- Option 1: Introducing a dedicated AI module within the middleware.
- Option 2: Embedding AI functionalities within each component of the middleware.
- Option 3: Implementing a standalone centralised AI entity outside the middleware.

Each of these options had its unique merits and drawbacks. Option 1, introducing an AI module within the middleware, offered a fine balance between enhancing the system with AI capabilities and preserving the decentralised nature of the middleware. This approach ensured centralised control over the AI functionality while maintaining the autonomy of other middleware modules. It aligned with the principle of separation of concerns, allowing each component to concentrate on its core functionalities while the dedicated AI module focuses on enhancing system-wide performance and learning. It further streamlined the management, up-gradation, and scalability of the AI capabilities. However, the integration of a new module required significant architectural modifications.

Option 2, integrating AI within each component, promised a high level of tailored intelligence and autonomy for each component. This could result in more context-aware and adaptive functionality. Nevertheless, the downside was the potential for redundant AI development across components and the necessity for stringent oversight to maintain consistency and reliability of AI decisionmaking.

Option 3, a centralised AI entity, provided a singular point of control and consistency for AI functions. However, this approach contradicted the inherently decentralised nature of IoT middleware and could limit the autonomy of individual components and devices.

Upon weighing the pros and cons, we concluded that Option 1—introducing a dedicated AI module within the middleware—was the most suitable approach for our requirements. This decision hinged upon the need for centralised AI capability while still respecting the decentralised architecture of the middleware. The new AI module allows for continuous learning and improvement, thereby enhancing the overall middleware performance and usability.

3.2. The AI Feedback and Analysis Module: Role in the Middleware

The AI Feedback and Analysis Module is a crucial entity embedded at the core of SIM. It employs advanced machine learning techniques, including deep learning, natural language processing, clustering and classification, and reinforcement learning to improve the middleware's functional capabilities and efficiency. A schematic representation of this module is presented in Figure 3. The module primarily focuses on

1. Enhanced Insights Analysis for Service Integration: The AI module derives complex insights from data by utilising deep learning algorithms, which enriches the Service Integration and Composition Module's ability to manage services effectively.

2. Semantic Annotation Suggestions: Utilising natural language processing techniques, the module discerns the context and semantics of diverse IoT devices and data, thereby suggesting more accurate and relevant semantic annotations and enhancing the data processing efficiency.

3. Event and Feedback Analysis: Using clustering and classification techniques, the AI module comprehensively analyses system events and users' feedback, leading to the identification of patterns, trends, and potential areas for improvement.

4. Adaptive Learning and Continuous Improvement: Through reinforcement learning, the AI module perpetually learns and adapts from its interactions and experiences. It consistently monitors and assesses system operations, user feedback, and interactions, detecting potential areas for improvement and suggesting proactive modifications to other middleware components. This keeps the middleware adaptive, optimised, and user-centric.

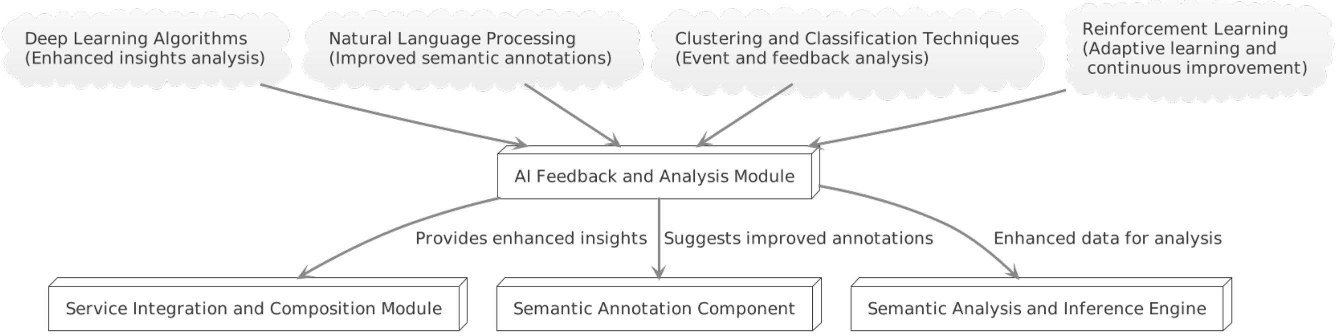
Deep Learning Algorithms
(Enhanced insights analysis)
Natural Language Processing
(Improved semantic annotations)
Clustering and Classification Techniques
(Event and feedback analysis)
Reinforcement Learning
(Adaptive learning and
continuous improvement)
AI Feedback and Analysis Module
Provides enhanced insights
Suggests improved annotations
Enhanced data for analysis
Service Integration and Composition Module
Semantic Annotation Component
Semantic Analysis and Inference Engine

Figure 3. The AI Feedback and Analysis Module. This image shows all the different machine learning techniques this module uses.

3.3. Ensuring Robust Security in the Middleware

Healthcare data, by their highly personal and sensitive nature, necessitate top-tier security measures. The Semantic IoT Middleware (SIM), as shown in Figure 1, integrates a layered approach to safeguarding data integrity and privacy, especially when transiting through different components. Figure 4 further details the security capabilities of SIM, mainly the following:

- Data Annotation: The process begins with the acquisition of raw health data and events from IoT devices. These raw data may include information such as the vital signs of a patient or specific medical events. Initially, interfacing with the Semantic Annotation Module occurs, where the data are labelled with relevant annotations, adding semantic context to raw readings. This step not only aids in data understandability but also prepares them for subsequent security measures.

- Encryption and Authentication: Once annotated, the health data enter the Data Security and Encryption Module. This pivotal component encompasses multiple operations to ensure data confidentiality and integrity:
  - Encryption: Using the AES-256 encryption standard.
  - Device Authentication: Through Public Key Infrastructure (PKI), the module authenticates the source IoT device. This ensures that the data origin is legitimate and trustworthy.
  - Authorisation: Role-Based Access Control (RBAC) is employed to authorise the data transfer, ensuring that only entities with the requisite permissions can access the data.
  - Digital Signing: The module employs the Elliptic Curve Digital Signature Algorithm (ECDSA) to digitally sign the data, ensuring the validity and integrity of the transmitted information.
  - Blockchain Integration: Once the health data are secured, they are passed on to the Blockchain Component. This step amalgamates the robustness of blockchain technology with the previously applied security protocols, granting the data an added layer of protection against tampering or unauthorised access.
  - Data Processing and Feedback: From the blockchain, the data progress to the Semantic Processing Component, where operations like query, analysis, and integration occur. The processed data are subsequently directed to the AI Feedback and Analysis Module. This AI-driven component harnesses the data to generate actionable insights or composed services, capitalising on rich, secured, and semantically rich information.

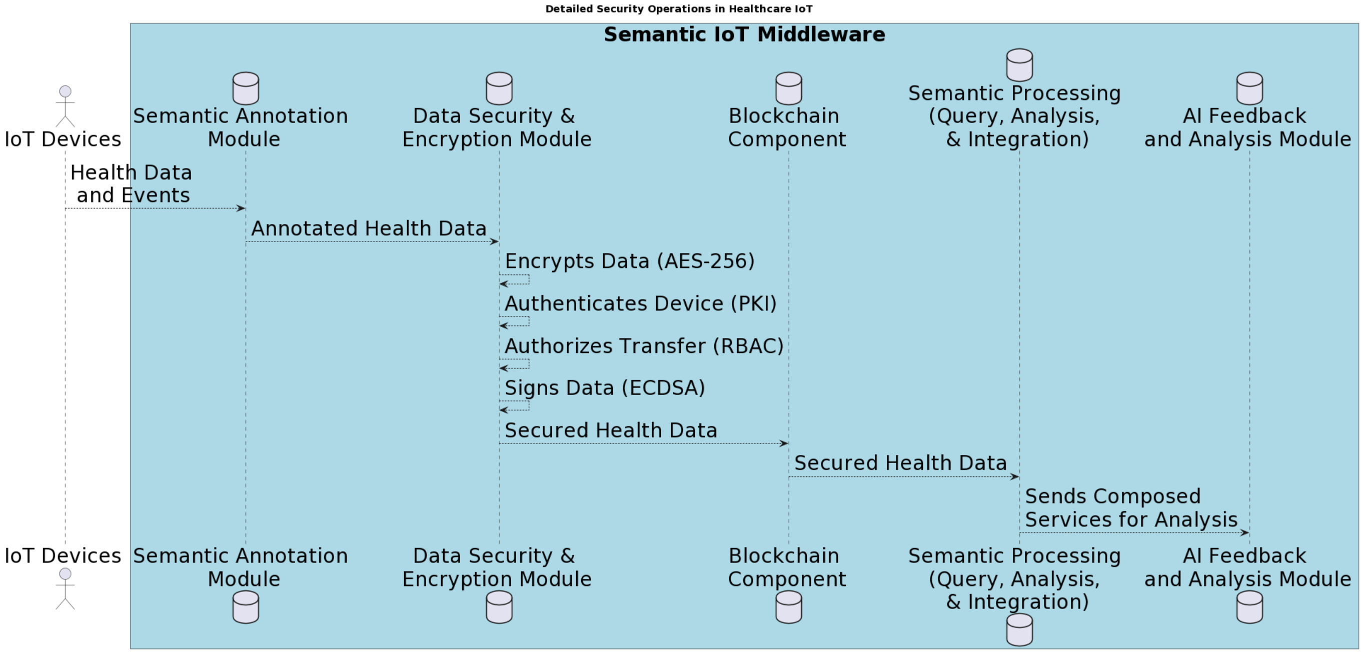
Detailed Security Operations in Healthcare IoT
Semantic IoT Middleware
IoT Devices
Semantic Annotation Module
Data Security & Encryption Module
Blockchain Component
Semantic Processing (Query, Analysis, & Integration)
AI Feedback and Analysis Module
Health Data and Events
Annotated Health Data
Encrypts Data (AES-256)
Authenticates Device (PKI)
Authorizes Transfer (RBAC)
Signs Data (ECDSA)
Secured Health Data
Secured Health Data
Sends Composed Services for Analysis
IoT Devices
Semantic Annotation Module
Data Security & Encryption Module
Blockchain Component
Semantic Processing (Query, Analysis, & Integration)
AI Feedback and Analysis Module

Figure 4. SIM security module processes.

4. Use Case Study: Alice's Healthcare Monitoring

This section illustrates the operation of the Semantic IoT Middleware (SIM) through a practical scenario involving Alice, an elderly lady with a history of high blood pressure and previous cardiac events. Alice utilises an array of IoT healthcare devices, including a heart rate monitor, blood pressure monitor, and temperature sensor to monitor her health conditions continuously. These devices are crucial for tracking her health and alerting her and her healthcare providers to potential risks or emergencies. The scenario also includes Bob, the provider of a health monitoring app; Charlie, part of an emergency response team; and Dave, a healthcare data analyst.

4.1. Scenario Overview

Alice's array of IoT healthcare devices are integral to her daily health monitoring routine. They capture critical data, such as heart rate, blood pressure, and body temperature. These data are then fed into SIM's Semantic Annotation Component, which utilises a specialised model to assign relevant medical terminology to the raw data, thereby transforming them into structured, semantically annotated data. For example, heart rate readings might be categorised as "Normal", "Elevated", or "Low" based on predetermined thresholds.

Upon structuring and annotating Alice's data, the Data Security and Encryption Module encrypts the information, ensuring its secure transfer to the Blockchain Component. The data are securely stored and safeguarded against unauthorised access and modification. When Bob's health monitoring app needs to access Alice's data, it queries the Semantic Query Module. This module utilises a semantic query language to search through the blockchain-stored annotations and retrieve relevant data. For example, it could search for instances where Alice's annotated heart rate data are labelled as "Elevated".

The Semantic Analysis and Inference Engine analyses the queried data. For example, continuous instances of "Elevated" heart rate could indicate a potential cardiac risk.

Insights derived by the analysis engine are then transferred to the Service Integration and Composition Module. This module composes relevant services based on these insights. For instance, if a potential cardiac risk is detected in Alice's health data, it could trigger a service to alert Charlie's emergency response team and send a health advisory to Alice via Bob's app.

All the information, from the original data to the final insights and services, is visualised using the Semantic Visualisation Component. This allows Alice, Bob, Charlie, and Dave to visually monitor the process and outcome, aiding in understanding and decision-making.

Lastly, the AI Feedback and Analysis Module captures user feedback and preferences to improve the system. Feedback from Alice about her health monitoring experience, Bob on the app's performance, Charlie on emergency response efficiency, and Dave on data analysis is collected and used to refine the system's operations. Figure 5 shows a diagram illustrating how Alice's data are collected and processed by different modules of SIM to deliver services or trigger alerts.

To further demonstrate the practical application of SIM in this scenario, several algorithms that act as a blueprint for implementation are provided. These algorithms outline the step-by-step operational workflow of SIM, showcasing its functionality. Algorithm 1 provides a high-level pseudo-code for SIM implementation for healthcare monitoring.

Figure 6 provides a visual guide to the system's process, from data collection to continuous monitoring and improvement.

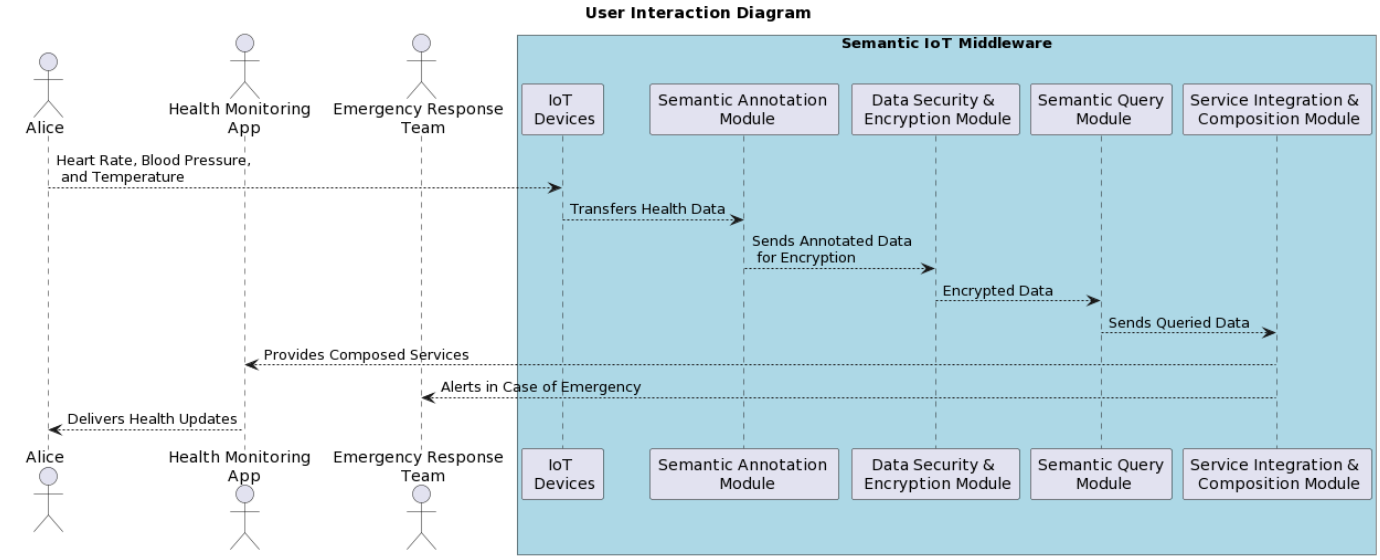
User Interaction Diagram
Semantic IoT Middleware
Alice
Health Monitoring App
Emergency Response Team
IoT Devices
Semantic Annotation Module
Data Security & Encryption Module
Semantic Query Module
Service Integration & Composition Module
Heart Rate, Blood Pressure, and Temperature
Transfers Health Data
Sends Annotated Data for Encryption
Encrypted Data
Sends Queried Data
Provides Composed Services
Alerts in Case of Emergency
Delivers Health Updates
Alice
Health Monitoring App
Emergency Response Team
IoT Devices
Semantic Annotation Module
Data Security & Encryption Module
Semantic Query Module
Service Integration & Composition Module

Figure 5. Scenario data flow diagram.

Algorithm 1 SIM Implementation for Healthcare Monitoring

```
Initialise SIM System
for each IoT device in Alice's network do
    Collect Data from Device
    if Data is collected successfully then
        Apply Semantic Annotation to Data
        Encrypt Data for Secure Transmission
        Send Data to Blockchain Component
            - Perform Blockchain Verification
            - Store Data in Blockchain
    end if
end for
On Receiving a Query (e.g., from Bob's health app):
    Extract Required Data from Blockchain
    Decrypt Data
    Apply Semantic Query Processing
    Return Processed Data
Analyse Data for Potential Risks or Alerts
if Risk Detected then
    Trigger Emergency Response Protocol
    Notify Relevant Stakeholders (e.g., Charlie's team)
end if
Collect and Process Feedback
    From User Feedback and System Events
    Analyse Feedback using AI Techniques
    Identify Patterns or Improvement Areas
    Implement Changes in the System
Update System based on Feedback Analysis
    Modify Semantic Annotations
    Adjust Alert Parameters
    Refine Data Processing Algorithms
Repeat Process for Continuous Monitoring and Improvement
```

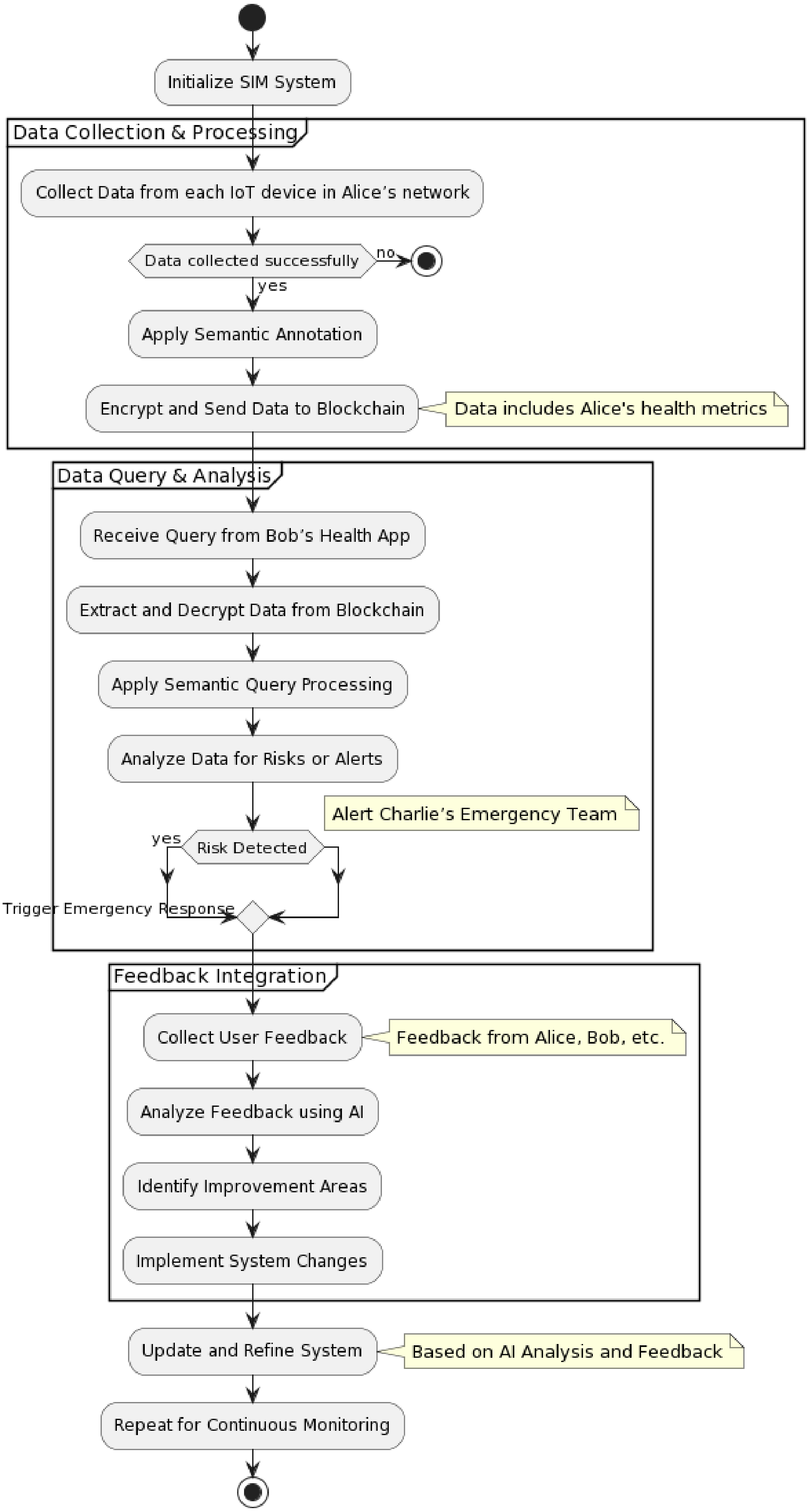
Initialize SIM System
Data Collection & Processing
Collect Data from each IoT device in Alice’s network
Data collected successfully
no
yes
Apply Semantic Annotation
Encrypt and Send Data to Blockchain
Data includes Alice's health metrics
Data Query & Analysis
Receive Query from Bob’s Health App
Extract and Decrypt Data from Blockchain
Apply Semantic Query Processing
Analyze Data for Risks or Alerts
Alert Charlie’s Emergency Team
yes
Risk Detected
Trigger Emergency Response
Feedback Integration
Collect User Feedback
Feedback from Alice, Bob, etc.
Analyze Feedback using AI
Identify Improvement Areas
Implement System Changes
Update and Refine System
Based on AI Analysis and Feedback
Repeat for Continuous Monitoring

Figure 6. Flowchart illustrating the practical application of SIM in the scenario.

Figure 7 provides a detailed view of the operations within each module of the middleware. It highlights the role of the AI Feedback and Analysis Module in refining system performance and demonstrates the sophisticated process that transforms Alice's raw data into actionable insights and services.

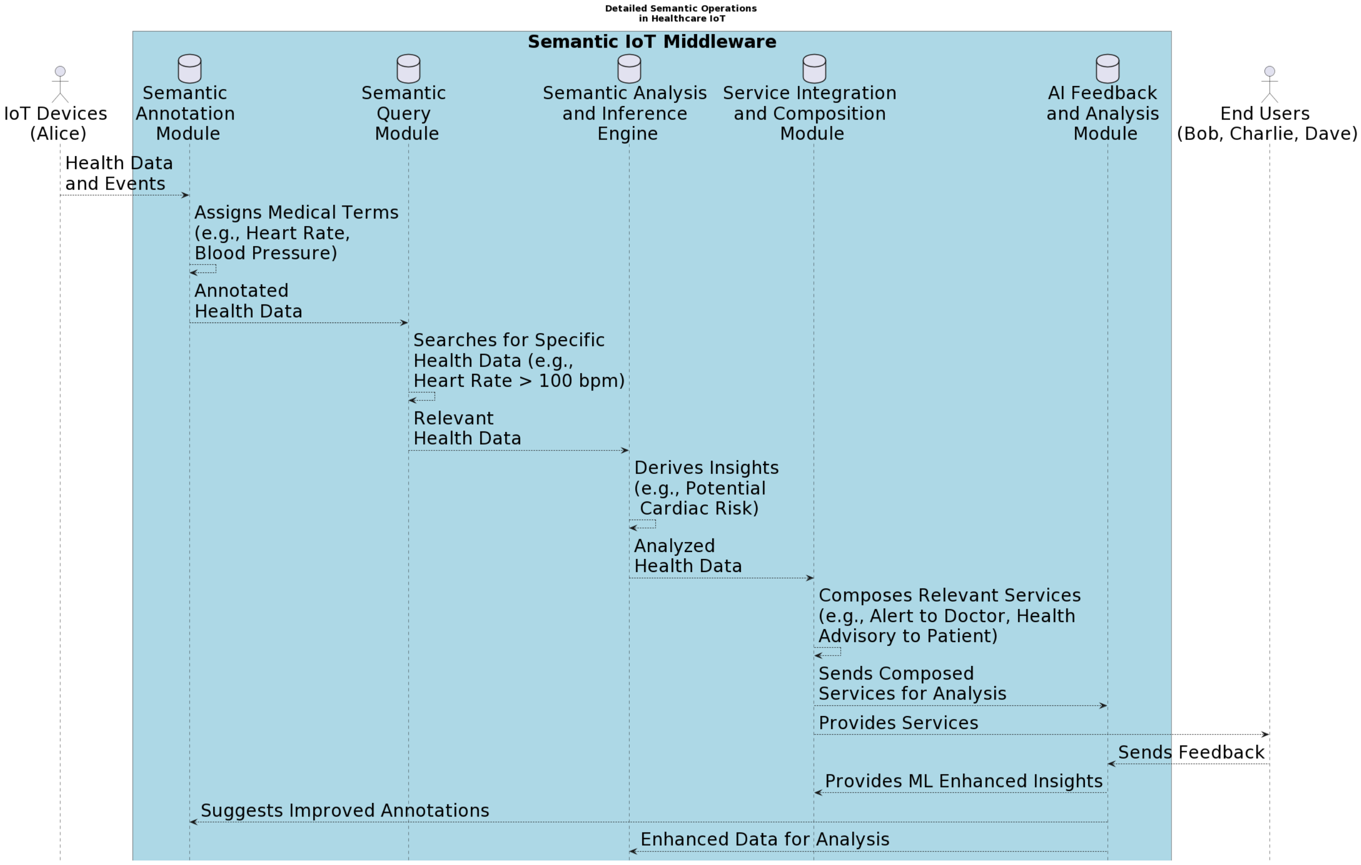
Detailed Semantic Operations
in Healthcare IoT
Semantic IoT Middleware
IoT Devices (Alice)
Semantic Annotation Module
Semantic Query Module
Semantic Analysis and Inference Engine
Service Integration and Composition Module
AI Feedback and Analysis Module
End Users (Bob, Charlie, Dave)
Health Data and Events
Assigns Medical Terms (e.g., Heart Rate, Blood Pressure)
Annotated Health Data
Searches for Specific Health Data (e.g., Heart Rate > 100 bpm)
Relevant Health Data
Derives Insights (e.g., Potential Cardiac Risk)
Analyzed Health Data
Composes Relevant Services (e.g., Alert to Doctor, Health Advisory to Patient)
Sends Composed Services for Analysis
Provides Services
Sends Feedback
Provides ML Enhanced Insights
Suggests Improved Annotations
Enhanced Data for Analysis

Figure 7. Detailed semantic annotations sequence diagram showing the ML-enhanced insights.

4.2. The Pivotal Role of Blockchain in Augmenting the Security of SIM

Blockchain serves as a key security feature of the Semantic IoT Middleware, providing an immutable, transparent, and secure mechanism for handling health data. This critical role is depicted in the sequence diagram presented in Figure 8. The data flow within this sequence diagram is as follows:

1. Data Generation and Initial Processing: The starting point involves the generation of data from IoT devices and end users. These raw data, which might be derived from sources like Alice's health monitors, first interface with the 'Data Security and Encryption Module'. This module ensures that the data undergo essential encryption and security measures before moving forward.
2. Blockchain Interaction: Upon being secured and annotated, the health data are relayed to the 'Blockchain Component'. Each data entry, conceptualised as a transaction within the blockchain, undergoes rigorous verification. Subsequently, a new block, exclusive to the specific data (e.g., Alice's health readings), is formulated.
3. Achieving Consensus: Before its incorporation into the blockchain, the new block must be unanimously validated by nodes within the network. This is achieved through the 'Consensus Mechanism'. Once consensus is ascertained, the block—now housing Alice's secured health data—joins the chain, offering permanence and tamper resistance.
4. Integration with Data Processing: After its blockchain journey, the health data find themselves in the 'Integrated Data Processing Module'. This module acts as a nexus,

facilitating the retrieval of blockchain-secured health data for diverse applications or analytics.

5. Data Access Protocols for End Users: Encompassed within the 'end users' label are distinct entities such as Dave, a healthcare data analyst, and the Emergency Services. Their interactions with the blockchain are driven by specific requirements. For instance, Dave's analysis endeavours may demand a deep dive into Alice's health data, while Emergency Services might seek swift access to Alice's records during exigent situations. Smart contracts provision these interactions, ensuring that data access occurs only after thorough authentication and following the predefined contractual conditions.

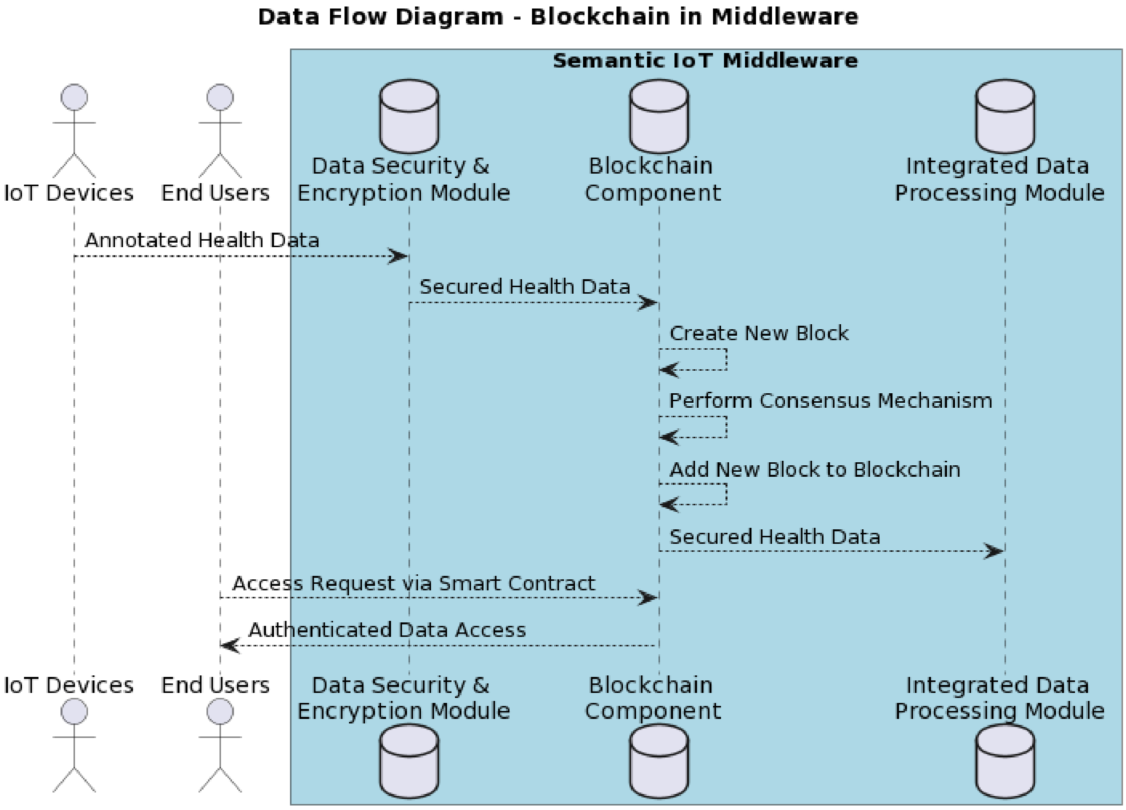
Data Flow Diagram - Blockchain in Middleware
Semantic IoT Middleware
IoT Devices
End Users
Data Security & Encryption Module
Blockchain Component
Integrated Data Processing Module
Annotated Health Data
Secured Health Data
Create New Block
Perform Consensus Mechanism
Add New Block to Blockchain
Secured Health Data
Access Request via Smart Contract
Authenticated Data Access
IoT Devices
End Users
Data Security & Encryption Module
Blockchain Component
Integrated Data Processing Module

Figure 8. Sequence diagram depicting the generic data flow. It shows how annotated health data are passed from the data security module to the blockchain module and the operations involved in this module.

After detailing the pivotal role of blockchain in enhancing the security of SIM, it becomes essential to understand the specific processes involved in this security enhancement. To this end, a supplementary algorithm that details the operational steps of the Blockchain Component within SIM is provided in Algorithm 2. Algorithm 2 provides a comprehensive view of how data from IoT devices, such as Alice's health monitors, are securely processed, verified, and stored within the blockchain framework. It also details the mechanisms for data retrieval and access by authorised entities, such as healthcare data analysts and emergency services.

Algorithm 2 shows the sequence of operations, starting from the initial encryption and semantic annotation of the data through its journey in the blockchain network, including transaction creation, data verification, block addition, and consensus achievement. Furthermore, it highlights how data integrity and security are maintained during access requests, ensuring that only authenticated and authorised requests are processed. It provides a practical guide on how these security measures can be implemented in real-world scenarios.

Algorithm 2 Blockchain Role in SIM for Enhanced Security

```
Initialise Blockchain Component
for each piece of data from IoT devices do
    Encrypt Data using Data Security Module
    Annotate Data with Semantic Information
        e.g., Annotate heart rate data as “Normal” or “Elevated”
    Send Data to Blockchain Component
        - Create New Blockchain Transaction
        - Perform Data Verification
        - Achieve Consensus on New Block
        - Add Block to Blockchain
end for
Upon Data Request (e.g., from Dave or Emergency Services)
Verify Request Authenticity
Retrieve Data from Blockchain
    Decrypt and Process Data for Specific Use
    e.g., Provide Alice’s heart rate history to her doctor
Provide Access to Authorised Entities
Continuously Monitor Blockchain for Integrity
Update Security Protocols as Needed
```

Building upon the enhanced security features of SIM, a comparative analysis with other middleware solutions in IoT and smart city applications is presented in Table 3. This analysis highlights the unique security implementations of SIM, including its blockchain integration and encryption techniques, in comparison with other recently proposed platforms in the literature.

Table 3. Comparative analysis of middleware solutions in IoT and smart city applications.

Feature	SIM	SEDIA [53]	S2NetM [52]	SeMoM [57]	GMSCA [51]
Blockchain Implementation	Integrated for data integrity and security; utilises consensus mechanism	Not Used	Not Used	Not Used	Not Used
Encryption Techniques	AES-256 for data security; ECDSA for digital signing	Various Network Layer Protocols	Access Control	Not Specified	Role-based Authorization
Access Control Mechanisms	PKI for device authentication; RBAC for authorising data transfer	Protocol-based Security	Owner Control Component	Not Specified	Data Encapsulation and Hiding
Unique Security Features	AI-driven feedback for continuous security enhancement; smart contracts for authenticated data access	Protocol Translation Gateway for Secure Data Transfer	Trustworthiness Management	Cognitive Semantic Sensor Network Ontology	Data Analytics and AI Integration

4.3. Applying the AI Feedback and Analysis Module to the Scenario

The AI Feedback and Analysis Module, depicted in Figure 9, plays a crucial role in improving the middleware's functioning based on feedback from stakeholders. It employs a variety of machine learning techniques, such as deep learning, natural language processing (NLP), clustering and classification, and reinforcement learning (RL), to analyse the feedback and historical data, identify patterns, and suggest improvements.

Consider a case where Dave, the healthcare data analyst, identifies a pattern where high heart rate alerts are being triggered during Alice's exercise routines, a known situation that does not require immediate alerts. Dave provides feedback to the system, suggesting that Alice's physical activities should be taken into account alongside her heart rate before triggering an alert.

This feedback is sent to the AI Feedback and Analysis Module. In this module, deep learning algorithms evaluate the feedback alongside historical data and infer that certain high heart rate events correlate with exercise sessions. It suggests that the middleware should contextualise heart rate readings with concurrent physical activity data, thereby helping to reduce unnecessary alerts.

Meanwhile, NLP techniques are employed to improve the semantic annotations. Based on the feedback and the identified pattern, NLP suggests refining the annotation schemes of physical activity data to better capture the context in future data collection. On the other hand, clustering and classification techniques help to recognise patterns and classify them into actionable segments. This makes the feedback more structured and insightful.

RL methods foster adaptive learning and continuous improvement. They incentivise the system to adjust its decisionmaking strategy based on the feedback and the outcome of the decisions made, leading to a system that evolves and improves its alert generation strategy.

Incorporating the insights and suggestions from the AI Feedback and Analysis Module, the Service Integration and Composition Module adjusts the alert system to consider Alice's physical activities in its decisionmaking process. The Semantic Annotation Module improves its annotation schemes as suggested, and the Semantic Analysis and Inference Engine incorporates the enhanced data for its analyses.

Lastly, the Semantic Visualisation Component reflects these updates, and Dave is informed that the alert system now considers physical activities in its analysis. Through this AI-driven iterative process, the system becomes smarter, providing more context-aware and personalised services to its users.

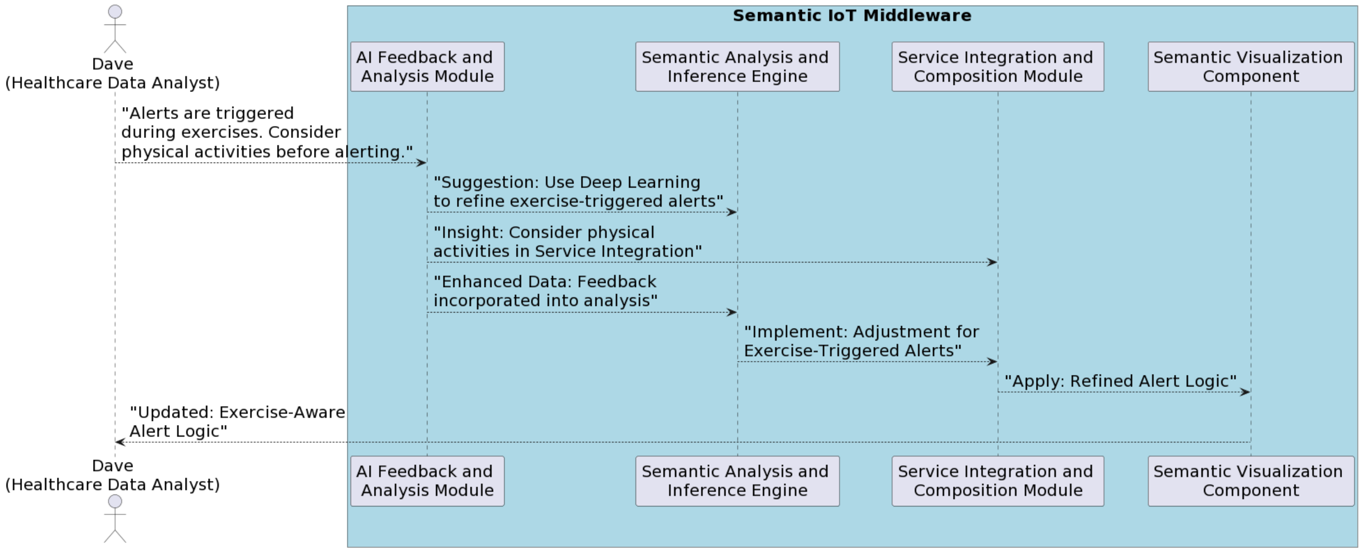
Semantic IoT Middleware
Dave
(Healthcare Data Analyst)
AI Feedback and Analysis Module
Semantic Analysis and Inference Engine
Service Integration and Composition Module
Semantic Visualization Component
"Alerts are triggered during exercises. Consider physical activities before alerting."
"Suggestion: Use Deep Learning to refine exercise-triggered alerts"
"Insight: Consider physical activities in Service Integration"
"Enhanced Data: Feedback incorporated into analysis"
"Implement: Adjustment for Exercise-Triggered Alerts"
"Apply: Refined Alert Logic"
"Updated: Exercise-Aware Alert Logic"
Dave
(Healthcare Data Analyst)
AI Feedback and Analysis Module
Semantic Analysis and Inference Engine
Service Integration and Composition Module
Semantic Visualization Component

Figure 9. AI module: usage of deep learning to implement adjustment for alerts.

To demonstrate the operation of the AI Feedback and Analysis Module within the scenario discussed in this work, Algorithm 3 is provided. It delineates the module's process of responding to and incorporating user feedback for system enhancement. Algorithm 3 illustrates how the module employs advanced machine learning techniques, including deep learning, natural language processing (NLP), clustering and classification, and reinforcement learning (RL), to analyse user feedback, similar to the insights provided by Dave. It details the iterative process of identifying patterns, refining semantic annotations, and making informed adjustments to the system. It also details the steps within the rest of the SIM modules, such as the analysis of feedback content, the application of various AI techniques for pattern recognition and contextual understanding, and the subsequent system modifications based on the insights gained. This includes adjustments in the alert mechanisms to consider factors like physical activities during heart rate monitoring. Algorithm 3 also shows how these refinements are integrated back into the system, culminating in enhanced personalised user experiences.

Algorithm 3 AI Feedback and Analysis in SIM for Personalised Healthcare

```
Initialise AI Feedback and Analysis Module
for each feedback instance from users do
    Analyze Feedback Content
        e.g., Dave's observation on heart rate alerts during exercise
    Apply Deep Learning for Pattern Recognition
        - Correlate heart rate with exercise sessions
    Use NLP to Refine Semantic Annotations
        - Improve context understanding in data
    Employ Clustering and Classification
        - Identify actionable feedback segments
    Implement Reinforcement Learning for Adaptive Improvements
        - Adjust alert parameters based on feedback
end for
Update Service Integration and Composition Module
    - Integrate refined data and parameters
Enhance Semantic Annotation and Analysis Engine
    - Incorporate improved annotations
Reflect Updates in Semantic Visualisation Component
    - Visualise the updated alert system
Notify Users of System Improvements
    - Inform Dave about the enhanced alert mechanism
Repeat Process for Continuous Learning and System Evolution
```

4.4. User-Centric Operations in SIM: Beyond Healthcare

This section details the user-centric characteristics of SIM through multiple scenarios.

4.4.1. Healthcare Scenario: Context-Aware Health Monitoring

Architecture Utilisation: - The IoT Data and Event Generation Module captures detailed health metrics from Alice, including heart rate, blood pressure, and activity levels. - The Semantic Annotation Component labels these metrics, identifying periods of rest, activity, and potential health anomalies. - The AI Feedback and Analysis Module processes Alice's feedback on false alerts during exercise, adjusting the context recognition algorithms to differentiate between exercise-induced and health-related heart rate elevations. - The Blockchain Component securely logs these adjustments for consistent application in future scenarios.

Outcome: Alice receives personalised health monitoring that intelligently distinguishes between her physical activity and genuine health risks, enhancing her trust in the system's alerts.

4.4.2. Smart Home Management: Tailored Environmental Preferences

Architecture Utilisation: - The system learns Emma's preferences for lighting, temperature, and security settings through continuous interaction with the IoT Data and Event Generation Module. - The Semantic Analysis and Inference Engine integrates these preferences to automate home environment adjustments based on time of day, weather conditions, and Emma's presence in the home. - The Service Integration and Composition Module synchronises various smart devices to create a seamless living experience. - Emma uses the Semantic Visualisation Component to easily adjust settings or override automated controls.

Outcome: Emma's home environment dynamically responds to her lifestyle, providing comfort and efficiency without the need for constant manual adjustments.

4.4.3. Agricultural Monitoring: Precision Agriculture for Enhanced Crop Yield

Architecture Utilisation: - Lucas's farm sensors track soil moisture levels, weather patterns, and plant growth, feeding data into the Semantic Annotation Component. - The Semantic Analysis and Inference Engine analyses these data to predict optimal watering times, fertiliser needs, and potential pest threats. - The AI Feedback and Analysis Module refines predictions based on Lucas's input and observed crop responses, enhancing the accuracy of future recommendations. - Data integrity and history are maintained in the Blockchain Component for long-term agricultural planning.

Outcome: Lucas benefits from data-driven insights that improve his crop yields and resource efficiency, demonstrating SIM's capability to support advanced agricultural practices.

4.4.4. Industrial Automation: Proactive Anomaly Detection and Resolution

Architecture Utilisation: - Factory sensors monitor machine performance, sending real-time data to the IoT Data and Event Generation Module. - The Semantic Annotation Component contextualises these data, identifying patterns indicative of potential equipment failures. - The AI Feedback and Analysis Module uses historical data and Aisha's feedback to refine its predictive maintenance algorithms, reducing false alarms and pinpointing actual issues. - The Blockchain Component ensures an immutable record of machine performance and maintenance actions for compliance and auditing purposes.

Outcome: Aisha oversees a more efficient and proactive maintenance regime, with SIM providing critical insights to address manufacturing issues, enhancing productivity, and reducing downtime preemptively.

These scenarios illustrate the depth and practicality of SIM's user-centric approach, leveraging its comprehensive architecture to deliver tailored, intelligent, and efficient experiences across diverse domains.

5. Proof of Concept: Demonstrating SIM in Action

This section presents a proof of concept of the Semantic IoT Middleware (SIM) developed in Python, specifically designed to demonstrate the feasibility of the core functionalities proposed for SIM within the context of the practical scenario described in Section 4. The proof of concept specifically implements Alice's scenario, showcasing how SIM can be applied to real-world health monitoring and decision making processes. As a reminder, the scenario involves Alice, an elderly lady with health conditions, using various IoT healthcare devices to monitor her health, supported by healthcare providers and other stakeholders for timely and effective health management. To bridge the theoretical concepts with this practical application, certain assumptions and abstractions were made for simplicity and to focus on conceptual demonstrations:

- Assumptions: The sensor data for heart rate, blood pressure, and temperature are simulated using random number generation within typical physiological ranges, with thresholds set for elevated levels.
- Abstractions: Complex functionalities such as blockchain transactions are abstracted with placeholders, allowing us to focus on the data flow and logic rather than the technical specifics of these operations.

The codebase for this proof of concept includes scripts for generating sensor data, annotating these data semantically, simulating encryption for secure data transfer, and representing blockchain operations. These elements directly correspond to the IoT Data and Event Generation Module, Semantic Annotation Component, Data Security and Encryption Module, and Blockchain Component of the SIM architecture, respectively. By simulating these operations, we demonstrate how each module of SIM could interact and process data in the context of Alice's scenario, providing a holistic and secure health monitoring solution.

A key aspect of the proof of concept is the simulation of the AI Feedback and Analysis Module, which showcases SIM's adaptability and potential for real-world application by adjusting the system based on user feedback. This reflects the scenario's need for a responsive system that can adapt to Alice's unique health condition and requirements.

Selected code snippets from the proof of concept implementation are provided below to illustrate these interactions:

Generating Sensor Data: The code snippet provided in Listing 1 simulates the generation of health data from IoT devices, akin to those used by Alice for monitoring her heart rate, blood pressure, and temperature. These data are the starting point in the SIM architecture, feeding into subsequent modules for processing and analysis.

Listing 1. Generate Sensor Data Function.

```python
def generate_sensor_data(num_readings):
    # Code to generate random sensor data
    data = []
    for _ in range(num_readings):
        heart_rate = random.randint(55, 120)
        blood_pressure_systolic = random.randint(85, 140)
        blood_pressure_diastolic = random.randint(55, 90)
        temperature = round(random.uniform(36.0, 39.0), 1)
        data.append({
            "heart_rate": heart_rate,
            "blood_pressure": (blood_pressure_systolic, blood_pressure_diastolic),
            "temperature": temperature
        })
    return data
```

Listing 2 shows the code for annotating sensor data. The heart rate readings are annotated as normal, elevated, or low, as shown in Figure 10.

Listing 2. Annotate Sensor Data.

```python
def annotate_sensor_data(sensor_data):
    # Code to annotate sensor data
    annotated_data = []
    for reading in sensor_data:
        heart_rate_status = "Normal" if reading["heart_rate"] <= 100 else "Elevated"
        blood_pressure_status = "Normal" if 90 <= reading["blood_pressure"][0] <= 120 else "Elevated or Low"
        temperature_status = "Normal" if 36.5 <= reading["temperature"] <= 37.5 else "Elevated or Low"
        annotated_data.append({
            "heart_rate": reading["heart_rate"],
            "heart_rate_status": heart_rate_status,
            "blood_pressure": reading["blood_pressure"],
            "blood_pressure_status": blood_pressure_status,
            "temperature": reading["temperature"],
            "temperature_status": temperature_status
        })
    return annotated_data
```

Figure 11 depicts the distribution of heart rate readings generated by the above script, illustrating the type of data that SIM would handle and analyse in real-world applications.

These data serve as a basis for the subsequent annotation, encryption, and blockchain operations, all crucial for the secure and effective management of health data within the SIM framework. By simulating these operations, we demonstrate how SIM handles and processes data and also show its alignment with the needs and complexities of real-world health monitoring scenarios like Alice's.

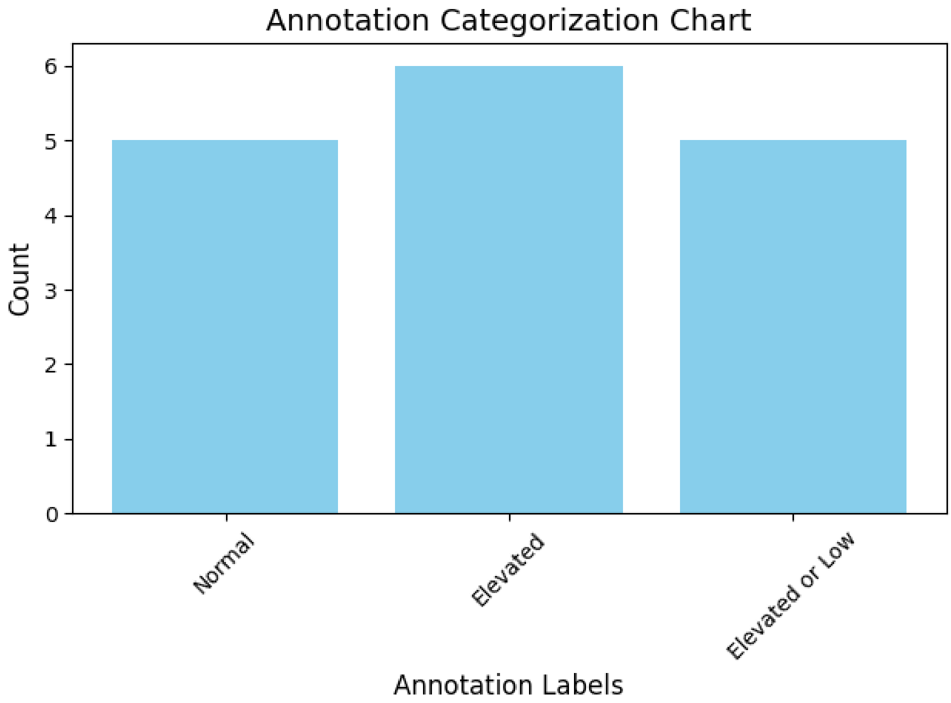

Figure 10. Annotation categorisation chart.

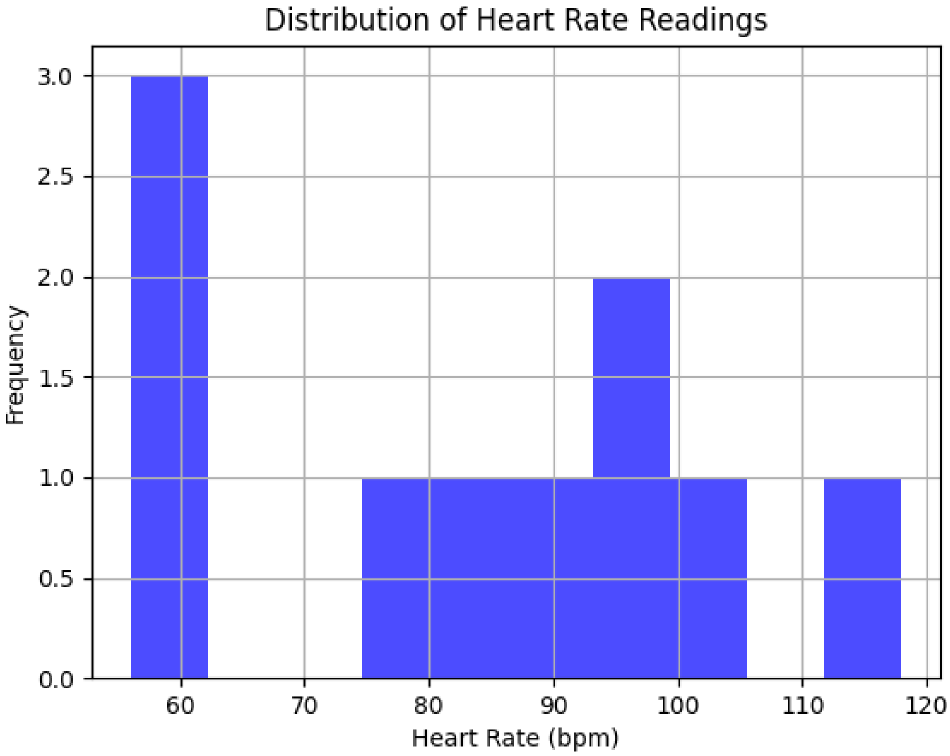

Figure 11. Distribution of heart rate readings.

Simulating Data Encryption: The encryption process is a critical aspect of data security in SIM. It ensures that Alice's health data remains confidential and secure during transit and storage. The code shown in Listing 3 simulates the encryption of data using the SHA-256 hashing algorithm, reflecting the type of cryptographic operations that would be performed in the Data Security and Encryption Module.

Listing 3. Encryption using SHA-256.

```
def encrypt_data(data):
    # Code to simulate encryption using SHA-256 hash
    data_string = json.dumps(data).encode()
    hash_object = hashlib.sha256(data_string)
    return hash_object.hexdigest()
```

Simulating Smart Contract Execution: After securing the data, SIM interacts with the Blockchain Component to ensure the integrity and traceability of health data. The following snippet shown in Listing 4 simulates the execution of a smart contract within a blockchain network, an operation that would handle tasks such as verifying health data transactions or alerting healthcare providers in response to specific conditions detected in the data.

Listing 4. Smart Contract Function.

```
def execute_smart_contract(encrypted_data):
    # Code to simulate smart contract execution
    if ’a’ in encrypted_data:  # Placeholder condition
        print("Smart Contract: Alert sent to healthcare provider.")
    else:
        print("Smart Contract: No action needed.")
```

These simulations represent how SIM's Data Security and Encryption Module and Blockchain Component work together to maintain the security, integrity, and utility of health data. By encrypting the data and utilising smart contracts for data management, SIM ensures that health data like Alice's are handled securely and efficiently, facilitating trustworthy and responsive health monitoring and care. These operations, while simplified in the proof of concept, illustrate the potential of SIM to provide a robust framework for health data security and management in real-world applications.

5.1. Simulating Third-Party Interactions

Within the comprehensive SIM framework, third-party interactions are facilitated by the Service Integration and Composition Module, Semantic Visualisation Component, and AI Feedback and Analysis Module. These modules ensure that the system not only captures and processes data efficiently but also interacts seamlessly with healthcare providers and patients. Here, we simulate potential interactions to demonstrate SIM's versatility and user-centric design.

5.1.1. Healthcare Provider Interaction

Healthcare providers, pivotal in the healthcare ecosystem, interact with the system to monitor and manage patient health. SIM facilitates these interactions by providing streamlined access to processed health data and relevant alerts. The code provided in Listing 5 simulates a healthcare provider's interaction with the system, focusing on how they might review and respond to elevated health alerts, reflecting the real-time decisionmaking facilitated by SIM.

This simulation underlines how the Service Integration and Composition Module and Semantic Visualisation Component could empower healthcare providers to make informed decisions, tailoring care to individual patient needs.

Listing 5. Healthcare Provider Interaction Function.

```
def healthcare_provider_interaction(elevated_alerts):
    for alert in elevated_alerts:
        if alert['type'] == 'heart_rate':
            print("Healthcare Provider Reviewing Elevated Heart Rate Alert")
            print("Adjusting alert parameters based on patient's medical history")
    return "Parameters adjusted"
```

5.1.2. Patient Interaction

Patients' active participation in their health monitoring is crucial for the efficacy of healthcare systems. SIM acknowledges this by incorporating mechanisms for patients to provide feedback and contextual information, which is crucial for accurate and personalised health monitoring. Listing 6 represents how patients might interact with SIM, providing context such as recent physical activities, which can significantly influence health data interpretation.

Listing 6. patient_feedback.

```
    for feedback in patient\_feedback:
        if feedback['type'] == 'exercise\_context':
            print("Patient indicated recent exercise. Re-evaluating heart rate alerts.")
    return "Context updated in patient profile"
```

Incorporating patient feedback into the health monitoring process, as simulated above, showcases the potential of the AI Feedback and Analysis Module to adapt and refine the system continuously. It ensures that the health monitoring is as accurate and personalised as possible, aligning with SIM's goal of providing a user-centric and adaptable healthcare monitoring solution.

5.2. Adaptability Through AI Feedback and Analysis

The AI Feedback and Analysis Module processes user input to continuously refine and personalise the health monitoring experience. This adaptability is demonstrated through a proof of concept visualisation, illustrating how SIM responds to user feedback regarding exercise context, thereby adjusting health data categorisation.

Figure 12 effectively demonstrates the dynamic nature of SIM. Initially, without considering exercise context, some health readings might be misinterpreted as anomalies or signs of distress (indicated by the blue bars). However, after integrating user feedback about recent physical activities, the system adjusts its interpretation (indicated by the orange bars). This leads to a more accurate representation of the user's health status, avoiding unnecessary alerts and providing a tailored health monitoring experience.

This ability to incorporate and respond to user feedback is pivotal, especially in diverse and variable scenarios such as health monitoring. It allows SIM to adapt over time, improving its accuracy and effectiveness. The AI Feedback and Analysis Module does not just adjust parameters but learns from interactions, ensuring that the system evolves to meet the unique needs of each user.

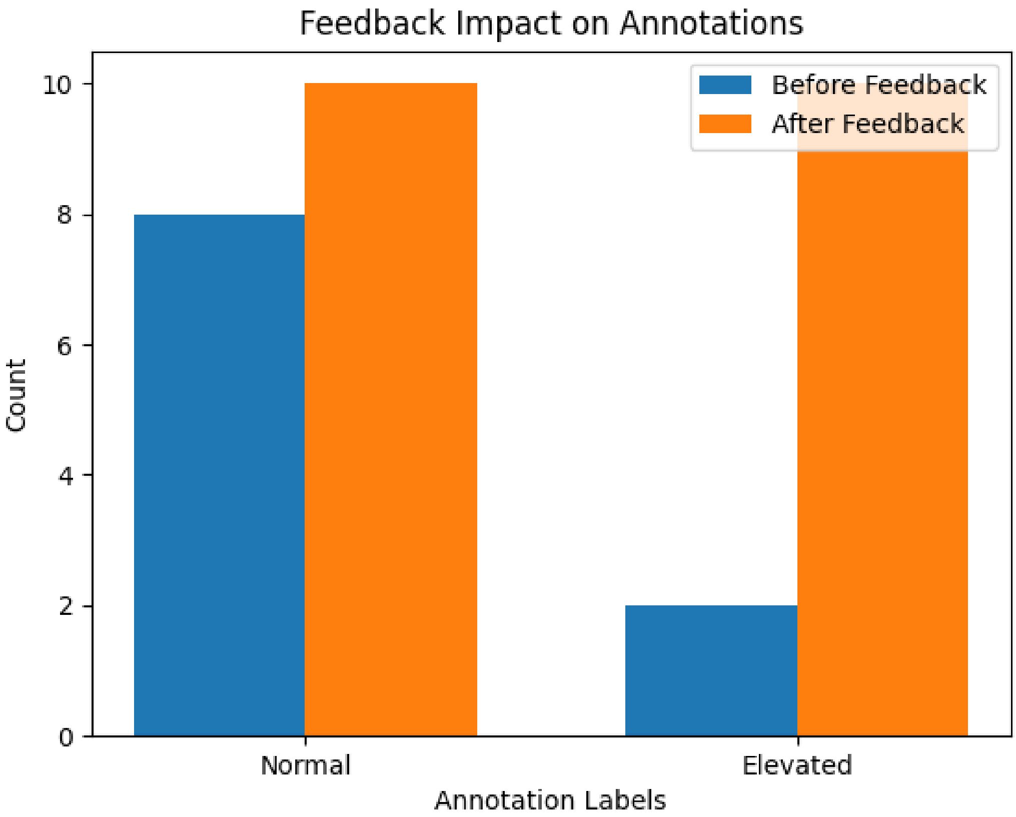

Figure 12. Combined visualisation of annotation categorisation before and after AI feedback. The blue bars represent the initial annotations, and the orange bars show the updated annotations following feedback, demonstrating the system's adaptability to incorporate user-provided exercise context.

5.3. Performance Considerations and Typical Delays

One of the critical aspects of middleware systems, especially those dealing with real-time data and decisionmaking like SIM, is performance. Performance in such systems is often gauged by their latency, or the time taken to complete an operation, from data acquisition to actionable insights. In the context of SIM, several operations could introduce delays:

- **Data Acquisition and Annotation:** The initial phase involves collecting data from IoT devices and annotating them. While generally fast, this process's speed can vary based on the complexity of the data and the efficiency of the annotation algorithms.
- **Encryption and Security:** Encrypting data and ensuring their security is paramount, especially in healthcare applications. The process of encryption and any associated security checks (like verifying digital signatures or interfacing with a blockchain) can introduce delays. The specific amount of time taken can depend on the encryption algorithm's efficiency and the underlying hardware.
- **Blockchain Transaction:** Interacting with a blockchain can introduce variable delays. Typical blockchain transactions may take from several seconds to minutes depending on the network's current load, the consensus mechanism in place, and the specific blockchain configuration. For SIM, this step is crucial for ensuring data integrity and auditability but is also one of the most significant sources of latency.
- **Smart Contract Execution:** Executing smart contracts involves running code on the blockchain, which can vary in execution time based on the contract's complexity and the current state of the blockchain network.
- **AI Feedback and Analysis:** The AI-driven feedback and analysis module, while providing valuable adaptability and learning capabilities, can also introduce computational delays. The extent depends on the amount of data processed and the efficiency of the implementation.

While this proof of concept abstracts many of these details, it is important to consider these factors in a real-world implementation. Optimising each step to reduce latency without compromising functionality or security is crucial for the success of middleware solutions like SIM. Future work will involve empirical testing and optimisation of these components to meet the stringent performance requirements of healthcare and IoT applications.

The full project, including all the source code and visualisations, is available on GitHub for further exploration and contribution by the research community. The repository can be accessed at https://github.com/MahmoudElkhodr/SIM.git accessed on 1 January 2024.

6. Comparing the Semantic IoT Middleware with other Middleware Approaches

In this section, we conduct a theoretical comparative analysis of SIM against traditional IoT middleware, cloud-centric middleware, and edge-centric middleware. This analysis uses key metrics crucial for evaluating IoT systems' performance and adaptability, such as computational cost, scalability, semantic capabilities, data integrity, decentralization, and user control. The comparison, illustrated in Table 4, offers a comprehensive view of the strengths and weaknesses of each approach.

Table 4. Comparison of metrics for different middleware approaches. In each row, the best-scoring middleware approach is highlighted in bold.

Metric	**Traditional IoT Middleware**	**Cloud-Centric Middleware**	**Edge-Centric Middleware**	**Semantic IoT Middleware**
Computational Cost	Medium	Low	Medium	**Low**
Scalability	Medium	**High**	High	**High**
Semantic Capabilities	None	Low	Medium	**High**
Data Integrity	Low	Medium	Medium	**High**
Decentralisation	Low	Low	Medium	**High**
User Control	Medium	Medium	High	**High**
Latency	Medium	High	Low	**Low**

The assessments presented in Table 4 are based on a theoretical framework that considers the inherent design and feature set of SIM as compared to existing middleware approaches. This comparison offers a broad view of the relative strengths and weaknesses of each middleware type, with the following justifications for the anticipated performance metrics:

- Computational Cost: SIM's expected low computational cost is based on its efficient data handling and processing algorithms, which are designed to minimise resource usage. In contrast, traditional and edge-centric middleware may have moderate costs due to less optimised data processing.
- Scalability: High scalability of SIM is anticipated due to its decentralised architecture and blockchain integration, which are inherently scalable. Cloud-centric middleware also scores high in scalability due to its cloud-based nature.
- Semantic Capabilities: SIM's semantic approach is expected to offer superior capabilities in this area as it is specifically designed to understand and process data semantically, unlike traditional middleware, which lacks this focus.
- Data Integrity: The use of blockchain in SIM is expected to ensure high data integrity through immutable transaction records. Traditional middleware might have lower data integrity due to the absence of such robust mechanisms.
- Decentralisation: SIM's Blockchain Component inherently promotes decentralization, contrasting with the more centralised nature of traditional and cloud-centric middleware.

- User Control: Enhanced user control in SIM is anticipated owing to its Blockchain Component, which allows for transparent and user-controlled data access and manipulation.
- Latency: The distributed nature of SIM, with processing completed closer to data sources, is expected to result in lower latency compared to other approaches that might rely on centralised processing.

The justifications for these assessments are based on the anticipated performance metrics derived from the design and features of SIM. However, it is critical to note that these theoretical evaluations are conjectural and await empirical validation. The insights gained from this comparison set the stage for more extensive research, where SIM can be empirically tested and validated.

This groundwork is the beginning of a broader journey to transform SIM from a theoretical model into a practical and impactful IoT system. Moving forward, our focus is on empirical research to validate the effectiveness of SIM in real-world applications, crucial for its evolution and implementation.

SIM exhibits key benefits, such as enhanced interoperability through its semantic approach, intelligent decisionmaking via AI integration, and robust security and data integrity through Blockchain Components. These features distinguish SIM from traditional, cloud-centric, and edge-centric middleware, each having its own merits in isolated metrics. Our comparative analysis underscores SIM's comprehensive strengths, marking it as a promising choice for modern and future IoT applications.

7. Challenges and Advancements in SIM

Although the Semantic IoT Middleware (SIM) demonstrates numerous potential benefits for robust and efficient data sharing in distributed systems, several challenges are apparent that must be addressed in future research.

7.1. Computational Complexity and Storage Requirements

One significant limitation of SIM involves the computational complexity and storage requirements associated with the integration of semantic annotation and blockchain technology. Semantic annotation, which involves attaching metadata to content, is a high-complexity and computing-intensive task, particularly when automated using natural language processing and machine learning techniques. Blockchain technology, known for transaction processing and smart contracts, adds to this complexity, especially in decentralised implementations.

Implications: These complexities can impact the scalability and real-time processing capabilities of SIM. High computational demands may hinder the system's ability to efficiently process large volumes of data or operate effectively in resource-constrained environments.

Potential Solutions: To mitigate these challenges, future research could explore more efficient data processing algorithms, the utilization of cloud-based services for storage, or implementing hybrid blockchain models to balance decentralization with computational efficiency.

Contextualization Within Design: Within the overall design of SIM, these complexities are crucial considerations. The middleware's architecture may need to incorporate mechanisms to manage these demands effectively, ensuring that the system remains both functional and efficient.

An analysis of these complexities is summarised in Table 5, providing a theoretical assessment based on existing literature and design considerations.

Table 5. Detailed assessment of computational complexity and storage in SIM.

Aspect	Semantic Annotation	Blockchain	Combined Complexity	Potential Solutions
Computational Complexity	High (due to NLP and ML algorithms)	Moderate to High (dependent on consensus mechanisms)	High	Optimised ML models, lighter consensus protocols
Storage Requirement	Moderate (metadata storage)	High (ledger and transaction data)	High	Data pruning strategies, distributed cloud storage

7.2. Data Privacy and Security with Insights from BioChainReward (BCR)

While the Semantic IoT Middleware (SIM) offers robust data management capabilities, there are inherent concerns related to data privacy and security. The semantic layer, although beneficial for understanding and managing data, might inadvertently expose sensitive data patterns or semantics to unauthorised entities. To address these risks, it is crucial to implement advanced encryption and obfuscation techniques tailored for semantic data.

Our previous work, "BioChainReward: A Secure and Incentivised Blockchain Framework for Biomedical Data Sharing", presents a relevant and effective approach to this challenge. In the BCR framework, we developed an AI-enabled privacy Preservation sublayer, which automatically manages the selection and application of privacy-preserving techniques based on the data transaction context.

This sublayer incorporates methods such as anonymisation, obfuscation, and differential privacy. Anonymisation is used when the data request does not require personally identifiable information (PII), obfuscation is applied to protect specific sensitive attributes in the data, and differential privacy is utilised for generating statistical summaries while maintaining individual privacy. The selection of these methods is driven by an AI system, which uses decision trees to determine the most suitable privacy technique based on the data request's purpose, data sensitivity, and the data owner's privacy preferences.

Incorporating a similar AI-enabled privacy preservation approach into SIM could significantly enhance its data security capabilities. The AI-driven decision-making process from BCR can be adapted to the needs of SIM, ensuring that data privacy is maintained without compromising the utility of the data. Moreover, this approach aligns with SIM's focus on user-centric operations as it allows for customisable privacy settings based on user preferences.

7.3. Other Challenges

Beyond computational and storage challenges, other limitations include:

Semantic Layer Maintenance: The comprehensive creation and maintenance of semantic representations, especially in rapidly evolving domains, might prove challenging.

Standardisation Adoption: The middleware's effectiveness depends on the widespread adoption of standardised semantic representations, where inconsistency can dilute potential benefits.

Legacy System Integration: While SIM endeavours to bridge the gap between different data sharing systems, integrating legacy systems that do not support semantic technologies remains a challenge, requiring the development of adaptors or translators.

8. Conclusions

This study introduced SIM, a novel semantic-, blockchain-, and IoT-based middleware designed to enhance the secure sharing of medical data with third-party entities. The architecture's pivotal Semantic Annotation Component transcends traditional data representation, powering raw data with a structured, universally understood vocabulary that encompasses the vast heterogeneity intrinsic to IoT environments.

SIM seamlessly integrates nine elements, combining the benefits of blockchain technology, AI, and IoT. These elements synergistically deliver secure data sharing, real-time annotation, adaptive access controls, and profound insights drawn from semantic analysis.

A key feature of SIM is the integration of cutting-edge cryptographic measures within the Data Security and Encryption Module. This module, interacting closely with the Blockchain Component, guarantees the secure transition of semantically annotated data to a blockchain network, addressing multifaceted concerns in data security and user privacy.

Moreover, the incorporation of an AI Feedback and Analysis Module harnesses artificial intelligence capabilities in order to continually refine the middleware, ensuring holistic enhancement of the middleware based on user feedback and intricate system event analyses.

Author Contributions: Conceptualisation, M.E.; methodology, M.E.; software, M.E.; validation, S.K. and E.G.; resources, E.G.; writing—original draft preparation, M.E. and S.K.; writing—review and editing, M.E., S.K. and E.G.; funding acquisition, M.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available in this article.

Acknowledgments: The authors acknowledge the use of ChatGPT 4 in the preparation of this article but confirm that no artificial intelligence (AI) tools were used in the actual writing. ChatGPT 4 assisted with specific formatting tasks, including converting content from Word to LaTeX. Additionally, the tool was employed for copyediting and proofreading select sections, checking the flow between subsections, and aiding in identifying the limitations of this work. The authors have taken measures to ensure that any text introduced by ChatGPT 4 remained consistent with the original intent and content. All suggestions provided by ChatGPT 4 were thoroughly reviewed and revised by the authors to uphold the accuracy and integrity of the final manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Elkhodr, M.; Shahrestani, S.; Cheung, H. Internet of things research challenges. In *Security Solutions for Hyperconnectivity and the Internet of Things*; IGI Global: Hershey, PA, USA, 2017; pp. 13–36.
2. Statista. Available online: https://www.statista.com/topics/2637/internet-of-things/ (accessed on 21 August 2023).
3. Statista. Available online: https://www.statista.com/statistics/1194709/iot-revenue-worldwide/ (accessed on 21 August 2023).
4. Statista. Available online: https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/ (accessed on 21 August 2023).
5. Statista. Available online: https://www.statista.com/outlook/tmo/internet-of-things/healthcare-iot/worldwide (accessed on 21 August 2023).
6. Centers for Disease Control and Prevention. Available online: https://www.cdc.gov/phlp/publications/topic/hipaa.html (accessed on 22 August 2023).
7. Intersoft Consulting. Available online: https://gdpr-info.eu/ (accessed on 22 August 2023).
8. Elkhodr, M.; Shahrestani, S.; Cheung, H. Managing the Internet of Things. In Proceedings of the 2015 IEEE International Conference on Data Science and Data Intensive Systems, Sydney, NSW, Australia, 11–13 December 2015; pp. 579–585. [CrossRef]
9. Elkhodr, M.; Shahrestani, S.; Cheung, H. A Middleware for the Internet of Things. *Int. J. Comput. Netw. Commun.* **2016**, *8*, 159–178. [CrossRef]
10. Farid, F.; Elkhodr, M.; Sabrina, F.; Ahamed, F.; Gide, E. A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services. *Sensors* **2021**, *21*, 552. [CrossRef] [PubMed]
11. Elkhodr, M.; Gide, E.; Farid, F.; Ahamed, F. A Blockchain and IoT-Enabled Secure Health Data Handling Framework. In Proceedings of the 7th International Conference on Advances in Biomedical Engineering, Beirut, Lebanon, 12–13 October 2023; *in press*.
12. Elkhodr, M.; Gide, E.; Darwish, O.; Al-Eidi, S. BioChainReward: A Secure and Incentivised Blockchain Framework for Biomedical Data Sharing. *Int. J. Environ. Res. Public Health* **2023**, *20*, 6825. [CrossRef] [PubMed]
13. Jabbar, S.; Ullah, F.; Khalid, S.; Khan, M.; Han, K. Semantic interoperability in heterogeneous IoT infrastructure for healthcare. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 9731806. [CrossRef]
14. Cardoso, J.; Sheth, A. The Semantic Web and its applications. In *Semantic Web Services, Processes and Applications*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 3–33.

15. Aiken, B.; Strassner, J.; Carpenter, B.; Foster, I.; Lynch, C.; Mambretti, J.; Moore, R.; Teitelbaum, B. Network Policy and Services: A Report of a Workshop on Middleware; Technical Report; IETF. 2000. Available online: https://www.ietf.org/rfc/rfc2768.txt (accessed on 20 November 2023).
16. Zhang, J.; Ma, M.; Wang, P.; dong Sun, X. Middleware for the Internet of Things: A survey on requirements, enabling technologies, and solutions. *J. Syst. Archit.* **2021**, *117*, 102098. [CrossRef]
17. da Cruz, M.A.; Rodrigues, J.J.; Sangaiah, A.K.; Al-Muhtadi, J.; Korotaev, V. Performance evaluation of IoT middleware. *J. Netw. Comput. Appl.* **2018**, *109*, 53–65. [CrossRef]
18. Zgheib, R.; Conchon, E.; Bastide, R. Semantic middleware architectures for IoT healthcare applications. In *Enhanced Living Environments: Algorithms, Architectures, Platforms, and Systems*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 263–294.
19. Razzaque, M.A.; Milojevic-Jevric, M.; Palade, A.; Clarke, S. Middleware for Internet of Things: A Survey. *IEEE Internet Things J.* **2016**, *3*, 70–95. [CrossRef]
20. Han, Q.; Venkatasubramanian, N. Autosec: An integrated middleware framework for dynamic service brokering. *IEEE Distrib. Syst. Online* **2001**, *2*, 22–31.
21. Huebscher, M.C.; McCann, J.A. Adaptive middleware for context-aware applications in smart-homes. In Proceedings of the 2nd Workshop on Middleware for Pervasive and Ad-hoc Computing, Toronto, ON, Canada, 18–22 October 2004; pp. 111–116.
22. Muldoon, C.; O'Hare, G.M.; Collier, R.; O'Grady, M.J. Agent factory micro edition: A framework for ambient applications. In *Computational Science–ICCS 2006: Proceedings of the 6th International Conference, Reading, UK, 28–31 May 2006*; Proceedings, Part III 6; Springer: Berlin/Heidelberg, Germany, 2006; pp. 727–734.
23. Terziyan, V.; Kaykova, O.; Zhovtobryukh, D. Ubiroad: Semantic middleware for context-aware smart road environments. In Proceedings of the 2010 Fifth International Conference on Internet and Web Applications and Services, Barcelona, Spain, 9–15 May 2010; pp. 295–302.
24. Fok, C.L.; Roman, G.C.; Lu, C. Agilla: A mobile agent middleware for self-adaptive wireless sensor networks. *ACM Trans. Auton. Adapt. Syst.* **2009**, *4*, 16. [CrossRef]
25. Michiels, S.; Horré, W.; Joosen, W.; Verbaeten, P. DAViM: A dynamically adaptable virtual machine for sensor networks. In Proceedings of the International Workshop on Middleware for Sensor Networks, Melbourne, Australia, 28 November 2006; pp. 7–12.
26. Levis, P.A. *Application Specific Virtual Machines: Operating System Support for User-Level Sensornet Programming*; University of California: Berkeley, CA, USA, 2005.
27. Hasiotis, T.; Alyfantis, G.; Tsetsos, V.; Sekkas, O.; Hadjiefthymiades, S. Sensation: A middleware integration platform for pervasive applications in wireless sensor networks. In Proceedings of the Second European Workshop on Wireless Sensor Networks, Istanbul, Turkey, 2 February 2005; pp. 366–377.
28. Bonnet, P.; Gehrke, J.; Seshadri, P. Towards sensor database systems. In *Mobile Data Management*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 3–14.
29. Gibbons, P.B.; Karp, B.; Ke, Y.; Nath, S.; Seshan, S. Irisnet: An architecture for a worldwide sensor web. *IEEE Pervasive Comput.* **2003**, *2*, 22–33. [CrossRef]
30. Murphy, A.L.; Picco, G.P.; Roman, G.C. Lime: A middleware for physical and logical mobility. In Proceedings of the Proceedings 21st International Conference on Distributed Computing Systems, Mesa, AZ, USA, 16–19 April 2001; pp. 524–533.
31. Costa, P.; Mottola, L.; Murphy, A.L.; Picco, G.P. Teenylime: Transiently shared tuple space middleware for wireless sensor networks. In Proceedings of the International Workshop on Middleware for Sensor Networks, Melbourne, Australia, 28 November 2006; pp. 43–48.
32. Lima, R.d.C.A.; Rosa, N.S.; Marques, I.R.L. TS-Mid: Middleware for wireless sensor networks based on tuple space. In Proceedings of the 22nd International Conference on Advanced Information Networking and Applications-Workshops (Aina Workshops 2008), Ginowan, Japan, 25–28 March 2008; pp. 886–891.
33. Mohamed, N.; Al-Jaroodi, J. A survey on service-oriented middleware for wireless sensor networks. *Serv. Oriented Comput. Appl.* **2011**, *5*, 71–85. [CrossRef]
34. Ribeiro, A.R.; Silva, F.C.; Freitas, L.C.; Costa, J.C.; Francês, C.R. SensorBus: A middleware model for wireless sensor networks. In Proceedings of the 3rd International IFIP/ACM Latin American Conference on Networking, Cali, Columbia, 10–13 October 2005; pp. 1–9.
35. Souto, E.; Guimaraes, G.; Vasconcelos, G.; Vieira, M.; Rosa, N.; Ferraz, C.; Kelner, J. Mires: A publish/subscribe middleware for sensor networks. *Pers. Ubiquitous Comput.* **2006**, *10*, 37–44. [CrossRef]
36. AWS IoT Core. Available online: https://aws.amazon.com/iot-core/ (accessed on 11 August 2023).
37. Fiware-IoT-Agent. Available online: https://www.fiware.org/ (accessed on 11 August 2023).
38. Fiware Orion. Available online: https://fiware-orion.readthedocs.io/en/master/ (accessed on 11 August 2023).
39. LinkSmart. Available online: https://openhub.net/p/linksmart (accessed on 11 August 2023).
40. Microsoft Azure. Available online: https://azure.microsoft.com/en-au/ (accessed on 11 August 2023).
41. Soldatos, J.; Kefalakis, N.; Hauswirth, M.; Serrano, M.; Calbimonte, J.P.; Riahi, M.; Aberer, K.; Jayaraman, P.P.; Zaslavsky, A.; Žarko, I.P.; et al. Openiot: Open source internet-of-things in the cloud. In *Interoperability and Open-Source Solutions for the Internet of Things: Proceedings of the International Workshop, FP7 OpenIoT Project, Held in Conjunction with SoftCOM 2014, Split, Croatia, 18 September 2014*; Invited Papers; Springer: Berlin/Heidelberg, Germany, 2015; pp. 13–25.

42. Symbius IoT. Available online: https://www.alliot.co.uk/product/symbius-iot-middleware-platform/ (accessed on 11 August 2023).
43. Fortino, G.; Guerrieri, A.; Pace, P.; Savaglio, C.; Spezzano, G. Iot platforms and security: An analysis of the leading industrial/-commercial solutions. *Sensors* **2022**, *22*, 2196. [CrossRef] [PubMed]
44. Gokilakrishnan, G.; Varthnan, P.A.; Kumar, D.V.; Subbiah, R.; Anandakumar, H. Modeling and Performance Evaluation for Intelligent Internet of Intelligence Things. In Proceedings of the 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 17–18 March 2023; Volume 1, pp. 2316–2323.
45. Dongre, Y.; Patil, P.D. An Analysis of Heterogeneous Device Middleware for Quality Metrics. In Proceedings of the 2023 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 1–3 March 2023; pp. 1–6.
46. Gorrepati, R.R.; Jonnala, P.; Guntur, S.R.; Kim, D.H. Semantic Web of Things for Healthcare Interoperability using IoMT Technologies. In *Semantic Technologies for Intelligent Industry 4.0 Applications*; River Publishers: New York, NY, USA, 2023; pp. 49–82.
47. IBM Watson IoT Platform. Available online: https://internetofthings.ibmcloud.com/ (accessed on 12 October 2023).
48. Google Cloud IoT Core. Available online: https://cloud.google.com/iot-core (accessed on 12 October 2023).
49. Xie, C.; Yu, B.; Zeng, Z.; Yang, Y.; Liu, Q. Multilayer Internet-of-Things Middleware Based on Knowledge Graph. *IEEE Internet Things J.* **2021**, *8*, 2635–2648. [CrossRef]
50. da Cruz, M.A.A.; Rodrigues, J.J.P.C.; Lorenz, P.; Korotaev, V.V.; de Albuquerque, V.H.C. In.IoT—A New Middleware for Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 7902–7911. [CrossRef]
51. Ali, Z.; Mahmood, A.; Khatoon, S.; Alhakami, W.; Ullah, S.S.; Iqbal, J.; Hussain, S. A generic Internet of Things (IoT) middleware for smart city applications. *Sustainability* **2023**, *15*, 743. [CrossRef]
52. Pliatsios, A.; Lymperis, D.; Goumopoulos, C. S2NetM: A Semantic Social Network of Things Middleware for Developing Smart and Collaborative IoT-Based Solutions. *Future Internet* **2023**, *15*, 207. [CrossRef]
53. Lymperis, D.; Goumopoulos, C. SEDIA: A Platform for Semantically Enriched IoT Data Integration and Development of Smart City Applications. *Future Internet* **2023**, *15*, 276. [CrossRef]
54. Abdelrazig Abubakar, M.; Jaroucheh, Z.; Al-dubai, A.; Liu, X. Blockchain-Based Identity and Authentication Scheme for MQTT Protocol. In Proceedings of the 2021 the 3rd International Conference on Blockchain Technology (ICBCT ’21), Shanghai, China, 26–28 March 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 73–81. [CrossRef]
55. Bahga, A.; Madisetti, V.K. Blockchain platform for industrial internet of things. *J. Softw. Eng. Appl.* **2016**, *9*, 533–546. [CrossRef]
56. Rizzardi, A.; Sicari, S.; Miorandi, D.; Coen-Porisini, A. Securing the access control policies to the Internet of Things resources through permissioned blockchain. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6934. [CrossRef]
57. Zgheib, R.; Kristiansen, S.; Conchon, E.; Plageman, T.; Goebel, V.; Bastide, R. A scalable semantic framework for IoT healthcare applications. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *14*, 4883–4901. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.