Smart Home IoT System with AI Decision Making

Ala'aldin Odeh
dept. Natural Sciences - Artificial Intelligence
An-Najah National University
Nablus, Palestine

Mousa Ziadeh
dept. Natural Sciences - Artificial Intelligence
An-Najah National University
Nablus, Palestine

***Abstract*—This paper presents the design and implementation for a standard IoT smart home system. The architecture of the system focuses on extensibility, security, and the integration of AI models for decision making. The system provides early data anomaly detection using predefined rules and thresholds that are configurable through the system. Also, the system provides real-time data analytics capabilities and devices control using a user friendly portal. The AI model used in the system is Random Forest which performs well on decision making tasks.**

Keywords— IoT, Smart Home, AI decision making, Analytics.

I. Introduction

Smart home system adaption has accelerated globally during the past 10 years. This growth is mainly due to the advancements in IoT systems, AI, and energy management systems. The global smart home market was valued between $127 billion and $183 billion in 2024–2025, and it is forecasted to grow to $414–633 billion by 2032–2034, with CAGR ranges from 8.5% to 27%. This high and increasing growth underlines how people are looking for more convenience, secure, and energy efficient homes to live in. [1]

Looking at the adoption from a regional perspective, there are significant disparities. North America accounts for approximately 35–40% of global spending, and U.S. household penetration estimated at 45–63% and over 72 million smart devices in use. There is an emerging market in Asia-Pacific, and it is projected to bypass other markets by 2030 with a CAGR 23%. Europe has a more steady growth with around 18% of global spending, with energy efficiency being the main driver. Adoption in the Middle East and Africa has lower rates, with security and privacy being the main challenges. [2]

In Academia, this growth is also reflected with a noticeable increase in publications related to smart home technologies. Around 2,507 papers were published between 2014 and 2024 on topics like IoT integration, AI-driven automation and healthcare [3] [4]. Research, also, emphasize on standardization for better system interoperability, privacy, and focus on user oriented design to ease the adaptation of systems and address security and privacy concerns [5].

Transition from basic automation toward AI-powered predictive systems is a major going forward movement, with energy efficiency and security being the main drivers. This is compacted by challenges like installation costs, privacy, and lack of standardization. Policies and regulation could play a major rule to increase the adaptation of smart home systems, and address consumer concerns. [3]

There are several simulation platforms that can model smart home environments. OpenSHS is an open-source, cross-platform 3D simulator that enables researches to design virtual homes. Other simulation tools include TAESim and ns-3 [6]. Some general purpose tools also exist like AnyLogic, FlexSim, and Simulink, which are widely used foe agent-based and discrete-event modeling [7].

This paper provides a simple implementation of smart home IoT system that focuses on ease of use, real-time analytics, monitoring, and the use of AI decision making.

II. Literature Review

A Smart home uses IoT interconnected system to enable automation and context-aware services. The integration of AI models further enhances a smart home system and infer the correct decisions based on inputs from the sensors. This have a lot of benefits on improving the quality of life in human residents and could help in making homes more energy efficient.

There is a growing body of work that examines how AI models could enhance smart home IoT systems. Rodriguez-Garcia et al. (2023) provide a complete review of AI and IoT convergence in smart home systems. The surveyed work stresses the importance of AI for decision making in integrated AI-IoT systems. It also highlights the strategic decision support frameworks that combine machine learning and IoT data analysis [8].

Other researches implemented AI-based smart security systems that uses IoT sensors for threat detection and response. And example of that is the work done by Sabit (2025) that presents an AI-enabled smart security system utilizing video processing infused with sensors to automatically detect and classify security events [9].

ML continues to be researched for exploring enhancements of IoT smart home functionalities. Hizal et al. (2024) explored ML models for detecting intrusion, and they showcased how leveraging classification algorithms could improve system responses to anomaly behavior. Those decision-making models also show the importance for security and general AI decision logic in smart homes [10].

In addition to security and automation, decision making in increasingly becoming context-aware. López-Rodríguez et al. (2025) review adaptive smart home automation systems and categorize the approaches used based on the inference strategy of user behavior and surrounding environment changes. The

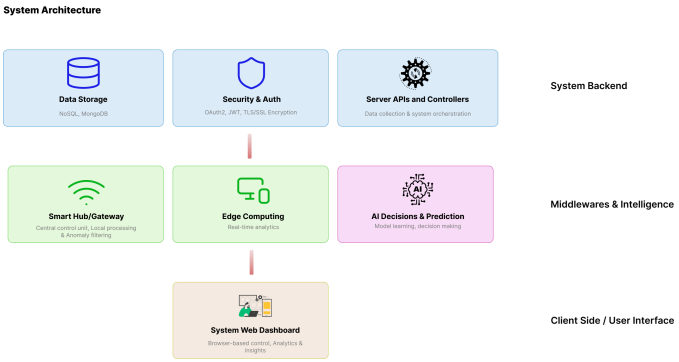

Fig. 1. System architecture.

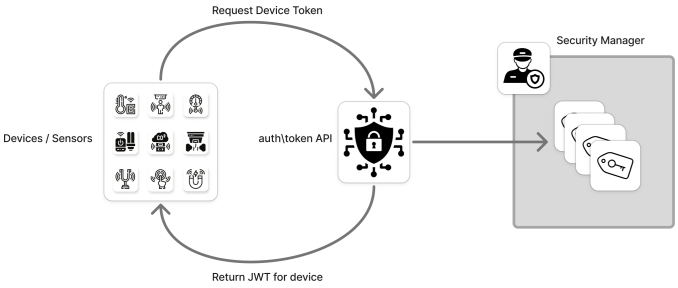

Fig. 2. Authentication flow between the devices and the system backend.

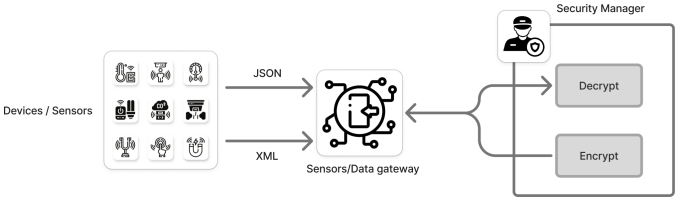

Fig. 3. Data encryption and decryption.

analysis highlights the usage of ML and symbolic reasoning for comfort oriented and general decision making functionalities in smart homes [11].

More over, there are challenges that are specific to decision making when it comes to humans' preferences. Shajalal et al. (2024) explores the reasoning in AI decision within smart home environments pushing towards having more human-centered explainable AI frameworks. The decisions taken by such frameworks should be transparent and to consumers. These system improve trust between the system and its users, and should increase the satisfaction with automated decisions [12].

Mousavi et al. (2025) conduct a systematic literature review on AI in IoT systems. It categorizes the AI prediction and pattern recognition. The finding of the study show that common prediction tasks are common but explicit decision-making are not being focused on. This shows a major research gap that could be further explored [13].

III. Proposed Design

A. High-Level Architecture

Fig. 1 depicts the components:

- **System backend:** Consists of the storage/database which was implemented using MongDB for data flexibility and extendibility. Also contains the security infrastructure of the system and the main controllers and APIs.
- **Gateway and intelligence:** Contains the middle-wares that handle the data coming from the devices. It also contains the AI model management and decision making logic.
- **Client side:** This includes the user facing application enabling the user to interact with the system and view real-time data analytics. Also, it offers some control capabilities and the handling model training.

B. Security Implementation

- **Authentication flow:** The system provides and authentication flow for the devices to connect with the backend of the system. This ensures that only allowed devices send data to the system and prevents intrusions from other devices that could affect the decision making system. Fig. 2 illustrates the flow. The device send a request to the authentication endpoint requesting a JWT token. The token is then used to authenticate requests coming from the device. The token expires after 3600 seconds and a new JWT token should be requested by the device.
- **Data encryption and decryption:** The data provided by the sensors get encrypted before passing it on the network. The encryption of the data ensures that the data is not tampered with and comes from a valid source. The backend decrypt the data using a pre-defined key specific for the device that sent the data and validates its integrity before committing it the database and running analysis on it. Fig. 3 shows the encryption/decryption flow and the components involved.

C. AI Model and Decision Making

The system integrates an AI model based on RandomForest Algorithm. The model learns from the data coming from the sensors and makes the decisions of what command should be executed. The system is pre-loaded on system startup from local storage. The local storage includes a snapshot of the latest trained model. The system admin can trigger the learning process of the model from the portal specifying the amount of the data that it should train on.

Another level of decision making is also included as an auxiliary system. This level depends on heuristically defined rules that can be used to further support the decision taken of the AI model. These rules also can be used as a fallback when the AI model is not able to predict the correct action/command. Fig. 4 shows the execution flow of the decision making using the AI model and the heuristic rules subsystem. Fig. 5 shows the training flow for the model which can be triggered at anytime through the system portal.

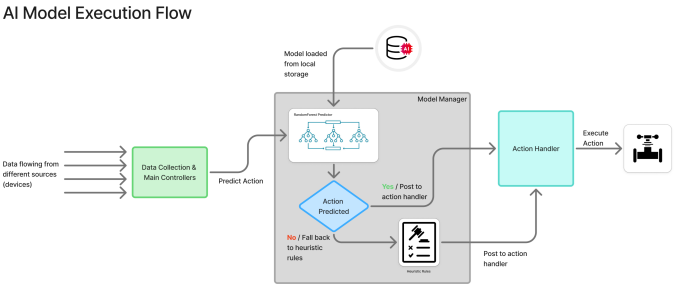

Fig. 4. AI Model execution flow.

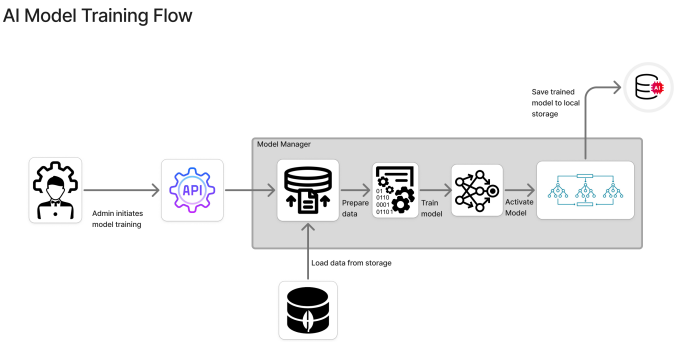

Fig. 5. AI Model train flow.

D. Anomaly Detection

Another level of data filtering comes from the data gateway, which receives the data from the devices and has a pre-defined set of thresholds for each device. This is configured in the system to allow for early detection of wrong values and to prevent further processing of them. This enhances the system performance and makes sure that no outliers are included within the data. Dropping the outliers and anomalies further enhances the AI model quality when the data is used for training.

E. Sensor Data Representation and Interoperability

The system supports heterogeneous sensor communication by handling different payload representations coming from the devices. This is important in smart home environments, since devices can differ in their supported protocol stacks and data formats. For this reason, the system can accept sensor data using JSON payloads for most devices, and XML payloads for selected devices that follow a SOAP style structure. The backend parses both formats and maps them to a unified internal representation, which ensures that decision making and analytics are independent from the incoming format.

F. Controller Interfaces and Real-Time Monitoring

The controller exposes a set of REST endpoints that receive sensor readings and provide access to system status and actuator control. In addition, the system provides a real-time communication channel between the backend and the user portal to support live monitoring of sensor updates, actuator states, and recent decisions. This real-time flow improves usability in simulation scenarios, since the user can directly observe how the system reacts to sensor changes and how fast commands are executed.

G. Data Analytics, Visualization, and Export

In addition to storing readings and commands, the system provides analytics capabilities that summarize the collected data over time. The analytics module generates descriptive statistics and time-based aggregations that help the user understand the system behavior, detect abnormal patterns, and validate decision outcomes. The system also supports exporting data into common formats to allow offline analysis and reporting. This makes it easier to evaluate the system results, reuse datasets for model training, and share outputs with other tools.

H. Model Maintenance and Continuous Quality

To keep the AI decision making reliable over time, the system manages the model lifecycle beyond the initial training. The training process uses historical system data that links sensor context to the commands executed previously. After training, the system stores model metadata such as the training window size, sample count, and evaluation score to support traceability between versions. The system also monitors recent sensor statistics to detect drift compared to the training baseline. When drift becomes noticeable, retraining can be scheduled to refresh the model snapshot and reduce performance degradation.

I. Extended Security Controls and Access Separation

The security implementation is extended with controls that separate device access from administrative access to the system. Administrative operations, such as actuator manual control and system configuration, can be protected using dedicated access credentials that are independent from device authentication. In addition, the system can apply request validation controls, such as signed requests and rate limiting, to reduce misuse and prevent abnormal traffic from affecting system availability. These controls complement the authentication and encryption mechanisms and provide a clearer separation between sensor data ingestion and privileged system operations.

IV. Conclusions and Future Work

The system designed provides a simulation of a IoT smart home system with flexible configuration that allows for extending the system with any device, either been a sensor or an actuator. The system also provides security measures that prevents non-authenticated devices to connect to it, and validates that the data received and processed is authentic. The system also provides the capability for early detection of anomalies to prevent further processing of outlier data. AI model decision making was integrated within the system to allow for smart prediction of actions. The AI model learns from the data within the system and uses the historical commands taken previously by the system to learn future predictions. In addition to the

framework, the system provides a user facing portal that can be used to monitor and configure the system.

Future work and enhancements to the system include: exploring more AI model techniques and algorithms and compare between them for better model selection, supporting cloud computing solution for further performance enhancements and big data handling.

REFERENCES

[1] "Smart home market size worldwide," 2025, accessed: Dec. 2025. [Online]. Available: https://www.statista.com

[2] "Global smart home market forecast 2024–2034," 2024, accessed: Dec. 2025. [Online]. Available: https://www.marketresearch.com

[3] Y. Sun and X. Li, "Iot-based smart home evolution: A review," *IEEE Internet of Things Journal*, 2021.

[4] J. Doe and A. Smith, "Bibliometric analysis of smart home research (2014–2024)," in *Proc. Int. Conf. Smart Systems*, 2024.

[5] A. Khana *et al.*, "Systematic review on smart home safety and healthcare," *Journal of Ambient Intelligence*, 2024.

[6] N. K. Trivedi and G. V. Chowdhary, "Comparative analysis of simulation tools and iot platforms for middleware," in *Information System Design: Communication Networks and IoT (ISDIA)*, ser. Lecture Notes in Networks and Systems, vol. 1057. Springer, 2024, pp. 123–142.

[7] N. Alshammari, T. Alshammari, M. Sedky, J. Champion, and C. Bauer, "Openshs: Open smart home simulator," *Sensors*, vol. 17, no. 5, p. 1003, 2017.

[8] P. Rodriguez-Garcia, Y. Li, D. Lopez-Lopez, and A. A. Juan, "Strategic decision making in smart home ecosystems: A review on the use of artificial intelligence and internet of things," *Internet of Things*, vol. 22, p. 100772, 2023.

[9] H. Sabit, "Artificial intelligence-based smart security system using internet of things for smart home applications," *Electronics*, vol. 14, no. 3, p. 608, 2025.

[10] S. Hızal, U. Çavuşoğlu, and D. Akgün, "Iot-based smart home security system with machine learning models," *Academic Platform Journal of Engineering and Smart Systems*, vol. 12, no. 1, pp. 28–36, 2024.

[11] L. López-Rodríguez *et al.*, "Adaptation in smart home automation systems: A systematic review of decision-making and interaction," *Internet of Things*, vol. 31, p. 101588, 2025.

[12] M. Shajalal, A. Boden, G. Stevens, D. Du, and D.-R. Kern, "Explaining ai decisions: Towards achieving human-centered explainability in smart home environments," *arXiv preprint arXiv:2404.16074*, 2024.

[13] A. Mousavi *et al.*, "A systematic literature review on artificial intelligence in internet of things systems: Tasks, applications, and deployment," *Internet of Things*, vol. 34, p. 101779, 2025.