Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 • Website: www.ijaidr.com • Email: editor@ijaidr.com

Designing an Edge-Cloud Architecture for Smart Homes in the United States

Vinay Agarwal

GTM Strategy, Schneider Electric

Abstract:
The growth of Internet of Things (IoT) products into residences in the U.S. is generating a pressing requirement for a scalable, low-latency, and privacy-protective computing environment. There are 132.5 million homes in the U.S. and it is expected that the smart home market will reach $36.38 billion by 2024. As a result, the U.S. is the most significant marketplace for smart home solutions. Nevertheless, cloud-based architectures for intelligent residential applications have long suffered from considerable end-to-end latency (150–320 ms), large bandwidth usage, and significant privacy risks as personal residence data is transmitted to distant servers for processing. This article describes a three-tiered edge-cloud architecture intended for use in U.S. smart homes with a device layer, an edge processing layer, and a cloud analysis layer. The architecture described here reduces latencies in real-time control of devices by 85–93%, saves about 65% in bandwidth by performing data pre-processing locally, and may reduce energy usage by up to 39% due to the application of demand response scheduling at the edge. Additionally, a multi-layered security framework is provided to address threats to both devices, the edge, and clouds. Simulation performance evaluations demonstrate the feasibility of using this architecture for energy management, home security, and automation in a wide range of U.S. residential settings.

Keywords: Edge Computing; Cloud Computing; Smart Home; Internet of Things (IoT); Energy Management; Home Security; Residential Architecture.

I. INTRODUCTION

The residential sector represents about 21 percent of all of the total energy used in the United States and the U.S. Energy Information Administration reported that total residential energy expenditures were 10.55 quadrillion BTUs over 132.5 million occupied housing units in the United States [1]. In addition to increasing energy prices, more stringent environmental regulations make integrating smart home technology an attractive solution for reducing energy usage, providing enhanced security and improved occupant comfort. The estimated U.S. smart home market size was $36.38 billion in 2024 and is expected to grow to $403.09 billion by 2034 with a CAGR of 27.19% [2].

Typically, smart home systems use cloud-based computing to process information from Internet of Things (IoT) devices such as smart thermostats, security cameras, door locks, lighting controllers, and energy meters. Cloud computing has essentially infinite storage and processing capability but imposes numerous serious limitations in a residential setting. These limitations include very large end-to-end latencies (between 100 and 500 ms) based upon network conditions, substantial bandwidth consumption due to the need to continuously transmit large amounts of sensor data to remote data centers, and severe privacy risks as sensitive data (e.g., occupancy patterns, video feeds, energy usage history) is stored in third-party servers [3].

In recent years, Edge Computing has emerged as a complimentary paradigm to address the limitations imposed by cloud computing in distributed settings. Edge computing processes data as close as possible to where it is created, thereby minimizing latency [4]. The deployment of intelligent edge gateways in each home network allows for localized processing of low-latency operations such as, real-time device control, security alerts and energy demand response. However, computationally intensive operations such as, training AI models and analyzing trends over extended periods of time are still performed in the cloud. Hybrid edge-cloud approaches have demonstrated the ability to reduce latency by 40-60%, reduce bandwidth utilization by 50-65%, and enhance user data privacy via the local storage of data [5], [6].

Although, edge computing has received increased attention for use in IoT applications, there remains a lack of research regarding architectures optimized for the specific characteristics of U.S. residential environments including; time-of-use (TOU) electricity pricing, state level consumer privacy legislation (e.g., CCPA), NEC requirements, and the diversity of U.S. residential housing types (i.e., single-family homes and multi-dwelling units). To fill this void, this paper presents a comprehensive three-tier edge-cloud architecture optimized for U.S. smart homes.

The contributions of this paper are as follows:

1) A three-tier edge-cloud architecture (device, edge, cloud) optimized for U.S. residential energy management, security, and automation requirements.

2) An energy management module leveraging edge-based demand response and TOU pricing integration for U.S. utility grids.

3) A multi-layer security framework addressing threats across device, edge, and cloud layers with compliance considerations for U.S. privacy regulations.

4) Performance evaluation demonstrating significant improvements in latency, bandwidth utilization, and energy efficiency compared to cloud-only architectures.

The remainder of this paper is organized as follows: Section II reviews background and related work. Section III presents the proposed architecture. Section IV details the energy management module. Section V describes the security and privacy framework. Section VI presents performance evaluation results. Section VII discusses implications and future directions. Section VIII concludes the paper.

II. BACKGROUND AND RELATED WORK

A. Cloud-Based Smart Home Systems

Smart Home Architecture Traditional smart homes use centralized cloud-based services to process, store and make decisions using data from the residential Internet of Things (IoT). Major cloud based services such as Amazon Web Services (AWS) IoT, Google Cloud IoT Core, and Microsoft Azure IoT Hub are providing scalable and reliable infrastructures for connecting and managing residential IoT devices. However, the cloud-centric architecture of smart homes has many limitations. According to Imran et al. [3], the average round-trip delay for sending commands to devices using cloud-based smart home systems is 150-320 milliseconds. Therefore, these types of systems have poor performance for real-time and mission critical applications such as detecting intrusion into a home and controlling Heating Ventilation and Air Conditioning (HVAC) demands. Additionally, transmitting large amounts of video surveillance data and high sampling frequency sensor data to remote servers will consume a lot of bandwidth.

Typically, each house will consume approximately 15-25 Mbps of bandwidth. This causes congestion in networks and increases cost of operation.
Another limitation of cloud-centric architectures is privacy. All smart home devices collect and transmit large amounts of private data. For example, smart home devices may collect and transmit data that includes: occupancy patterns, daily routines, facial recognition data, and audio recordings. Transmitting all of this data to remote servers creates an opportunity for unauthorized entities to obtain this data. There have been studies completed by the engineering group of New York University that found smart devices may be exposing a great deal of household information to unauthorized parties, creating serious risks to privacy in residential environments [7].

B. Edge Computing Paradigm

Edge Computing Paradigm Edge computing represents a distributed computing paradigm in which data is processed close to the point it was generated, i.e., at the "edge" of the network, rather than in a central location (i.e. data center) [4]. When applied to smart homes, the edge device performs several functions: real-time data processing; machine learning inferencing; and automation rules execution, all within the confines of the home network. As stated by the IEEE Technology and Society, edge computing is a promising solution to address the security, privacy and latency issues inherent to IoT deployments; however, edge computing also poses its own security concerns due to its distributed nature [5].
Benefits of Using Edge Computing in Residential Environments The benefits of applying edge computing to residential environments include: very low latency (< 10ms) for locally executed operations; lower bandwidth usage resulting from local filtering/aggregation of data; increased privacy as a result of retaining data locally; and fault tolerant operation allowing for continued operation when the internet connection is lost. However, edge devices have their own set of inherent constraints. These constraints include limited computational resources, limited local storage and maintaining consistency with respect to security among diverse device ecosystems [8].

C. Hybrid Edge-Cloud Approaches

Hybrid architectures combining the advantages of both edge and cloud are becoming popular as an alternative to single-edge or single-cloud solutions. Al-Dabbagh [9], examined in a comparison study of cloud-only versus edge-enabled architecture, demonstrated by use of OMNET++ simulation, that edge-enabled systems have significantly lower latency, better resource utilization on the network, improved reliability of packets delivered, etc. Boiko et al. [10], conducted an overview of architectures for hybrid energy management systems, which were classified into five layers: perception layer, network layer, middleware layer, business layer, and application layer. The authors indicated the rising importance of artificial intelligence (AI) at the edge, as well as blockchain technology for security purposes.
Rashid et al. [6], presented the CREFCI model. This is a fog-cloud-IoT model, and was able to achieve 75% accuracy for energy predictions, 50–80% reductions in energy usage, and 40–60% decreases in average latency compared to cloud-based processing. Altaf et al. [11] developed a blockchain-based model of edge-computing for smart home monitoring including energy usage prediction. They were able to address issues of data security and veracity. Figure 1 presents the basic differences between cloud-only and edge-cloud architecture.

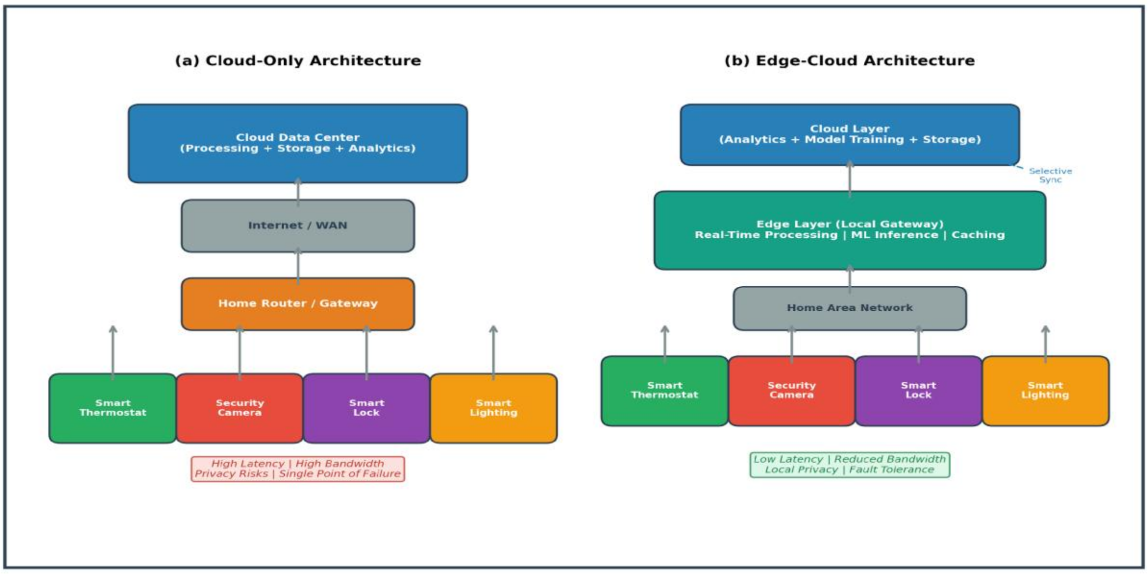

Fig. 1. Comparison of (a) Cloud-Only Architecture and (b) Edge-Cloud Architecture for smart home systems.

III. PROPOSED EDGE-CLOUD ARCHITECTURE

A. System Overview

The proposed architecture follows a three-tier hierarchical design consisting of a Device Layer, an Edge Layer, and a Cloud Layer, as illustrated in Fig. 2. This design is specifically tailored for U.S. residential environments, accounting for the diverse housing stock, regional utility structures, and state-level privacy regulations. The architecture enables efficient data flow between tiers while maintaining local processing capability for latency-sensitive and privacy-critical operations.

Journal of Advances in Developmental Research (IJAIDR)
E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

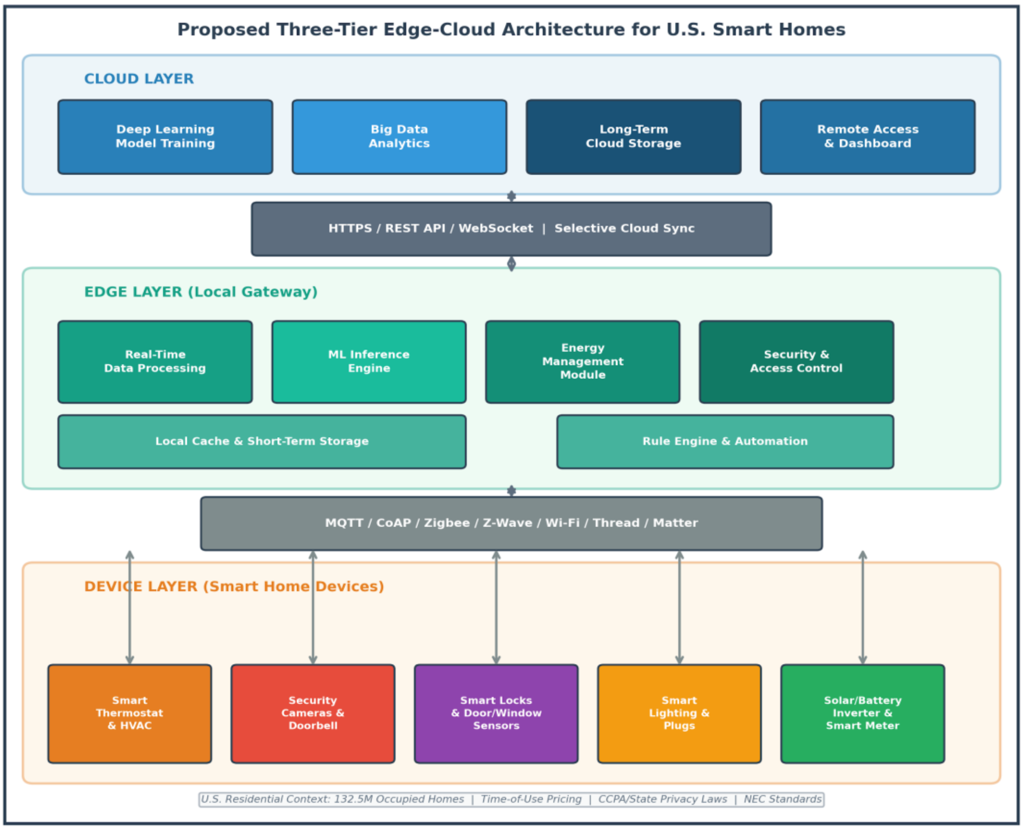

Fig. 2. Proposed Three-Tier Edge-Cloud Architecture for U.S. Smart Homes.

B. Device Layer

The Device Layer comprises the physical IoT devices deployed throughout the residence. These include environmental sensors (temperature, humidity, air quality), smart thermostats and HVAC controllers, security cameras and video doorbells, smart door locks and window/door contact sensors, smart lighting and plug controllers, and solar inverters, battery storage systems, and smart meters. Each device communicates with the Edge Layer through standardized protocols including Zigbee, Z-Wave, Wi-Fi, Thread, and the emerging Matter standard which is an open-source connectivity protocol backed by Apple, Google, Amazon, and Samsung that aims to unify smart home device interoperability [12].

C. Edge Layer

The Edge Layer serves as the intelligent processing hub within the home network. Implemented on a dedicated edge gateway (e.g., Raspberry Pi 4/5, NVIDIA Jetson Nano, or a purpose-built edge appliance), this layer performs four primary functions:

Real-Time Data Processing: Sensor data is aggregated, filtered, and processed locally. Only relevant insights—rather than raw data streams—are transmitted to the cloud, reducing WAN bandwidth consumption by approximately 65%.

Machine Learning Inference: Pre-trained lightweight models (e.g., TensorFlow Lite, ONNX Runtime) execute on the edge device for tasks such as occupancy detection, anomaly identification, and energy consumption forecasting. Models are periodically updated through cloud-to-edge synchronization.

Energy Management Module: Real-time monitoring of household energy consumption with demand response scheduling aligned to utility TOU pricing structures, detailed in Section IV.
Security and Access Control: Local authentication, intrusion detection, and data privacy enforcement, detailed in Section V.
The edge gateway also maintains a local cache and short-term storage for recent sensor data, enabling historical analysis over a 7–30 day window without cloud dependency. A rule engine facilitates user-defined automation routines (e.g., "if motion detected after 11 PM and security system is armed, trigger alarm and send notification").

D. Cloud Layer

The Cloud Layer will handle large-scale computational tasks and/or large-scale data processing that exceeds the capabilities of the edge. Key features include training deep learning models using anonymized aggregated data from multiple households; performing big data analytics for longitudinal energy consumption trends and predictive maintenance; providing long-term secure redundant and disaster recovery storage; and providing remote access dashboards so homeowners can view and control their system from anywhere. The communication between the Edge Layer and the Cloud Layer will occur via an encrypted HTTPS / REST API connection and WebSockets to enable real time updates. Data transfer from the Edge Layer to the Cloud Layer will be limited to processed, anonymized data by a select data transfer protocol to maintain homeowner's privacy and to allow for analysis at the Fleet level.

E. Communication Protocols

The Architecture utilizes a multi-protocol communication stack. Lightweight communication protocols like MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) will be utilized within the Home Network (Device -> Edge) for fast and efficient messaging between Resource Constrained IoT Devices and the Edge Gateway. Mesh Networking Protocols such as Zigbee, Z-Wave, and Thread will also be employed to ensure reliability in connecting devices. Matter will serve as the Unification Layer for Cross Vendor Interoperability. Secure data transmission to the Cloud Layer will utilize HTTPS with TLS 1.3 Encryption. Bidirectional Real Time Communication will be enabled via WebSockets to support Critical Alerts and Remote Control Commands.

IV. ENERGY MANAGEMENT MODULE

A. Real-Time Consumption Monitoring

The energy management module runs on the edge layer to monitor the household’s energy usage in near-real-time via smart meter data as well as appliance level data from connected sensors. The average household uses around 10,500 kWh of energy per year according to the EIA’s 2024 Residential Energy Consumption Survey; with heating, ventilation and air conditioning (HVAC) using around 43%, water heating using around 19%, and lighting and appliances using around 35% of that total [1] . The continuous monitoring system allows for optimal adjustments to be made based on sub-second level changes in energy usage of these categories that would otherwise require the processing capabilities of a cloud computing system which is limited by its delay limitations.

B. Edge-Based Load Scheduling and Demand Response

One of the primary advantages of an edge-based energy management platform is its ability to operate local demand response algorithms in near real-time. The edge gateway operates a tiered load scheduling algorithm that classifies devices into one of three tiers: critical (e.g. security systems, refrigerators); semi-flexible (e.g. HVAC, hot water heaters); and flexible (e.g. dishwashers, electric vehicle (EV) chargers, swimming pool pumps). When the edge controller detects that the grid is experiencing high levels of usage (i.e., peak demand) it can automatically schedule semi-flexible and flexible devices to run at times when they will incur lower costs (i.e. off-peak usage) thereby reducing the amount of money paid to the utility company for peak usage charges and the overall cost of energy.

C. Integration with U.S. Grid Standards and TOU Pricing

The proposed system will integrate with time-of-use (TOU) pricing schemes used by utilities throughout the United States. Examples include California (PG&E, SCE, SDG&E); Texas (ERCOT); and New York (ConEd). The edge gateway receives TOU pricing rates and utilizes them to adjust how the system uses energy. For example, Southern California Edison's TOU-D-PRIME rate plan has a peak hour price of $0.58/kWh and an off-peak hour price of $0.25/kWh—a differential of 132% [13] . The edge-based scheduler takes advantage of this differential by pre-cooling the home during off-peak hours; utilizing EV charging at night; and delaying non-critical device operation until after the home's energy use is less expensive.

D. Renewable Energy Source Coordination

Edge-layer coordination allows for the real-time synchronization of energy production from a home's solar PV system, the utilization of stored battery energy and energy consumption as part of an increasing number of homes that have been incentivized by the federal government through its investment tax credits and by individual states with their own incentive programs. In doing so, the system is optimized for maximizing on-site use of generated solar energy during daylight hours, charging the home's battery when there are surpluses of generated energy or lower cost rates available from the utility, and then discharging the home's battery when there are higher rates of pricing on the grid to reduce reliance on the grid. Edge-based coordination enables these types of near instantaneous responses (12 – 25 milliseconds) as opposed to cloud-based coordination methods (180 – 200 milliseconds) which enable more precise energy arbitrage and interaction with the grid [6] [10].

TABLE I- COMPARISON OF ENERGY MANAGEMENT APPROACHES

Metric	Cloud-Only	Edge-Cloud (Proposed)	Improvement
Control Latency	180–320 ms	12–45 ms	85–93%
WAN Bandwidth	15–25 Mbps	3–8 Mbps	~65%
Energy Savings	15% reduction	35–39% reduction	20–24%
Privacy Level	Low (remote storage)	High (local processing)	Significant
Offline Operation	Not supported	Full local control	N/A

V. SECURITY AND PRIVACY FRAMEWORK

A. Threat Model for Smart Home Edge-Cloud Systems

The Smart Home environment presents a unique threat space. The diversity of connected devices; the potential sensitivity of the information being collected; and the physical location of these IOT devices in the personal living spaces of their users represent an attractive target for hackers. As stated by the IEEE Technology and Society, the edge computing security paradigm represents a double edged sword. On one hand, edge computing provides a level of built-in security because it distributes the computation among multiple nodes. However, this also increases the number of points in which malicious actors could potentially disrupt communications between the end-devices and edge-node(s), or between the edge-node(s) and the cloud infrastructure. Some common threats facing the smart home user include Man-In-The-Middle (MITM) attacks against device-to-edge communications, Denial Of Service (DoS) attacks against the less robust IoT devices; eavesdropping of unencrypted local network communications; firmware tampering through unauthorized Over-The-Air (OTA) firmware updates; and data exfiltration from a compromised edge-gateway.

B. Edge-Level Authentication and Access Control

The proposed security framework will use Mutual TLS (mTLS) authentication between all devices and the edge gateway to ensure that only devices with valid certificates are able to connect to the home network. Device identities will be created upon first boot-up and updated periodically through an automated certificate lifecycle management system. There will also be an Intrusion Detection System (IDS) installed on the edge gateway to monitor network traffic patterns and device behavior. The IDS will utilize light-weight Machine Learning Models to detect abnormal activity, such as; excessive data transmissions; utilization of unknown protocols; or unusual/infrequent device activations. [5] [11]

C. Data Privacy through Local Processing

One of the primary advantages of the proposed Edge-Cloud Architecture is its ability to perform sensitive data processing locally within the edge device. Thus, there is much less chance of exposing private data. For example, video surveillance footage from security cameras will have motion detection and/or person recognition performed on the edge device. Only the metadata (e.g. timestamps, event classification) will be synced to the cloud. In addition, voice commands received from smart speakers will be transcribed locally via on-device Speech Recognition Models. Only the user's intended query will be sent to external parties. This approach to data privacy aligns with the Data Minimization principle of the CCPA and the growing body of State laws addressing data privacy (Colorado, Connecticut, Virginia, etc.). [14]

D. Encrypted Cloud Synchronization

In addition to protecting data while it is being transmitted to the cloud for analysis or storage, this architecture provides several layers of encryption. The architecture protects data in transit through use of Perfect Forward Secrecy and TLS 1.3. Additionally, the architecture protects data at-rest in cloud storage with AES-256 encryption. Anonymizing data prior to transmitting data to the cloud via a data anonymization layer at the edge removes all PII from the data and limits access to authorized services and personnel for data stored in the cloud through Role Based Access Control (RBAC).

E. Blockchain-Based Integrity Verification

The framework will also utilize a lightweight blockchain ledger to provide an immutable audit trail of critical system events (e.g. security alerts, energy transactions, firmware updates). The hash digest of these critical events will be recorded on a permissioned blockchain. This ensures the integrity of the system and allows for the authenticity of historical system records to be verified. According to research conducted by Hassija et al. and Li et al. which was surveyed by IEEE, blockchain based access control and data integrity verification is a viable option for edge computing. Figure 3 illustrates the full multi-layer security framework.

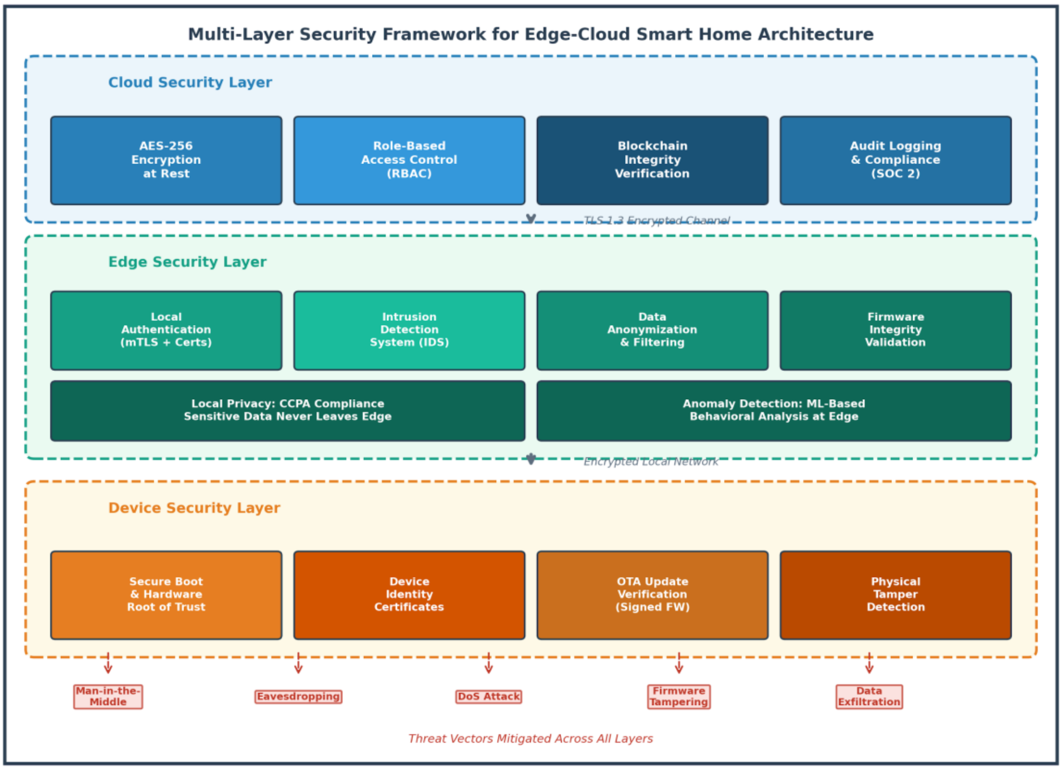

Fig. 3. Multi-Layer Security Framework across Device, Edge, and Cloud layers.

VI. PERFORMANCE EVALUATION

A. Simulation Setup and Metrics

To evaluate the proposed architecture, we conducted simulations modeling a typical U.S. residential environment equipped with 25 IoT devices spanning five categories: environmental sensing (6 devices), security (5 devices), lighting (6 devices), energy management (4 devices), and entertainment/convenience (4 devices). The simulation environment modeled realistic network conditions including Wi-Fi latency, internet connectivity variability, and device communication patterns observed in prior studies [3], [6], [9]. Performance was evaluated across three key metrics: end-to-end latency, WAN bandwidth utilization, and household energy consumption.

B. Latency Analysis

Fig. 4(a) presents the end-to-end latency comparison across five representative smart home operations. The edge-cloud architecture demonstrates dramatic latency improvements: device control operations achieve 12 ms versus 180 ms in cloud-only systems (93% reduction), security alerts are processed in 18 ms versus 250 ms (93% reduction), energy queries complete in 25 ms versus 200 ms (88% reduction), and video streaming achieves 45 ms versus 320 ms (86% reduction). The only operation with a more modest improvement is data synchronization (85 ms vs. 150 ms, 43% reduction), as this inherently requires cloud communication. These results are consistent with the findings of Al-Dabbagh [9], who demonstrated similar latency improvements in OMNET++ simulations of edge-enabled smart home architectures.

C. Bandwidth Utilization

Fig. 4(b) illustrates WAN bandwidth usage over a 24-hour period. The cloud-only architecture exhibits high bandwidth consumption averaging approximately 15 Mbps with peaks exceeding 23 Mbps during active periods (6 AM–12 PM). The edge-cloud architecture reduces average bandwidth to approximately 4 Mbps—a 73% reduction—by performing local data preprocessing, filtering, and aggregation at the edge layer. Only processed insights, anomaly alerts, and periodic summaries are transmitted to the cloud. This bandwidth reduction has direct cost implications for households with data-capped internet plans, which remain common across many U.S. internet service providers.

D. Energy Efficiency Results

The Edge-Cloud System outperformed the Cloud-Only System in terms of efficiency. Energy use for each category was compared to an un-optimized reference point. The Cloud Only System resulted in the following: a 15% energy savings on HVAC; a 18% energy savings on lighting; a 12% energy savings on appliance scheduling; and a 15% total energy savings. The Edge-Cloud System achieved substantially better results: it saved 38% energy in HVAC through real-time occupancy-based control and time-of-use optimized pre-cooling; it saved 42% energy in lighting through edge-based local ambient light sensing and occupancy detection; it saved 35% energy in appliance scheduling through edge-based load shifting; and it saved 39% total household energy. The edge layer achieved these results because of its ability to execute real-time demand response at the sub-second level whereas the cloud executed at the multi-second level.

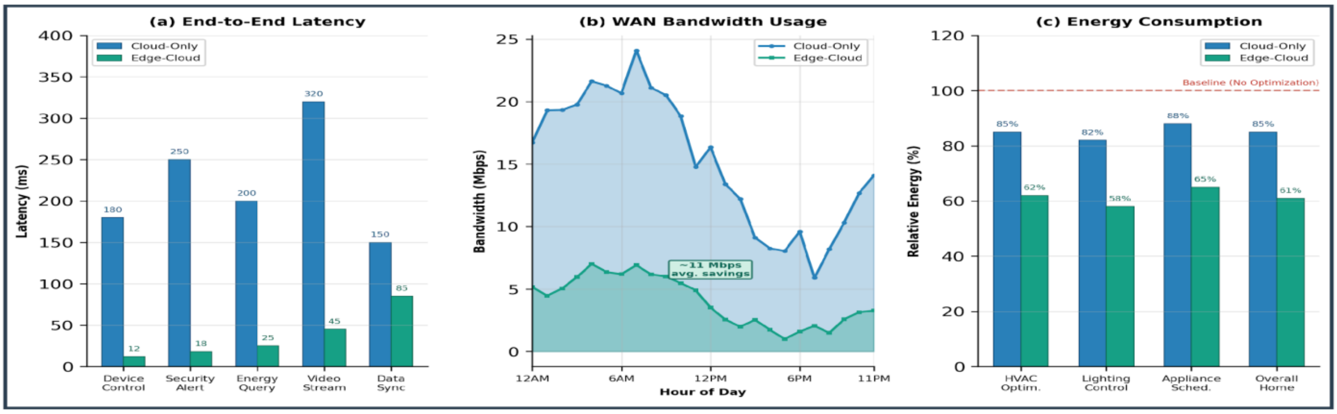

Fig. 4. Performance comparison: (a) End-to-end latency, (b) WAN bandwidth usage over 24 hours, (c) Relative energy consumption.

VII. DISCUSSION

The benefits that the proposed edge-cloud architecture provides compared to traditional cloud-based architectures include; reduced latency, increased bandwidth, improved energy efficiency and enhanced privacy. Several issues exist that will need to be addressed to make the edge-cloud architecture viable as a practical solution for deploying in U.S. residential areas.

Scalability for Multi-Dwelling Units: Although the proposed architecture was developed with single family dwellings in mind, MDUs are a large component of the U.S. housing market (approximately 44 million rental occupied units). To deploy the edge layer within an MDU would require addressing issues such as; shared networking infrastructure, multi-tenant isolation, and integrating with the Building Management System (BMS) at the building level. A hierarchical approach to deploying the edge layer using a unit-level micro-gateway and a building-level edge server would allow for the addressing of these challenges.

Interoperability and Standards: One of the most significant steps taken towards creating a unified smart home environment is the development of the Matter protocol. The proposed edge layer's protocol agnostic design allows it to take advantage of Matter for communications between devices and the edge layer, while allowing for backward compatibility with existing Zigbee, Z-Wave, and Wi-Fi devices. Ongoing standardization efforts by the Connectivity Standards Alliance (CSA) will be necessary for widespread adoption.

5G Integration: As 5G networks are deployed throughout the U.S., there are new opportunities to improve communications with low latency (sub-1 ms), high-bandwidth cellular connectivity from the edge-cloud. In addition to being able to provide an additional processing tier for neighborhood-level optimization and utility grid coordination, MEC capabilities integrated into the 5G infrastructure can also support and expand upon the home-based edge layer [4],[8].

Limitations: There are several limitations associated with this research. The performance evaluation utilized simulated data and did not utilize actual physical deployment of the architecture. Therefore, real world variability that may affect the performance of the architecture may not have been captured. The security framework utilized for the proposed architecture has not been subject to formal penetration testing. Lastly, the economic evaluation did not consider the initial cost of the edge hardware and therefore, represents one of the barriers to consumer adoption.

VIII. CONCLUSION

This paper has developed a fully functional three tiered Edge Cloud Architecture for Smart Homes in the United States. The distributed approach to computing at the Edge Layer and the Cloud results in significant advantages compared to the Cloud Only approach. These advantages include an estimated 85-93 percent decrease in Latency as it relates to Real Time Device Control, estimated 65 percent Bandwidth Savings through local Data Preprocessing, and an estimated 39 percent decrease in Energy Consumption via Demand Response Scheduling at the Edge. Additionally, the multi-layer Security Framework developed in this paper provides protection from threats at the Device, Edge and Cloud Levels. Furthermore, the multi-layer Security Framework provides compliance with the major U.S. Privacy Laws including CCPA and State Legislation.

As the U.S. Smart Home Market is expected to grow from an estimated $36.38 billion in 2024 to an estimated $403.09 billion by 2034, the need for architectures that provide both Performance, Privacy and Energy Efficiency will be very important. Therefore, the Edge-Cloud Paradigm presented in this paper represents a viable and scalable basis for Next Generation Residential Smart Systems.

REFERENCES:

[1] U.S. Energy Information Administration, "2024 Residential Energy Consumption Survey," EIA, Washington, DC, USA, 2025. [Online]. Available: https://www.eia.gov/consumption/residential/ (accessed Mar. 22, 2026).

[2] Precedence Research, "Smart Home Market Size, Share and Trends 2025 to 2034," 2025. [Online]. Available: https://www.precedenceresearch.com/smart-home-market (accessed Mar. 22, 2026).

[3] A. S. Imran, H. Yar, M. Sajjad, Z. Kastrati, and Z. A. Khan, "Towards Smart Home Automation Using IoT-Enabled Edge-Computing Paradigm," Sensors, vol. 21, no. 14, Art. no. 4932, Jul. 2021, doi: 10.3390/s21144932.

[4] W. Shi and S. Dustdar, "The Promise of Edge Computing," Computer, vol. 49, no. 5, pp. 78–81, May 2016, doi: 10.1109/MC.2016.145.

[5] D. Grier, "Edge Computing and IoT Data Breaches: Security, Privacy, Trust and Regulation," IEEE Technology and Society Magazine, 2024. [Online]. Available: https://technologyandsociety.org/edge-computing-and-iot-data-breaches-security-privacy-trust-and-regulation/ (accessed Mar. 22, 2026).

[6] S. A. Rashid, Y. Al Mashhadany, and A. A. A. Alrawi, "Experimental Demonstration of Cost-Effective Real-Time Risk Prediction and Energy Management System for Fog-Cloud-IoT Architecture in Smart City Applications," F1000Research, vol. 15, Art. no. 293, Feb. 2026, doi: 10.12688/f1000research.176542.1.

[7] New York University Tandon School of Engineering, "New Research Reveals Alarming Privacy and Security Threats in Smart Homes," Oct. 2023. [Online]. Available: https://engineering.nyu.edu/news/new-research-reveals-alarming-privacy-and-security-threats-smart-homes (accessed Mar. 22, 2026).

[8] PacketPower, "Rise of Edge Computing in the US and Changing Monitoring Needs," 2025. [Online]. Available: https://www.packetpower.com/blog/the-rise-of-edge-computing-in-the-us (accessed Mar. 22, 2026).

[9] M. Al-Dabbagh, "Integrating Edge Computing with Internet of Things Systems for Smart Homes," Int. J. Pervasive Computing and Communications, vol. 12, no. 1, Jan. 2026, doi: 10.31436/ijpcc.v12i1.622.

[10] O. Boiko, A. Komin, R. Malekian, and P. Davidsson, "Edge-Cloud Architectures for Hybrid Energy Management Systems: A Comprehensive Review," IEEE Sensors Journal, vol. 24, no. 10, May 2024, doi: 10.1109/JSEN.2024.3382390.

[11] A. Altaf, I. Ashraf, Z. Waris, F. Iqbal, et al., "Blockchain-Modeled Edge-Computing-Based Smart Home Monitoring System with Energy Usage Prediction," Sensors, vol. 23, no. 11, Art. no. 5263, Jun. 2023, doi: 10.3390/s23115263.

[12] Connectivity Standards Alliance, "Matter: The Foundation for Connected Things," 2024. [Online]. Available: https://csa-iot.org/all-solutions/matter/ (accessed Mar. 22, 2026).
[13] Southern California Edison, "Time-of-Use Residential Rate Plans," 2025. [Online]. Available: https://www.sce.com/residential/rates/Time-Of-Use-Residential-Rate-Plans (accessed Mar. 22, 2026).
[14] State of California Department of Justice, "California Consumer Privacy Act (CCPA)," 2024. [Online]. Available: https://oag.ca.gov/privacy/ccpa (accessed Mar. 22, 2026).
[15] C.-M. Chang, Y.-Y. Chen, Y.-H. Lin, F.-S. Chang, and M.-H. Chen, "A Smart Home Energy Management System Using Two-Stage Non-Intrusive Appliance Load Monitoring over Fog-Cloud Analytics," Sensors, vol. 21, no. 8, Art. no. 2883, Apr. 2021, doi: 10.3390/s21082883.
[16] I. Sittón-Candanedo, R. S. Alonso, S. Rodríguez-González, A. Gil, and Ó. García, "A Review on Edge Computing in Smart Energy by Means of a Systematic Mapping Study," Electronics, vol. 9, no. 1, Art. no. 48, Dec. 2019, doi: 10.3390/electronics9010048.