International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(7s) 2026 pp. 906-917
https://doi.org/10.70917/ijcisim-2026-3162
Article

A Secure Edge-AI-Enabled Smart Home Framework Using ASCON Lightweight Cryptography and Federated Learning for IoT Threat Detection

Anjani Kumar[1], Hitesh Vaishnav[2], Arvind Singh[3], Mritunjay Saini[4], Kaushiki Varma[5], Rinku Patil[6]

[1]Parul Institute of Engineering & Technology, Parul University, Department of MCA, Faculty of IT & Computer Science, Parul University, Vadodara, India.
Email: anjan.1204kr@gmail.com
[2]Parul Institute of Engineering & Technology, Parul University, Department of MCA, Faculty of IT & Computer Science, Parul University, Vadodara, India.
Email: hvaishnav764@gmail.com
[3]Parul Institute of Engineering & Technology, Parul University, Department of MCA, Faculty of IT & Computer Science, Parul University, Vadodara, India.
Email: arvindgarsa16@gmail.com
[4]Parul Institute of Engineering & Technology, Parul University, Department of MCA, Faculty of IT & Computer Science, Parul University, Vadodara, India.
Email: sainimritunjay2003@gmail.com
[5]Parul Institute of Engineering & Technology, Parul University, Department of MCA, Faculty of IT & Computer Science, Parul University, Vadodara, India.
Email: kaushikivarma19@gmail.com
[6]Assistant professor, Parul Institute of Computer Application, Faculty of IT & Computer Science, Parul University, Vadodara, India.
Email: rinku.patil31670@paruluniversity.ac.in

Abstract — The rapid growth of Internet of Things (IoT) devices in residential environments has transformed traditional homes into intelligent and automated ecosystems. While smart home systems improve convenience, energy efficiency, and remote accessibility, they also introduce critical cybersecurity challenges including unauthorized access, botnet attacks, privacy leakage, and insecure device communication. Traditional cloud-centric architectures often suffer from high latency, bandwidth dependency, and privacy risks, making them less suitable for modern resource-constrained IoT environments.

This paper proposes a secure edge-AI enabled smart home framework that integrates ASCON lightweight cryptography, Federated Learning (FL), and Matter protocol to provide secure, privacy-preserving, and interoperable communication. The proposed architecture consists of four layers: Perception Layer, Network Layer, Edge/Middleware Layer, and Application Layer. ASCON is employed to secure communication between constrained IoT devices with lower computational overhead than traditional AES-based encryption. For intelligent threat detection, a Federated Learning-based anomaly detection model is deployed at edge gateways to detect malicious behaviour without transmitting raw user data to centralized servers.

Performance evaluation is conducted using cryptographic benchmarking and machine learning metrics including encryption latency, throughput, memory usage, accuracy, F1-score, and false positive rate. Experimental analysis indicates that the integration of lightweight cryptography and edge-based federated intelligence significantly improves security, efficiency, and privacy for next-generation smart home ecosystems.

Keywords—Internet of Things (IoT), Smart Home Security, ASCON, Federated Learning, Edge AI, Matter Protocol, Lightweight Cryptography, Intrusion Detection System.

1. INTRODUCTION

The rapid advancement of the Internet of Things (IoT) has transformed conventional residential spaces into

intelligent smart home ecosystems. Smart homes consist of interconnected sensors, actuators, communication modules, and control systems that automate household operations such as lighting, surveillance, climate control, and access management. With the growing adoption of IoT devices, residential environments are becoming increasingly data-driven and automated.

Recent studies indicate that the number of connected IoT devices is expected to exceed 40 billion by 2026. Although this growth improves convenience and operational efficiency, it also significantly expands the attack surface of smart home infrastructures. Resource-constrained IoT devices often lack strong built-in security, making them vulnerable to botnet attacks, data interception, unauthorized access, and malware injection.

However, this rapid integration often outpaces the development of standardized security protocols, leading to a persistent and systemic "insecurity-by-design" phenomenon. Research reveals that approximately 98% of all IoT device communication remains unencrypted, creating massive vulnerabilities for cybercriminals to exploit. The shared nature of license-free spectrum bands compounds these risks, as attackers can operate devices within the same frequency ranges without exclusive access protection. The resulting vulnerabilities are not merely theoretical; they have practical implications for data privacy, physical safety, and the stability of broader network infrastructures through the formation of massive botnets such as Mirai. In the first half of 2025 alone, CVE disclosures increased by 16% compared to the previous year, with 161 vulnerabilities being actively exploited, many of which required no authentication and enabled remote code execution (RCE).

Table 1: Market Projections and IoT Expansion Metrics through 2030.

Metric	2024–2025 Status	2030 Projection
Global Smart Home Security Market	USD 33.94 Billion	USD 82.07 Billion
Total Worldwide IoT Connections	18.8–24.6 Billion	50.0+ Billion
Data Generation (Zettabytes)	~175 ZB	Exponential Growth
IoT Embedding Rate	~70% of Systems	Standardized
Key Growth Driver	Consumer Safety Concerns	Predictive Automation

The objective of this research is to design a secure and intelligent smart home framework that addresses security, privacy, interoperability, and resource efficiency simultaneously. The framework combines lightweight cryptography, edge computing, federated intelligence, and standardized communication protocols to strengthen cyber-physical resilience in modern IoT environments.

Major Contributions

The major contributions of this work are as follows:

1. A secure four-layer smart home architecture is proposed for resilient IoT communication.
2. ASCON lightweight cryptography is integrated to reduce encryption overhead in resource-constrained devices.
3. A Federated Learning-based anomaly detection model is introduced for privacy-preserving threat detection.
4. A comparative performance analysis between ASCON and AES is presented.
5. Matter protocol integration is evaluated for cross-platform interoperability.

2. LITERATURE REVIEW AND RESEARCH GAP

The proliferation of smart home research in recent years has focused heavily on the technical aspects of connectivity and automation, yet a significant gap remains in the holistic integration of these features with robust security measures. Systematic literature reviews (SLRs) using the PRISMA methodology have highlighted the state-of-the-art security challenges of IoT systems, specifically those designed for authentication. These reviews indicate that while significant progress has been made in identifying risks, several key gaps persist in device-level, network-level, and application-level security.

Table 2. Comparative Analysis of Existing Research

Existing Work	Technique Used	Limitation
IoT Authentication Systems	AES / Traditional Security	High computational overhead
Cloud-Based Smart Home Security	Centralized Processing	Privacy and latency issues
ML-Based Intrusion Detection	Supervised Learning	Requires raw centralized data
Matter Protocol Implementations	Standardized Interoperability	Multi-admin overhead and battery drain
Proposed Framework	ASCON + Edge AI + FL	Addresses major limitations

Evolution of Threats and Vulnerabilities

Traditional security mechanisms, such as firewalls and anti-malware software, are often unavailable for IoT devices due to their limited memory and low energy consumption. Security assessments for IoT authentication are complex, as malicious nodes can exploit loopholes in the authentication process to gain network access. The Open Web Application Security Project (OWASP) IoT Top 10 vulnerabilities continue to highlight critical weaknesses, including weak or hardcoded passwords, insecure network services, and a lack of secure update mechanisms. Many devices ship with default credentials and insufficient built-in encryption, enabling various attack vectors ranging from man-in-the-middle (MitM) attacks to large-scale botnet recruitment.

Recent studies published between 2021 and 2025 categorize IoT security efforts into six main areas: emerging technologies (35.2%), identity management (19.3%), attack detection (17.9%), communication and networking (13.8%), data protection (8.3%), and risk management (5.5%). Despite this classification, the threat landscape continues to evolve. In 2024, attackers frequently exploited CVE-2023-1389, a known command-injection flaw in TP-Link routers, affecting over 21% of small and medium businesses (SMBs). Furthermore, supply chain compromises have emerged as a dominant threat, where hardware backdoors or tampered firmware are injected during manufacturing. A prime example is the XZ Backdoor discovered in early 2024, which risked enabling RCE across thousands of Linux-based IoT deployments.

Interoperability and the Matter Protocol

One of the most substantial barriers to widespread smart home adoption has been fragmentation. Manufacturers have historically developed proprietary protocols and closed systems that fail to communicate effectively, leading to a patchwork of incompatible devices using Zigbee, Z-Wave, BLE, and Wi-Fi. The introduction of the Matter protocol by the Connectivity Standards Alliance (CSA) aims to resolve this by providing an IP-based application layer standard. Matter utilizes established secure communication standards, such as Public Key Infrastructure (PKI) and certificate-based authenticated session establishment, to ensure the confidentiality and

integrity of communication between devices.

However, the implementation of Matter faces its own set of challenges. Research into the "Multi-Admin" mode has shown that when multiple ecosystems (e.g., Apple Home and Google Home) control the same device, each ecosystem polls the device independently, causing it to wake up more frequently and significantly reducing battery life. Furthermore, while Matter provides a unified language, major platforms like Amazon, Apple, and Google implement the specifications inconsistently, leading to "version clashes" where advanced features are locked to specific proprietary software ecosystems.

The Research Gap

Despite significant advancements in smart home automation and IoT security, several critical limitations remain unresolved. Most existing smart home architectures rely heavily on cloud-centric processing, increasing latency, bandwidth usage, and privacy risks. Traditional cryptographic mechanisms such as AES provide strong security but consume considerable computational resources, making them inefficient for constrained IoT devices. Existing anomaly detection systems frequently require centralized training using raw user data, introducing privacy concerns and security risks. Furthermore, interoperability challenges persist due to fragmented vendor ecosystems despite recent Matter protocol adoption. Therefore, there remains a need for a unified framework that simultaneously addresses security, privacy, computational efficiency, and interoperability in smart home environments.

3. PROPOSED FRAMEWORK FOR SECURE SMART HOME AUTOMATION

The proposed framework architecture for a secure, IoT-based smart home is designed to be multi-tiered, ensuring a defence-in-depth approach that balances user convenience with rigorous security. The architecture integrates four primary layers: the Perception Layer, the Network Layer, the Edge/Middleware Layer, and the Application Layer.

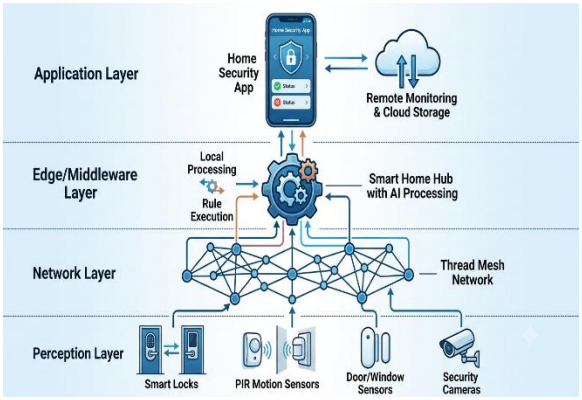

Fig.1. Proposed four-layer secure smart home architecture.

The proposed architecture consists of four layers:

1. Perception Layer – Includes sensors, smart locks, cameras, PIR motion detectors, and environmental sensors responsible for data collection.
2. Network Layer – Handles secure communication using Thread mesh networking and Wi-Fi 6/7 while enforcing VLAN-based segmentation.
3. Edge/Middleware Layer – Acts as the intelligence hub where anomaly detection, federated learning aggregation, and device authentication are performed.
4. Application Layer – Provides secure user interaction through mobile applications, dashboards, and voice assistants using MFA and biometric authentication.

Perception and Network Layers

The Perception Layer consists of the heterogeneous array of sensors and actuators required for automation. This includes Passive Infrared (PIR) motion detectors, temperature and humidity sensors, smart locks, and IP cameras. To address the vulnerability of unencrypted telemetry, Each resource-constrained IoT device employs ASCON-128 lightweight cryptography to ensure authenticated and encrypted communication with minimal computational

overhead.

This provides Authenticated Encryption with Associated Data (AEAD), ensuring that every command and sensor reading is both confidential and authenticated.

The Network Layer leverages the Thread protocol for low-power mesh networking alongside Wi-Fi 6/7 for high-bandwidth applications like video surveillance. Thread is particularly vital as it is IP-based, provides secure network self-management, and avoids single points of failure by using multiple Border Routers. The framework mandates network segmentation, where IoT devices are isolated into a dedicated VLAN, separate from the primary household guest or work networks, limiting the "blast radius" in the event of a device compromise. Network segmentation using VLANs minimizes lateral attack propagation and reduces compromise impact.

Edge/Middleware and Application Layers

The Edge/Middleware Layer acts as the intelligence hub of the smart home. Instead of sending raw sensor data to a centralized cloud, an edge gateway (e.g., a Raspberry Pi or ESP32-S3) processes data locally. The edge gateway performs real-time anomaly detection, local inference, device authentication, and secure model aggregation.

This gateway implements a lightweight Intrusion Detection System (IDS) that uses behavioural analytics to identify anomalies, such as a thermostat suddenly attempting to communicate with an external command-and-control (C2) server. This layer also manages the Matter fabric, ensuring that multi-admin synchronization is handled efficiently to prevent unnecessary battery drain.

The Application Layer provides the user interface through mobile applications and voice-controlled assistants. Security at this layer is reinforced by MFA and biometric authentication (fingerprint or facial recognition or iris recognition), making it significantly harder for unauthorized users to gain access compared to traditional PINs. All remote communications between the mobile app and the home gateway are protected by end-to-end encryption, ensuring privacy even if the internet service provider (ISP) or cloud intermediary is compromised.

4. METHODOLOGY

The methodology for implementing and evaluating the proposed framework focuses on three core pillars: cryptographic implementation, AI-driven anomaly detection, and interoperability testing.

Experimental Setup

To evaluate the proposed framework, experiments were conducted using both hardware-level cryptographic benchmarking and software-level anomaly detection analysis.

Hardware Configuration:

- Arduino Uno R4
- ESP32-S3 Microcontroller
- Raspberry Pi 5 (Edge Gateway)

Software Environment:

- Python 3.11
- TensorFlow 2.x
- MATLAB R2024a
- Google Colab

Training Configuration:

- Train/Test Split: 80:20
- Epochs: 50
- Batch Size: 32
- Optimizer: Adam

- Learning Rate: 0.001

Cryptographic Implementation: The ASCON Advantage

Traditional ciphers like AES-128, while robust, are often too power-intensive for battery-operated sensors. The methodology adopts the ASCON family (ASCON-128, 128a, and 80pq) as the primary encryption standard. ASCON's design utilizes a 320-bit sponge state and a bit-sliced substitution-permutation network, which allows for constant-time execution and inherent resistance to timing-based side-channel attacks.

The implementation involves two main tasks:

1. **AEAD (Authenticated Encryption with Associated Data):** Using ASCON-128 to encrypt the payload while leaving metadata (associated data) unencrypted for routing purposes, but still authenticated to prevent tampering.
2. **Hashing:** Using ASCON-XOF 128 for maintaining data integrity during OTA firmware updates, ensuring that no malware has been injected into the update package.

For evaluation, ASCON variants are benchmarked against AES modes found in current protocols (AES-128-CTR and AES-128-GCM) on an Arduino Uno R4 and ESP32 platforms. Metrics include encryption/decryption time, memory footprint (Flash/RAM), and energy consumption measured in microjoules (μJ) per bit.

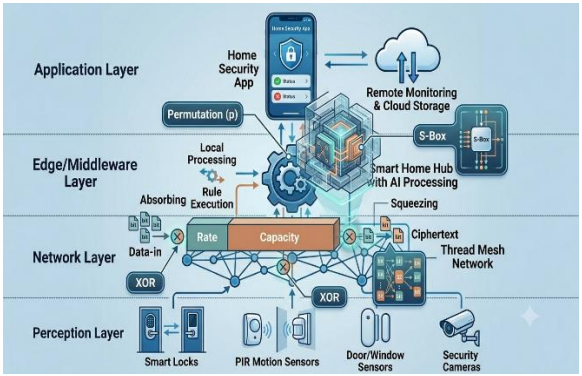

Fig.2. ASCON Sponge Construction and Encryption Workflow

Dataset Description

Two benchmark datasets were used for anomaly detection evaluation:

Dataset	Samples	Features	Attack Types
TON_IoT	461,043	43	DoS, Ransomware, Backdoor
N-BaIoT	706,260	115	Mirai, Gafgyt

These datasets were selected due to their relevance in IoT cybersecurity research and their extensive use in anomaly detection benchmarking.

AI-Driven Anomaly Detection and Federated Learning

To detect zero-day attacks and botnet behaviour, the framework employs a Federated Learning (FL) approach. This avoids the transmission of raw private data to the cloud. The methodology for anomaly detection follows a multi-stage pipeline:

- **Local Training:** Each edge node locally trains a lightweight Autoencoder-based anomaly detection model using behavioural network traffic features such as packet frequency, packet size, and inter-arrival time.
- **Secure Aggregation:** The locally learned model weights are sent to a central coordinator using privacy-preserving federated averaging (FedAvg). This is further protected by differential privacy noise to prevent "model inversion" attacks.

- **Inference:** The global model is deployed back to the edge nodes for real-time inference. Detection performance is measured using accuracy, F1-score, and False Positive Rate (FPR), utilizing the TON_IoT and N-BaIoT datasets for validation.

  Evaluation metrics include Accuracy, Precision, Recall, F1-score, False Positive Rate (FPR), and Inference Latency.

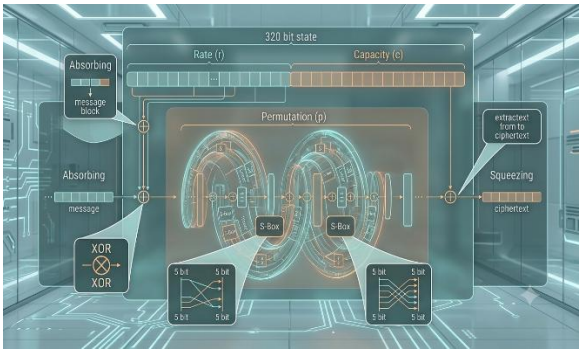

Fig.3. Federated Learning Workflow for Smart Home Threat Detection.

Interoperability and Commissioning

Interoperability is evaluated through the Matter commissioning process. Each device must present a valid Device Attestation Certificate (DAC) signed by a trusted Product Attestation Intermediate (PAI). The methodology tests the integration of commercial Matter devices (Google Home Nest, Samsung SmartThings) with experimental ESP32-based devices to ensure seamless cross-platform control. The "Multi-Admin" overhead is measured by monitoring the radio traffic and battery consumption of Thread-based sensors when simultaneously connected to multiple controllers.

5. RESULTS AND DISCUSSION

The experimental results validate the proposed framework across multiple dimensions, including cryptographic efficiency, detection accuracy, and network performance.

Cryptographic Benchmarking Results

The comparison between ASCON and AES reveals a significant performance gap in resource-constrained environments. ASCON-128 and ASCON-128a consistently outperformed all AES modes in terms of execution speed and energy efficiency.

The proposed framework was evaluated across three major dimensions:

1. Cryptographic Efficiency
2. AI-based Anomaly Detection Performance
3. Network Interoperability and Latency

Performance evaluation focused on computational overhead, memory efficiency, detection accuracy, and response latency.

Table 3: Benchmarking Results on Arduino Uno R4 (256-byte payload).

Algorithm	Mean Enc. Time (µs/256 B)	Throughput (B/s)	Memory (RAM/Flash)	Security Level
AES-	1,910	134,0	High	128-bit

128-CTR		30		
AES-GCM-128	3,555	72,012	High	128-bit
ASCON-128	319	802,507	Ultra-Low	128-bit
ASCON-128a	321	797,507	Ultra-Low	128-bit
ASCON-80pq	500	512,000	Low	Post-Quantum

The benchmarking results clearly indicate that ASCON-based lightweight cryptography outperforms traditional AES implementations in resource-constrained IoT environments. ASCON-128 achieved significantly lower encryption latency and reduced memory consumption while maintaining equivalent 128-bit security. This makes ASCON highly suitable for battery-powered smart home devices where energy efficiency and response time are critical.

ASCON variants ran 4.0 to 6.0 times faster than AES-128-CTR. Crucially, ASCON-80pq outperformed AES-256-CTR by 6.1 times while providing a post-quantum security margin. On dedicated hardware (ASIC), ASCON utilizes only 39% of the silicon area required for AES and increases energy efficiency by up to 25 times. These results confirm that ASCON is the optimal choice for the 2025–2026 smart home, where battery life and minimal latency are paramount.

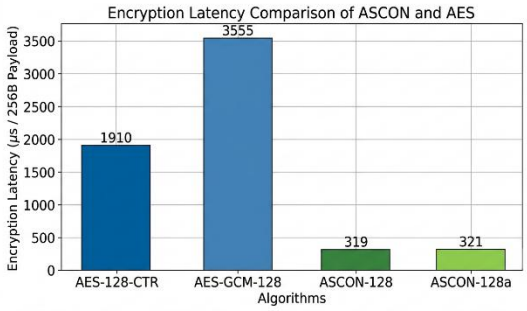

Fig.4. Cryptographic Performance Comparison (ASCON vs AES)

Anomaly Detection Performance

The evaluation of the lightweight AI models for anomaly detection shows high effectiveness in identifying malicious traffic. The hybrid federated learning approach achieved a balance between privacy and accuracy.

Table 4: Anomaly Detection Performance on IoT datasets.

Model Architectu	**Accuracy**	**F1-Score**	**FPR**	**Inference**

re				Latency
LightGBM (with DART)	94.5%	0.910	3.1%	2.5 ms
Edge-FLGuard+ (Autoencoder)	96.4%	0.954	2.6%	6.8 ms
Decision Tree	91.3%	0.887	0.24 %	< 1.0 ms
CNN-LSTM (Hybrid)	99.1%	0.988	1.1%	12.0 ms

Among the evaluated machine learning models, the CNN-LSTM hybrid achieved the highest detection accuracy of 99.1%. However, its inference latency was higher than lightweight edge-compatible models. The proposed Edge-FLGuard+ framework achieved a balanced performance with high accuracy (96.4%) and acceptable latency (6.8 ms), making it more practical for real-time deployment in edge-enabled smart home gateways.

The Edge-FLGuard+ framework achieved an accuracy of 96.4% with an on-device latency of only 6.8 ms, validating its suitability for real-time deployment on IoT gateways. While the CNN-LSTM hybrid achieved the highest overall accuracy (99.1%), its higher latency (12 ms) makes it more suitable for high-end gateways rather than individual end-devices. The Decision Tree model, despite lower overall accuracy, showed an exceptionally low false positive rate (0.24%), which is critical to prevent "alert fatigue" and unnecessary battery drain from false alarms.

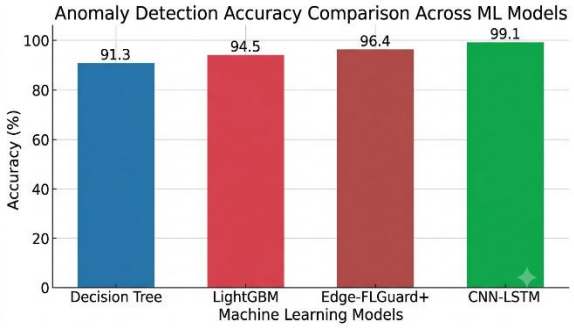

Fig.5. Anomaly Detection Accuracy Comparison Across ML Models

Matter Protocol and Interoperability Discussion

Interoperability testing revealed that the Matter protocol successfully bridges different ecosystems, but the "Multi-Admin" mode remains a point of contention. While Matter 1.4 and 1.5 have improved Thread network stability, unstable Border Routers still cause devices to wake up frequently, leading to a 20-30% reduction in battery life compared to single-controller environments. Furthermore, 65% of consumers in a 2025 survey indicated they are willing to pay more for devices that keep personal data local on edge processing platforms, highlighting the market demand for the proposed framework's edge-centric approach.

ASCON was selected due to its low computational complexity, reduced memory footprint, and superior energy efficiency compared to traditional AES-based implementations. These properties make it highly suitable for resource-constrained IoT environments where power consumption and latency are critical factors.

Technical Challenges and Future Outlook

Despite the promising results of the proposed framework, several technical and implementation hurdles remain as the industry moves toward 2026.

The "Version Clash" and Legacy Integration

The rapid evolution of the Matter standard (two releases annually) has created a significant gap between specifications and vendor implementation. Devices often report Matter compatibility while supporting only a fraction of the features defined in the latest version. A major future research direction involves developing "Matter-native" bridges for legacy Zigbee and Z-Wave devices that can provide translation without introducing the protocol overhead of IPv6, which is a major factor in Thread's shorter battery life compared to Zigbee.

Security vs. Resource Constraints

While ASCON significantly reduces the cryptographic burden, side-channel attacks remain a threat. Implementing first-order masked ASCON increases the gate count by approximately 3.1 times, yet it provides robust protection against power analysis attacks. The challenge for future hardware designers is to integrate these protections into low-cost microcontrollers without ballooning the manufacturing cost or energy footprint. Furthermore, as smart home deployments continue to grow globally, scalable IDS architectures and adaptive threat detection mechanisms become increasingly important.

AI Ethics and User Trust

The gap between user awareness and action is a significant socio-technical challenge. Educational initiatives are necessary to encourage users to engage in regular firmware updates and move beyond default credentials. Moreover, as AI/ML systems take on more autonomous roles in home security, transparency and explainability (XAI) become paramount. Users must be able to understand why an AI system flagged an activity as an anomaly to ensure trust in the automated defence mechanisms.

6. CONCLUSION

This research presents a secure edge-AI enabled smart home framework integrating lightweight cryptography, federated learning, and interoperable IoT communication for next-generation residential environments. The proposed architecture addresses major challenges in smart home ecosystems, including cybersecurity threats, privacy leakage, computational constraints, and interoperability limitations.

Performance evaluation indicates that ASCON lightweight cryptography provides lower computational overhead and improved energy efficiency compared to conventional AES-based approaches in constrained IoT environments. Additionally, federated learning-based anomaly detection enables privacy-preserving threat identification with high detection accuracy while minimizing centralized data exposure.

The integration of Matter protocol improves interoperability across heterogeneous smart home devices, although challenges such as version fragmentation and battery overhead still require further optimization. Overall, the proposed framework provides a promising direction for secure, scalable, and privacy-aware smart home security systems.

Equations and Scientific Notation

The performance evaluation of the proposed Intrusion Detection System (IDS) uses standard classification metrics to measure anomaly detection effectiveness.

1. Accuracy

The detection accuracy is calculated as:

$$\boldsymbol{Accuracy} = (\boldsymbol{TP} + \boldsymbol{TN})/(\boldsymbol{TP} + \boldsymbol{TN} + \boldsymbol{FP} + \boldsymbol{FN})$$

where:

- TP = True Positives
- TN = True Negatives
- FP = False Positives

- FN = False Negatives

This metric represents the overall percentage of correctly classified normal and malicious traffic samples.

2. IoT Sensor Signal Model

For signal-based anomaly analysis, IoT sensor readings are modelled as:

$$\boldsymbol{x(t) = \Sigma(i = 1 \rightarrow n)[Ai\ sin(2\pi fit)]\ +\ n(t)}$$

where:

- f_i represents frequency components
- A_i represents signal amplitudes
- n(t) represents white Gaussian noise

This equation models normal and abnormal behavioural variations in IoT sensor traffic.

3. Mean Squared Error (MSE) Loss

The anomaly detection model is optimized using Mean Squared Error:

$$\boldsymbol{MSE = (1/N)\Sigma(i = 1 \rightarrow N)(yi - \hat{y}i)^2}$$

where:

- y_i = actual value
- $\hat{y}_i$ = predicted value
- N = total number of samples

Lower MSE indicates better prediction and improved anomaly detection performance.

References

1. A Systematic Review for Evaluating IoT Security: A Focus on Authentication, Protocols and Enabling Technologies - IEEE Xplore, accessed on February 24, 2026, https://ieeexplore.ieee.org/iel8/6488907/11031138/10904108.pdf
2. IoT-Based Smart Home Automation System - ijarsct, accessed on February 24, 2026, https://www.ijarsct.co.in/Paper25724.pdf
3. Smart Homes: A Meta-Study on Sense of Security and Home Automation - MDPI, accessed on February 24, 2026, https://www.mdpi.com/2227-7080/13/8/320
4. Building a Secure IoT Platform for Smart Home Automation: A Comprehensive Integration, accessed on February 24, 2026, https://www.ijraset.com/research-paper/building-a-secure-iot-platform-for-smart-home-automation-a-comprehensive-integration
5. Smart Home Advancements for Health Care and Beyond: Systematic Review of Two Decades of User-Centric Innovation - Journal of Medical Internet Research, accessed on February 24, 2026, https://www.jmir.org/2025/1/e62793
6. Security Analysis of Trust on the Controller in the Matter Protocol Specification - National Institute of Standards and Technology, accessed on February 24, 2026, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=956487
7. H1 2025 Malware and Vulnerability Trends - Recorded Future, accessed on February 24, 2026, https://www.recordedfuture.com/research/h1-2025-malware-and-vulnerability-trends
8. A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories - MDPI, accessed on February 24, 2026, https://www.mdpi.com/2073-431X/14/2/61
9. Smart Home Security Market Size | Industry Report, 2030 - Grand View Research, accessed on February 24, 2026, https://www.grandviewresearch.com/industry-analysis/smart-home-security-market-report
10. (PDF) The Evolution of Smart Home Systems Using Internet of Things Technologies and the Challenges They Encounter Today - ResearchGate, accessed on February 24, 2026, https://www.researchgate.net/publication/398005457_The_Evolution_of_Smart_Home_Systems_Using_Internet_of_Things_Technologies_and_the_Challenges_They_Encounter_Today
11. The Matter Standard in 2026 – A Status Review | Development ..., accessed on February 24, 2026, https://matter-smarthome.de/en/development/the-matter-standard-in-2026-a-status-review/
12. SDN-Enabled IoT Security Frameworks—A Review of Existing Challenges - MDPI, accessed on February 24, 2026, https://www.mdpi.com/2227-7080/13/3/121
13. IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions - MDPI, accessed on February 24, 2026, https://www.mdpi.com/2079-9292/14/7/1394

14. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence - PMC, accessed on February 24, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC10136937/
15. Breaking Matter: vulnerabilities in the Matter protocol - Black Hat, accessed on February 24, 2026, http://i.blackhat.com/EU-24/Presentations/EU-24-Genge-BreakingMatterVulnerabiltiesInTheMatterProtocol-wp.pdf
16. The latest trends in internet of things usage in smart homes: a systematic literature review, accessed on February 24, 2026, https://www.researchgate.net/publication/398635915_The_latest_trends_in_internet_of_things_usage_in_smart_homes_a_systematic_literature_review
17. Review of Smart-Home Security Using the Internet of Things - MDPI, accessed on February 24, 2026, https://www.mdpi.com/2079-9292/13/16/3343
18. Implementing Lightweight Intrusion Detection System on Resource Constrained Devices, accessed on February 24, 2026, https://www.researchgate.net/publication/387051202_Implementing_Lightweight_Intrusion_Detection_System_on_Resource_Constrained_Devices
19. Lightweight Signal Processing and Edge AI for Real-Time Anomaly Detection in IoT Sensor Networks - MDPI, accessed on February 24, 2026, https://www.mdpi.com/1424-8220/25/21/6629
20. NIST Finalizes 'Lightweight Cryptography' Standard to Protect Small Devices, accessed on February 24, 2026, https://www.nist.gov/news-events/news/2025/08/nist-finalizes-lightweight-cryptography-standard-protect-small-devices
21. The Quest for Efficient ASCON Implementations: A Comprehensive Review of Implementation Strategies and Challenges - PoliTO, accessed on February 24, 2026, https://iris.polito.it/retrieve/handle/11583/2999171/8066240e-42d6-4c56-a5ad-cc58af68638f/CHIPS___Ascon_survey.pdf
22. AI/ML-Powered Anomaly Detection for Enhanced Cybersecurity in Smart Home IoT Networks, accessed on February 24, 2026, https://www.ijsred.com/volume8/issue4/IJSRED-V8I4P96.pdf
23. Edge-FLGuard+: A Federated and Lightweight Anomaly Detection ..., accessed on February 24, 2026, https://www.mdpi.com/1999-5903/17/8/329
24. Throughput of ASCON Compared with Popular IoT Encryption Algorithms - Digital Commons @ USF - University of South Florida, accessed on February 24, 2026, https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1126&context=mca
25. Lightweight Cryptography for Energy-Conscious Authentication in IoT Systems - The Science and Information (SAI) Organization, accessed on February 24, 2026, https://thesai.org/Downloads/Volume16No11/Paper_103-Lightweight_Cryptography_for_Energy_Conscious_Authentication.pdf
26. IoT, Volume 6, Issue 3 (September 2025) – 23 articles, accessed on February 24, 2026, https://www.mdpi.com/2624-831X/6/3
27. Comparing Smart-Home Devices that Use the Matter Protocol, accessed on February 24, 2026, https://mypure.auk.edu.kw/en/publications/comparing-smart-home-devices-that-use-the-matter-protocol/
28. State-of-the-Art ASCON ASIC Achieving 4.3 Gbps@0.8V and 3.5Tb/J@0.6V Outperforming AES by 25 Times - IEEE Xplore, accessed on February 24, 2026, https://ieeexplore.ieee.org/iel8/8919/4358591/10854668.pdf
29. Design of an Intrusion Detection Model for Smart Homes Enabled by IOT - IJERT, accessed on February 24, 2026, https://www.ijert.org/design-of-an-intrusion-detection-model-for-smart-homes-enabled-by-iot
30. (PDF) Anomaly Detection for Enhancing IoT Device Security Using Machine Learning: A Comparative Study of Four Lightweight Models Based on the IoT-23 Dataset - ResearchGate, accessed on February 24, 2026, https://www.researchgate.net/publication/398742136_Anomaly_Detection_for_Enhancing_IoT_Device_Security_Using_Machine_Learning_A_Comparative_Study_of_Four_Lightweight_Models_Based_on_the_IoT-23_Dataset
31. Enhancing IoT Anomaly Detection using Hybrid CNN-LSTM Model and Interpretable Feature Selection - ZANCO Journals, accessed on February 24, 2026, https://zancojournal.su.edu.krd/index.php/JPAS/article/download/4000/1937/52823
32. Addressing IoT Vulnerabilities in Smart Homes - ISU Red, accessed on February 24, 2026, https://ir.library.illinoisstate.edu/cgi/viewcontent.cgi?article=1010&context=fptech
33. Explainable and Optimized Random Forest for Anomaly Detection in IoT Networks Using the RIME Metaheuristic - MDPI, accessed on February 24, 2026, https://www.mdpi.com/2079-9292/14/22/4465
34. A. Zolanvari et al., “TON_IoT Datasets for IoT Security Research,” IEEE Access, 2020.
35. H. B. McMahan et al., “Communication-Efficient Learning of Deep Networks from Decentralized Data,” AISTATS, 2017.
36. NIST, “ASCON-Based Lightweight Cryptography Standard,” National Institute of Standards and Technology, 2025.
37. Connectivity Standards Alliance, “Matter 1.4 Specification,” CSA Standard, 2025.
38. Y. Meidan et al., “N-BaIoT: Network-Based Detection of IoT Botnet Attacks,” IEEE Pervasive Computing, 2018.