Adaptive Multi-Layer Encryption for Enhancing Security in Smart Home IoT Ecosystems

Dancan Obuya Machuki[1], Kennedy Ronoh[2]
Research Scholar, School of Computing and Engineering, Strathmore University, Nairobi, Kenya[1]
Senior Lecturer, School of Computing and Engineering Sciences, Strathmore University, Nairobi, Kenya[2]

***Abstract*—The proliferation of Internet of Things (IoT) devices in smart home environments has introduced significant security challenges, largely due to device heterogeneity, constrained computational resources, and limited native support for robust encryption mechanisms. This study presents an Adaptive Multi-Layer Encryption (AMLE) model designed to enhance security across the device, network, and cloud layers of smart home IoT ecosystems. The proposed model integrates lightweight encryption mechanisms at the device layer, machine learning-based anomaly detection at the network layer, and strong cryptographic protection combined with Attribute-Based Access Control (ABAC) at the cloud layer. Evaluation was conducted in a controlled, simulated environment to assess functional correctness, security behavior under representative threat scenarios, and system performance. Results demonstrate that the AMLE framework is capable of detecting and responding to simulated unauthorized access attempts, anomalous traffic patterns associated with botnet-like behavior, and data exfiltration scenarios, while maintaining operational performance suitable for typical smart home use cases. The Isolation Forest algorithm, configured with a contamination threshold of 0.05, successfully identified deviations from baseline traffic behavior and triggered policy-driven security responses. The findings indicate that AMLE provides a practical reference framework for implementing adaptive, layered security controls in smart home IoT environments, balancing security requirements with operational constraints.**

***Keywords*—Smart home security; IoT encryption; adaptive security; multi-layer protection; resource-constrained devices**

I. Introduction

Smart home IoT ecosystems consist of interconnected devices such as sensors, cameras, thermostats, and smart locks that collectively automate and enhance residential environments. While these systems offer increased convenience and functionality, their rapid adoption has intensified security challenges related to confidentiality, integrity, and access control [1]. A defining characteristic of smart home IoT devices is their constrained computational and memory resources, which limit the feasibility of implementing conventional cryptographic mechanisms commonly used in traditional computing environments [2].

As a result, many IoT devices deploy weak or inconsistent encryption, exposing them to threats including unauthorized access, man-in-the-middle (MitM) attacks, and botnet recruitment [3]. The heterogeneity of smart home devices further complicates security implementation, as devices vary widely in processing capabilities, communication protocols, and data sensitivity [4]. Prior studies identify insufficient encryption and weak access control as primary contributors to data exposure and privacy breaches in IoT environments [5].

Unencrypted or poorly protected communication between devices and cloud services enables attackers to intercept sensitive data, manipulate device behavior, or exploit compromised nodes to launch distributed attacks [6]. Botnets leveraging insecure IoT devices have been shown to significantly disrupt network reliability and compromise user safety [7].

A. Limitations of Existing Solutions

Existing cryptographic solutions face limitations when applied to resource-constrained IoT contexts. AES, although efficient in general-purpose systems, may impose computational overhead and complex key management requirements on low-power devices [8]. RSA supports secure key exchange but introduces high computational costs and latency unsuitable for frequent IoT communications [9]. Elliptic Curve Cryptography (ECC) reduces key sizes while maintaining security strength but presents challenges related to computational complexity, curve selection, side-channel vulnerabilities, and key management [10].

Beyond cryptography, traditional network security mechanisms such as firewalls and signature-based intrusion detection systems often lack adaptability and granular control suitable for IoT environments [11]. Signature-based approaches are particularly ineffective against previously unseen attacks, limiting their applicability in dynamic and evolving threat landscapes [12].

B. Research Contribution

This research addresses these challenges by proposing an Adaptive Multi-Layer Encryption (AMLE) model tailored for smart home IoT ecosystems. The model applies layered security controls across the device, network, and cloud layers, with encryption strength and security responses adjusted based on predefined policies that consider device capabilities, data sensitivity, and detected threat indicators.

The remainder of this study is organized as follows. Section II reviews related work on IoT security mechanisms and identifies the gap this study addresses. Section III describes the research methodology and system architecture. Section IV presents the evaluation results. Section V discusses the findings, and Section VI concludes the study.

II. Related Work

Research on smart home IoT security has explored encryption, anomaly detection, and access control as distinct mechanisms, yet integrated frameworks that adapt security

posture dynamically across all layers remain limited. The studies reviewed below highlight both the advances made and the persistent gaps that motivate the present work.

A. Encryption in Resource-Constrained IoT Environments

Lightweight cryptographic approaches have been proposed to address the resource constraints of IoT devices. Rahman et al. [14] proposed chaos-based AES key generation to strengthen symmetric encryption for smart home devices, demonstrating improved resistance to brute-force attacks while retaining computational feasibility. Tripathy and Singh [8] evaluated AES software implementations on IoT-class hardware, finding that standard AES configurations require optimization to meet real-time latency requirements on constrained processors. Fernandez et al. [9] conducted a comparative evaluation of RSA and ECC cipher suites on fog and mist computing devices, concluding that ECC provides a more favorable security-to-overhead ratio for IoT applications, though it introduces key management and side-channel considerations [10].

Patil et al. [2] proposed a hybrid adaptive cryptographic authentication approach that selects encryption algorithms based on device context, demonstrating that adaptive selection can reduce computational overhead without compromising security guarantees. These works collectively establish that no single cryptographic primitive satisfies the full range of IoT security requirements, motivating layered and adaptive approaches.

B. Anomaly Detection and Intrusion Detection in IoT

Khraisat and Alazab [12] provide a comprehensive review of intrusion detection techniques for IoT environments, highlighting that signature-based methods fail against novel attack patterns and that machine learning approaches, particularly unsupervised methods, offer broader detection coverage. Hamarsheh [15] proposed an adaptive security framework combining Software-Defined Networking (SDN) and machine learning for dynamic IoT threat response, demonstrating measurable improvement in detection latency and policy enforcement speed relative to static rule-based systems. Anthi et al. [17] developed EclipseIoT, a hub-based adaptive security system that monitors device behavior and enforces isolation policies in response to detected anomalies, providing a concrete point of comparison for hub-centric adaptive frameworks.

Both Hamarsheh [15] and EclipseIoT [17] address adaptive detection but do not integrate layered cryptographic policy enforcement across device, network, and cloud tiers simultaneously. This distinction is central to the contribution of AMLE.

C. Access Control in IoT Cloud Environments

Attribute-Based Access Control (ABAC) has been studied as a flexible mechanism for IoT access management. Pajooh et al. [16] proposed a multi-layer blockchain-based security architecture that incorporates ABAC-style policies for IoT data access, demonstrating that attribute-driven authorization can be enforced at the cloud layer without requiring device-side computation. Mosenia and Jha [5] identify weak access control as a primary vulnerability in deployed IoT systems, noting that most consumer devices lack configurable authorization mechanisms, underscoring the importance of cloud-tier access control solutions that operate independently of device capabilities.

D. Identified Research Gap

The reviewed literature demonstrates that encryption optimization, anomaly detection, and access control have each been studied in isolation or in partial combinations. However, a unified framework that coordinates adaptive encryption policy enforcement across device, network, and cloud layers in response to real-time threat signals remains absent from the literature. Existing adaptive frameworks such as Hamarsheh [15] and EclipseIoT [17] address detection and isolation but do not systematically couple detection outcomes to multi-level cryptographic responses. The AMLE model presented in this study addresses this gap by integrating lightweight device-layer encryption, machine learning-based network anomaly detection, and cloud-layer ABAC within a unified policy-driven architecture.

III. Methodology

A. Research Design

The study adopted a prototype development methodology using an Agile approach with iterative development cycles. This approach supported incremental design, implementation, and validation of AMLE components through successive sprints. The development process comprised four phases: planning, sprint execution, review, and deployment.

During the planning phase, key security challenges in smart home IoT ecosystems were identified, including limited device resources, diverse communication protocols, and scalability requirements [3]. These constraints informed design decisions, particularly the selection of encryption mechanisms and anomaly detection techniques compatible with resource-constrained environments.

B. System Architecture

The AMLE architecture follows a three-layer IoT security model aligned with established IoT cloud environment frameworks [13]. Each layer addresses distinct security requirements while contributing to an integrated security posture. Fig. 1 illustrates the overall system architecture showing security enforcement across device, network, and cloud layers.

1) Device layer: At the device layer, lightweight encryption mechanisms including ECC and AES-128 are employed to protect data at the source while accommodating device resource constraints [8]. Encryption strength is assigned based on predefined policies that consider device computational capacity and data sensitivity [14]. For example, devices handling sensitive data such as video streams apply stronger encryption compared to low-risk devices such as temperature sensors. This policy-driven differentiation reflects the finding that cryptographic mechanisms must be tailored to device capabilities and application context in IoT environments [2].

2) Network layer: The network layer incorporates anomaly detection using the Isolation Forest machine learning algorithm to analyze traffic patterns and identify deviations from established baseline behavior [12]. When anomalous activity is detected, predefined response policies may trigger actions such as increased encryption strength, connection restriction, or alert generation. This approach addresses limitations of traditional

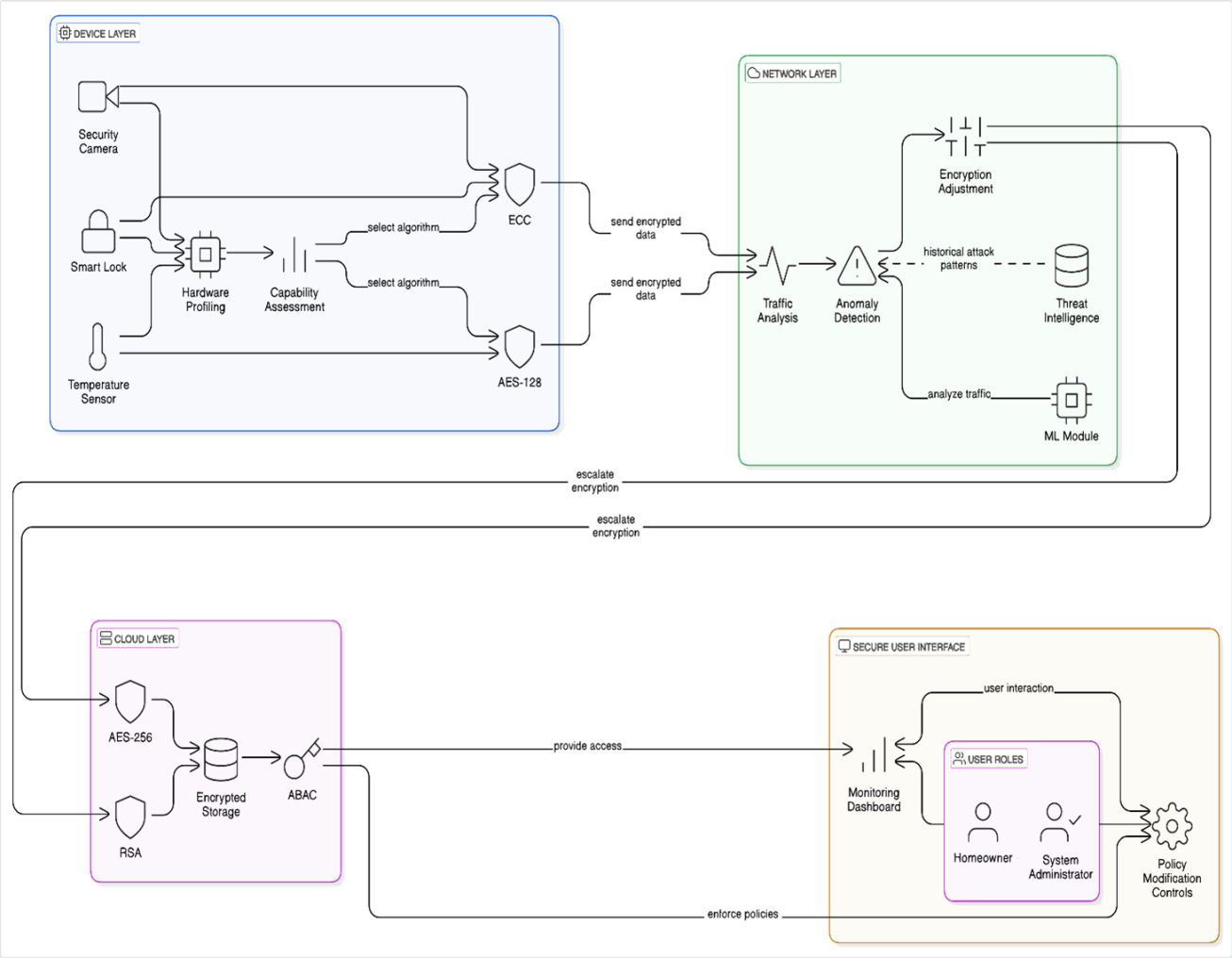

Fig. 1. Overall AMLE system architecture illustrating security enforcement across device, network, and cloud layers.

signature-based intrusion detection systems by enabling detection of previously unseen patterns without requiring labeled training data.

3) Cloud layer: The cloud layer applies robust encryption mechanisms including AES-256 and RSA for data at rest and in transit, combined with Attribute-Based Access Control (ABAC) to enforce fine-grained access policies. ABAC decisions are based on user attributes, resource characteristics, and environmental conditions, providing flexible and context-aware access control.

This approach is consistent with findings from Pajooh et al. [16], who demonstrate that attribute-driven authorization is computationally feasible at the cloud tier of IoT architectures and can be enforced without imposing additional processing burdens on resource-constrained edge devices.

C. Implementation Environment

The system was implemented using a software stack selected to support cryptographic operations, machine learning, and scalable API services. Table I summarizes the implementation environment and toolchain used throughout the development and testing phases.

TABLE I. IMPLEMENTATION ENVIRONMENT AND TOOLCHAIN

Component	Technology / Specification
Programming Language	Python
API Framework	FastAPI v0.104.1
Machine Learning Library	Scikit-learn v1.3.0
Cryptographic Library	Cryptography v41.0.5
Database ORM	SQLAlchemy v2.0.23
Hardware Platform	Intel i7 CPU, 16 GB RAM, SSD
Deployment Context	Controlled simulation environment

This environment supported development and validation of encryption operations, anomaly detection, and access control logic under repeatable test conditions. Testing was conducted on an Intel i7 processor with 16 GB RAM and SSD storage.

IoT devices were simulated in software to represent typical smart home devices with varying processing capabilities and security requirements [17]. No physical IoT hardware was used; all device behavior, traffic generation, and threat

TABLE II. ISOLATION FOREST CONFIGURATION PARAMETERS

Parameter	Value	Rationale
Algorithm	Isolation Forest	Unsupervised anomaly detection
Number of Estimators	100	Balance between accuracy and efficiency
Contamination Rate	0.05	Consistent with IoT anomaly proportion estimates [12]
Feature Normalization	StandardScaler	Prevent feature dominance
Detection Frequency	Every 15 min	Periodic behavioral analysis

scenarios were produced within the simulation environment. Performance and security results therefore reflect behavior under controlled simulation conditions, and generalization to bare-metal IoT hardware requires further empirical validation on representative physical platforms.

D. Anomaly Detection Implementation

Isolation Forest was selected due to its suitability for unsupervised anomaly detection in high-dimensional datasets without requiring labeled training data [12]. Feature selection included traffic volume metrics, connection characteristics, and encryption-related attributes such as algorithm type and key rotation frequency. Table II presents the configuration parameters used for the Isolation Forest implementation.

The contamination rate of 0.05 was selected based on reported estimates of anomalous traffic proportions in IoT network studies [12]. It is acknowledged that this value was not empirically derived from a dedicated IoT attack dataset in this study; sensitivity to this parameter is noted as a limitation, and future work should calibrate the contamination rate against established IoT traffic benchmarks such as N-BaIoT and IoT-23 to better characterize detection performance across varying threat densities.

Data preprocessing applied normalization using StandardScaler, and traffic data were aggregated into fixed time intervals to capture behavioral patterns over time. Anomaly detection was executed at scheduled intervals, with detected anomalies logged and assigned severity levels for monitoring and response.

E. Encryption Management

AMLE defines four encryption levels (LOW, MEDIUM, HIGH, and VERY HIGH) based on algorithm selection, key size, and rotation frequency [15]. Table III details the characteristics of each encryption level and their intended device profiles.

Devices are assigned encryption levels according to predefined policies considering device capabilities, data sensitivity, and detected threat indicators. Key management includes per-device key generation and rotation, implemented using time-based schedules and threat-triggered events. Supported algorithms include AES, RSA, and ECC, enabling flexibility across heterogeneous IoT devices [9], [10].

F. Testing Methodology

Testing comprised unit, integration, functional, performance, and security testing phases. Unit tests verified encryption operations, key management functions, and policy enforcement mechanisms. Integration testing validated secure data flow across layers. Performance testing evaluated encryption latency, system scalability, and resource utilization under varying simulated loads. Security testing included penetration testing and threat modeling to assess system behavior under representative attack scenarios.

It is noted that all threat scenarios were generated internally within the simulation environment; evaluation against established IoT attack datasets such as those reviewed by Khraisat and Alazab [12] represents an important direction for future validation, as externally sourced datasets would provide a more rigorous basis for assessing detection coverage and false positive rates.

IV. RESULTS

A. Key Management System

Key management tests confirmed correct execution of key lifecycle operations, including automated rotation, state-aware updates, and audit trail generation. Invalid configurations were rejected, and inactive devices were excluded from key updates, demonstrating correct policy enforcement and system robustness. Table IV summarizes the functional test outcomes for the key management system.

B. Encryption and Decryption

Encryption and decryption processes functioned as intended across all tested scenarios. Encrypted data could not be accessed without valid keys, and decrypted data matched original input, confirming data confidentiality and integrity. Multi-layer encryption remained consistent across device, network, and cloud layers. Table V presents validation results for encryption and decryption operations.

C. System Performance

Encryption and decryption operations completed within latency ranges suitable for typical smart home interactions, such as sensor updates and control commands. The system handled concurrent simulated device connections without observable degradation in response time. Resource utilization remained within acceptable limits under the tested conditions, although increased latency was observed for configurations representing highly constrained devices.

Table VI summarizes the observed performance characteristics. Performance measurements are reported qualitatively because the evaluation was conducted in a software simulation environment on a general-purpose workstation rather than on physical IoT hardware; precise numerical latency benchmarks on constrained devices remain a subject for future empirical study, and direct measurement on representative hardware platforms will be necessary to establish deployment-ready performance profiles.

D. Anomaly Detection

The Isolation Forest model identified deviations from baseline traffic behavior, including abnormal transmission volumes, unusual connection patterns, and inconsistent encryption parameters. Detected anomalies were logged with severity

TABLE III. ENCRYPTION LEVELS AND CHARACTERISTICS

Level	Algorithms	Key Size	Rotation Policy	Intended Device Profile
LOW	AES	128-bit	Periodic	Low-risk sensors
MEDIUM	AES	192-bit	Periodic	Standard IoT devices
HIGH	AES / ECC	256-bit	Periodic + Threat-triggered	Sensitive devices
VERY HIGH	AES / RSA	256-bit	Frequent + Threat-triggered	Cloud and critical assets

TABLE IV. KEY MANAGEMENT FUNCTIONAL TEST OUTCOMES

Test Case	Expected Behavior	Outcome
Automatic key rotation	Rotation at scheduled intervals	Successful
Invalid interval handling	Reject invalid values	Successful
Inactive device handling	Exclude from updates	Successful
Rotation audit logging	Retain rotation history	Successful
Encryption disabled state	Suspend rotation	Successful

TABLE V. ENCRYPTION AND DECRYPTION VALIDATION RESULTS

Scenario	Expected Outcome	Result
Correct key usage	Successful decryption	Confirmed
Incorrect key usage	Decryption failure	Confirmed
Multi-layer encryption	End-to-end protection	Confirmed
Data integrity check	Original data restored	Confirmed

TABLE VI. OBSERVED PERFORMANCE CHARACTERISTICS

Metric	Observation
Encryption latency	Within acceptable range for simulated smart home interactions
Concurrent device handling	Stable under simulated load
CPU utilization	Moderate under peak conditions
Memory usage	Within available limits

TABLE VII. DETECTED ANOMALY CATEGORIES

Category	Description
Traffic volume anomalies	Unexpected data transmission spikes
Connection pattern anomalies	Abnormal frequency or duration
Encryption anomalies	Deprecated algorithms or irregular key rotation
Destination anomalies	Connections to unknown or blacklisted IPs

ratings and visualized via the monitoring dashboard, enabling timely security responses. Table VII categorizes the types of anomalies detected during testing.

E. Security Behavior Under Simulated Threats

The framework demonstrated the ability to detect and respond to simulated unauthorized access attempts, MitM-like traffic interception patterns, and botnet-associated communication behaviors. Cloud-layer ABAC policies restricted unauthorized access attempts based on attribute mismatches, supporting effective access control enforcement. Table VIII summarizes the security response outcomes under various threat scenarios.

All threat scenarios were generated internally within the simulation environment; validation against externally sourced IoT attack datasets is acknowledged as a limitation and is identified as a direction for future work, as such validation would provide stronger evidence of the framework's generalizability to real-world attack distributions and previously unseen threat variants.

TABLE VIII. SECURITY RESPONSE SUMMARY

Threat Scenario	Detection	Response Mechanism
Unauthorized access attempt	Detected	Access blocked via ABAC
MitM-like traffic pattern	Detected	Encryption escalation
Botnet-style behavior	Detected	Alert and connection restriction
Unauthorized cloud access	Detected	Policy-based denial

V. DISCUSSION

The AMLE framework demonstrates that layered, policy-driven security mechanisms can enhance protection in smart home IoT environments while accommodating resource constraints. Lightweight encryption at the device layer provides baseline protection, while network-level anomaly detection enables adaptive responses to detected deviations.

A. Device Layer Performance

The device layer implementation of ECC and AES-128 provided data security at the source while accommodating computational constraints characteristic of IoT devices [8], [10]. Dynamic adjustment of encryption strength based on device capabilities and data sensitivity optimized the balance between security and performance [14]. The differential encryption approach, where security cameras utilize stronger protocols than temperature sensors, is consistent with the adaptive selection approach demonstrated by Patil et al. [2], who show that context-driven algorithm selection reduces overhead without degrading security guarantees.

B. Network Layer Effectiveness

The network layer machine learning-based anomaly detection successfully identified suspicious traffic patterns, enabling real-time encryption escalation when threats were detected. The Isolation Forest unsupervised learning approach proved effective for detecting previously unseen attack patterns without requiring labeled training data, addressing a critical gap in conventional intrusion detection systems [12]. The configuration with 100 estimators and a 0.05 contamination threshold balanced detection sensitivity with computational efficiency.

Direct quantitative comparison with Hamarsheh [15] and EclipseIoT [17] on shared detection metrics was not performed in this study because the evaluation environments and datasets differ; such comparison on common benchmarks is identified as a priority for future work and would substantially strengthen

claims regarding the relative performance of AMLE's anomaly detection component.

C. Cloud Layer Security

The cloud layer implementation of AES-256, RSA encryption, and ABAC mechanisms ensured secure data storage and restricted unauthorized access [16]. The combination of robust encryption algorithms and attribute-based access control provided comprehensive protection for sensitive information.

ABAC's ability to make decisions based on user attributes, resource characteristics, and environmental conditions enabled flexible and context-aware security enforcement, consistent with findings from Pajooh et al. [16] in multi-layer IoT architectures. This flexibility is particularly valuable in smart home contexts where access permissions may need to vary dynamically based on factors such as time of day, device health status, or detected threat level.

D. Performance and Scalability

Performance results indicate that the framework is suitable for simulated smart home scenarios, though the simulation on a general-purpose Intel i7 workstation does not directly confirm feasibility on physically constrained IoT hardware. Encryption and decryption operations completed within latency ranges suitable for interactive smart home functions such as door lock commands, thermostat adjustments, and security alerts. The system scaled effectively to accommodate multiple simultaneous device connections under simulation.

Increased latency was observed for configurations representing highly constrained devices, consistent with findings from studies on cryptographic implementation in minimal IoT devices [8].

This limitation indicates that further optimization of encryption algorithms for physically constrained devices, potentially through hardware acceleration or more efficient algorithmic implementations, is necessary before deployment on actual IoT hardware can be claimed. Future iterations of AMLE should therefore incorporate profiling on representative low-power platforms such as Raspberry Pi Zero or Arduino-class microcontrollers to quantify the overhead imposed by each encryption level.

E. System Integration

The modular architecture supports extensibility and integration with existing IoT infrastructures. The scheduled anomaly detection executing every 15 minutes, combined with database integration and RESTful API endpoints, provides practical security monitoring that can be integrated into existing smart home management systems. The dashboard implementation offers administrators comprehensive visibility into encryption status, device health, and security metrics, enabling proactive security management and rapid response to detected threats.

VI. Conclusion

This study presented an Adaptive Multi-Layer Encryption framework for smart home IoT ecosystems that integrates lightweight cryptography, network-level anomaly detection, and cloud-based access control. Evaluation in a controlled simulation environment demonstrated the framework's capability to detect and respond to representative security threats while maintaining operational performance suitable for typical smart home applications.

It is explicitly acknowledged that the evaluation was conducted entirely in software simulation on a general-purpose workstation and that performance and detection claims require further validation on physical IoT hardware and against established IoT attack datasets. These limitations define clear boundaries on the current findings and motivate the empirical extensions outlined in the future work directions below.

The research contributes to the field of IoT security by providing a practical encryption framework that balances security requirements with operational constraints of smart home environments. The validated implementation of multi-layer adaptive encryption across device, network, and cloud layers establishes a reference architecture for future smart home security systems. Integration of machine learning-based anomaly detection for real-time threat response demonstrates the feasibility of intelligent, adaptive security mechanisms in simulated resource-constrained environments.

A. Key Contributions

The findings support the feasibility of layered, adaptive security architectures for IoT environments and provide a reference implementation for future research and development. Key contributions include a practical encryption framework validated through comprehensive testing, demonstration of anomaly detection using Isolation Forest with a 0.05 contamination threshold calibrated to IoT traffic estimates in the literature [12], and evidence of acceptable performance characteristics for typical smart home applications under controlled simulation conditions.

B. Future Work

Future work should focus on: validation in real-world deployments on physical IoT hardware; calibration of the anomaly detection contamination parameter against established IoT attack datasets such as N-BaIoT and IoT-23; quantitative benchmarking against adaptive IoT security frameworks such as Hamarsheh [15] and EclipseIoT [17] on shared metrics; optimization for highly constrained devices via hardware acceleration; expanded protocol support for broader compatibility; integration with blockchain for distributed trust, enabling immutable audit trails and non-repudiation through digital signature schemes [18]; and development of standardized AMLE protocols for industry adoption.

The AMLE model provides a foundation for developing more robust, adaptive security solutions for the expanding smart home IoT ecosystem, contributing to safer and more reliable deployment of IoT technologies in residential environments.

Declaration on Generative AI Use

The authors declare that generative artificial intelligence (GenAI) tools were used solely for language refinement, grammar checking, and improving clarity and readability of the

manuscript. The scientific content, methodology, experimental design, analysis, results, and conclusions were entirely developed by the human authors. All AI-assisted text was carefully reviewed, verified, and edited to ensure accuracy, originality, and compliance with academic integrity standards. The authors take full responsibility for the content of this manuscript.

REFERENCES

[1] A. Chakraborty, M. Islam, F. Shahriyar, S. Islam, H. U. Zaman, and M. Hasan, "Smart home system: A comprehensive review," *J. Electr. Comput. Eng.*, vol. 2023, Article ID 7616683, 2023.

[2] K. Patil, I. Mandal, and C. Rangaswamy, "Hybrid and adaptive cryptographic-based secure authentication approach in IoT-based applications using hybrid encryption," *Pervasive Mobile Comput.*, vol. 82, p. 101552, 2022.

[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, Jan. 2015.

[4] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, and Q. Arshad, "Data and privacy: Getting consumers to trust products enabled by the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 35–38, Mar. 2019.

[5] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerging Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct.–Dec. 2017.

[6] P. Radanliev, D. De Roure, K. Page, J. R. C. Nurse, R. M. Montalvo, O. Santos, L. Maddox, and P. Burnap, "Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial Internet of Things and Industry 4.0 supply chains," *Cybersecurity*, vol. 3, no. 1, p. 13, Jun. 2020.

[7] R. Das and M. Z. Gündüz, "Analysis of cyber-attacks in IoT-based critical infrastructures," *Int. J. Inf. Secur. Sci.*, vol. 8, no. 4, pp. 122–133, 2019.

[8] A. Tripathy and B. Singh, "A study of AES software implementation for IoT systems," in *Proc. 3rd Int. Conf. Issues Challenges Intell. Comput. Techn. (ICICT)*, Feb. 2022, pp. 1–4.

[9] T. Fernández-Caramés, P. Fraga-Lamas, and M. Suárez-Albela, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, p. 3868, Nov. 2018.

[10] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic curve cryptography: Applications, challenges, recent advances, and future trends: A comprehensive survey," *Comput. Sci. Rev.*, vol. 47, p. 100530, Feb. 2023.

[11] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security evaluation of home-based IoT deployments," in *Proc. IEEE Symp. Security Privacy (SP)*, May 2019, pp. 1362–1380.

[12] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the Internet of Things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, no. 1, p. 18, May 2021.

[13] A. Bouaouad, A. Cherradi, S. Assoul, and N. Souissi, "The key layers of IoT architecture," in *Proc. 5th Int. Conf. Cloud Comput. Artif. Intell.: Technol. Appl. (CloudTech)*, Nov. 2020, pp. 1–4.

[14] Z. Rahman, X. Yi, M. Billah, M. Sumi, and A. Anwar, "Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home," *Electronics*, vol. 11, no. 7, p. 1083, Apr. 2022.

[15] A. Hamarsheh, "An adaptive security framework for Internet of Things networks leveraging SDN and machine learning," *Appl. Sci.*, vol. 14, no. 11, p. 4530, May 2024.

[16] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-layer blockchain-based security architecture for Internet of Things," *Sensors*, vol. 21, no. 3, p. 772, Jan. 2021.

[17] E. Anthi, S. Ahmad, O. Rana, G. Theodorakopoulos, and P. Burnap, "EclipseIoT: A secure and adaptive hub for the Internet of Things," *Comput. Security*, vol. 78, pp. 477–490, Sep. 2018.

[18] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, "Digital signature scheme for information non-repudiation in blockchain: A state-of-the-art review," *EURASIP J. Wireless Commun. Networking*, vol. 2020, p. 56, 2020.