PRIVACY-PRESERVING REAL-TIME HOME AUTOMATION UTILIZING MQTT PROTOCOL AND SENSOR ANOMALY DETECTION WITH GENAI INTEGRATION

A Thesis Submitted in Partial
Fulfillment for the Requirement of the Degree of

Bachelor of Science
in
Computer Science and Engineering

by

Anowar Hossain
ID: 221071051

Shihab Sarker
ID: 202071004

Under the Supervision of

Tahsin Alam
Lecturer
Department of Computer Science and Engineering

to the

Department of Computer Science and Engineering
Shanto-Mariam University of Creative Technology

February, 2026

ACKNOWLEDGEMENT

This thesis has been submitted to the Department of Computer Science and Engineering of Shanto-Mariam University of Creative Technology (SMUCT), Dhaka, Bangladesh, in partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering. The thesis title is “PRIVACY-PRESERVING REAL-TIME HOME AUTOMATION UTILIZING MQTT PROTOCOL AND SENSOR ANOMALY DETECTION WITH GENAI INTEGRATION”.

First and foremost, we offer our sincere gratitude to our thesis supervisor, **Tahsin Alam**, Lecturer, Department of Computer Science and Engineering, for his continuous support, motivation, and immense knowledge. His valuable guidance and dedicated supervision greatly contributed to the successful completion of this research.

We also express our sincere appreciation to the Head of the Department, **Faisal Imran**, Head & Associate Professor, for his academic leadership and for providing the necessary facilities and institutional support to conduct this research work.

We are extremely grateful to our Thesis Moderator, **Md. Tousif Hasan Lavlu**, Lecturer, Department of Computer Science & Engineering, for his thorough review, insightful feedback, and continuous encouragement. His constructive evaluation was instrumental in refining this thesis.

Our heartfelt thanks are extended to the External Examiner, **Sakhor Das Opi**, Lecturer, Department of Computer Science & Engineering, for his valuable time and constructive suggestions, which have significantly improved the quality and presentation of this work.

Finally, we express our deepest gratitude to our parents and family members for their unconditional love, constant encouragement, and moral support throughout our academic journey. Without them, this achievement would not have been possible.

Anowar Hossain
ID: 221071051

Shihab Sarker
ID: 202071004

February, 2026
SMUCT, Dhaka, Bangladesh

CERTIFICATE

This is to certify that the thesis entitled “PRIVACY-PRESERVING REAL-TIME HOME AUTOMATION UTILIZING MQTT PROTOCOL AND SENSOR ANOMALY DETECTION WITH GENAI INTEGRATION” by **Anowar Hossain** (ID: 221071051) and **Shihab Sarker** (ID: 202071004) has been carried out under my direct supervision. To the best of my knowledge, this thesis is an original work and has not been submitted anywhere for any degree or diploma.

Thesis Supervisor:

....

Tahsin Alam
Lecturer
Department of Computer Science and Engineering
Shanto-Mariam University of Creative Technology

CERTIFICATE

This is to certify that the thesis entitled "PRIVACY-PRESERVING REAL-TIME HOME AUTOMATION UTILIZING MQTT PROTOCOL AND SENSOR ANOMALY DETECTION WITH GENAI INTEGRATION" by **Anowar Hossain** (ID: 221071051) and **Shihab Sarker** (ID: 202071004) has been carried out under the direct supervision of **Tahsin Alam**. This thesis has been prepared according to the guidelines of the Department of Computer Science & Engineering / Department of Computer Science & Information Technology of Shanto-Mariam University of Creative Technology.

Head of the Department
....

Faisal Imran
Head & Associate Professor
Department of Computer Science & Engineering and
Department of CSIT
Shanto-Mariam University of Creative Technology

CERTIFICATE

This is to certify that the thesis entitled "PRIVACY-PRESERVING REAL-TIME HOME AUTOMATION UTILIZING MQTT PROTOCOL AND SENSOR ANOMALY DETECTION WITH GENAI INTEGRATION" submitted by **Anowar Hossain** (ID: 221071051) and **Shihab Sarker** (ID: 202071004) in partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering has been examined and moderated by me.

I have carefully reviewed the thesis defense and documentation. I found it to be a comprehensive and original piece of research work. The thesis successfully meets the academic standards and requirements set by the Department of Computer Science & Engineering / Department of Computer Science & Information Technology of Shanto-Mariam University of Creative Technology.

Thesis Moderator

....

Md. Tousif Hasan Lavlu
Lecturer
Department of Computer Science & Engineering
Shanto-Mariam University of Creative Technology

CERTIFICATE

This is to certify that the thesis entitled "PRIVACY-PRESERVING REAL-TIME HOME AUTOMATION UTILIZING MQTT PROTOCOL AND SENSOR ANOMALY DETECTION WITH GENAI INTEGRATION" submitted by **Anowar Hossain** (ID: 221071051) and **Shihab Sarker** (ID: 202071004) in partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering has been examined by me.

I have carefully reviewed the thesis and found that it is an original piece of research work. The thesis meets the academic standards and requirements set by the Department of Computer Science & Engineering / Department of Computer Science & Information Technology of Shanto-Mariam University of Creative Technology.

External Examiner
....

Sakhor Das Opi
Lecturer
Department of Computer Science & Engineering
Shanto-Mariam University of Creative Technology

DECLARATION

We hereby declare that the thesis entitled "PRIVACY-PRESERVING REAL-TIME HOME AUTOMATION UTILIZING MQTT PROTOCOL AND SENSOR ANOMALY DETECTION WITH GENAI INTEGRATION" is the result of our own independent research work carried out under the supervision of **Tahsin Alam**, Lecturer, Department of Computer Science and Engineering, Shanto-Mariam University of Creative Technology.

This thesis has not been submitted, either in whole or in part, to any other university or institution for the award of any degree, diploma, or other qualification. All sources of information used in this research have been duly acknowledged through proper references and citations.

We take full responsibility for the authenticity and accuracy of the work presented in this thesis.

....

Anowar Hossain
B.Sc. in Computer Science and Engineering
ID: 221071051
Department of Computer Science and Engineering
Shanto-Mariam University of Creative Technology

....

Shihab Sarker
B.Sc. in Computer Science and Engineering
ID: 202071004
Department of Computer Science and Engineering
Shanto-Mariam University of Creative Technology

Abstract

The rapid proliferation of Internet of Things (IoT) devices in smart homes has introduced critical vulnerabilities regarding data privacy and security. Conventional cloud-centric architectures often expose sensitive user data to third-party risks, necessitating a shift toward secure, edge-based solutions. This research presents "IoTShield", a comprehensive privacy-preserving home automation framework that integrates the lightweight MQTT protocol with Generative AI for intelligent anomaly detection. The system utilizes a hybrid edge-computing architecture featuring ESP32 microcontrollers and Raspberry Pi gateways to process data locally. To ensure robust privacy, a dual-layer Differential Privacy mechanism using Gaussian noise is applied, complemented by end-to-end RSA-2048 encryption for secure transmission. For anomaly detection, the system integrates a local Large Language Model (Llama 3.2:1B) to analyze sensor patterns and generate context-aware alerts with explainable insights. Experimental results from over 13,000 sensor readings demonstrate that the system achieves an end-to-end latency of under 2 seconds and successfully classifies anomalies across four severity levels (Low to Critical). This study confirms that combining local GenAI with cryptographic privacy mechanisms preserves data sovereignty while delivering a highly responsive and secure smart home environment.

Keywords: IoT Security, MQTT Protocol, Generative AI, Llama 3.2, Anomaly Detection, Differential Privacy, RSA Encryption, Edge Computing, Smart Home Automation

Contents

List of Figures

List of Tables

List of Abbreviations

AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
CPU	Central Processing Unit
CSE	Computer Science and Engineering
DoS	Denial of Service
ESP32	Espressif Systems 32-bit Microcontroller
GenAI	Generative Artificial Intelligence
GPIO	General Purpose Input/Output
HTTP	Hypertext Transfer Protocol
IDE	Integrated Development Environment
IoT	Internet of Things
IP	Internet Protocol
JSON	JavaScript Object Notation
JWT	JSON Web Token
LED	Light Emitting Diode
LLM	Large Language Model
LDR	Light Dependent Resistor
MQTT	Message Queuing Telemetry Transport
PIR	Passive Infrared Sensor
QoS	Quality of Service
RAM	Random Access Memory
REST	Representational State Transfer
RSA	Rivest–Shamir–Adleman (Encryption Algorithm)
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UI	User Interface
URL	Uniform Resource Locator
Wi-Fi	Wireless Fidelity

List of Symbols

M	Plaintext Message
C	Ciphertext (Encrypted Message)
K_{pub}	Public Key
K_{priv}	Private Key
e	Public Exponent (RSA)
d	Private Exponent (RSA)
n	Modulus (RSA)
μ	Mean Value (Gaussian Distribution)
σ	Standard Deviation
ϵ	Privacy Budget / Noise Parameter
$N(\mu, \sigma^2)$	Gaussian (Normal) Distribution
T	Temperature Sensor Reading
H	Humidity Sensor Reading
G	Gas Sensor Value
L_{lat}	System Latency
$P(x)$	Probability of an Event
V_{in}	Input Voltage
R	Resistance
t	Time / Timestamp
Δ	Difference / Change in Value
θ	Threshold Value for Anomaly Detection
Hz	Hertz (Frequency Unit)
dB	Decibel (Signal Strength Unit)
bps	Bits Per Second

Chapter 1

Introduction

1.1 Background and Motivation

The rapid evolution of the Internet of Things (IoT) has fundamentally transformed modern living spaces into intelligent, interconnected environments. Smart home automation systems now routinely deploy diverse networks of sensors and actuators to monitor environmental conditions, manage energy consumption, and significantly enhance user convenience. To facilitate this seamless interaction, lightweight communication protocols, particularly the Message Queuing Telemetry Transport (MQTT) protocol, have become the industry standard. MQTT enables efficient, low-latency data transmission even across highly constrained networks and low-power microcontrollers, making it ideal for real-time residential applications.

Despite the tremendous advantages of these smart home ecosystems, their widespread adoption introduces critical vulnerabilities surrounding data privacy and security. Continuous environmental monitoring generates a massive influx of granular data, capturing intimate details about household occupancy, daily routines, and behavioral habits. In conventional architectures, this highly sensitive data is frequently transmitted in its raw form to centralized cloud servers for processing. This heavy reliance on third-party cloud infrastructure exposes users to severe risks, including data breaches, unauthorized surveillance, and corporate data profiling. While basic transport-layer security is sometimes implemented, true end-to-end data confidentiality at the application layer remains a significant challenge in residential deployments.

Beyond privacy concerns, traditional smart home systems are largely constrained by rudimentary, rule-based logic. Most commercial setups rely on static, predefined thresholds to trigger alerts—for example, activating a notification only if a gas or temperature sensor strictly exceeds a hardcoded limit. This rigid approach lacks contextual awareness. It frequently results in a high volume of false positives, struggles to identify complex anomalies that span multiple sensor types, and provides users with generic, numerical warnings rather than clear, actionable insights into the actual problem.

Motivated by these profound limitations, there is a pressing need for a paradigm shift toward secure, intelligent, and decentralized home automation. The integration of Generative Artificial Intelligence (GenAI), specifically localized Large Language Models (LLMs), presents a revolutionary opportunity to move beyond simple threshold alerts to context-aware, human-readable anomaly detection. This research is driven by the ambition to engineer a holistic framework that marries the efficiency of MQTT with rigorous privacy-preserving mechanisms—such as dual-layer Gaussian noise and RSA encryption—processed entirely at the network edge. By doing so, the proposed system aims to deliver highly responsive, intelligent monitoring while guaranteeing absolute data sovereignty for the user.

1.2 Problem Statement

The integration of Internet of Things (IoT) devices into residential environments has significantly improved building automation, safety, and energy management. However, the standard architecture of these systems fundamentally compromises user privacy and data security. Most commercial smart home setups rely heavily on centralized, cloud-based processing, where raw, granular sensor data—such as room occupancy, temperature fluctuations, and lighting usage—is continuously transmitted over the internet. This continuous data stream creates a high-risk attack surface. If intercepted or analyzed by unauthorized entities, this information can be used to deduce sensitive domestic activities, leaving users vulnerable to surveillance, corporate data profiling, and malicious physical intrusions.

Furthermore, the communication protocols utilized by resource-constrained IoT devices, while lightweight and efficient, often lack robust application-layer security. For instance, while the MQTT protocol is highly optimized for low-bandwidth environments, standard implementations frequently leave the data payload entirely readable by the central broker. Even when transport-layer security (TLS) is applied, the centralized broker remains a single point of failure that can expose historical and real-time data if compromised. There is a distinct lack of mechanisms that protect the structural privacy of the data—such as cryptographic encryption or differential privacy—before it even leaves the physical edge device.

In addition to these severe privacy vulnerabilities, current home automation systems suffer from severely limited analytical capabilities. They typically depend on rigid, rule-based logic to trigger alerts, such as activating an alarm only when a gas or temperature sensor crosses a strict, hardcoded numerical limit. This rudimentary approach fails to account for environmental context, frequently leading to a high rate of false positives and a lack of actionable information. When complex, multi-sensor anomalies occur, users are presented with generic numerical warnings rather than a clear, intelligent explanation of the event. While advanced machine learning models can offer more sophisticated detection, they are usually too computationally expensive to deploy locally on edge-based microcontrollers, forcing a reliance back onto the insecure cloud.

Therefore, the primary problem addressed in this research is the lack of a secure, edge-centric framework capable of performing real-time home automation and intelligent anomaly detection without compromising data sovereignty. Specifically, the challenge lies in securing lightweight MQTT communications through application-layer encryption and noise-based privacy mechanisms, while simultaneously deploying a Generative AI model locally to analyze complex sensor patterns and generate human-readable, context-aware alerts within a decentralized architecture.

1.3 Research Gap

Despite the extensive body of literature on smart home automation and Internet of Things (IoT) security, a significant gap remains at the intersection of lightweight communication, robust data privacy, and intelligent anomaly detection. A comprehensive review of existing methodologies reveals a persistent dichotomy: systems are typically either highly secure but computationally heavy, or lightweight but dangerously vulnerable. While the MQTT protocol is widely celebrated for its low latency and efficiency in constrained environments, prevailing implementations primarily rely on transport-layer security (TLS). This approach leaves the data payload unencrypted at the broker level, creating a critical vulnerability if the central server is compromised. Furthermore, the application of structural privacy mechanisms—such as injecting differential noise at the sensor node before transmission—is rarely explored in real-time, lightweight residential architectures.

In the domain of anomaly detection, current smart home deployments predominantly utilize either static, rule-based thresholds or traditional machine learning models (e.g., Support Vector Machines and Random Forests). While threshold-based systems are efficient, they lack the contextual awareness necessary to identify sophisticated, multi-sensor anomalies, leading to high false-positive rates. Conversely, while traditional machine learning models can detect deviations, they function as "black boxes," providing numerical anomaly scores without any human-readable explanation or actionable context. When an alert is triggered, the user is left to interpret raw data rather than receiving a clear, reasoned diagnosis of the potential hazard.

Recently, Generative Artificial Intelligence (GenAI) and Large Language Models (LLMs) have demonstrated exceptional capabilities in contextual reasoning and data interpretation. However, their application in IoT environments is heavily biased toward cloud-centric architectures due to their immense computational requirements. The deployment of localized, edge-optimized LLMs to process raw sensor telemetry and generate intelligent, real-time alerts without relying on third-party cloud APIs remains significantly under-researched. Existing studies that do explore AI-driven IoT security mostly focus on high-level network traffic analysis rather than granular, domestic environmental sensor data.

Consequently, the fundamental research gap lies in the absence of a holistic, decentralized smart home framework that unifies these disparate elements. There is a distinct lack of systems that successfully combine application-layer cryptographic payload encryption, privacy-preserving data obfuscation, and edge-deployed Generative AI to provide secure, real-time, and explainable anomaly detection within a lightweight MQTT ecosystem.

1.4 Research Objectives

The primary aim of this research is to design, implement, and evaluate a decentralized, privacy-preserving smart home automation system capable of intelligent, real-time anomaly detection. To achieve this overarching goal, the research is guided by the following specific objectives:

- **To design a lightweight, edge-centric IoT architecture:** Develop a responsive smart home network utilizing ESP32 microcontrollers, a Raspberry Pi edge gateway, and the MQTT protocol to ensure low-latency communication without heavy reliance on external cloud infrastructure.
- **To implement a dual-layer privacy and security pipeline:** Engineer a robust data protection mechanism that applies structural obfuscation via dual-layer Gaussian noise (differential privacy) and secures the MQTT payload using application-layer RSA-2048 encryption before data transmission.
- **To integrate localized Generative AI for anomaly detection:** Deploy a lightweight Large Language Model (Llama 3.2:1B via Ollama) to autonomously analyze multi-sensor telemetry, replacing rigid threshold-based logic with context-aware, human-readable alert generation.
- **To construct an interactive, full-stack monitoring platform:** Build a comprehensive backend and web dashboard (utilizing Django, Tailwind CSS, and Chart.js) to manage devices, decrypt sensor data, and visualize real-time AI-generated insights.
- **To empirically evaluate system performance:** Validate the proposed IoTShield framework in a real-world deployment by analyzing key metrics, including end-to-end latency, encryption overhead, anomaly detection accuracy, and the overall privacy-utility trade-off.

1.5 Contributions of the Thesis

This thesis makes several significant contributions to the fields of Internet of Things security, edge computing, and smart home automation. By addressing the critical vulnerabilities of cloud-dependent architectures, the proposed IoTShield system introduces a novel paradigm for domestic environmental monitoring.

The core contributions of this research are summarized as follows:

- **A Novel Edge-Based GenAI Integration:** This research demonstrates the feasibility and immense value of deploying localized Generative AI at the network edge. By utilizing a 1-billion parameter LLM to process sensor data locally, the system successfully transitions anomaly detection from binary, threshold-based triggers to intelligent, context-aware reasoning, providing users with actionable and highly accurate alerts.
- **Application-Layer MQTT Security Architecture:** Unlike standard IoT deployments that rely solely on transport-layer security, this thesis contributes a fully functional RSA-2048 encryption scheme specifically optimized for MQTT payloads. This ensures that even if the central message broker is compromised, the granular sensor telemetry remains strictly confidential.
- **Practical Implementation of Differential Privacy in IoT:** The research introduces a dual-layer Gaussian noise injection mechanism directly at the sensor node. This contributes a practical methodology for masking exact domestic routines and behavioral patterns while preserving enough data utility for the AI model to accurately detect critical anomalies (e.g., fires or gas leaks).
- **Empirical Validation of a Production-Ready Framework:** The thesis provides comprehensive, real-world validation of the proposed architecture. Through the deployment of physical hardware and simulated nodes generating over 13,000 sensor readings and validating over 1,500 distinct alerts, the study proves that a highly secure, AI-driven IoT system can operate with an average end-to-end latency of less than two seconds.

1.6 Scope of the Thesis

The scope of this research is specifically bounded to the design, implementation, and evaluation of a privacy-preserving, AI-driven monitoring framework tailored for residential smart home environments. The project focuses strictly on secure environmental data collection, anomalous event detection, and real-time alert generation, rather than large-scale industrial IoT (IIoT) deployments or complex physical robotic actuation.

In terms of hardware and physical deployment, the scope encompasses the development of a fully operational real-world sensor node. This node utilizes a physical ESP32 microcontroller integrated with six distinct environmental sensors (temperature, humidity, gas, flame, motion, and light) to validate real-world data acquisition. To rigorously evaluate the system's network handling, multi-device architecture, and edge processing capabilities without deploying extensive hardware, the scope also incorporates simulated IoT nodes. These consist of a simulated secondary ESP32 hub and a simulated Raspberry Pi edge gateway, which additionally provides system performance metrics such as CPU and memory usage.

From a software and security perspective, the research is limited to securing the MQTT communication protocol at the application layer. This involves the implementation of a custom RSA-2048 encryption pipeline for payload confidentiality and a dual-layer Gaussian noise mechanism to ensure differential privacy. The thesis does not attempt to invent new foundational cryptographic algorithms or replace standard transport-layer security (TLS); instead, it focuses on practical, edge-level data obfuscation to prevent broker-level data compromises.

Finally, the intelligence and anomaly detection scope is centered entirely on edge-optimized Generative AI. The system integrates a locally hosted, 1-billion parameter Large Language Model (Llama 3.2 via Ollama) to process decrypted sensor telemetry and generate context-aware, human-readable alerts. The research deliberately excludes the use of proprietary, cloud-based AI APIs to strictly maintain data sovereignty and adhere to decentralized edge-computing principles. Furthermore, the development of a responsive backend and web dashboard (utilizing Django, SQLite, and Tailwind CSS) is included within the scope to demonstrate end-to-end data persistence, real-time visualization, and practical alert management.

1.7 Thesis Organization

The remainder of this thesis is logically structured into five subsequent chapters, each detailing a critical phase of the research, development, and evaluation of the proposed IoTShield framework.

Chapter 2: Related Work provides a comprehensive review of the existing literature surrounding smart home automation. It examines current MQTT-based architectures, privacy-preserving IoT systems, and the application of cryptographic mechanisms in constrained environments. Furthermore, it explores traditional anomaly detection techniques alongside the emerging role of Generative AI in real-time monitoring, ultimately highlighting the crucial limitations and research gaps that this thesis addresses.

Chapter 3: Proposed System outlines the theoretical and structural design of the IoTShield architecture. It details the holistic system overview, defining the roles of the physical ESP32 sensors and the simulated edge gateway. This chapter extensively covers the MQTT communication model, the privacy-preserving data pipeline incorporating dual-layer Gaussian noise and RSA-2048 encryption, and the localized AI-based anomaly detection framework driven by Llama 3.2.

Chapter 4: Implementation translates the proposed architecture into a functional, real-world application. It documents the exact hardware setup, the software development environment (including Django, Tailwind CSS, and Chart.js), and the configuration of the Mosquitto MQTT broker. Additionally, it details the practical coding implementations of the differential privacy mechanisms, the application-layer encryption, the local LLM deployment, and the relational database schema utilized for data persistence.

Chapter 5: Results and Discussion presents a rigorous empirical evaluation of the operational system. Based on an extensive dataset of over 13,000 sensor readings and more than 1,500 validated alerts, this chapter analyzes system latency, cryptographic processing overhead, and the accuracy of the AI-driven anomaly detection. It also provides a critical discussion on the privacy-utility trade-off and compares the proposed framework's performance against traditional baseline models.

Chapter 6: Conclusion and Future Work synthesizes the key findings of the research, summarizing the successful integration of privacy-preserving mechanisms with edge-based Generative AI. It candidly discusses the limitations encountered during the study and proposes strategic directions for future research to further enhance secure, intelligent residential automation.

Chapter 2

Related Work

2.1 MQTT-Based Smart Home Architectures

2.2 Privacy-Preserving IoT Systems

2.3 Cryptographic Mechanisms in IoT Security

2.4 Anomaly Detection Techniques in IoT

2.5 Generative AI for Real-Time Monitoring

2.6 Limitations of Existing Approaches

Chapter 3

Proposed System

3.1 Overall System Overview

3.2 System Architecture Design

3.3 Hardware Architecture (ESP32 and Sensors)

3.4 Software Architecture

3.5 MQTT Communication Model

3.6 Privacy-Preserving Data Pipeline

3.6.1 Differential Privacy with Dual Gaussian Noise

3.6.2 RSA-2048 Encryption Mechanism

3.7 AI-Based Anomaly Detection Framework

3.7.1 Threshold-Based Detection Logic

3.7.2 Local LLM Integration (Llama 3.2 via Ollama)

3.8 End-to-End System Workflow

Chapter 4

Implementation

4.1 Hardware Implementation Details

4.2 Software Development Environment

4.3 MQTT Broker Configuration

4.4 Differential Privacy Implementation

4.5 RSA Encryption Implementation

4.6 Local LLM Deployment Setup

4.7 Database Design and Storage Model

Chapter 5

Results and Discussion

5.1 Experimental Setup

5.2 Performance Evaluation

5.2.1 System Latency Analysis

5.2.2 Encryption Overhead Analysis

5.3 Anomaly Detection Results

5.4 AI Response Evaluation

5.5 Privacy–Utility Trade-off Analysis

5.6 Security Analysis

5.7 Comparative Discussion

Chapter 6

Conclusion and Future Work

6.1 Summary of the Work

6.2 Key Findings

6.3 Limitations of the Study

6.4 Future Research Directions

Bibliography

[1] M. M. Hasan, A. Rahman, and S. Ahmed, "Internet of Things-based Home Automation with Network Mapper and MQTT Protocol," *Computers & Education: Artificial Intelligence*, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790624007341

[2] A. Author, B. Author, and C. Author, "Generative AI Techniques for Anomaly Detection in IoT Devices," 2024. [Online]. Available: https://www.researchgate.net/publication/395801862_GENERATIVE_AI_TECHNIQUES_FOR_ANOMALY_DETECTION_IN_IOT_DEVICES

[3] B. Author, D. Author, and E. Author, "Anomaly Detection in IoT Using Generative AI Models," *SPIE Conference Proceedings*, vol. 13473, 2024. [Online]. Available: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/13473/134730J/AD-GAM--anomaly-detection-in-IoT-using-generative-AI/10.1117/12.3058632.full

[4] C. Author, F. Author, and G. Author, "Review: Generative Adversarial Networks-Enabled Anomaly Detection in IoT," *Expert Systems with Applications*, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417425025953

[5] D. Author, H. Author, and I. Author, "AI-Driven Anomaly Detection for Securing IoT Devices in Smart Cities," *Electronics*, vol. 14, no. 12, p. 2492, 2025. [Online]. Available: https://www.mdpi.com/2079-9292/14/12/2492

[6] E. Author, J. Author, and K. Author, "Privacy-Preserving Security of IoT Networks: A Comparative Study," *ScienceDirect*, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2772918425000013

[7] F. Author, L. Author, and M. Author, "Leveraging IoT, Cloud, and Edge Computing with AI," *Sensors*, vol. 25, no. 6, p. 1763, 2025. [Online]. Available: https://www.mdpi.com/1424-8220/25/6/1763

[8] G. Author, N. Author, and O. Author, "Towards Smart Home Automation Using IoT-Enabled Edge-Computing Paradigm," 2021. [Online]. Available: https://www.researchgate.net/publication/353372471_Towards_Smart_Home_Automation_Using_IoT-Enabled_Edge-Computing_Paradigm

[9] H. Author, P. Author, and Q. Author, "Improving Smart Home Security via MQTT: Maximizing Data Confidentiality and Energy Efficiency," *CSSE*, vol. 48, no. 6, p. 58697, 2025. [Online]. Available: https://www.techscience.com/csse/v48n6/58697

[10] I. Author, R. Author, and S. Author, "Enhancing MQTT Security on the Internet of Things with an Enhanced Symmetric Algorithm," 2025. [Online]. Available: https://www.researchgate.net/publication/379866006_Enhancing_MQTT_Security_in_the_Internet_of_Things_with_an_Enhanced_Symmetric_Algorithm

[11] J. Author, K. Author, and L. Author, "Hybrid Approaches to Predictive Maintenance: Combining Generative AI with IoT Sensor Data for Enhanced Failure Prediction," 2024. [Online]. Available: https://www.researchgate.net/publication/395791187_Hybrid_Approaches_to_Predictive_Maintenance_Combining_Generative_AI_with_IoT_Sensor_Data_for_Enhanced_Failure_Prediction

[12] K. Author, M. Author, and N. Author, "Generative AI for Internet of Things Security: Challenges and Opportunities," 2025. [Online]. Available: https://arxiv.org/abs/2502.08886

[13] L. Author, O. Author, and P. Author, "The Role of Smart Homes in Providing Care for Older Adults," *MDPI*, vol. 7, no. 4, p. 62, 2025. [Online]. Available: https://www.mdpi.com/2624-6511/7/4/62

[14] M. Author, Q. Author, and R. Author, "Internet of Robotic Things for Independent Living Support," *ScienceDirect*, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660524000623

[15] N. Author, S. Author, and T. Author, "Design and Implementation of Smart Home System Based on IoT," *ScienceDirect*, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2590123024016621

[16] O. Author, U. Author, and V. Author, "Design of an Innovative Solution to Integrate and Automate Smart Homes via Multiple Chatbots," *ScienceDirect*, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660525002070

[17] P. Author, W. Author, and X. Author, "Adoption of Internet of Things in Residential Smart Homes," *ScienceDirect*, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666188825002333

[18] Q. Author, Y. Author, and Z. Author, "MQTT_UAD: MQTT Under Attack Dataset — A Public Benchmark for MQTT Security Research," *ScienceDirect*, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352340925008881

[19] R. Author, A1. Author, and B1. Author, "Edge AI Enabled IoT Framework for Secure Smart Home Infrastructure," *ScienceDirect*, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050924009979

[20] S. Author, C1. Author, and D1. Author, "Machine Learning and IoT in Healthcare," *ScienceDirect*, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2543106425000201

[21] T. Author, E1. Author, and F1. Author, "Toward Generating a Large-Scale IoT-Z-Wave Intrusion Detection Dataset: Smart Device Profiling, Intruder Behavior, and Traffic Characterization," *ScienceDirect*, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660525002616

[22] U. Author, G1. Author, and H1. Author, "Smart Home System: A Comprehensive Review," *Wiley Interdisciplinary Reviews*, 2023. [Online]. Available: https://onlinelibrary.wiley.com/doi/epdf/10.1155/2023/7616683

[23] V. Author, I1. Author, and J1. Author, "Artificial Intelligence in Smart Cities — Applications, Barriers, and Future Directions: A Review," *MDPI*, vol. 7, no. 3, p. 57, 2025. [Online]. Available: https://www.mdpi.com/2624-6511/7/3/57

[24] W. Author, K1. Author, and L1. Author, "IoT — A Promising Solution to Energy Management in Smart Buildings: A Systematic Review, Applications, Barriers, and Future Scope," *MDPI*, vol. 14, no. 11, p. 3446, 2025. [Online]. Available: https://www.mdpi.com/2075-5309/14/11/3446

[25] X. Author, M1. Author, and N1. Author, "Review of Smart-Home Security Using the Internet of Things," *MDPI Electronics*, vol. 13, no. 16, p. 3343, 2025. [Online]. Available: https://www.mdpi.com/2079-9292/13/16/3343

[26] Y. Author, O1. Author, and P1. Author, "Smart Home Advancements for Health Care and Beyond: Systematic Review of Two Decades of User-Centric Innovation," *JMIR*, 2025. [Online]. Available: https://www.jmir.org/2025/1/e62793

[27] Z. Author, Q1. Author, and R1. Author, "Machine Learning in Smart Buildings: A Review of Methods, Challenges, and Future Trends," *MDPI Applied Sciences*,

vol. 15, no. 14, p. 7682, 2025. [Online]. Available: https://www.mdpi.com/2076-3417/15/14/7682

[28] A1. Author, B1. Author, and C1. Author, "Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions," *Springer*, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s43926-024-00084-3

[29] B1. Author, D1. Author, and E1. Author, "IoT-Based Security and Privacy Implementation in Smart Home," *IJFANS*, 2022. [Online]. Available: https://www.ijfans.org/issue?volume=Volume%2011&issue=Issue%205&year=2022

[30] C1. Author, F1. Author, and G1. Author, "Smart Home Remote Control System Prototype Using Internet of Things (IoT) Based ESP8266 Microcontroller," 2023. [Online]. Available: https://www.researchgate.net/publication/376060810_Smart_Home_Remote_Control_System_Prototype_Using_Internet_of_Things_IoT_Based_ESP8266_Microcontroller

[31] D1. Author, H1. Author, and I1. Author, "IoT Enabled Smart Homes in Tropical Regions as a Means of Sustainable Development," *IOP Conference Series*, 2023. [Online]. Available: https://iopscience.iop.org/article/10.1088/1755-1315/1306/1/012035/pdf

[32] E1. Author, J1. Author, and K1. Author, "A Comprehensive Survey on Generative AI Solutions in IoT Security," *MDPI Electronics*, vol. 13, no. 24, p. 4965, 2025. [Online]. Available: https://www.mdpi.com/2079-9292/13/24/4965

[33] F1. Author, L1. Author, and M1. Author, "IoT Based Smart Door Unlock and Intruder Alert System," 2021. [Online]. Available: https://www.researchgate.net/publication/356206104_IoT_Based_Smart_Door_Unlock_and_Intruder_Alert_System

[34] G1. Author, N1. Author, and O1. Author, "An Internet of Things-driven Smart Key System with Real-Time Alerts: Innovations in Hotel Security," 2025. [Online]. Available: https://www.researchgate.net/publication/389470099_An_internet_of_things-driven_smart_key_system_with_real-time_alerts_innovations_in_hotel_security

[35] H1. Author, P1. Author, and Q1. Author, "Design of ESP8266 Smart Home Using MQTT and Node-RED," 2021. [Online]. Available: https:

//www.researchgate.net/publication/350935668_Design_of_ESP8266_Smart_Home_Using_MQTT_and_Node-RED

[36] [Author(s)], "Smart Home Privacy: A Scoping Review," 2024. [Online]. Available: https://www.scitepress.org/Papers/2024/122559/122559.pdf

[37] [Author(s)], "IoT Based Security and Privacy Implementation in Smart Home," 2024. [Online]. Available: https://www.researchgate.net/publication/378739063_IoT_based_security_and_privacy_implementation_in_smart_home

[38] [Author(s)], "Generative AI for Internet of Things Security: Challenges and Opportunities," 2025. [Online]. Available: https://arxiv.org/abs/2502.08886

[39] [Author(s)], "AD-GAM: Anomaly Detection in IoT Using Generative AI Models," 2025. [Online]. Available: https://www.researchgate.net/publication/392192530_AD-GAM_anomaly_detection_in_IoT_using_generative_AI_models

[40] [Author(s)], "Generative AI Techniques for Anomaly Detection in IoT Devices," 2025. [Online]. Available: https://www.researchgate.net/publication/395801862_GENERATIVE_AI_TECHNIQUES_FOR_ANOMALY_DETECTION_IN_IOT_DEVICES

[41] [Author(s)], "LLM-Enhanced Security Framework for IoT Network: Anomaly Detection," 2025. [Online]. Available: https://ieeexplore.ieee.org/iel8/6287639/10820123/11175688.pdf

[42] [Author(s)], "An LLM-Powered AI Agent Framework for Holistic IoT Traffic Interpretation," 2025. [Online]. Available: https://arxiv.org/abs/2510.13925

[43] [Author(s)], "Efficient Real-Time Anomaly Detection in IoT Networks Using One-Class Autoencoder," 2025. [Online]. Available: https://www.mdpi.com/2079-9292/14/1/104

[44] [Author(s)], "Large Language Models in the IoT Ecosystem: A Survey on Security Challenges," 2025. [Online]. Available: https://arxiv.org/abs/2505.17586

[45] [Author(s)], "Secure Enhancement for MQTT Protocol Using Distributed Machine Learning," 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/5/1638

[46] [Author(s)], "Federated Learning for IoT: A Survey of Techniques, Challenges, and Applications," 2024. [Online]. Available: https://www.mdpi.com/2224-2708/14/1/9

[47] [Author(s)], "Anomaly Detection in IoT Networks Using Federated Machine Learning Approaches," 2025. [Online]. Available: https://www.researchgate.net/publication/392893320_Anomaly_Detection_in_IoT_Networks_Using_Federated_Machine_Learning_Approaches

[48] [Author(s)], "Privacy Preserving Federated Anomaly Detection in IoT Edge Computing," 2025. [Online]. Available: https://www.techscience.com/cmc/v84n2/62939

[49] [Author(s)], "DLKS-MQTT: A Lightweight Key Sharing Protocol for Secure IoT Communications," 2025. [Online]. Available: https://etasr.com/index.php/ETASR/article/view/10216

[50] [Author(s)], "Integrating Blockchain, MQTT, and Machine Learning for Enhanced IoT Applications," 2025. [Online]. Available: https://www.researchgate.net/publication/396031010_Integrating_Blockchain_MQTT_and_Machine_Learning_for_Enhanced_IoT_Applications_A_Comprehensive_Survey

[51] [Author(s)], "MQTT in Action: Building Reliable and Scalable Home Automation Systems," 2024. [Online]. Available: https://www.researchgate.net/publication/387574531_MQTT_in_Action_Building_Reliable_and_Scalable_Home_Automation_Systems

[52] [Author(s)], "Improving IoT Management with Blockchain: Smart Home Access Control," 2024. [Online]. Available: https://www.ejobsat.cz/pdfs/ejo/2024/02/04.pdf

[53] [Author(s)], "A Survey on Diffusion Models for Anomaly Detection," 2025. [Online]. Available: https://arxiv.org/abs/2501.11430

[54] [Author(s)], "SCConv-Denoising Diffusion Probabilistic Model Anomaly Detection," 2025. [Online]. Available: https://www.mdpi.com/2079-9292/14/4/746

[55] [Author(s)], "On Diffusion Modeling for Anomaly Detection," 2024. [Online]. Available: https://openreview.net/forum?id=lR3rk7ysXz

[56] [Author(s)], "Anomaly Detection and Generation with Diffusion Models: A Survey," 2025. [Online]. Available: https://arxiv.org/abs/2506.09368

[57] [Author(s)], "A Low-Cost IoT-Based Smart Home Automation System for Urban Sustainability," 2025. [Online]. Available: https://link.springer.com/article/10.1007/s43926-025-00207-4

[58] [Author(s)], "Generative AI Advances for Data-Driven Insights in IoT and Cloud," 2025. [Online]. Available: https://www.researchgate.net/publication/387773122_Generative_AI_advances_for_data-driven_insights_in_IoT_cloud_technologies_and_big_data_challenges

[59] [Author(s)], "Combining Edge Computing-Assisted IoT Security with Artificial Intelligence," 2024. [Online]. Available: https://www.mdpi.com/2076-3417/14/16/7104

[60] [Author(s)], "Differential Privacy for IoT-Enabled Critical Infrastructure: A Comprehensive Survey," 2022. [Online]. Available: https://www.researchgate.net/publication/355765966_Differential_Privacy_for_IoT-Enabled_Critical_Infrastructure_A_Comprehensive_Survey

[61] [Author(s)], "Achieving Differential Privacy in Smart Home Scenarios," 2022. [Online]. Available: https://scispace.com/pdf/achieving-differential-privacy-in-smart-home-scenarios-1akhdv9y9j.pdf

[62] [Author(s)], "Enhancing Smart Home Security: Blockchain-Enabled Federated Learning with Knowledge Distillation for Intrusion Detection," [Year]. [Online]. Available: https://www.mdpi.com/2624-6511/8/1/35

Appendix A

Appendix