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

ACKNOWLEDGEMENT **i**

CERTIFICATE **ii**

CERTIFICATE **iii**

CERTIFICATE **iv**

CERTIFICATE **v**

DECLARATION **vi**

Abstract **vii**

List of Figures **xi**

List of Tables **xii**

List of Abbreviations **xiii**

List of Symbols **xiv**

1 Introduction **1**

1.1 Background and Motivation 1
1.2 Problem Statement 1
1.3 Research Gap 1
1.4 Research Objectives 1
1.5 Contributions of the Thesis 1
1.6 Scope of the Thesis 1
1.7 Thesis Organization 1

2 Related Work **2**

2.1 MQTT-Based Smart Home Architectures 2
2.2 Privacy-Preserving IoT Systems 2
2.3 Cryptographic Mechanisms in IoT Security 2

2.4 Anomaly Detection Techniques in IoT 2
2.5 Generative AI for Real-Time Monitoring 2
2.6 Limitations of Existing Approaches 2

3 Proposed System **3**
3.1 Overall System Overview 3
3.2 System Architecture Design 3
3.3 Hardware Architecture (ESP32 and Sensors) 3
3.4 Software Architecture 3
3.5 MQTT Communication Model 3
3.6 Privacy-Preserving Data Pipeline 3
3.6.1 Differential Privacy with Dual Gaussian Noise 3
3.6.2 RSA-2048 Encryption Mechanism 3
3.7 AI-Based Anomaly Detection Framework 3
3.7.1 Threshold-Based Detection Logic 3
3.7.2 Local LLM Integration (Llama 3.2 via Ollama) 3
3.8 End-to-End System Workflow 3

4 Implementation **4**
4.1 Hardware Implementation Details 4
4.2 Software Development Environment 4
4.3 MQTT Broker Configuration 4
4.4 Differential Privacy Implementation 4
4.5 RSA Encryption Implementation 4
4.6 Local LLM Deployment Setup 4
4.7 Database Design and Storage Model 4

5 Results and Discussion **5**
5.1 Experimental Setup 5
5.2 Performance Evaluation 5
5.2.1 System Latency Analysis 5
5.2.2 Encryption Overhead Analysis 5
5.3 Anomaly Detection Results 5
5.4 AI Response Evaluation 5
5.5 Privacy–Utility Trade-off Analysis 5
5.6 Security Analysis 5
5.7 Comparative Discussion 5

6 Conclusion and Future Work **6**
6.1 Summary of the Work 6

6.2 Key Findings 6
6.3 Limitations of the Study 6
6.4 Future Research Directions 6

References **6**

A Appendix **12**

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

1.2 Problem Statement

1.3 Research Gap

1.4 Research Objectives

1.5 Contributions of the Thesis

1.6 Scope of the Thesis

1.7 Thesis Organization

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

Appendix A

Appendix