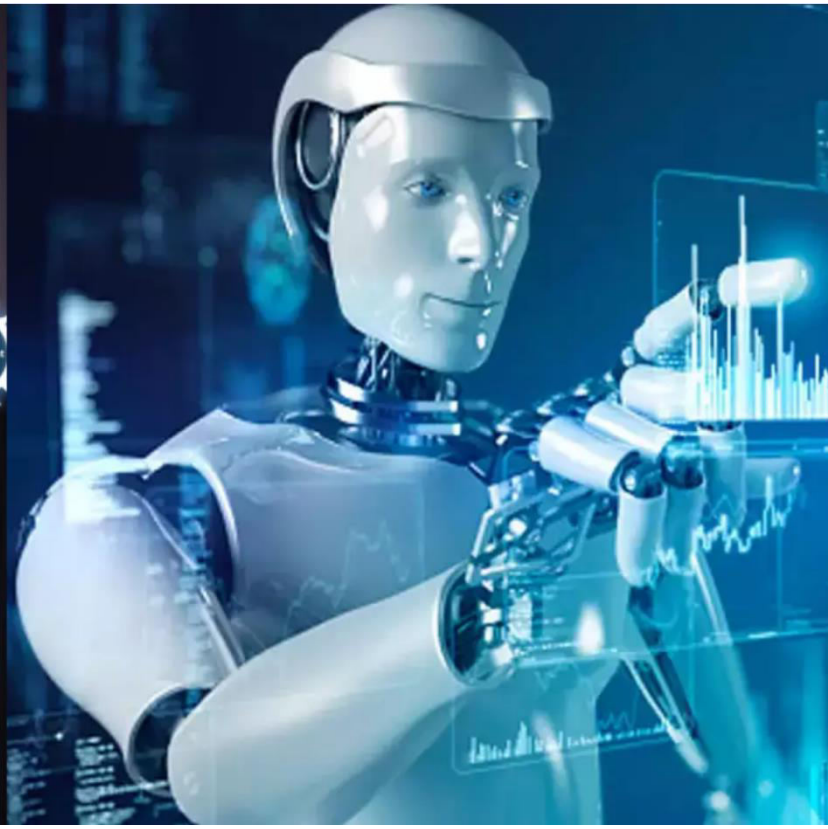
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404554|

A Secure and Anonymous user Authentication Scheme for IoT- Enabled Smart Home Environments using PUF

Ms.Lethisia Nithiya[1], Kavala Raja Surendra[2], Kollimarla Prem Sagar[3], Kintada Durga Bhavani[4], Kaviya Ramakrishnan[5]

IV – B. Tech Students, Bharath Institute of Higher Education and Research, Selaiyur, Chennai, Tamil Nadu, India [2-4]

Professor, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Selaiyur, Chennai, Tamil Nadu, India [1]

ABSTRACT: This report presents a secure and anonymous user authentication scheme tailored for IoT-enabled smart home environments, where the increasing interconnectivity of devices has raised serious concerns about security and privacy. Traditional authentication techniques often fail to accommodate the limitations of smart devices, such as limited processing power, energy constraints, and susceptibility to physical attacks. To overcome these challenges, the proposed scheme leverages Physical Unclonable Functions (PUFs) — hardware-based security primitives that generate unique and tamper-resistant device identities. These PUFs enable strong authentication without revealing personal user information, thereby preserving anonymity and preventing tracking. The scheme employs lightweight cryptographic operations including hash functions (SHA-3, HMAC) and XOR operations, making it highly efficient and suitable for resource-constrained environments. It encompasses multiple phases such as device registration, user registration, secure login, mutual authentication, and password updates. The system is designed to withstand common attacks like replay, impersonation, and man-in-the-middle by incorporating mutual authentication and forward secrecy. Security analysis and performance evaluations confirm the scheme's effectiveness, scalability, and practicality. By integrating PUF-based authentication, this report offers a robust, scalable, and privacy-preserving solution for enhancing trust and security in smart home ecosystems.

I. INTRODUCTION

The Internet of Things (IoT) refers to the vast network of interconnected devices embedded with sensors, software, and communication technologies that enable them to collect, exchange, and act upon data. Over the past decade, IoT has gained significant momentum in various domains, including healthcare, agriculture, transportation, and notably, smart homes. In the context of smart homes, IoT devices are integrated into residential environments to provide automated control, monitoring, and management of home systems such as lighting, security, heating, ventilation, air conditioning (HVAC), entertainment, and appliances.

The smart home ecosystem typically includes multiple components such as sensors, actuators, smart appliances, mobile devices, and gateways that communicate over wireless networks like Wi-Fi, Zigbee, Z-Wave, or Bluetooth. These components work in tandem to enhance comfort, efficiency, and safety within the home. For instance, smart thermostats learn user preferences to optimize energy consumption, me while smart locks and surveillance systems offer enhanced security and remote monitoring capabilities.

Smart homes offer significant benefits, including increased energy efficiency, convenience, remote accessibility, and improved lifestyle quality. The convenience of controlling household functions from a mobile device or through voice assistants such as Amazon Alexa or Google Assistant has made smart home technology increasingly attractive and accessible to the average consumer. Additionally, the integration of machine learning and artificial intelligence (AI) allows smart systems to adapt to user behavior over time, further enhancing the automation and intelligence of home environments.

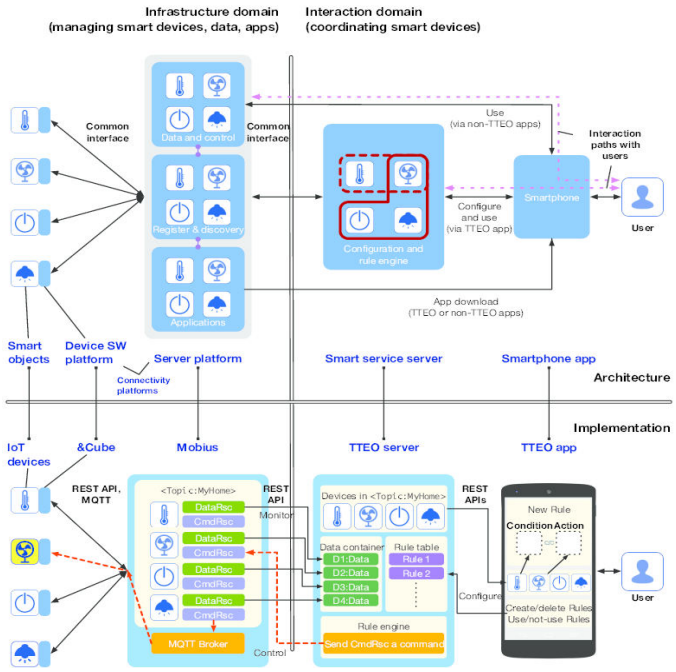
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404554|



IoT devices in smart homes introduces numerous challenges, especially in terms of security, privacy, and trust. The exchange of sensitive data over public or private networks raises the risk of unauthorized access, data breaches, and cyberattacks. Moreover, many IoT devices are designed with limited processing power, memory, and energy resources, making it difficult to implement traditional heavy-weight security protocols.

herefore, as the demand for smarter living spaces continues to grow, ensuring secure and private communication between users and devices becomes critical. Authentication mechanisms must evolve to meet the specific constraints and requirements of IoT devices, ensuring not only system integrity and confidentiality but also user anonymity. The background and growth of IoT in smart homes highlight the need for innovative, lightweight, and scalable authentication solutions tailored for resource-constrained environments.

II. METHODOLOGY

The Smart Service Platform for IoT device coordination is built on a layered and modular architecture, enabling interoperability, scalability, and user-centric control. The architecture is divided into five primary modules:

- Smart Object & Connectivity Module
- Device & Server Platform Module
- Smart Service & Rule Engine Module
- User Interaction Module (Smartphone App)
- Application & Control Interface Module

System Requirements and Specifications

The Secure Authentication System using PUF for IoT-based Smart Home Applications requires a combination of suitable hardware and software environments to ensure secure data handling, efficient processing, and a smooth user experience. The requirements are

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404554|

Hardware Requirements

This system is designed to work on IoT-enabled smart home devices and an administrative dashboard. The following specifications are recommended:

Minimum Requirements:

- Processor: ARM Cortex-M4 or equivalent microcontroller (for IoT device)
- RAM: 2 GB (for dashboard/client interface)
- Storage: 10 GB free disk space (for logs and activity tracking)
- Connectivity: Wi-Fi/Bluetooth module for IoT communication
- Display: 1024x600 pixels (for interface-based interaction)
- Operating System: Windows 10 / Linux / Raspbian OS (for Raspberry Pi)

Recommended Requirements:

- Processor: ARM Cortex-A72 or higher (for edge devices) / Intel i5 or above (for server-side)
- RAM: 4 GB or more (client) / 8 GB or more (server)
- Storage: 30 GB free disk space
- Connectivity: Wi-Fi 6 / Zigbee / LoRa (for advanced smart home mesh)

Operating System: Linux (Ubuntu 20.04 or above), Raspbian OS, Windows

Software Requirements

The system integrates cryptographic operations, user authentication protocols, and device identity verification. The software stack includes:

Supported Operating Systems:

Windows 10 or above
Linux (Ubuntu 20.04 or above)
Raspbian OS for Raspberry Pi-based devices

Programming Language:

- **Python (Version 3.8 or above)**
- **C/C++** (for low-level PUF device interactions)

Python Libraries and Dependencies:

- cryptography: For encryption and secure key generation
- pySerial: For communication with IoT PUF devices
- Flask or Django: For web interface/dashboard
- sqlite3 or MySQL: For authentication data storage
- RPi.GPIO: For GPIO interfacing with Raspberry Pi (if used)
- requests: For REST API communications

Installation Tools:

- pip: For Python package installation
- venv: For virtual environment setup
- Make/GCC: For compiling embedded C code on microcontrollers

Technical Specifications

The system comprises multiple interconnected modules to ensure security, usability, and privacy.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404554|

- **PUF Module:** Generates a unique fingerprint for each device using inherent manufacturing variability. This serves as a hardware root of trust.
- **Authentication Protocol Module:** Implements challenge-response mechanisms using the PUF's response and secure hashing algorithms (SHA-256, HMAC).
- **User Interface Module:** Built using Flask/Tkinter (optional), allowing users to log in, monitor devices, and manage authentication settings.
- **Data Storage Module:** Stores user session data, encrypted logs, and device IDs. Provides access control based on user roles.
- **Communication Module:** Uses secure REST APIs over HTTPS or MQTT for encrypted communication between devices and the server.
- **Security Monitoring Module:** Tracks failed login attempts, unauthorized access patterns, and logs activity for audit purposes.

PRELIMINARIES

In this section, we describe the system model, PUF, fuzzy extractor, notations, and threat model to review the Zou *et al.*'s scheme and to help the understanding of our proposed scheme.

III. SYSTEM MODEL

The entities in our system model are composed of the regis- tration center, home users, gateway, and home devices. In our scheme, home users store secret credentials on a smart card by registering in the registration center. Similarly, home devices register with the registration center to generate a unique secret key using PUF. The gateway maintains a verification table to authenticate home users and home devices. Afterword, home users and home devices perform mutual authentication with each other using the secret credentials and secret key gener- ated during the registration phase. If mutual authentication succeeds, home users, gateway, and home devices compute a shared session key and use it to communicate with each other. Descriptions of each entity are as follows.

Registration center: The registration center registers the home users and home devices in the smart home. In our system model, the registration center is regarded as a fully trusted entity.

- **Home users:** These are residents of the smart home. Before using the smart home service, home users register with the registration center. Home users can authenticate with home devices using a smart card obtained from the registration center.
- **Gateway:** The gateway oversees public channel com- munication of entities. The gateway supports mutual authentication between home users and home devices.

Home devices: Before home devices are deployed in the smart home, they register based on the physical properties of the device, it is impossible to replicate and predict even if the manufacturing process is reproduced. The characteristics of PUF used in our paper are summarized below.

- When C is the challenge and R is the response, $PUF(C) = R$.
- Even if the challenge value is known, it is impossible to predict the response value of a specific device.
- All PUF devices output different response values even if the same challenge value is input.

To utilize the characteristics of PUF for authentication, it is necessary to stabilize the noise that occurs when the response is generated. We use a fuzzy extractor to remove the noise of the PUF and extract a constant output.

FUZZY EXTRACTOR

Fuzzy extractor [27] is a technology that generates a fixed secret key when a noise-containing value is input. When the fuzzy extractor receives an input value, it generates a bit string s as a secret key and a helper bit string h for error correction. Even if there is a slight error in the input value, the fuzzy extractor can extract the same secret key with the help of helper bit string. In our scheme, we use the generation and reproduction functions of the fuzzy extractor. The

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404554|

description of each function is as follows.

- $Gen(Y) = (h, s)$: Generation function generates helper bit string h and secret bit string s by inputting a random value Y including noise.
- $Rep(Y^r, h) = s^r$: Reproduction function extracts the secret bit string s^r using a random value Y^r containing noise and the helper bit string h^r. The generated s^r is the same as the generated s in $Gen(Y)$.

NOTATIONS

The notations used in our paper are listed in Table 1.

THREAT MODEL

We consider Dolev-Yao (DY) model [28] for security analysis of our scheme. DY model is a popular analysis tool used for security analysis of multiple authentication schemes. Under the DY model, a malicious adversary can control all messages exchanged in public channels. Furthermore, we apply Canetti-Krawczyk (CK) model [29] to validate the security of our scheme on a more robust adversary assumption. In the CK model, the adversary can corrupt the session state and obtain the short-term key or long-term key. According to the DY model and the CK model, we assume that the adversary's

capabilities are as follows:

The adversary can completely control communications over public channels by interfering with, modifying, or deleting messages. Then, the adversary can attempt passive or active security attacks. The adversary can conduct offline password guess- ing attack within the polynomial

Symbol	Description
ID_i, PW_i	Identity and password of home user
PID_i	Temporary identity of home user
SID_j	Identity of home device
RID_i, DID_j	Pseudo identity of home user and home device
K_{GU}, K_{GS}	Secret key of home user and home device
K_{UG_i}, K_{HD_j}	Long-term key of home user and home device
s, t, b	Master key of registration center, gateway, and home device
C_j, R_j	Challenge and response of PUF
n_0, w	Fuzzy verifier
$PUF(.)$	PUF operation
SK	Session key
a_1, a_2, a_3	Random nonce
$Gen(.)/Rep(.)$	Generation/reproduction function
$h(.)$	One-way hash function
$\oplus$	Exclusive-OR (XOR) operation
$\|\|$	Message concatenation operarion

TABLE 1. Notations.

- Under the CK model assumption, the adversary can obtain session-specific temporary information, such as a random nonce generated in each session. Thereafter, the adversary tries to compute the session key [31].
- The adversary can extract the sensitive information stored in the user smart card or the home device using a power analysis attack [32]. The adversary can use this information to attempt to generate a valid authentication message.
- The adversary can register as a legitimate user of the smart home. The adversary then attempts to impersonate another legitimate user with his/her secret credentials.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404554|

REVIEW OF ZOU *et al.*'s SCHEME

In this section, we quickly review Zou *et al.*'s user authenti- cation scheme. Zou *et al.*'s scheme has system setup, home device registration, home user registration, login and verifi- cation, and password update phases. A detailed description of each phase is as follows.

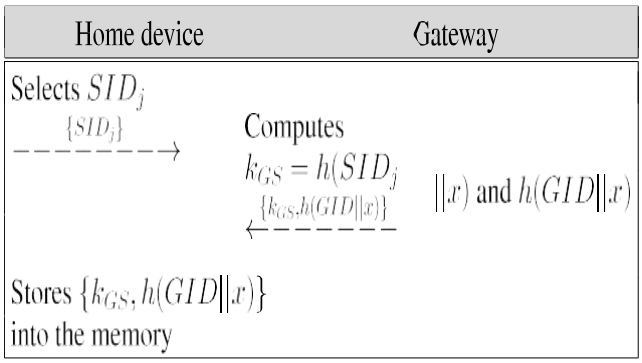
SYSTEM SETUP PHASE

In the system setup phase, the gateway chooses an elliptic curve $E(F_p)$ and a base point P on the finite field. Then, the gateway generates long-term key x e F_p and computes $h(GID||x)$ as secret parameter. The gateway publishes $X = x \cdot P$ as an open parameter of the system.

HOME DEVICE REGISTRATION PHASE

Before deploying the home device to the smart home, the home device registers to the gateway as shown in Figure 2.

HDR 1: The home device selects SID_j and sends it to the gateway.



IV. PROPOSED SCHEME

In this section, we propose a PUF-based user authentication scheme for smart home that overcomes the security vulnera- bilities of Zou *et al.*'s scheme. The proposed scheme consists of system setup, home device registration, home user regis- tration, login and verification, and password update phases. The following subsections describe each phase.

SYSTEM SETUP PHASE

Before the gateway and home device are deployed in the smart home, the registration center generates t as the gate- way's master key and C_j as the home device's challenge value. After that, the registration center stores it securely in each entity's memory. The registration center selects one-way hash function $h(.) : \{0,1\}^* \rightarrow \{0,1\}^l$ as system parameter and the $h(DID_j||t)$. After that, the registration center stores $\{DID_j, C_j, PD_j, B_j\}$ into the memory of GW and trans- mits $\{DID_j, K_{HDj}, h_j\}$ to the home device.

- HDR 3: Upon receiving them, the home device com- putes $H_j = D_j \oplus h_j$ and deletes D_j. Finally, the home device stores $\{HS_j, H_j, K_{HDj}\}$ into the its memory.

V. CONCLUSION

In this work, a secure and anonymous user authentication scheme for IoT-enabled smart home environments using Physical Unclonable Functions (PUFs) has been proposed and analyzed. The integration of PUFs significantly enhances device-level security by providing unique and tamper-resistant hardware identifiers, thereby reducing the risk of cloning and impersonation attacks. The proposed scheme ensures user anonymity, mutual authentication, and resistance to various common cyber threats, including replay and man-in-the-middle attacks. Additionally, it maintains lightweight computational and communication overhead, making it highly suitable for resource-

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404554|

constrained IoT devices commonly found in smart homes. This approach strengthens trust and privacy in smart environments, paving the way for safer and more robust smart home systems

VI. ACKNOWLEDGMENT

The author would like to express their thanks & gratitude to all those who gave suggestions and valuable contributions to this work. The authors would also like to thank the reviewers for their comments to improve this paper. Our special thanks to Prof
Vineet Richaria, Head, Computer Science and Engg Dept.,LNCT, Bhopal, India. And Asst Prof Vijay Kumar Trivedi Computer Science and Engg Dept., LNCT, Bhopal, India whose help, stimulating suggestions, experience and encouragement helped us in all the times of study and analysis of this work.

REFERENCES

1. W. Yan, Z. Wang, H. Wang, W. Wang, J. Li, and X. Gui, "Survey on recent smart gateways for smart home: Systems, technologies, and challenges," Trans. Emerg. Telecommun. Technol., vol. 33, no. 6, p. e4067, Jun. 2022.
2. D. Bouchabou, S. M. Nguyen, C. Lohr, B. LeDuc, and I. Kanellos, "A survey of human activity recognition in smart Homes based on IoT sensors algorithms: Taxonomies, challenges, and opportunities with deep learning," Sensors, vol. 21, no. 18, p. 6037, Sep. 2021.
3. Z. A. Almusaylim and Z. Noor, "A review on smart home present state and challenges: Linked to context-awareness Internet of Things (IoT)," Wireless Netw., vol. 25, no. 6, pp. 3193–3204, Aug. 2019.
4. D. K. Kwon, S. J. Yu, J. Y. Lee, S. H. Son, and Y. H. Park, "WSN-SLAP:
5. Secure and lightweight mutual authentication protocol for wireless sensor networks," Sensors, vol. 21, no. 3, p. 936, Jan. 2021.
6. Marella, B. C. C., & Kodi, D. (2025). Generative AI for Fraud Prevention: A New Frontier in Productivity and Green Innovation. In Advancing Social Equity Through Accessible Green Innovation (pp. 185-200). IGI Global Scientific Publishing.
7. A. K. Sutrala, M. S. Obaidat, S. Saha, A. K. Das, M. Alazab, and Y. Park, "Authenticated key agreement scheme with user anonymity and untrace- ability for 5G-enabled softwarized industrial cyber-physical systems," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 3, pp. 2316–2330, Mar. 2022.
8. G. Abbas, M. Tanveer, Z. H. Abbas, M. Waqas, T. Baker, and
9. D. Al-Jumeily, "A secure remote user authentication scheme for 6LoWPAN-based Internet of Things," PLoS ONE, vol. 16, no. 11, Nov. 2021, Art. no. e0258279.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details