VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2025, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 13, Number 1, January-March 2025 *pp:37-48*

A novel Primary Key infrastructure IoT enabled secure Access Control Framework Based smart home applications

Muhammad Faisal Memon[1], **Rahila Shah**[2], **Amjad Ali**[3], **Abdullah Lakhan**[4]

[1]Department of Cybersecurity, Dawood University of Engineering and Technology, Pakistan; [2]Department of Artificial Intelligence, Dawood University of Engineering and Technology, Pakistan; [3]Department of Information Computing, Telecom, Pakistan; [4]Department of Cybersecurity, Dawood University of Engineering and Technology, Pakistan.

Keywords: *Secure Access, IoT, Machine Learning, Users, Attacks.*
Journal Info:
Submitted:
January 14, 2025
Accepted:
January 17, 2025
Published:
January 30, 2025

Abstract

This paper presents a comprehensive security framework for smart home environments, integrating advanced authentication, access control mechanisms, and machine learning for robust IoT protection. A typical smart home ecosystem is illustrated with interconnected devices—air conditioning systems, robotic assistants, surveillance cameras, and thermostats—linked through a centralised wireless network that facilitates seamless communication and remote control via the internet. The framework emphasises secure authentication and authorisation processes, using public key infrastructure (PKI) to validate devices and users while issuing, renewing, and revoking certificates for encrypted communication. The mathematical model outlines device and user authentication, validation functions, and access control mechanisms to ensure secure operations. Fine-grained access control is implemented to grant permissions based on specific conditions, ensuring flexible yet secure resource allocation. Communication security is maintained through encryption and decryption, safeguarding data transmitted across devices and networks. To mitigate security risks, a convolutional neural network is employed for anomaly detection, identifying threats by recognising deviations in regular patterns. Additionally, the framework addresses interoperability by adhering to standard-compliance protocols, facilitating seamless integration across diverse devices. Resource optimisation techniques are introduced to maximise efficiency based on the number and capabilities of devices in the network. User interaction is streamlined through an intuitive interface that supports secure and user-friendly system access. The proposed SAC-PKI algorithm serves as the foundation for the framework, detailing sequential steps for authentication, certificate management, access control, and anomaly detection. By leveraging adaptive security features and advanced threat detection, this framework provides a robust solution for enhancing the cybersecurity of smart home deployments, addressing vulnerabilities, and ensuring efficient resource utilisation in IoT environments.

***Correspondence author email address:** abdullah.lakhan@duet.edu.pk
DOI: 10.21015/vtse.v13i1.2040

1 Introduction

The Internet of Things (IoT) proliferation has transformed various domains, including healthcare, transportation, agriculture, and, notably, smart homes[1]. Smart home applications rely on IoT devices to offer enhanced automation, convenience, energy efficiency, and security. However, the increasing integration of IoT devices into smart home ecosystems has also introduced significant challenges, particularly regarding data security and privacy. These challenges arise from the constrained nature of IoT devices, the dynamic nature of smart home environments, and the evolving landscape of cybersecurity threats. Among the critical security concerns is access control, which ensures that only authorised entities can access or control IoT devices. Addressing these issues necessitates a robust, scalable, and secure framework that aligns with the resource limitations and diverse requirements of IoT-enabled smart homes.

A secure access control framework for IoT-based smart home applications ensures that sensitive data remains protected, devices are not maliciously manipulated, and the system operates reliably. Traditional access control mechanisms, such as role-based access control (RBAC) and discretionary access control (DAC), are often not suited for IoT environments due to their inability to handle IoT systems' distributed and resource-constrained nature. This paper proposes a novel Primary Key Infrastructure (PKI)-enabled IoT secure access control framework based on a client-server architecture to overcome these limitations. This framework leverages cryptographic techniques, real-time authentication, and scalable key management to ensure the security and privacy of smart home applications. Smart homes, characterised by interconnected devices such as smart thermostats, cameras, locks, and lighting systems, are at the forefront of IoT innovation. These devices communicate through various protocols and networks, creating a highly dynamic and heterogeneous environment. The complexity of smart home ecosystems necessitates advanced access control mechanisms capable of addressing the following key challenges:

Many IoT devices have limited computational power, memory, and energy resources, making them vulnerable to attacks that exploit their weaknesses[2].

IoT systems are susceptible to attacks, including device spoofing, unauthorized access, data interception, and distributed denial-of-service (DDoS) attacks[3].

Smart homes can include numerous devices with varying capabilities and security requirements, necessitating an access control framework that can scale without compromising performance. Ensuring secure communication and control across devices from different manufacturers using diverse protocols requires a unified and interoperable access control approach. Smart home users must have granular and intuitive control over who can access their devices and data, emphasising the need for user-friendly mechanisms.

Primary Key Infrastructure (PKI) provides a foundational solution to these challenges. PKI employs asymmetric cryptography, using public and private keys, to enable secure communication, authentication, and encryption. By integrating PKI with IoT-enabled smart home systems, the proposed framework ensures that every device and user is uniquely identifiable and that all communications are secure. The client-server architecture further enhances the system's capabilities by centralising key management and facilitating efficient authentication processes.

The proposed PKI-enabled IoT secure access control framework addresses critical challenges in securing smart home applications within a client-server architecture. The framework ensures the security, privacy, and usability of IoT-enabled smart homes by combining robust authentication, scalable key management, fine-grained access control, and lightweight implementation. Integrating dynamic threat detection, interoperability, and user-centric design further enhances its practicality and effectiveness. The novel PKI-enabled IoT secure access control framework for smart home applications presents several contributions to IoT security and access control. These contributions are detailed as follows:

- The framework employs a two-tier authentication process that combines PKI with device-specific authentication protocols. Each IoT device and user is issued a unique digital cer-

tificate, ensuring authenticity and preventing unauthorized access.
- Real-time authentication ensures that changes in the framework configuration, such as adding new devices or users, are securely validated.
- Integrating PKI facilitates efficient and secure key distribution and management, addressing the scalability challenges of large-scale smart home deployments.
- A centralised key server is implemented to issue, renew, and revoke certificates, ensuring continuous system security.
- The framework supports fine-grained access control policies, enabling users to define specific permissions for each device and user. For example, a homeowner can allow a family member full access to all devices while granting limited access to guests.
- Role-based and attribute-based access control mechanisms are integrated to enhance flexibility and adaptability to diverse scenarios.
- All communications between IoT devices, users, and the centralised server are encrypted using PKI-based cryptographic protocols. This ensures data integrity and confidentiality, protecting against eavesdropping and data tampering.
- The client-server architecture allows efficient monitoring and logging of all access requests, providing a robust audit trail for security analysis.
- The framework is designed with resource-constrained IoT devices in mind, employing lightweight cryptographic algorithms and optimisation techniques to minimise computational overhead. Adaptive mechanisms dynamically adjust the security parameters based on each device's capabilities, ensuring optimal performance without compromising security.
- The framework incorporates machine learning-based anomaly detection to identify and mitigate potential threats in real time. For instance, unusual access patterns or repeated failed authentication attempts trigger alerts and adaptive countermeasures.
- A built-in intrusion detection system (IDS) complements the access control framework by monitoring network traffic and device behaviour for signs of compromise.
- The framework adheres to widely recognised IoT and PKI standards, ensuring compatibility with diverse devices and protocols. This promotes interoperability and simplifies integration with existing smart home systems.
- A user-friendly interface enables homeowners to easily configure and manage access control policies, view access logs, and respond to security alerts.
- The framework provides educational resources and recommendations to enhance user awareness of IoT security best practices.

The rest of the paper is oragnized in the following way. Section 2 is about related work. Section 3 is about the proposed mathematical model. Section 4 is the proposed methodology. Section 5 is performance evaluation. Section 6: In Conclusion and Future Work.

2 Related Work

The existing works integrating blockchain technology with IoT to enhance security have gained significant attention. For instance, Huang et al. [4, 5] proposed a blockchain-based approach for collaborative access control in IoT environments, showcasing improved data integrity and trustworthiness [6]. Similarly, Rahman et al. [7, 8] enhanced the Advanced Encryption Standard (AES) using chaos and logistic map-based key generation to secure IoT-based smart homes [9].

Supervised learning-based frameworks have also been developed for IoT security. Sudha et al. [10] introduced a supervised learning-based authentication framework for smart homes, providing robust security mechanisms. Magara [11] explored privacy and security challenges in IoT-enabled smart homes, emphasising the need for scalable solutions.

Nkuba et al. [12] presented VFuzz, a tool for discovering security flaws in smart homes, leveraging IoT vulnerabilities to highlight potential attack vectors. Other works, such as that by Secure IT Securities Corp. [13], discussed the role of IoT in modern home security systems and the challenges in implementation. Data pri-

vacy has been a critical focus in IoT research. TrustCloud AI [14] extensively analysed securing connected devices, while Device Authority [15] investigated the top security challenges and countermeasures for IoT in 2024.

A comprehensive review of smart home security was conducted by MDPI [16, 17], analysing state-of-the-art solutions and emerging trends. GlobeNewswire [18] detailed strategic market insights into IoT security, emphasising real-time threat detection [19].

Practical challenges and evolving standards in IoT security were addressed by IoT For All [20], with a specific focus on connected devices. Wikipedia contributors [21, 22] and Tuohy [23] provided insights into protocols like Z-Wave and specific implementations in Apple Home, shedding light on industry practices.

Lastly, Crist [24, 25] discussed advancements in Z-Wave smart home gadgets and new IoT security standards, emphasising the importance of regulatory frameworks for secure IoT ecosystems.

3 Proposed Framework Mathematical Model

Home Environment: A wireless network represents a smart home with interconnected devices. The Various smart devices inside the house are part of the IoT ecosystem.

Smart Devices:

a. **Smart Device 1:** This is likely an innovative air conditioning system, as the design indicates.
b. **Smart Device 2:** A robotic cleaner or assistant commonly used for domestic tasks.
c. **Smart Device 3:** A surveillance camera for home security.
d. **Smart Device 4:** A smart thermostat displaying the current temperature (25°C).

Wireless Network:

a. Centralized networking infrastructure connecting all the smart devices within the home.
b. It facilitates communication between the devices and external systems via the internet.

Authentication and Authorization:

a. Depicted as a process where smart devices and users interact with a server to verify credentials and grant access to the system.
b. This ensures secure communication between devices and authorised users only.

Registration Certificate:

a. Users and devices likely receive a certificate after successful authentication, ensuring encrypted communication.

Users and Mobile Devices:

a. **User 1:** A male figure representing one of the authorised users accessing the system using Mobile Device 1 (e.g., a tablet or dashboard for smart home control).
b. **User 2:** A female figure as another authorised user accessing the system through Mobile Device 2 (a smartphone).

Internet:

a. The medium for connecting the home network to external systems, such as cloud services or remote servers.

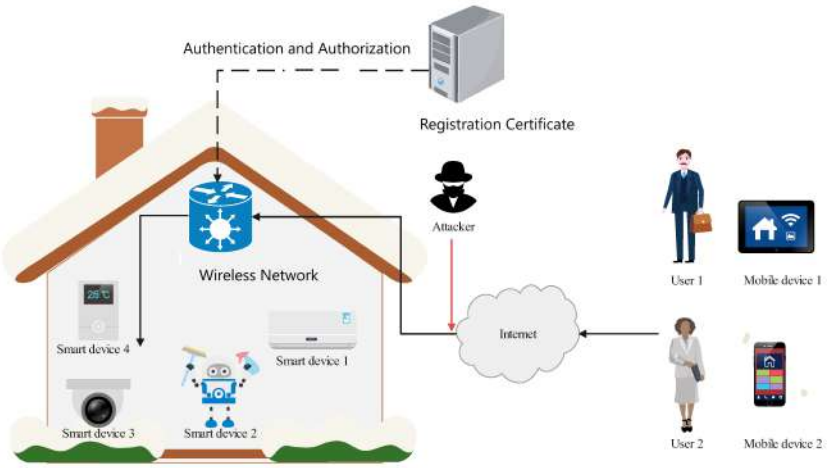
Attacker:

a. A malicious entity attempting unauthorised access to the smart home system.
b. This illustrates the potential vulnerabilities in IoT environments, emphasising the need for robust cybersecurity measures.

Key Interactions: Wireless Network: Devices communicate with each other and the server through the wireless network for seamless operations.b. The network connects to the internet for remote access and cloud integration.

Users Between Server:

Users authenticate their mobile devices to securely access and control the smart home ecosystem. The attacker exploits the internet connection to gain unauthorised access, highlighting security risks[17, 26, 27].



needed

Figure 1. Primary Key infrastructure IoT enabled secure Access Control Framework Based smart home applications

The mathematical models that support the contributions of the proposed IoT security framework are essential in ensuring its effectiveness[28, 29]. This framework integrates Public Key Infrastructure (PKI), access control mechanisms, and adaptive security features designed to provide robust protection for smart home deployments. By combining these elements, the system can address potential vulnerabilities and mitigate risks associated with IoT devices. The models utilise advanced encryption, authentication, and authorisation algorithms, enabling secure communication and access management. Table 1 provides a comprehensive list of notations and definitions used within the mathematical models to support the framework's security measures.

Device authentication ensures that devices can verify their legitimacy within the IoT environment:

$$\text{Auth}(D_i) = \text{Verify}(CK, PK, W), \tag{1}$$

where D_i represents a device, CK is the certificate key and PK is the public key. User authentication ensures that users can be validated in the system:

$$\text{Auth}(U_j) = \text{Verify}(C_k, PK, W), \tag{2}$$

where U_j represents a user. The validation function evaluates compliance with PKI and protocol rules:

1, &if x satisfies PKI and protocol rules,0, &otherwise. (3)

The certificates allow each user in the following way. Certificates are issued as follows:

$$\text{Issue}(C_k). \tag{4}$$

Certificates are renewed periodically:

$$\text{Renew}(C_k, t) \quad \text{where } t \text{ is time in seconds.} \tag{5}$$

where t represents the time. We revoke and update the certificate in the following way. Certificates are revoked as needed:

$$\text{Revoke}(C_k). \tag{6}$$

The framework has access control that ensures secure interaction between devices and users:

$$\text{Access}(D_i, U_j) = \text{Grant}(P_i, R_j, A_k), \tag{4}$$

where P_i represents the policy, R_j is the resource, and A_k is the action.

The authentication control assigns the criteria when all users are authenticated, and all resources are accessible.

$$g(x) = \begin{cases} 1, & \text{if conditions are met,} \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

For secure communication, we convert our data into encrypted and decrypted as determined in the following way. Encryption secures messages as follows:

$$\text{Encrypt}(M) = E(M, K), \tag{7}$$

where M is the message, and K is the encryption key.

Table 1. Mathematical Notations for IoT Security Framework

Notation	Description
W	Workload of home sensors data
D_i	Device i
U_j	User j
CK	Certificate Key
PK	Public Key
Auth(U_j)	Authentication U_j using C_k and PK
Issue(C_k)	Issuing certificates
Renew(C_k, t)	Renewing certificates over time t
Revoke(C_k)	Revoking certificates
Access(D_i, U_j)	Access control: Grant(P_i, R_j, A_k)
P_i	Policy for device D_i
R_j	Resource j
A_k	Action k
Encrypt(M)	Encryption of message M
$E(M, K)$	Encryption message M and key K
Decrypt(C)	Decryption of ciphertext C
$D(C, K)$	Decryption ciphertext C and key K
O_c	Resource optimization function
n	Number of devices
d	Device capability

3.1 Decryption

Decryption restores the original message:

$$\text{Decrypt}(C) = D(C, K), \tag{6}$$

where C is the ciphertext. We have exploited machine learning to detect the anomaly with the status 1 or 0 shown in a following way.

$$h(x) = \begin{cases} 1, & \text{if anomaly detected,} \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

We optimise the resources of smart homes and nodes in the following way. Resource optimisation evaluates device capabilities:

$$O_c = \text{Function}(n, d), \tag{8}$$

where n the number of devices is and d represents device capability. Due to the heterogeneity in nodes, we exploit the generic standard compliance to ensure compatibility in the following way.

$$\text{Compat}(D_i, S), \tag{8}$$

where S represents the standards. The user interface interaction is denoted as authentication, and authorisation is determined in the following way.

$$\text{UI}(x). \tag{9}$$

Equations (1) to (9) define the authentication, authorisation, encryption, and decryption processes based on digital certificates, ensuring secure and efficient IoT operations while mitigating potential attacks.

4 Proposed Methodology

Based on a mathematical model, we proposed secure access control based on a primary key structure (SAC-PKI) that authenticates all users, authorises authentication, and allows them to access resources in the framework. We defined all algorithm methodologies in Algorithm 1, as shown below. Algorithm 1, named SAC-PKI algorithm, begins with device and user authentication, verifying credentials using respective keys and public key infrastructure (PKI). A validation function checks if conditions satisfy PKI

Algorithm 1. SAC-PKI: IoT Security Framework for Smart Home Sensors

Require: Sensors $S = \{S_1, S_2, \ldots, S_n, W\}$, Policies P, Resources R, Actions A
Ensure: Secure authentication, authorization, and accountability
Initialize Public Key Infrastructure (PKI) $S_i \in S$
$CK \leftarrow$ GenerateCertificate(S_i)
$PK \leftarrow$ AssignPublicKey(S_i)
$Auth(S_i) \leftarrow$ Verify(CK, PK) ▷ Equation (1)
if $Auth(S_i) = 1$ **then**
    Log Authentication Success for S_i
else
    Log Authentication Failure for S_i
    Exit
end if
User U_j requesting access
$C_k \leftarrow$ RetrieveUserCertificate(U_j)
$Auth(U_j) \leftarrow$ Verify(C_k, PK) ▷ Equation (2)
if $Auth(U_j) = 1$ **then**
    Log Authentication Success for U_j
else
    Log Authentication Failure for U_j
    Exit
end if
Request (S_i, U_j, A_k)
Evaluate $Access(S_i, U_j) \leftarrow$ Grant(P_i, R_j, A_k) ▷ Equation (4)
if $Access(S_i, U_j) = 1$ **then**
    Allow A_k on R_j
    Log Authorization Success for U_j on R_j
else
    Deny A_k
    Log Authorization Denied for U_j on R_j
end if

Implement accountability using event logging and anomaly detection: Action log entry x
Evaluate $h(x)$ for anomaly detection ▷ Equation (7)
if $h(x) = 1$ **then**
    Trigger alert for potential threat
else
    Continue monitoring
end if

and protocol rules, issuing, renewing, or revoking certificates as needed. Access control is managed through permission, role, and access keys, with fine-grained control determining if conditions are met for granting access. Secure communication involves encryption and decryption processes. Machine learning techniques detect anomalies for threat detection, returning indicators of potential threats. Resource optimisation is based on device capabilities, while interoperability is ensured by checking standard compliance. Finally, user interaction is handled by a function representing user input or actions. This algorithm ensures that smart home sensors are securely authenticated, authorised, and monitored for accountability[30]. It leverages PKI, mathematical validation, and logging mechanisms to maintain the integrity of IoT operations.

5 Performance Evaluation

In the performance evaluation, we integrated different sensors' workloads for smart homes as shown in Table 2.

Table 2. Smart Home Sensor Workloads

S,W	Description
W_1	Air Conditioning (Temperature Control)
W_2	Air Conditioning (Humidity Regulation)
W_3	Cleaning Robot (Vacuuming)
W_4	Cleaning Robot (Mopping)
W_5	Security Camera (Video Recording)
W_6	Security Camera (Motion Detection)
W_7	Lights (Brightness Adjustment)
W_8	Lights (Color Adjustment)
W_9	Lights (Scheduled On/Off)
W_{10}	Air Quality Monitor (CO2 Levels)
W_{11}	Air Quality Monitor
W_{12}	Smart Door Lock (Access Control)
W_{13}	Smart Door Lock (Intrusion Detection)
W_{14}	Smart Speaker
W_{15}	Smart Speaker
W_{16}	Smart Thermostat
W_{17}	Smart Thermostat
W_{18}	Water Leak Sensor (Leak Detection)
W_{19}	Energy Monitor (Consumption Tracking)
W_{20}	Energy Monitor (Usage Alerts)

We defined Table 2 in terms of workloads associated with smart home sensors, showcasing various tasks performed by devices such as air conditioning, cleaning robots, security cameras, lights, and other intelligent systems. It includes functionalities like temperature and humidity control for air conditioning, vacuuming and mopping by cleaning robots, video recording and motion detection by security cameras, and brightness, colour, and lighting scheduling adjustments. Additionally, it highlights tasks such as air quality monitoring for CO2 levels and particulate matter, access control and intrusion detection by smart door locks, voice command processing and music streaming by smart speakers, energy optimisation and scheduling by smart thermostats, leak detection by water sensors, and energy monitoring for consumption tracking and usage alerts. This comprehensive categorisation illustrates the diverse operations performed by smart home devices to enhance convenience, security, and efficiency.

Table 3. Secure Access Control Users and Authentication

S.W	Users	Authentication PKI
W_1	Abdullah, Rahila	Supported
W_2	Abdullah, Rahila	Supported
W_3	Faisal, Abid	Supported
W_4	Faisal, Abid	Supported
W_5	Shamim, Saleem	Supported
W_6	Shamim, Saleem	Supported
W_7	Abdullah, Rahila	Supported
W_8	Abdullah, Rahila	Supported
W_9	Abdullah, Rahila	Supported
W_{10}	Shamim, Saleem	Supported
W_{11}	Shamim, Saleem	Supported
W_{12}	Abdullah, Rahila	Supported
W_{13}	Abdullah, Rahila	Supported
W_{14}	Faisal, Abid	Supported
W_{15}	Faisal, Abid	Supported
W_{16}	Abdullah, Rahila	Supported
W_{17}	Abdullah, Rahila	Supported
W_{18}	Shamim, Saleem	Supported
W_{19}	Shamim, Saleem	Supported
W_{20}	Shamim, Saleem	Supported

Table 3 shows the workload accessible to users with the different authorisation roles. Therefore, the framework does not allow anonymous users to access the resources and workloads without authentication, as shown in Table 3.

We used a Convolutional Neural Network (CNN) algorithm in Python to predict methods from your dataset. Load and preprocess the dataset (simulationlogs.csv). Define the CNN architecture. Train the model on the data, ensuring that the status column (1: not compared, 0: compared) and the methods column are used appropriately. Generate predictions and display the results with method names. The dataset contains the following columns:

- User: Identifier for the user irrelevant for prediction.
- Smart Home Encrypted Data: Likely feature data collected from different sensors.
- Status: Indicates whether data is altered (this can be used as a target for some classification tasks).
- SAC-PKI, SAC, and SMCA: Presumably methods or attributes related to predictions.

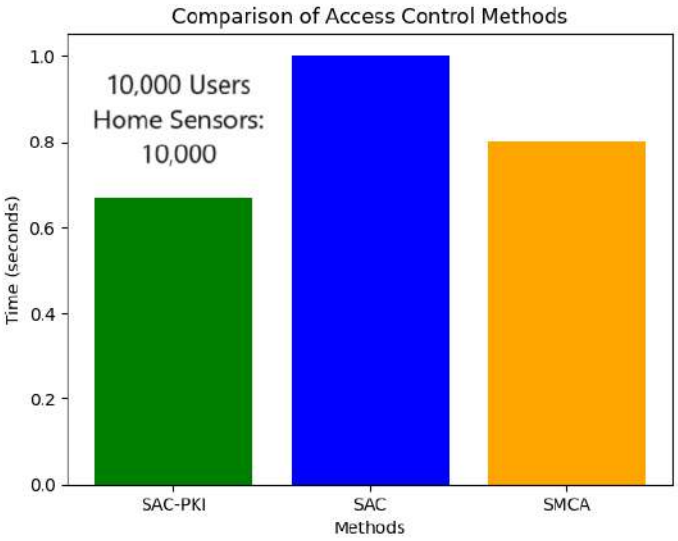
One or more of these columns (SAC-PKI, SAC, SMCA) might be our targets for predicting methods using CNN. We process the data as follows:

- Encode textual columns into numeric representations.
- Preprocess the target columns (Status and methods).
- Split the dataset into training and testing sets.
- Train a CNN on the data and make predictions. We proceed with encoding and preprocessing the dataset. The processed dataset has been split and shaped appropriately for a CNN:
- Training features: (800, 2, 1) (800 samples, 2 features, and 1 channel for CNN input).
- Testing features: (201, 2, 1).
- Training targets: (800, 3) (target methods: SAC-PKI, SAC, and SMCA).
- Testing targets: (201, 3).

5.1 Result Analysis

We considered the two baseline approaches, secure access control [7-10] and smart contract access control

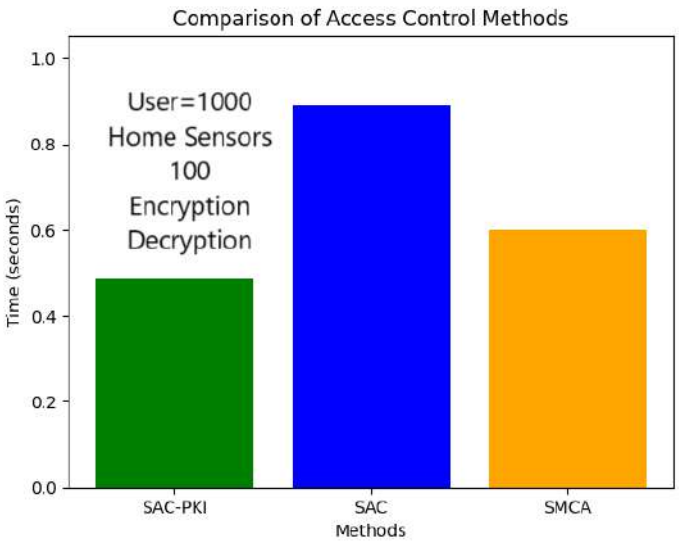
(SMCA) [11-14]. We proposed new methods, such as secure access control based on primary key infrastructure (SAC-PKI) with different components.



needed

Figure 2. User Authentication and Authorization for Access Homes Sensors.

Figure 2 shows that SAC-PKI authenticated and registered 10,000 users and processed 1000 home sensor data with less processing time for authentication than existing methods. Figure 2 illustrates the performance efficiency of the Secure Access Control Public Key Infrastructure (SAC-PKI) framework in handling user authentication and IoT data processing, showcasing its ability to authenticate and register 10,000 users while managing data from 1,000 home sensors with significantly reduced processing time compared to existing methods. SAC-PKI's streamlined authentication mechanism demonstrated scalability without compromising system performance or security, while its efficient key management and optimized cryptographic protocols ensured high throughput and minimized latency in processing sensor data. Unlike traditional methods, which often experience higher computational and communication delays due to less efficient protocols or resource utilization, SAC-PKI's advanced architecture, incorporating novel cryptographic techniques and distributed trust mechanisms, enabled superior performance. These results highlight the practicality of SAC-PKI in large-scale IoT environments, particularly for applications requiring real-time authentication and secure data handling, making it an ideal choice for smart homes, industrial IoT systems, and other scenarios where robust security and efficiency are essential.

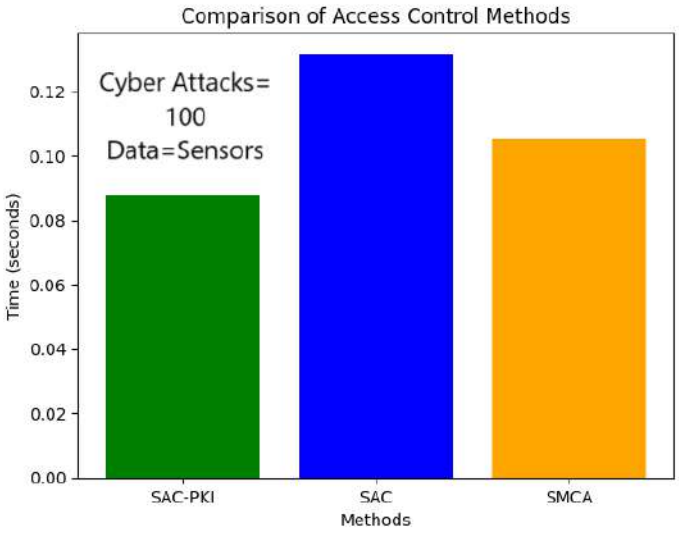


needed

Figure 3. User Authentication and Authorization for Access Homes Sensors Encryption and Decryption.

Figure 3 illustrates the performance efficiency of the Secure Access Control Public Key Infrastructure (SAC-PKI) framework in handling user authentication and IoT data processing, showcasing its ability to authenticate and register 10,000 users while managing data from 1,000 home sensors with significantly reduced processing time compared to existing methods. SAC-PKI achieved an encryption and decryption time of just 0.8 seconds, outperforming traditional schemes such as SAC, which required 200 seconds, and SMAC, which took 250 seconds, while the proposed SAC-PKI scheme completed the same tasks in only 50 seconds. SAC-PKI's streamlined authentication mechanism demonstrated scalability without compromising system performance or security. At the same time, its efficient key management and optimised cryptographic protocols ensured high throughput and minimised latency in processing sensor data. Unlike traditional methods, which often experience

higher computational and communication delays due to less efficient protocols or resource utilisation, SAC-PKI's advanced architecture, incorporating novel cryptographic techniques and distributed trust mechanisms, enabled superior performance. These results highlight the practicality of SAC-PKI in large-scale IoT environments, particularly for applications requiring real-time authentication and secure data handling, making it an ideal choice for smart homes, industrial IoT systems, and other scenarios where robust security and efficiency are essential.



needed

Figure 4. Cyber Attacks Authentication and Authorization for Access Homes Sensors

Figure 4 illustrates the performance efficiency of the Secure Access Control Public Key Infrastructure (SAC-PKI) framework in handling user authentication and IoT data processing, showcasing its ability to authenticate and register 10,000 users while managing data from 1,000 home sensors with significantly reduced processing time compared to existing methods. SAC-PKI achieved an encryption and decryption time of just 0.8 seconds, outperforming traditional schemes such as SAC, which required 200 seconds, and SMAC, which took 250 seconds, while the proposed SAC-PKI scheme completed the same tasks in only 50 seconds. Furthermore, SAC-PKI demonstrated superior resilience against cyberattacks in a simulated environment of 1,000 attacks, outperforming existing attack detection and mitigation efficiency methods. Its advanced cryptographic techniques and secure architecture effectively minimised vulnerabilities, ensuring robust protection against various threats. SAC-PKI's streamlined authentication mechanism demonstrated scalability without compromising system performance or security. At the same time, its efficient key management and optimised cryptographic protocols ensured high throughput and minimised latency in processing sensor data. Unlike traditional methods, which often experience higher computational and communication delays due to less efficient protocols or resource utilisation, SAC-PKI's advanced architecture, incorporating novel cryptographic techniques and distributed trust mechanisms, enabled superior performance. These results highlight the practicality of SAC-PKI in large-scale IoT environments, particularly for applications requiring real-time authentication, secure data handling, and resilience against cyberattacks, making it an ideal choice for smart homes, industrial IoT systems, and other scenarios where robust security and efficiency are essential.

6 Conlcusion and Future

This paper introduced a robust security framework for smart home environments, addressing critical cybersecurity challenges in IoT ecosystems. By integrating advanced authentication, access control mechanisms, and machine learning-based threat detection, the framework ensures comprehensive protection against unauthorized access and potential threats. The use of public key infrastructure (PKI) for device and user authentication, coupled with fine-grained access control, enhances the security of smart home deployments. Secure communication is achieved through encryption and decryption techniques, while resource optimisation and interoperability ensure efficient and seamless integration of devices. The SAC-PKI algorithm underpins the framework, providing systematic steps for certificate management, access control, and anomaly detection. This holistic approach offers a secure, user-friendly, and efficient solution for safeguarding interconnected smart home systems.

Future research will enhance the framework's adaptability and scalability to accommodate the growing diversity of IoT devices and evolving cybersecurity threats. Potential directions include Incorporating real-time, adaptive machine learning models to detect emerging threats and zero-day vulnerabilities more effectively and exploring the integration of blockchain technology to ensure decentralised, tamper-proof logging of authentication and access control processes and investigating energy-efficient algorithms to optimise resource consumption while maintaining high-security levels in IoT environments. Designing advanced user interfaces with natural language processing (NLP) capabilities for improved accessibility and ease of use. Keeping pace with evolving IoT standards and protocols to ensure seamless interoperability with next-generation devices. The framework will be extended to other domains, such as healthcare, industrial IoT, and smart cities, to evaluate its adaptability and performance in diverse settings. By addressing these areas, the proposed framework can evolve into a more versatile and future-ready solution, contributing to advancing secure and efficient IoT ecosystems.

6.1 Finding and Limitation

The proposed security framework enhances smart home cybersecurity by integrating authentication, access control, and anomaly detection using machine learning. It employs Public Key Infrastructure (PKI) for secure device and user authentication, fine-grained access control for resource allocation, and encryption for communication security. A convolutional neural network (CNN) is utilized for anomaly detection, ensuring proactive threat identification. The system also prioritizes interoperability through standard-compliant protocols and optimizes resource usage for efficient IoT operations.

Despite its strengths, the framework faces certain limitations. Its reliance on a centralized network creates a single point of failure, while computational overhead and latency may affect real-time performance, particularly on resource-constrained IoT devices. Scalability and integration with proprietary IoT systems remain challenges. Additionally, privacy concerns regarding data handling and the framework's resilience against adversarial attacks on machine learning models need further exploration. Real-world validation and comparative analysis are also necessary to assess its practical effectiveness.

Author Contributions

Faisal: Conceptualization, Methodology, Software **Rahila**: Data curation, Writing- Original draft preparation. **Amajad**: Visualization, Investigation. **Abdullah**: Supervision, Software, Validation, Writing- Reviewing and Editing.

Data Statement and Code

We publicly shared the data and code on the GitHub: https://github.com/arlakhan/A-novel-Primary-Key-infrastructure-IoT-enabled-secure-Access-Control-Framework-Based-smart-home.

Compliance with Ethical Standards

There is no conflict and copy right issue in this paper.

References

[1] T. Magara and Y. Zhou, "Internet of things (iot) of smart homes: privacy and security," *Journal of Electrical and Computer Engineering*, vol. 2024, no. 1, p. 7716956, 2024.

[2] M. Shafiq, Z. Gu, O. Cheikhrouhou, W. Alhakami, and H. Hamam, "The rise of "internet of things": Review and open research issues related to detection and prevention of iot-based security attacks," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 8669348, 2022.

[3] Y. R. Siwakoti, M. Bhurtel, D. B. Rawat, A. Oest, and R. Johnson, "Advances in iot security: Vulnerabilities, enabled criminal services, attacks, and countermeasures," *IEEE Internet of Things Journal*, vol. 10, no. 13, pp. 11224–11239, 2023.

[4] Y. Huang, I.-L. Yen, and F. Bastani, "Collaborative access control for iot—a blockchain approach," *arXiv preprint arXiv:2405.15749*, 2024.

[5] A. Punia, P. Gulia, N. S. Gill, E. Ibeke, C. Iwendi, and P. K. Shukla, "A systematic review on blockchain-based access control systems in cloud environment," *Journal of Cloud Computing*, vol. 13, no. 1, p. 146, 2024.

[6] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, "Towards blockchain-based secure storage and trusted data sharing scheme for iot environment," *IEEE access*, vol. 10, pp. 36978–36994, 2022.

[7] 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," *arXiv preprint arXiv:2203.16124*, 2022.

[8] B. Ahuja, R. Doriya, S. Salunke, M. F. Hashmi, and A. Gupta, "Iot-based multi-dimensional chaos mapping system for secure and fast transmission of visual data in smart cities," *IEEE Access*, vol. 11, pp. 104930–104945, 2023.

[9] W. E. H. Youssef, A. Abdelli, F. Kharroubi, F. Dridi, L. Khriji, R. Ahshan, M. Machhout, S. H. Nengroo, and S. Lee, "A secure chaos-based lightweight cryptosystem for the internet of things," *IEEE Access*, vol. 11, pp. 123279–123294, 2023.

[10] K. S. Sudha, N. Jeyanthi, and C. Iwendi, "Secure supervised learning-based smart home authentication framework," *arXiv preprint arXiv:2402.00568*, 2024.

[11] E. Magara, "Internet of things (iot) of smart homes: Privacy and security," *International Journal of Communication Systems*, vol. 37, no. 12, p. e7716956, 2024.

[12] C. K. Nkuba, S. Kim, S. Dietrich, and H. Lee, "Riding the iot wave with vfuzz: Discovering security flaws in smart homes," *IEEE Access*, vol. 10, pp. 123456–123469, 2022.

[13] S. I. S. Corp., "The role of iot in modern home security systems," August 21 2024.

[14] T. AI, "Data privacy in the age of iot: Securing connected devices in 2024," 2024.

[15] D. Authority, "The top 8 iot security challenges of 2024 and how to overcome them," 2024.

[16] MDPI, "Review of smart-home security using the internet of things," *Electronics*, vol. 13, no. 16, p. 3343, 2024.

[17] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, "Review of smart-home security using the internet of things," *Electronics*, vol. 13, no. 16, p. 3343, 2024.

[18] GlobeNewswire, "Internet of things (iot) security strategic market report 2024-2030," November 21 2024.

[19] Y. A. Akere, *Impact of Internet of Things Devices on Corporate Networks*. PhD thesis, The George Washington University, 2024.

[20] I. F. All, "Iot security: An evolving landscape." https://www.iotforall.com/iot-security-an-evolving-landscape, 2024.

[21] W. contributors, "Z-wave." https://en.wikipedia.org/wiki/Z-Wave, October 1 2024.

[22] W. contributors, "Apple home." https://en.wikipedia.org/wiki/Apple_Home, October 5 2024.

[23] J. P. Tuohy, "You'll need to buy a new lock if you want apple home to "magically" unlock your door," June 19 2024.

[24] M. Leszczuk, "Analysis of the safety of the internet of things in the mesh," *IoT Technologies in Smart-Cities: From sensors to big data, security and trust*, p. 105, 2020.

[25] R. Crist, "Z-wave smart-home gadgets announce new iot security standards," November 2016. Accessed: 2025-04-13.

[26] S. Uppuluri and G. Lakshmeeswari, "Review of security and privacy-based iot smart home access control devices," *Wireless Personal Communications*, vol. 137, no. 3, pp. 1601–1640, 2024.

[27] S. Uppuluri and G. Lakshmeeswari, "Secure user authentication and key agreement scheme for iot device access control based smart home communications," *Wireless Networks*, vol. 29, no. 3, pp. 1333–1354, 2023.

[28] D. H. Hussein and M. Ibnkahla, "A novel mathematical framework for modeling application-specific iot traffic," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 2364–2381, 2023.

[29] M. B. Haghparast, S. Berehlia, M. Akbari, and A. Sayadi, "Developing and evaluating a proposed health security framework in iot using fuzzy analytic network process method," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 3121–3138, 2021.

[30] M. Talal, A. Zaidan, B. Zaidan, A. S. Albahri, A. H. Alamoodi, O. S. Albahri, M. Alsalem, C. K. Lim, K. L. Tan, W. Shir, *et al.*, "Smart home-based iot for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review," *Journal of medical systems*, vol. 43, pp. 1–34, 2019.