Journal of Computer Science

Research Article

A Comparative Analysis of IoT Security Frameworks With BIoTC

Gaurav Vats[1], Sarvesh Tanwar[1] and Pankaj Kumar Sharma[2]

[1]*Amity Institute of Information Technology, Amity University, Noida, Uttar Pradesh, India*
[2]*Department of Computer Science and Engineering, ABES, Engineering College, Ghaziabad, India*

Article history
Received: 25-07-2025
Revised: 23-12-2025
Accepted: 26-12-2025

Corresponding Author:
Sarvesh Tanwar
Amity Institute of Information Technology, Amity University, Noida, Uttar Pradesh, India
Email: dr.sarveshtanwar@gmail.com

Abstract: The Internet of Things (IoT) has reshaped the modern intelligent environments, but it remains vulnerable to sophisticated attacks such as Man-in-the-Middle (MITM), RFID cloning, unauthorized access, and social engineering. Block Internet of Things Chain (BIoTC) introduces a simulation-based approach to address these security issues. While various frameworks have been proposed to secure IoT systems, most of them fall short in practical validation or comprehensive protection. This paper presents a comparative analysis of existing IoT security frameworks against a proposed solution named the Blockchain Internet of Things Chain (BIoTC). A Cisco Packet Tracer simulated smart home environment is used to construct the framework's architecture. This framework also consists of a lightweight blockchain infrastructure. This lightweight module uses smart contract- like policy logic. The logic is implemented at Python blockchain layer for access validation and includes rule-based anomaly detection. In this research work, the BIoTC discloses its ability to detect and address security issues.in simulated smart home environment. This is done by dividing the solution into different subparts. These subparts or modules mimic several issues like different attacks, anomaly detection and device verification. The findings indicates that the framework demonstrates adaptability, qualitative detection effectiveness, and visual feedback. The result indicates that the framework is suitable option for protecting smart home devices in simulated environments. This research work demonstrates that the blockchain based validation can effectively support IoT security in simulation driven environments.

Keywords: Security Frameworks, IoT, Blockchain, Cisco Packet Tracer, Smart Homes

Introduction

The Internet of Things (IoT) makes everyday objects smart and connected. This technology is especially powerful in smart homes environments, where it automates a wide range of functions (Omolara et al., 2022; Choudhary et al., 2024a). Few of them are appliance control, surveillance and also the secure entry methods. The rise of smart home automation introduces significant security challenges because these systems rely on open or weakly secured networks for communication. They are vulnerable to major threats (Vats et al., 2024) such as RFID cloning, Man-In-The-Middle (MITM) attacks (Ferraris et al., 2024), unauthorized access, and social engineering. These flaws not only damage the technical reliability of the devices but also erode user confidence and safety.

A large number of solutions have been introduced to increase IoT security in last few years. These solutions have either cryptography-based algorithms, or it relies on access control mechanisms. In an alternative way anomaly detection and blockchain-based architectures are also the part of feasible way to tackle this. Although these approaches are good and contributes to security in their own way but they have their own drawbacks and limitations. Most of them are unsuccessful in end-to-end security, live responses and in managing human-related risk. The best example for this is social engineering. Except all these things, there is no mechanism for clear visualization to explain security events.

To handle these kinds of concerns, this paper compares BIoTC a layered security framework designed, modular in nature, to enhance protection in smart home environments with other frameworks. The proposed work integrates blockchain characteristics like tamper-proof logging, smart-contract-like policy logic implemented at the Python blockchain layer for access control, and rule-based anomaly

detection logic driven by predefined behavioral patterns. There are also OCR-based image analysis and a visual dashboard. These features allow dynamic tracking and sometime also accessible user feedback. These features make the framework useful for all, either the person is technical and non-technical. This study is based on simulation driven implementation and validation. The research work is carried out on fully simulated smart home environment in Cisco Packet Tracer. This simulation has shown attacks like RFID cloning, MITM attack and unauthorized access. This method provides feasible approach for evaluating system's robustness. There are different parameters used for system evaluation. Some of them are ability to manage multi-vector composite threats, qualitative detection effectiveness and also system adaptability.

With the help of this analysis, the paper explains the framework's modular approach and validation logic. The interactive visual interface validates it to serve as an adaptive framework, especially for dynamic IoT environments like smart homes.

Why a Framework for IoT Security?

The main reason for the requirement of framework for IoT security is that there are different approaches used for IoT security. Like there are different security models that provides only an abstract representation of the system's conceptual behavior. Most of them only identify potential risks. In similar contexts there are different security architecture, but they have focus only on the system design and components like device configuration or communication pathway. On the same context the security framework provides mixed approach. It has both theoretical substance and practical applicability. It can act as a modular approach. The framework is also deployable solution that integrates policies, detection methods and in case of security framework it has adaptive control logic to fix threats in real-world IoT environments.

As in smart home the electronic devices operate in real time so many times they are exposed to diverse cyber-attacks. To tackle these kinds of problems there is a need of dynamic security framework. Unlike models or architectures that are often theoretical or structural in nature, a framework facilitates layered set of standardized rules. It has set of practices and policies. Framework is a systematic approach for identifying, protecting, detecting, responding and recovering from cyber threats. So, a strong and flexible security framework for smart home is need of the hour. Framework should protect networks and devices. It should not only fix technical errors but also human centric risks. Framework is important because it can analyse device-level authentication, and user behaviour analysis.

Model, Architecture, and Framework

As the prior works focuses only on abstract part of the problem and its conceptual solutions. This study argues about the need and importance of framework. The framework that can deploy, test and compatible under real world IoT environments. Table 1 is defining more closer and interrelated terms often used in the context of system design, security, or engineering.

Research Questions

This paper aims to conduct a study of IoT security frameworks using real-time simulations. It has main focus on our implemented framework, BIoTC. The following Research Questions (RQs) guide the scope and experimentation of this study:

RQ1: How effectively can existing IoT security frameworks detect and mitigate multi-vector attacks? (RFID loning, MITM, and Social Engineering in smart home environment are few of them)

RQ2: Can the integration of blockchain and rule-based anomaly detection logic improve real-time threat identification?

RQ3: How do different frameworks compare in terms of flexibility, visualization capability, deployment complexity?

RQ4: What are the measurable differences in qualitative detection effectiveness and relative response behaviour across the evaluated frameworks?

Motivation

There are several conventional frameworks and models for IoT environment security. But their procedure and methodology heavily rely on few selected areas like cryptographic algorithms, access control methods. However, they often fail to address multi-vector attacks. Multi-vector attacks are like RFID cloning combined with social engineering, or like MITM layered over weak authentication. They often lack visualization, real-time feedback and also adaptability. The BIoTC framework integrates blockchain's immutability, authority driven validation and anomaly detection logic to bridge this gap. However, rather than proposing BIoTC in isolation, this paper evaluates it against existing frameworks to assess which strategies work best in practical simulations.

Literature Review

Yazdinejad et al. (2023) proposed a hybrid IoT security model integrating fuzzy logic with blockchain. This helps to analyze and log threats dynamically.

Table 1: Model, Architecture and Framework

Concept	Description
Model	Abstract representation
Architecture	Structural blueprint outlining components, protocols, and data flow
Framework	Practical, modular implementation integrating detection, prevention, and logging mechanisms

Their approach ensures decentralized, tamper-proof logging of detected anomalies through blockchain.it also offers transparent auditability of device behaviour. It is based on fuzzy logic evaluation.it has tunable and trust-preserving design. But the model lacks image-based validation, smart-contract-like policy logic implemented at the Python blockchain layer. It also lacks rule-based anomaly identification inspired by machine learning concepts, suitable for IoT environments. Similarly, Ismail et al. (2024) developed a resource-aware blockchain-based security solution for IoT that combines Hyperledger Fabric with lightweight anomaly detection. While their framework effectively addresses decentralized access control and reduces processing load for edge devices, it falls short in simulating physical device threats and omits smart contract automation and real-time image analytics, which are critical for home-scale security systems. In research-focused IoT deployments, Hızal et al. (2024) focused on utilizing blockchain in IDS for tamper-resistant logging. Although their framework provides robust traceability and trust, it primarily functions in post-breach scenarios and does not integrate with feedback-driven alert systems, which are crucial in adaptive environments, or provide real-time multi-modal threat sensing. Previous research has explored blockchain for IoT security but with limitations for smart home use. Anaam et al. (2023) examines the combination of IoT with private blockchain. Applicability to IoT, the research work addresses mechanisms like secure gateways for data Communication and also different consensus algorithms. The author says that by removing individual points of failure, this decentralized strategy would build a more robust environment for the operation of equipment.

This research proposes an understanding of How integration of blockchain with IoT helpful for security data records. Eghmazi et al. (2024) developed a four-layer IoT architecture integrated with a private Hyperledger Fabric. The authors presented Blockchain as Service (BaaS) application and used Hyperledger Fabric to address security and privacy concerns in IoT environments. The study proposes a different data structure with encryption. The encryption is based on public and private keys. Meanwhile in the research work, Sakib Sizan et al. (2025) analyzed different blockchain platforms like Hyperledger for IoT based industry.it is good for industry and its different application areas but not for smart home environments. It has so many gaps as it doesn't have attack simulation.it is industrial focused model.it shows more one-dimensional model. Emira et al. (2023) addressed the security challenges in smart networks based on IoT. Data integrity, authentication are few of them. It's not easy to standardize the protocols. The research proposes two-layer framework for security enhancement. Layer one has an Enhanced LEACH Clustering Protocol. Layer 2 has a Blockchain Simulator to handle immutability and integrity. The proposed simulator is validated as an effective tool for analyzing blockchain systems. Baral et al. (2024) addressed the complexity and volume of cybersecurity threats. Authors worked on real-time IoT attack detection and response that leverages Machine Learning (ML), Explainable AI (XAI). By combining XAI process like LIME and SHAP with some smart agent the given framework ensures the interpretability of ML model predictions. It provides detection of attacks and its possibilities. Overall, it enhances the overall security as it is transparent and actionable. In a similar way, Lilhore et al. (2024) introduced a security framework based on deep learning. The Framework uses pattern recognition to analyse possible breaches in real time. This research work proposed a solution for instruction in 5g network

In order to improve QoS in 5G-enabled IoT networks, Darshini and Vankadari (2024) suggested a CNN and blockchain-based framework that addresses security concerns and large data volumes. While federated learning protects privacy, the CNN model outperforms traditional neural networks with an accuracy of 81.27% after being trained on IoT traffic datasets. Data handling is tamper-proof thanks to the blockchain mechanism. Simulations show better anomaly detection, increased throughput, and a 25% reduction in relative response behaviour under simulation. However, the framework lacks visual traceability and modular threat emulation, and its computational intensity may limit its applicability for low-power IoT devices.

IoT Predictor, a predictive analytics-based machine learning model for identifying anomalous IoT behaviour patterns, was presented Kalaria et al. (2024). The audit trail and trust validation are compromised by the lack of blockchain integration, despite the fact that it is effective in identifying unusual patterns. Its deployment is also limited in visually monitored smart home settings where camera or OCR-based validation is essential due to the absence of visual or image-based multi-modal inputs. In order to safeguard Electronic Health Records (EHRs) in decentralized healthcare systems, Goel et al. (2024) created a blockchain protocol. The model effectively handles confidentiality issues and uses consensus-driven data integrity mechanisms. Nevertheless, it is domain-specific, does not track the behaviour of IoT devices, does not map physical devices, and is not appropriate for smart home threat landscapes where device diversity and real-time threat feedback are prevalent. Although their trust model works well for protecting healthcare data, it is inapplicable to diverse smart home environments that need to simulate and emulate a range of attack scenarios. Across all the surveyed works, blockchain is prominently used for immutable logging, trust assurance, and access decentralization. Machine learning and AI-based frameworks offer predictive capabilities and pattern-based anomaly detection. However, both categories frequently miss image-based authentication, physical device emulation, and real-time smart contract-based governance. Our proposed BIoTC framework stands out

by merging blockchain's immutability, smart-contract-like policy logic implemented at the Python blockchain layer for access control, and real-time image validation and rule-based anomaly detection inspired by Isolation Forest. It also simulates physical attacks and maps visual device behaviour within a real-time modular smart home simulation, uniquely addressing the comprehensive security needs that remain unfulfilled.

Fig. 1 shows the network visualization of authorships. The above network visualization generated by VOS viewer (Hajoary et al., 2024) provides an overview of the relationships among different entities (countries) based on co authorship.

Here each entity (country) is represented as a node in the network, and the connections between nodes (links) indicate co-authorship relationships between the countries. This network can also help to identify clusters of countries that frequently collaborate in the field of IoT security. The clusters represent groups of countries with stronger collaboration ties and similar research interests. By analyzing the network, researchers can gain insights into global research collaborations, emerging trends, and prominent contributors in the field of IoT security.

Table 2 is the comparison table of different recent IoT security frameworks that explains several gaps across key areas such as comprehensive attack coverage, use of lightweight blockchain, real-time anomaly detection, and visual feedback.

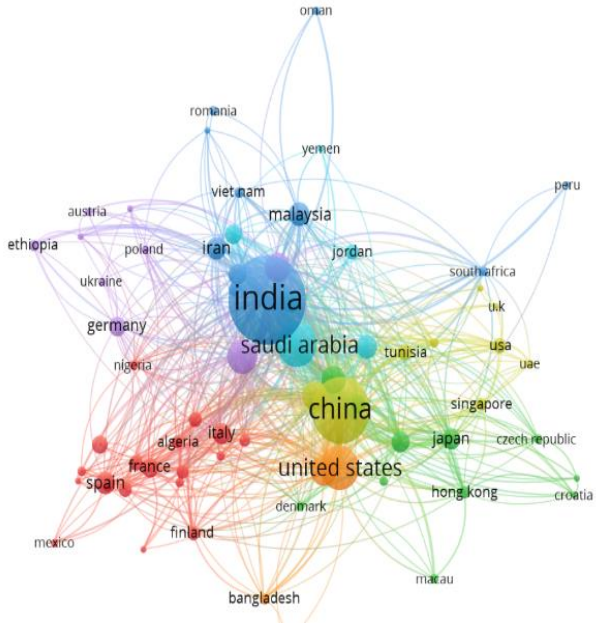

Fig. 1: Network Visualization

Table 2: Comparison of Recent IoT Security Frameworks

S. No.	Framework/Concepts (Authors, Year)	Attack Coverage & Vectors	Blockchain Integration	ML/Anomaly Detection	Visual Feedback	Level / Devices
1	Darshini et al. (2024)	5G-IoT QoS degradation	Yes	Yes	No	IIoT ,5G enabled devices
2	Xu et al. (2021)	Transaction conflict	Hyperledger	No	No	Protocol Level
3	Kasat (2022)	DDOS, Malware	No	No	No	IoT sensor
4	Anaam et al. (2023)	Secure local storage	Yes	No	No	Edge Devices
5	Emira et al. (2023)	Layered trust model +LEACH algorithm	Yes	No	No	IoT Network security
6	Dirin et al. (2023)	Device Integrity	Yes	No	No	Generic IoT
7	Rani et al. (2023)	SDN-based attacks	Yes	Yes	Partial	Network + Node
8	Ismail et al. (2024)	Access control & Anomaly	Ethereum	Lightweight ML	No	IoT Devices/Sensor network
9	Hızal et al. (2024)	Cyber security	Yes	Yes	No	IDS/Research Center
10	Sudipto et al. (2024)	Adaptive auth	No	LLMs + XAI	No	IoT Networks
11	Goel et al. (2024)	EHR data integrity	Yes	No	No	Healthcare IoT
12	Eghmazi et al. (2024)	Confidential data	Hyperledger	No	No	Generic IoT
13	Sakib et al. (2024)	Industry 5.0 traceability	Yes	No	No	Industrial IoT
14	Lilhore et al. (2024)	IoT + 5G anomaly detection	No	CNN model	No	5G IoT
15	Prakash et al. (2024)	IoT anomalies	No	MQTT +ML	No	IoT Systems
16	Almarri and Aljughaiman (2024)	SLR paper(concepts)	No	No	No	Not Applicable
17	Kalaria et al. (2024)	Malicious behaviour	No	Yes	No	Edge Devices
18	Ahakonye et al. (2024)	Blockchain vision	Conceptual	No	No	Not Deployed
19	Affinda (2025)	Vulnerability Detection	Yes	No	Yes	Cyber-attacks
20	IBM SPSS Modeler Subscription (2024)	MITM, RFID, SE, Unauthorized access	lightweight Blockchain	(Conceptual)	Yes	Smart home Simulation

While several frameworks focus on isolated threats or centralized models, few offer integrated solutions spanning blockchain, machine learning, and simulation. Few of them also lack support for real time smart home environments.

In contrast, BIoTC addresses and removes these limitations by combining lightweight blockchain validation, and visual traceability within a simulation of realistic smart home and making it a better security solution. Additional perspectives on the technical elements and deployment suitability of 20 modern IoT security frameworks are offered in Table 3. This assessment primarily focused on five important factors. These factors are use of blockchain, the kind of machine learning/artificial intelligence method used, anomaly detection support, image-based input processing capability, and compatibility with smart home settings. Ismail et al. and Sajal Saha et al., demonstrate high smart home suitability through strong ML integration and blockchain support, most others lack essential elements like visual input handling and policy enforcement via blockchain logic. BIoTC stands out with complete support across all fields. It includes image-based input analysis and access control. These features create it as a comprehensive and high-suitability framework for smart home security.

BIoTC is highly suitable for IoT security enhancement because it provides specific results after implementation. It does not have gaps like other frameworks. The proposed framework is not one dimensional like other frameworks. Few frameworks which either address the access control based on blockchain or rule-based anomaly detection. BIoTC integrates both mechanisms and integrated that in simulated smart home environment (IoT environment). In this research work, the framework successfully mitigates attacks like MITM, unauthorised access or RFID cloning. All these claims were validated with the help of the Cisco Packet Tracer environment and Python-based blockchain modules. The blockchain simulation ensures no unauthorized devices or access in the system. The framework has authority driven validation inspired by authority-driven validation inspired Proof of Authority (POA) principle. There is also a part that identifies anomalies. There are image-based inputs that verifies the system. Blockchain's smart contract concept for automated access control decision. It also includes transparent validation feature. All these properties combinedly results in security enhancement by preventing real time attacks. Framework explains that blockchain has high degree of suitability for IoT environments. This framework not only has concepts but also implementation and results. Therefore, it is "High" suitable for smart home environments.

Table 3: Comparative Framework II

S. No.	Author(s)	Blockchain Used	ML/AI Technique	Anomaly Detection	Image-based Input	Smart Contract Access Control	Smart Home Suitability
1	Darshini et al. (2024)	Yes	CNN	Yes	No	No	Low
2	Xu et al. (2021)	Yes	None	No	No	Yes	Low
3	Kasat (2022)	No	cryptography used	No	No	No	Not Available
4	Anaam et al. (2023)	Yes	None	No	No	Yes	Low
5	Emira et al. (2023)	Yes	None	No	No	Yes	Medium
6	Dirin et al. (2023)	No	None	No	Yes	No	Medium
7	Rani et al. (2023)	Yes	None	Yes	No	Yes	High
8	Ismail et al. (2024)	Yes	Lightweight ML	Yes	No	Yes	High
9	Hızal et al. (2024)	Yes	None	No	No	Yes	Medium
10	Sudipto et al. (2024)	No	Adaptive ML	Yes	No	No	Medium
11	Goel et al. (2024)	Yes	None	No	No	Yes	Low
12	Eghmazi et al. (2024)	Yes	None	No	No	No	Low
13	Sakib et al. (2024)	Yes	None	No	No	No	Medium
14	Lilhore et al. (2024)	Yes	Cognitive ML	Yes	No	No	Medium
15	Prakash et al. (2024)	No	Supervised ML	Yes	No	No	High
16	Almarri and Aljughaiman (2024)	Yes	N/A (Review)	N/A	N/A	No	N/A
17	Kalaria et al. (2024)	No	Prediction ML	Yes	No	No	High
18	Ahakonye et al. (2024)	Yes	None	No	No	No	Medium
19	Affinda (2025)	Yes	None	No	No	No	Low
20	IBM SPSS Modeler Subscription (2024)	Yes	(Conceptual)	Yes	Yes	Yes (Policy-based)	High

Materials and Methods

This research work introduces the framework Blockchain IoT Chain (BIoTC), to enhance security and operational transparency in smart home systems. This framework is the combination of IoT with blockchain with various techniques like visual verification and anomaly detection. Current part explains the simulation work that has smart home setup, vulnerabilities.it also has the blockchain enables security description. Basically, it explains the process and tools used in BIoTC design.

The key point of this framework is its simulation parts. This process is divided into two phases. At the very beginning phase the smart home is simulated in Cisco Packet Tracer. It has all basic electronic devices like RFID cards and readers for smart locks, motion detectors. In the second phase the same setup simulation is transformed into a python-based module. The python-based modules cover smart home setup, different attacks, blockchain characteristics and integration. This phase also shows the effectiveness of blockchain with IoT integration. The combined simulation evaluates the system's robustness against MITM, RFID cloning, and unauthorized access attacks.

Framework Architecture

The BIoTC framework is implemented as a layered, modular stack composed of:

(i) A device layer that models simulated IoT endpoints and event generation
(ii) A communication layer centered on the home gateway that mediates device messages
(iii) A blockchain layer that records validated transactions and enforces simple smart-contract-like policy logic rules
(iv) An anomaly-detection layer that inspects behavioural logs for outliers
(v) A visualization layer that renders blockchain state and alerts for human operators

Data flows upward from device events to blockchain logging and anomaly analysis, while policy decisions and visual feedback flow downward to effectors and user displays.

This concise architecture description links the experimental modules used in our implementation and provides the structural context for the attack simulations and evaluations described later.

IoT Smart Home Simulation Environment

The experimental environment was designed using Cisco Packet Tracer to emulate a complete smart-home network. Fig. 2 represents the smart home simulation. This work involves a realistic simulation of a smart home environment using Cisco Packet Tracer. The smart home setup consists of three zones: Room 1, Room 2, and a Garage. Devices include RFID-based smart locks, motion detectors, webcams, fans, air conditioners, smoke sensors, and IoT-enabled cars.

All devices are interconnected through a centralized home gateway. The simulation models legitimate control via a trusted smartphone and introduces a secondary, compromised mobile client to emulate unauthorized actions. Each security device possesses a unique IP and MAC address to ensure traceability within the simulated network the environment captures communication patterns, device responses, and network events. The entire topology was mapped again to Python modules so that every Packet Tracer event could be reproduced or analyzed through code execution. This approach enabled synchronized experimentation between the virtual environment and blockchain-enabled validation.

Tools and Implementation Setup

The software components of BIoTC were implemented using Python 3.10 on a Windows 11 workstation (Intel Core i3, 11th gen CPU, 16 GB RAM). Fig. 3 shows few libraries that were employed. Few major libraries are:

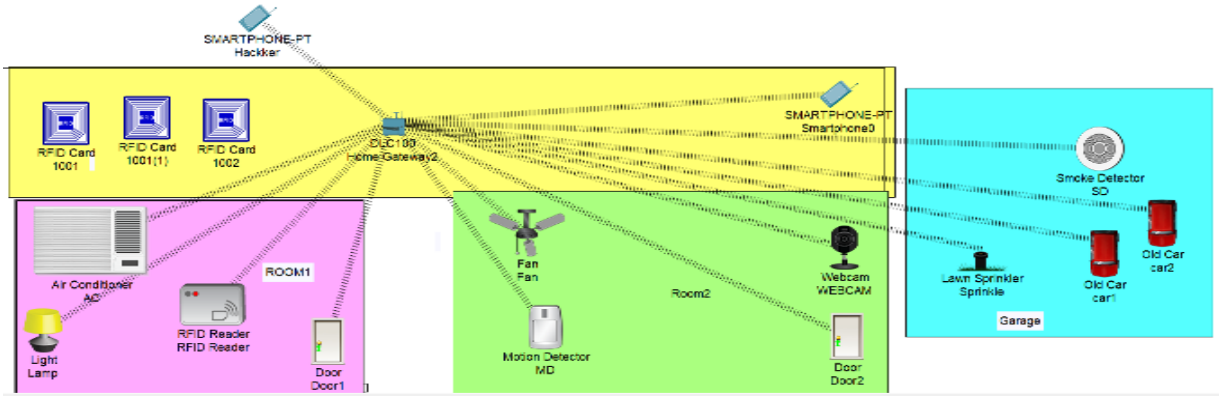

Fig. 2: Smart home Simulation

```
C: > Users > GRV > OneDrive > Desktop > BIOT > final > 4_validation_of_data.py > ...
1   import os
2   import cv2
3   import pytesseract
4   import re
5   import hashlib
6   import time
```

Fig. 3: Libraries used in Python Modules

1. OpenCV and Tesseract OCR: For image capture and text extraction from device snapshots
2. Matplotlib: for live visualization of blockchain activity and comparative security charts
3. Hashlib (SHA-256): for generating cryptographic hashes to maintain block immutability
4. Time and OS modules: For sequential execution, delay handling, and file processing

Cisco Packet Tracer handled network simulation, while Python handled blockchain, attack validation, and visualization, enabling end-to-end integration between virtual IoT nodes and blockchain verification. With simulation and mapping it again with smart home environment.

Attack Simulation and Threat Modeling

Fig. 4 demonstrates how the simulated attacks were executed within smart home environments to evaluate the framework. The figure highlights the communication flows targeted during attack. It includes:

i) RFID cloning: unauthorized unlocking attempts using duplicate credentials
ii) MITM attack: interception in gateway communication path
iii) Unauthorized access attempts: attacker controls the device using his own unauthorized mobile device
iv) Social Engineering Attacks (Chetioui et al., 2022): Demonstrates exploitation of user trust or misconfigurations. Social engineering risks were examined within the smart home simulation to highlight potential weaknesses and evaluate the response of the blockchain-enabled security framework

In Cisco Packet Tracer, two rooms were modeled: Room 1 contained an RFID reader, smart lock, air conditioner, and lamp, while Room 2 hosted a smart lock, fan, motion detector, and webcam.

All attacks are simulated deterministically at the logical level. It reproduces realistic IoT security threats. It does not rely on data-set driven training, probabilistic inference or on ML based decision making.

These settings allowed controlled unauthorized access and manipulation of devices. Such situations were mimicked using corresponding Python modules, by comparing devices with an authorized list and storing each interaction to the blockchain ledger. The simulations illustrate how social engineering attacks can be correlated to system behaviour, despite not carrying out any user trials. Unchangeable recording on the blockchain ensures transparency and accountability, which in turn discourages any wrongdoing and it also increases BIoTC framework role in securing smart home environments. This attack simulation scheduling is used as the basis for subsequent security defences and ensures a measure of realism even under duress.

Blockchain-Enabled Security and Validation

In this part blockchain is introduced as single-authority, tamper-evident validation system the framework utilizes its property of immutability, concepts of timestamping.

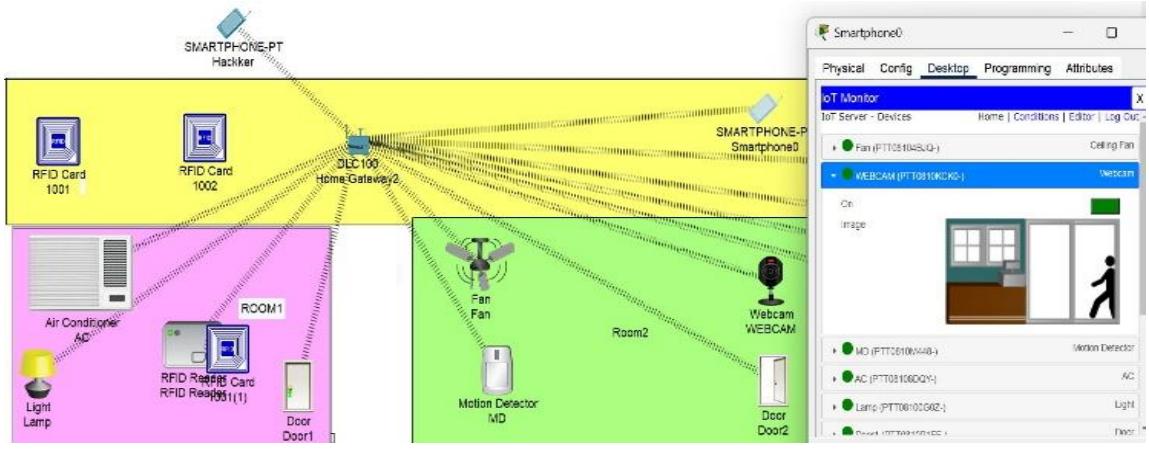

Fig. 4: Smart Home Vulnerabilities

DOI: 10.3844/jcssp.2026.1083.1099

Authority-driven block validation Here blockchain serves as backbone for smart home security. Instead of relying on centralized gateway, the framework enforces temper evident validation using single authority blockchain layer. For example, in room -1 only valid RFID can be accessed. Only the devices registered through the given values and verified keys are allowed in the system. This process removes the risk of cloning or some fake devices. Blockchain will not allow them in the system. The whole system is transparent in nature. Hash values are helpful in identifying immutability and changes.it immediately identifying the intrusion in the given system. The integration of blockchain enhances integrity and traceability in the smart home environments. For automation, smart-contract-like policy logic implemented at the Python blockchain layer features are used.

Fig. 5 is the blockchain output logs. It is showing blockchain enabled security and validation. Each block contains current hash, previous hash, Timestamp, even the status of device is mentioned in the block.it is either in active or inactive mode. Details like IP address and MAC address will prove the transparency of the framework.

The blockchain part in BIoTC is implemented as lightweight Python-based imitation to demonstrate immutability, traceability and unauthorized part detection. Each block stores device related data. It also has time Stamp, previous and current hash. This implementation does not include any distributed consensus, digital signature or executable smart contracts. The focus of this study is functional security validations rather than protocol level blockchain implementation.

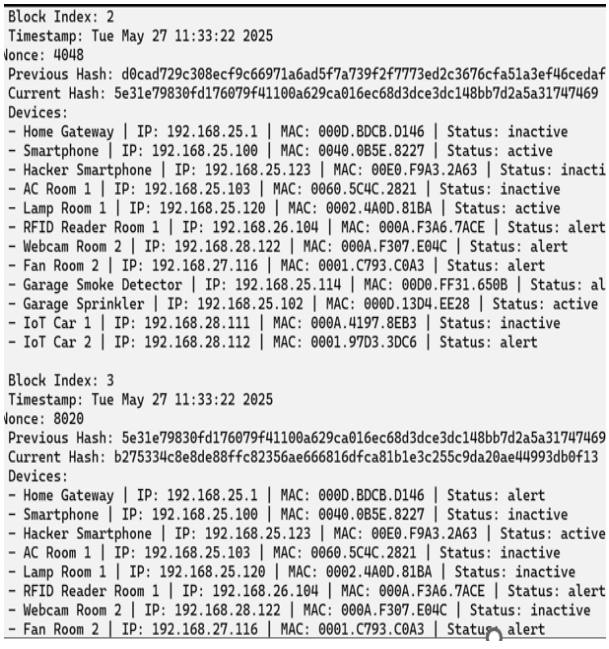

Fig. 5: Python Enabled Blockchain Simulation

Anomaly Detection and Intelligent Analysis

While blockchain ensures integrity, anomaly detection enhances responsiveness.

A rule-based anomaly logic inspired by Isolation Forest principles (Ahakonye et al., 2024) is integrated to evaluate predefined legitimate user/device behaviour patterns for deviations indicating potential attacks.

Fig. 6 represents the next part. The anomaly detection engine processes device metadata, access times, and behavioural logs stored in the blockchain. This dual validation anomaly-based and rule-based offers a hybrid security model. The anomaly detection mechanism in this work was designed by drawing inspiration from the principles of the Isolation Forest algorithm, particularly its ability to identify outliers without heavy training overhead. Instead of directly implementing Isolation Forest, the research work adapted the core idea to suit the smart home environment and the constraints of our simulation. The approach prioritizes efficiency and interpretability, ensuring it can be applied in resource-constrained IoT devices. Although more advanced models such as LSTM could capture temporal attack patterns, the intention was to establish a lightweight, proof-of-concept framework. A broader comparison with other machine learning techniques is left for future work to strengthen the generality of the proposed solution.

Isolation forest is referenced only as a conceptual example. It explains how anomaly detection could be integrated in BIoTC. The current implementation does not train or execute any machine learning model.

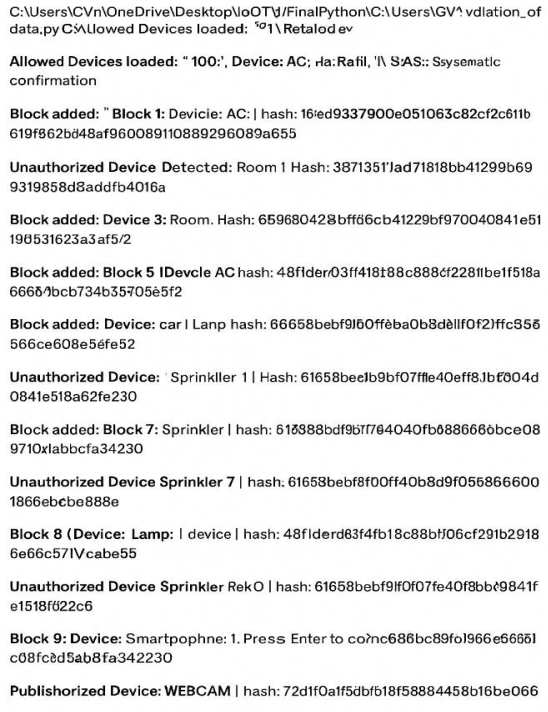

Fig. 6: Finding Anomalies

Testing, Visualization, and Security Validation

The next part is testing in BIoTC. The framework records all the information of smart IoT devices within the blockchain and later visualizes them. Its helps in analytical evaluation later. Fig. 7 explains the block creation time comparison for the authorised and unauthorised devices during testing phase.

It shows the variation in block creation timing. The observed variation in block creation time reflects differences in validation flow in between authorised and unauthorised interactions. This helps the security matrices to determine how effectively the blockchain distinguishes between legitimate and malicious IoT device.

For visual representation, during evaluation OpenCV and OCR (Optical Character Recognition) are used to extract the devices information. This also helps the framework to present them in real time visual. Different colored blockchain blocks intuitively visualize threats from unauthorized entities or devices. The system performance is systematically compared before and after the integration of blockchain to quantify security improvements. It can be validated that BIoTC improves the general resilience against unauthorized access and other kinds of cyber threats. The OCR procedure of the framework uses OpenCV and Pytesseract to read device labels and IP information from smart home photos that are stored in Allowed and mixed folders. Pre-processing of the images is performed by thresholding and grayscale conversion to improve recognition, after which structured information can be extracted with regular expressions. Further on, the detected device will be compared with a previously prepared whitelist. Immutability and traceability can be guaranteed by creating a block in the blockchain for each entry with the device data, timestamp, and cryptographic hash.

A visualization dashboard, created using Matplotlib, offers real-time blockchain monitoring. The authorized and unauthorized devices are color-coded differently, and the block sequence is represented as a linked structure.

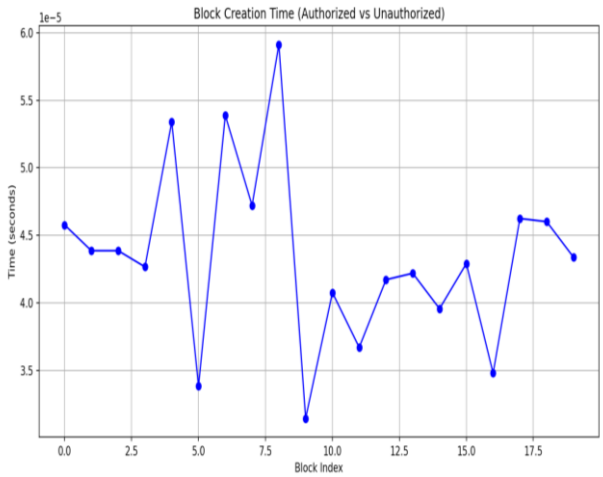

Fig. 7: Visualization of Block Creation Time

Additional graphs illustrate supplementary parameters: Block creation time, energy consumption per block, and the ratio between legitimate/unauthorized devices. The modular design thus enables continuous visual feedback and secure tracking of IoT activity inside the smart home, while keeping the implementation lightweight and scalable without the need for external dependencies.

Abstract View

The flow diagram of the proposed BIoTC framework, developed for addressing the security of IoT-based smart homes, is illustrated in Figure 8.

BIoTC framework starts with simulating a smart home in Cisco Packet Tracer with IoT-enabled devices in various locations such as rooms and garages. Additionally, these devices can simulate more complex scenarios than customary smart home devices, like RFID cloning, MITM attacks and illegal access attempts. Their programs also run on the popular Python programming language. The security components, once validated in terms of resilience and reaction with the help of the attack simulation layer, are presented, followed by the blockchain layer which constitutes the other base of the BIoTC system. It protects data integrity across the communication layer, enforces access control via smart-contract-like policy logic implemented at the Python blockchain layer and establishes an unalterable transaction log; any unauthorized access to data or systems and all updates to records are guaranteed to be recorded and made non-repudiable by this layer.

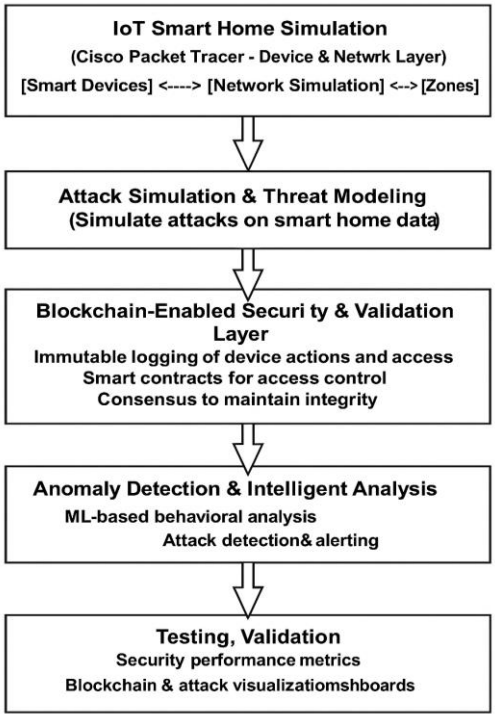

Fig. 8: Workflow of BioTC

Building on this is a analysis layer based on rule evaluation that uses anomaly detection algorithms to monitor device and user patterns in real time. This layer defines the changes from normal patterns and raises potential threats proactively for better resilience against advanced and adaptive attacks. The last tier of the framework is the visual validation and feedback layer. In this regard, outputs from the security components are aggregated and visualized with dynamic dashboards and image-based validation. This not only emulates the real-time interpretation of system patterns but also supports non-technical users in understanding and responding to security alerts. By combining the real-time simulation together with the transparency of blockchain and adaptive anomaly detection, the BIoTC architecture provides a practical and scalable solution to the security challenges of modern smart home ecosystems.

Figure 8 presents the layered approach to implement IoT smart home security from bottom to top. The simulation layer simulates the interaction between devices and networks using Cisco Packet Tracer. The activity data generated at this layer is provided to the other upper layers for implementing the required security. First, it is provided to the threat modeling layer where RFID cloning, MITM, and unauthorized access-based attacks are then considered for capturing vulnerabilities. In the blockchain layer, all device behavior is recorded on the blockchain, while access control rules and data integrity mechanisms are provided thorough smart contract like policy logic implemented in python. The anomaly detection layer applies rule-based logic inspired by anomaly detection process to identify whether the device is acting normally or behaving suspiciously, using the blockchain log as reference. The testing and validation layer aggregates this data and calculates metrics such as qualitative detection effectiveness, false positive rate, and relative response behaviour under simulation. It provides dashboards displaying this information as well as the blockchain log and attack scenarios.

Feedback loops are formed between these layers, with actions by the device, attacks, validation, and detection all sensed to create a security architecture for smart homes.

Implementation and Experimental Setup

A fully simulated experimental system was developed for the assessment of the practicality and resilience of the suggested BIoTC framework. This combines most of the key elements, such as blockchain validation, network simulation, cyberattack emulations, anomaly detection, and visual feedback layers. The key aim of this implementation was to enable statistical and pattern analysis of security performance while simultaneously offering a realistic smart home environment.

All experiments were executed in a simulation-driven environment on a Windows-based consumer-grade system serving as an edge or home-gateway class execution platform; hardware details are reported solely to clarify execution context rather than for performance benchmarking.

The proposed framework was implemented and validated in a simulation-based test environment. The smart home network, including rooms, a garage, and interconnected devices, was modelled using Cisco Packet Tracer, v. 8.2. All the security mechanisms such as blockchain emulation, anomaly detection logics, and visualization through OCR have been developed in Python, v. 3.10. All experiments were executed on a standard laptop with an Intel Core i3 processor, 16 GB of RAM, and Windows 11 as the operating system.

Although no specific IoT hardware was deployed at this stage, the combination of Cisco Packet Tracer and Python offers a reproducible environment that allows a study of the vulnerabilities, simulations of various attacks, and testing of the efficiency of the countermeasures proposed. Accordingly, the modular implementation ensures that the same framework will be easily ported later to real IoT devices and blockchain platforms without significant modification. The performance of different modules was investigated by using suitable indicators. Regarding anomaly detection, the framework considered the detection capability against simulated attack events. In turn, a blockchain module was evaluated based on how well it would ensure immutability and maintain verifiable logs. For OCR-based visualization, device recognition and feedback delivery were studied in the simulation.

Various aspects related to the framework's implementation are considered. In the first setup, Cisco Packet Tracer was used to visualize a virtual smart home with three different zones: Room 1, Room 2, and the Garage. Room 1 had an air conditioner, a lamp, and a smart lock that featured RFID. Room 2 contained a webcam, a ceiling fan, a motion sensor, and a smart lock. Correspondingly, the garage contained a smoke detector, a lawn sprinkler, and two cars embedded with IoT. All devices were connected by a central unit called the home gateway, which could be used for external control of the devices as well as their internal coordination. Each node, to enable deterministic communication, tracking of activities, and execution of attack scenarios, was assigned a unique IP address and MAC.

One legitimate smartphone was added to simulate authorized users' interactions, while one malicious phone, called an attacker's phone, was introduced to initialize unauthorized activities and probe vulnerabilities under stress.

To replicate real-world attacks, a suite of Python-based scripts was introduced. These scripts again simulated multiple cyber threats and attacks. These attacks were checked under controlled conditions, allowing for read and observation of system behaviour and response assessment mechanisms in real time. To

address and handle these threats, a lightweight, a blockchain layer was introduced and implemented using Python. This layer recorded each device interaction as an immutable transaction, starting with a Genesis block. Each subsequent block stored necessary information in metadata like timestamp, device ID, current status, technical details and smart-contract-like policy logic implemented at the Python blockchain layer validated whether each device or user was authorized to perform the action in question. The simplified authority driven block validation mechanism was implemented using a single logical miner to maintain the chain's integrity and consistency, tailored for use in the case of low relative response behaviour under simulation.

An anomaly detection module was added to the blockchain's reactive attack mitigation. The anomaly detection model includes access authorization, device behavior, and it was inspired by the Isolation Forest algorithm. During these early days following deployment, whenever anomalous behaviour was detected, it triggered an alert and recorded information about the attack on the blockchain, providing both real-time defense during these attacks and an auditable record of them. In the framework smart contract like access control behaviour is implemented using python modules. The policy automatically checks and validates each device's identity. Through this the system differentiates authorized and unauthorized entities. The automation continuously updates the device status (authorized /unauthorized) within the framework.

Except that, to enhance the interpretability of the system, visual analysis modules were added to the system. Using OpenCV and Tesseract OCR, (Affinda, 2025) the framework analyzed image-based inputs from two directories Allowed/ (legitimate devices) and mixed/ (test inputs). It extracted text-based identifiers from the images and compared them against a secure whitelist. Visual feedback was presented using a blockchain-themed graphical interface, where authorized devices were shown in color orange, and malicious ones in red color, enabling intuitive system monitoring. The visual validation uses OpenCV and Tesseract OCR on simulated device interface screen shots rather than physical camera feeds. Preprocessing is intentionally minimal and limited to thresholds. The objective is to whitelist based device identity validation rather than OCR accuracy evaluation.

Except that, the performance of the system before and after blockchain integration was evaluated and estimated through graphical charts. Using Matplotlib, bar graphs, pie charts, and radar plots were generated to illustrate improvements in attack qualitative detection effectiveness, vulnerability reduction, and also framework capabilities.

The entire BIoTC system was organized into seven modular Python programs, each handling a basic segment of the framework:

1. Smart home simulation
2. Threat injection and modelling
3. Blockchain ledger simulation
4. Blockchain-security integration
5. Anomaly detection and validation
6. Visualization and reporting
7. System integration and testing

The design specially emphasized modularity, reproducibility, and transparency, making BIoTC not only a theoretical or conceptual contribution but a practically verifiable prototype for advancing security in smart home IoT environments.

Discussion

In order to check the performance of the BIoTC framework to enhance the security of smart homes, a multi-stage evaluation was conducted. The evaluation only focused on major performance parameters such as attack detection, access verification, anomaly identification, and visual interpretability. The framework was tested within the simulated smart home environment developed in Cisco Packet Tracer. In simulation both malicious and legitimate interactions were implemented using Python-based scripts. The evaluation was categorized into three sequential phases: First phase is without blockchain, second is blockchain-enhanced, and third has intelligent analysis.

In the base configuration, the smart home ran without any security enhancements. At this level, attacking the system by duplicating RFID cards, performing a MITM attack, or gaining unauthorized access by spoofing credentials were all trivial to carry out. The smart home had no way to log, verify, or control interactions with devices. Because of this, low-complexity attacks like these were enough to subvert the system. This demonstrated the vulnerability of a typical IoT system where a lack of supervision and traceability results in uncontrolled device behaviour and loss of trust.

Moving to the blockchain maturity phase, research work had added a custom Python private blockchain and the improvements were substantial. All device communications and control commands were logged as an immutable transaction on a temper evident blockchain ledger. Each transaction included metadata such as timestamp, device id, operation type, and source. Smart contracts like policy logic implemented within the blockchain level were designed to evaluate specified access control policies and refuse commands from unauthorized sources. The comparative tests showed a reduction in successful attack attempts. Devices or users that were denied access due to failing in identity and whitelist verification and not satisfying smart contract rules were quickly refused access. The system

demonstrated tamper-resistance and provided a transparent audit trail of all device access. Automatically refusing access to suspicious calls without manual intervention proved the value of the blockchain layer in defending IoT environments. Within the BIoTC framework, smart contract like behaviour is implemented through the Python blockchain modules. Device activity is first checked against a predefined whitelist, with unauthorized devices identified and logged separately. Each new block stores device attributes and cryptographic hashes, ensuring records remain permanent and verifiable. Automated policy enforcement is further demonstrated by the anomaly detection module, which flags unusual device behaviour. Together, these mechanisms replicate the operational role of smart contracts by regulating access, enforcing security policies, and maintaining an auditable record of IoT interactions in the smart home simulation.

The analysis phase extends this by incorporating rule-based anomaly logic inspired by machine learning principal without executing any learning model. An anomaly detection logic inspired by isolation forest principle was evaluated using simulation for IoT devices in the smart home. When this rule-based anomaly logic was executed in simulation, it monitored ongoing process in sequential manner raising an alarm if any behaviour was deemed out of character. So, if an RFID card was read at an unexpected time of day or in an unexpected sequence it was flagged as anomalous and denied entry. This was particularly useful for not-so-obvious threats such as social engineering, which often circumvent fixed access control rules. The behavioral rule evaluation combined with the rule-based enforcement mechanism added a second layer of dynamic threat analysis, increasing the overall defense mechanism effectiveness.

To provide a point of contact between the technical operations layer and human monitoring, Visual dashboards were added to the system. From device images captured with OpenCV and Optical Character Recognition (OCR) using Tesseract, the devices were identified and their actions were displayed via a color-coded visual interface in which orange represented legitimate device behaviour and red represented malicious or unauthorized behaviour. This visual summary enabled administrators and users to observe the state of the system and security in real time without needing to translate technical logs. Charts and dashboards visualized the security posture before and after the blockchain.

This work is intentionally presented as a simulation-based PoC to examine how blockchain and visualization can be combined to enhance IoT security. The prototype relies on Python modules and Cisco Packet Tracer simulations rather than full-scale hardware deployment or on-chain smart contracts. However, the solution was designed in a modular way so that it can be migrated to practical environments with minimal changes. The smart contract rules for access control are already defined within the framework and could readily be implemented in Solidity or Hyperledger chaincode. Similarly, the virtual devices modeled in Packet Tracer, such as RFID locks, cameras, or motion sensors, correspond directly to physical IoT components, making hardware integration a natural next step. In this sense, the current study establishes a solid foundation, with future phases aimed at implementing smart contracts on a permissioned blockchain and testing the framework with real IoT hardware.

The current version of BIoTC is simulation centric. It does not model indoor localization, activity zone semantics and physical layer impairments. This is the reason it does not contain localization metrics, hard ware resource profiling. The future will focus on deploying on real edge devices or permissioned blockchain. This will enable to cover localization security policies ,hardware level evaluations.

In summary, by integrating real time anomaly detection, blockchain based transaction validation, and visual feedback, we believe that BIoTC is an integrated security framework. Different from existing frameworks which usually focus on single aspect (e.g. data integrity), BIoTC provided an integrated solution that not only defined the perimeter BIoTC but also detected multi-stage attacks, enforced secure proactive security policies, and provided visual transparency. BIoTC was implemented in a modular way and was lightweight, which is suitable for smart home deployment. Our results demonstrated the practical, layered and intelligent BIoTC as a solution to secure IoT in smart home.

Performance Evaluation and Results

To systematically evaluate the effectiveness of our proposed BIoTC framework, this research work performed a comprehensive evaluation of the framework with respect to both qualitative and feature-wise benchmarks. To this end, our evaluation method was designed to analyse the effectiveness of the BIoTC framework in several aspects, such as the ability to improve security, scalability, policy-driven decision logic,and practicality in smart home scenarios. Each parameter was chosen to represent a real-world challenge when applying IoT-based systems in smart homes. Through a combination of functional testing and comparison analysis, our evaluation approach could give us a comprehensive understanding of the effectiveness of BIoTC in terms of resisting threats, scalability, flexibility, and practicality in smart home scenarios. The rest of the results are visualized by some radar and bar charts to show the comparative advantage of BIoTC over other existing frameworks.

For comparison, four state-of-the-art frameworks from recent literature proposed by Roy, Sharma, Kumar, and Thomas were selected. These frameworks were chosen based on their relevance to IoT security, their publication

credibility, and their partial alignment with the objectives of this work (e.g., blockchain integration, anomaly detection, or simulation support). However, most of them lack a holistic, end-to-end solution encompassing real-time simulation, attack modeling, visualization, and policy enforcement via blockchain logic.

The following charts provide a comparative visualization of feature coverage, simulation strength, security validation, and architectural comprehensiveness across the selected frameworks and the proposed BIoTC.

In Fig. 9 there is a stacked bar chart that illustrates a comparative evaluation of key functional components across few existing IoT security frameworks Roy, Sharma, Kumar, and Thomas against the proposed BIoTC framework. While existing works exhibit partial feature coverage such as Roy and Kumar focusing solely on ML detection, Sharma incorporating simulation and attack modelling, and Thomas implementing only blockchain, none provide a comprehensive solution. In contrast, BIoTC integrates all five essential pillars: Blockchain for secure data integrity, simulation for realistic environment modelling, attack modeling for threat representation, Rule-based anomaly detection logic, and real-time visualization. This complete integration reflects the holistic and practical strength of BIoTC in addressing modern smart home security challenges.

Figure 10 illustrates coverage of security layer within the IoT stacks. It shows the coverage divided into five infrastructural layers, i.e., perception layer, device layer, network layer, application layer and data layer. The percentages are determined based on the number of security mechanisms at each layer. For both the network layer and application layer, the coverage is 25%.

This is because the protection of communication layer protocols and domain-specific software interfaces is conceptually the same. Coverage for the perception layer, device layer and data layer is at a moderate level of 16.7% each.

These layers are often not secured against physical sensor observation, device identity and data integrity. Especially, as the coverage of perceptions and devices is relatively low, the proposed BIoTC framework comparatively attempts to close the gap of customary solutions to provide layered security for all layers in the IoT stack.

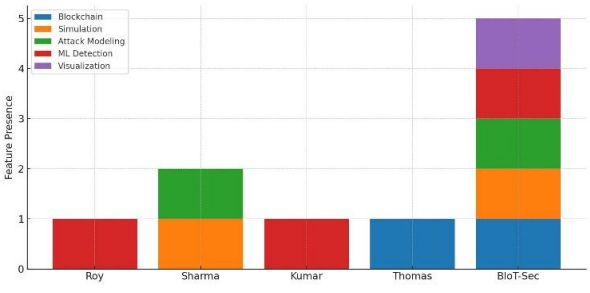

Fig. 9: Comparison between Functionalities

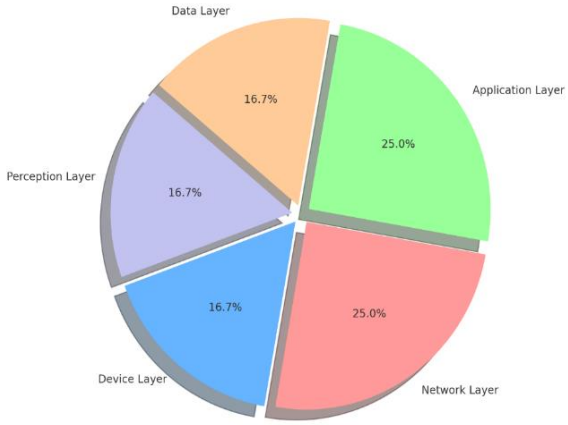

Fig. 10: Distribution of Security across Layers

Now calculating percentages:

Perception Layer: (2 / 12) × 100 = 16.7%
Device Layer: (2 / 12) × 100 = 16.7%
Network Layer: (3 / 12) × 100 = 25.0%
Application Layer: (3 / 12) × 100 = 25.0%
Data Layer: (2 / 12) × 100 = 16.7%

Table 4 summarizes the layer-wise coverage of IoT security frameworks, showing that BIoTC spans all major layers of the IoT architecture, while other frameworks address only specific layers. This highlights the layered security perspective adopted in the proposed framework.

Table 4: Layer-wise coverage

Layer	Covered by Frameworks	Count
Perception Layer	BIoTC only	2
Device Layer	Sharma, BIoTC	2
Network Layer	Kumar, Thomas, BIoTC	3
Application Layer	Roy, BIoTC	2
Data Layer	BIoTC, Sharma	2
Total		12

The next part of the evaluation focuses on the use of radar charts visualizing feature coverage of different IoT security frameworks (IBM SPSS Modeler Subscription, 2024; Choudhary et al., 2024b). This study proposes the use of radar charts to visualize differences in feature coverage. Figures are included to visually show comparative advantages of the proposed blockchain ML simulation and integration techniques over the prior state of the art, summarize the shortcomings of existing approaches, and show the completeness and utility of the BIoTC framework to an audience of varying technical fluency levels.

Fig. 11 compares five IoT security frameworks- Roy, Sharma, Kumar, Thomas, and proposed BIoTC-in a radar chart across five dimensions: Blockchain, Simulation, Attack Modeling, ML Detection, and Visualization. Each axis represents the binary presence

(1) or absence (0) of a feature. The proposed BIoTC enjoys full coverage across all five dimensions; hence, it is the most comprehensive and well-rounded for ensuring security in smart home IoT environments. In contrast, Sharma supports only Simulation and Attack Modeling, while Kumar includes only ML Detection, reflecting a limited scope. Thomas incorporates Blockchain alone, while Roy integrates ML Detection only. Further, this radar chart presents the fragmented nature of existing approaches and highlights BIoTC's holistic coverage of critical features in ensuring security within smart home IoT environments.

A benchmark scale of 0–5 was defined for the radar chart to show the extent of implementation for five core parameters: Simulation, Blockchain, Attack Modeling, Anomaly Detection Logic (Rule-based), and Visualization. The values are summarized in Table 5 based on reported implementations in existing works of Roy et al., Sharma et al., Kumar et al., Thomas et al., and the proposed BIoTC framework. These scores are plotted on the radar chart for a comparative visualization.

Figure 12 has been included to provide a visual, high-level comparison between the proposed BIoTC framework and the average feature coverage of several leading IoT security frameworks. The radar chart uses seven axes, each representing a vital capability for secure smart home systems namely: Blockchain Integration, Real-Time IoT Simulation, Attack Modeling, ML-based Anomaly Detection, Visualization, Smart Contract Support, and Cisco Packet Tracer Integration.

In Figure 12, the orange polygon represents the BIoTC framework, which extends fully across all axes indicating conceptual and functional support for all seven critical features comprehensively. In contrast, the blue polygon reflects the average capability of existing frameworks. This area is noticeably smaller and irregular, showing that while some features (e.g., blockchain or attack modeling) are partially addressed by prior work, many others like visual dashboards, ML detection, or real-time integration with simulators remain underdeveloped or completely absent.

This figure is crucial for two reasons:

1. It helps readers visually compare the technical completeness of BIoTC against traditional solutions
2. It emphasizes the practical relevance of each feature in the context of IoT smart homes, where layered, adaptive, and transparent security is essential

Thus, the chart not only shows BIoTC's broad coverage and maturity but also makes it easier for both technical and non-technical audiences to grasp its real-world applicability and advantages. In BIoTC, the 'ML Detection' label denotes rule-based anomaly logic inspired by machine-learning principles; no trained or executed machine-learning model is used in the current implementation and also smart contract functionality depicted in the figures refers to smart-contract-like policy logic implemented at the Python blockchain layer, rather than executable on-chain smart contracts.

Table 5: Quantitative Benchmarks

Method	Simulation	Blockchain	Attack Modeling	Anomaly Detection	Visualization
Roy	2	0	3	0	1
Sharma	4	0	5	1	2
Kumar	0	0	0	4	1
Thomas	0	0	0	5	1
BIoTC	5	5	5	5	5

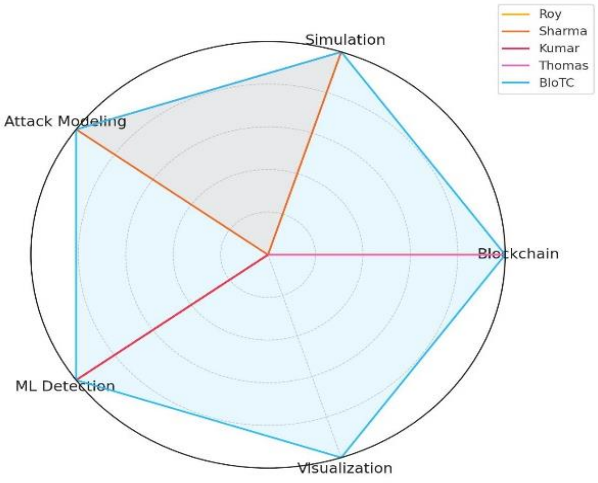

Fig. 11: Framework Feature Coverage

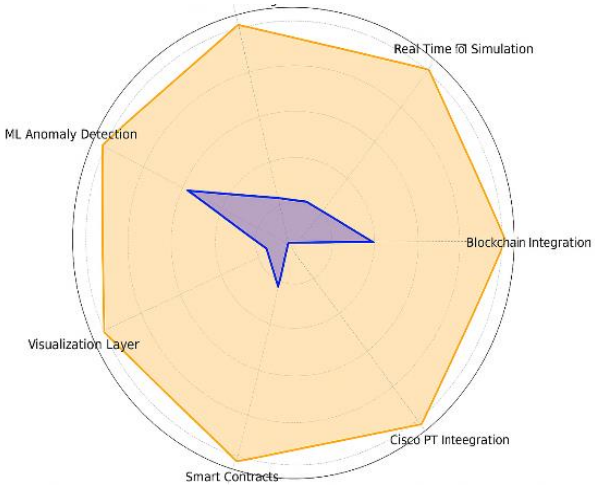

Fig. 12: BIoTC vs Others

Conclusion and Future Work

Smart homes have enabled the creation of numerous connected IoT appliances that symbolize new levels of convenience and automation. However, the number of appliances connected to the Internet has created new dynamic cybersecurity attack surfaces. Smart home devices, such as smart locks, fitness bands, etc., are also susceptible to unwanted access, RFID spoofing, man-in-the-middle attacks and social engineering. To reduce these issues, we have proposed a BIoTC based on an IoT chain architecture that uses blockchain technology. We designed the architecture of BIoTC as a layered defence consisting of simulation-based environment modeling in Cisco Packet Tracer, behavior-based scripting and threat emulation in Python, blockchain emulation for tamper-proof guarantee of the validation steps. All these components were designed specifically for the smart home environments on which BIoTC was to be deployed.

By hands-on experiments, BIoTC illustrated the ability for security mitigation through blockchain-based validation and rule-based anomaly detection logic. The visual part of the framework, based on OCR and OpenCV, offered end-users a possibility to get intuitive feedback - improving transparency and reaching real-time device legitimacy and system state interpretation. In contrast to most of the current methodologies which are either centralized, under-the-hood theoretical, or do not consider human interaction at system's use, BIoTC provides actionable and behaviour aware security mechanism built on tamper evident blockchain validation that addresses genuine attack vectors in an operational setting.

Moving forward, the research envisions the extension of BIoTC into a real-world testbed, where physical IoT hardware like Raspberry Pi, ESP32 will be integrated to emulate real smart home conditions operations and threat conditions. Smart contracts within the blockchain layer will be made more context-sensitive, enabling access policies that adapt based on factors such as device behaviour, location, or time of request. Enhance the accuracy of detection while protecting user privacy to train the anomaly detection model in a federated learning way, that is, train in each home but not necessarily store the behavioural data. Apply the lightweight cryptography algorithm to optimize the blockchain technology to be applicable in IoT devices, Extend the visual dashboard to be more interactive and explainable, Study how users can have more insights into the system decision and keep the visibility to the security of their home, Study about the possibility of decentralized blockchain cooperative defense network, that is, smart home can share the verified threat intelligence with each other. Smart homes will be connected in a web-like cybersecurity fabric in different homes.

By integrating layered validation, behavioural intelligence, and user-oriented design, the BIoTC framework provides a ready-for-the-future security infrastructure for IoT-based smart homes. In addition to filling current gaps in anomaly detection, real-time threat simulation, and visualization, BIoTC paves the way for new opportunities in collaborative and explainable security in increasingly complex digital homes.

Acknowledgment

I am really thankful to my supervisor, Prof (Dr.) Sarvesh Tanwar and my co-supervisor, Prof (Dr.) Pankaj Kumar Sharma. Their mentorship and support were fundamental to this research. I am deeply grateful for their expert directions and suggestions.

Funding Information

This research work was conducted without any external financial support. No specific grant from any agency was received for this work.

Authors Contributions

Gaurav Vats: Was responsible for overall research and the development of the framework. His contribution included executing all the experiments. He conducted the simulation work and implemented the python-based modules.

Sarvesh Tanwar: Provided essential supervision over methodology and technical design. Her feedback was crucial on validation part. Her suggestion in integration of different methodology played an important role.

Pankaj Kumar Sharma: Provided overall project guidance. He played a key role in revision process. His expertise helped in refining the final structure and clarity.

Ethics

On behalf of all authors, the corresponding author declares that this work is original and has not been published anywhere.

Conflict of Interest

The authors declares that they don't have any kind of potential conflicts of interest that directly or indirectly influences the work in this study.

References

Affinda, T. (2025). Data extraction with Tesseract OCR, OpenCV, and Python. *Affinda Blog*. https://www.affinda.com/blog/tesseract-ocr-opencv-and-python?utm_source=copilot.com

Ahakonye, L. A. C., Nwakanma, C. I., & Kim, D.-S. (2024). Tides of Blockchain in IoT Cybersecurity. *Sensors*, *24*(10), 3111. https://doi.org/10.3390/s24103111

Aljumah, A. (2025). Blockchain-inspired distributed security framework for Internet of Things. *Scientific Reports*, *15*(1), 10066. https://doi.org/10.1038/s41598-025-93690-2

Almarri, S., & Aljughaiman, A. (2024). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. *Sustainability*, *16*(23), 10177. https://doi.org/10.3390/su162310177

Anaam, E., Hasan, M. K., Ghazal, T. M., Haw, S.-C., Alzoubi, H. M., & Alshurideh, M. T. (2023). How Private Blockchain Technology Secure IoT Data Record. *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*, 1–6. https://doi.org/10.1109/icaic57335.2023.10044178

Baral, S., Saha, S., & Haque, A. (2024). An Adaptive End-to-End IoT Security Framework Using Explainable AI and LLMs. *2024 IEEE 10th World Forum on Internet of Things (WF-IoT)*, 469–474. https://doi.org/10.1109/wf-iot62078.2024.10811456

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, *198*, 656–661. https://doi.org/10.1016/j.procs.2021.12.302

Choudhary, V., Tanwar, S., & Choudhury, T. (2024a). Evaluation of contemporary intrusion detection systems for internet of things environment. *Multimedia Tools and Applications*, *83*(3), 7541–7581. https://doi.org/10.1007/s11042-023-15918-5

Choudhary, V., Tanwar, S., & Choudhury, T. (2024b). Generating IoT Specific Anomaly Datasets Using Cooja Simulator (Contiki-OS) and Performance Evaluation of Deep Learning Model Coupled with Aquila Optimizer. *Journal of Computer Science*, *20*(4), 365–378. https://doi.org/10.3844/jcssp.2024.365.378

Darshini, J., & Nagaraju, V. (2024). Enhancing the QoS in Intelligent 5G Enabled IoT using Novel Convolutional Neural Network and Blockchain-Empowered Security Framework. *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1–5. https://doi.org/10.1109/icccnt61001.2024.10724913

Dirin, A., Oliver, I., & Laine, T. H. (2023). A Security Framework for Increasing Data and Device Integrity in Internet of Things Systems. *Sensors*, *23*(17), 7532. https://doi.org/10.3390/s23177532

Emira, H. H. A., Elngar, A. A., & Kayed, M. (2023). Blockchain-Enabled Security Framework for Enhancing IoT Networks: A Two-Layer Approach. *International Journal of Advanced Computer Science and Applications*, *14*(10), 12. https://doi.org/10.14569/ijacsa.2023.0141059

Eghmazi, A., Ataei, M., Landry, R. J., & Chevrette, G. (2024). Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy. *IoT*, *5*(1), 20–34. https://doi.org/10.3390/iot5010002

Ferraris, D., Fernandez-Gago, C., Roman, R., & Lopez, J. (2024). A survey on IoT trust model frameworks. *The Journal of Supercomputing*, *80*(6), 8259–8296. https://doi.org/10.1007/s11227-023-05765-4

Goel, O., Gajbhiye, B., Gangu, K., Avancha, S., Rao Thumati, P. R., & Hussein, L. (2024). A Secure and Efficient Blockchain Protocol for Protecting Electronic Health Records. *2024 4th International Conference on Blockchain Technology and Information Security (ICBCTIS)*, 326–331. https://doi.org/10.1109/icbctis64495.2024.00058

Hajoary, D., Basumatary, R., & Narzary, R. (2024). Bibliometric Analysis of IoT Application Research: Unveiling Trends and Future Directions for Terahertz Communication in Wireless Systems. *2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS)*, 328–332. https://doi.org/10.1109/ictacs62700.2024.10841096

Hızal, S., Akhter, A. F. M. S., Çavuşoğlu, Ü., & Akgün, D. (2024). Blockchain-based IoT security solutions for IDS research centers. *Internet of Things*, *27*, 101307. https://doi.org/10.1016/j.iot.2024.101307

IBM SPSS Modeler Subscription. (2024). Radar charts. *IBM Documentation – SPSS Modeler (SaaS*. https://www.ibm.com/docs/en/spss-modeler/saas?topic=types-radar-charts

Ismail, S., Nouman, M., Dawoud, D. W., & Reza, H. (2024). Towards a lightweight security framework using blockchain and machine learning. *Blockchain: Research and Applications*, *5*(1), 100174. https://doi.org/10.1016/j.bcra.2023.100174

Kalaria, R., Kayes, A. S. M., Rahayu, W., Pardede, E., & Salehi S., A. (2024). IoTPredictor: A security framework for predicting IoT device behaviours and detecting malicious devices against cyber attacks. *Computers and Security*, *146*, 104037. https://doi.org/10.1016/j.cose.2024.104037

Kasat, K., Rani, D. L., Khan, B., J, Ashok., Kirubakaran, M. K., & Malathi, P. (2022). A novel security framework for healthcare data through IOT sensors. *Measurement: Sensors*, *24*, 100535. https://doi.org/10.1016/j.measen.2022.100535

Lilhore, U. K., Dalal, S., & Simaiya, S. (2024). A cognitive security framework for detecting intrusions in IoT and 5G utilizing deep learning. *Computers and Security*, *136*, 103560. https://doi.org/10.1016/j.cose.2023.103560

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Alshoura, W. H., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers and Security*, *112*, 102494. https://doi.org/10.1016/j.cose.2021.102494

Prakash, V., Odedina, O., Kumar, A., Garg, L., & Bawa, S. (2024). A secure framework for the Internet of Things anomalies using machine learning. *Discover Internet of Things*, *4*(1), 33. https://doi.org/10.1007/s43926-024-00088-z

Rani, S., Babbar, H., Srivastava, G., Gadekallu, T. R., & Dhiman, G. (2023). Security Framework for Internet-of-Things-Based Software-Defined Networks Using Blockchain. *IEEE Internet of Things Journal*, *10*(7), 6074–6081. https://doi.org/10.1109/jiot.2022.3223576

Sakib Sizan, N., Dey, D., Abu Layek, Md., Uddin, M. A., & Huh, E.-N. (2025). Evaluating blockchain platforms for IoT applications in Industry 5.0: A comprehensive review. *Blockchain: Research and Applications*, *6*(3), 100276. https://doi.org/10.1016/j.bcra.2025.100276

Vats, G., Tanwar, S., & Sharma, P. K. (2024). A Simulation-Based Analysis of IoT Security Architecture in Smart Homes. *2024 International Conference on Computing, Sciences and Communications (ICCSC)*, 1–4. https://doi.org/10.1109/iccsc62048.2024.10830301

Xu, X., Wang, X., Li, Z., Yu, H., Sun, G., Maharjan, S., & Zhang, Y. (2021). Mitigating Conflicting Transactions in Hyperledger Fabric-Permissioned Blockchain for Delay-Sensitive IoT Applications. *IEEE Internet of Things Journal*, *8*(13), 10596–10607. https://doi.rg/10.1109/jiot.2021.3050244

Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Karimipour, H. (2023). Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks. *Computers in Industry*, *144*, 103801. https://doi.org/10.1016/j.compind.2022.103801