Received: 15 September 2025 | Revised: 12 November 2025 | Accepted: 6 February 2026 | Published online: 20 March 2026

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2026, Vol. 00(00) 1–9
DOI: 10.47852/bonviewJCCE62027670

BON VIEW PUBLISHING

Performance Analysis of Block–Internet of Things–Chain (BIoTC) Framework for Smart Home

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

[1] *Amity Institute of Information Technology, Amity University, India*

[2] *ABES Engineering College, India*

Abstract: Smart-home systems built on Internet of Things (IoT) devices offer convenience, but they also introduce gaps in security and privacy that are often overlooked. Traditional protective measures such as lightweight encryption, access control rules, and intrusion alerts do help, but they do not fully address issues such as traceability, proof of device identity, or resistance to more adaptive attacks. In response to this, the research proposes a blockchain-supported security model called Block–Internet of Things–Chain (BIoTC), designed specifically for smart-home IoT networks. This work developed the setup using Cisco Packet Tracer to model a basic smart home. In this environment, the study carried out on four forms of attacks: Man in the Middle (12 attempts), RFID cloning (6 attempts), unauthorized access (1 case), and social engineering (1 case). Each attack was performed on a regular IoT configuration, and then the same test was repeated after introducing the BIoTC layer. The blockchain component, implemented through a lightweight Python module, maintains immutability and coordinates identity checks to confirm that a device should be allowed in the network. The distinct contribution of research comes from grounding the evaluation in actual experimental observation rather than theoretical claims. The results show that BIoTC is successful in the reduction of attack success rate with acceptable performance overhead for a smart-home environment. Using a real-world example, the mathematical validation was performed. This research paper presents verified and statistical methods for the security of IoT smart-home systems. The results demonstrate that integrating blockchains enhances defense against security threats in the IoT environment.

Keywords: IoT security, smart homes, blockchain, cybersecurity attacks, security frameworks

1. Introduction

The Internet of Things (IoT) has rapidly converted conventional living homes into intelligent and automated environments [1, 2]. Within smart homes, everyday devices such as Radio-Frequency Identification (RFID)-enabled locks, webcams, motion detectors, smart fans, and sprinklers can now communicate and coordinate actions through a central gateway. IoT brings connectivity, assistance, and automation. It directly gives enhanced control to users. The negative side of this advancement is that these electronic devices are facing a wide range of physical and cyber threats [3, 4]. Due to the expansion of IoT environments, it is not easy to protect these devices from recent advanced attacks.

1.1. Security challenges in smart homes

IoT-based smart homes are totally different from industry-level automation systems. The major difference is the devices used in both areas. In smart homes, smart devices have very limited memory and low processing power. They often rely on insecure communication protocols. For these reasons, the system is not very safe from outside attacks. They cannot run strong security protocols because devices do not have good computational power. The smart-home systems are always under external threats. These threats include attacks such as RFID cloning [5], Man-in-the-Middle (MITM) attacks [6], unauthorized access, and social engineering attacks [7]. An MITM attack occurs when an unauthorized person secretly intercepts communication between two entities. The person can then read and modify the communication during the attack. Similarly, in RFID cloning, the attacker duplicates the unique identifier or stored data from the original one. It is a threat to physical security. Unauthorized access happens when an individual or device gains entry into the system without proper authorization. This can compromise the security and privacy of the system and lead to potential attacks. Weak passwords and compromised credentials are among the primary causes of this vulnerability. Social engineering involves nontechnical attackers who exploit and manipulate human psychology to impersonate legitimate entities. Many times, this includes sensitive personal information. There are many algorithms such as lightweight cryptographic algorithms and intrusion detection that have made valuable contribution in security of IoT devices. In the context of

***Corresponding author:** Sarvesh Tanwar, Amity Institute of Information Technology, Amity University, India. Email: stanwar@amity.edu

smart home [8], these algorithms are not up to the expectations. They need additional computational power and extra memory for resolving the security issues.

Except for these issues, this system follows the concept of centralization [9]. In centralization, one major device controls all other devices. Now this can lead to a big problem called a single point of failure. In this study, the home gateway is the centralized authority. The gateway manages all the devices and their authentication in the system. Except that it has the responsibility of packet routing. Now, if the attacker gains control over this centralized node, they can read, manipulate, and even block the communication. They have the authority to change the routing tables. They can send wrong commands. This leads to the whole system failure. All these issues are really serious. A few minor things such as the lack of forensic traceability and no transparency in the system creates big problem during a mishappening. The current solution addresses only some parts of the problem. They do not provide a guarantee for fully secure smart-home systems.

1.2. Contribution and organization

The main contribution of this research is the introduction of a security framework for IoT systems. The Block–Internet of Things–Chain (BIoTC) framework is a blockchain-integrated approach designed for IoT-enabled smart homes. The main features of this research are:

1) Simulation of IoT-Based Smart Home: Cisco Packet Tracer–generated simulation that includes two rooms and a garage, inhabited with IoT devices, serves as the testbed.
2) Four Different Attacks: RFID cloning, MITM, unauthorized access, and social engineering are simulated to expose vulnerabilities.
3) Lightweight Python Blockchain: Instead of relying on heavy blockchain platforms, a custom blockchain is developed in Python to enable efficient event logging, scan-based validation, and rule enforcement. The framework applies a lightweight Proof-of-Authority (PoA) mechanism in which all IoT devices are predefined participants within the blockchain network, while two trusted nodes—the home gateway and the legitimate smartphone—operate as validators that authorize and append verified transactions to the ledger.
4) Statistical and Mathematical Validation: Unlike prior works, the evaluation is grounded in mathematical analysis. Metrics such as Attack Success Probability (ASP), Blockchain Verification Reliability (BVR), and Comparative Improvement (CI) are derived from experimental logs.

The paper is organized as follows: Section 2 reviews related work. Section 3 outlines the research methodology. Section 4 presents the mathematical and analytical validation. Section 5 details the results and discussion. Section 6 explains the conclusion and future scope. The novelty of this work lies in its real-time empirical validation of IoT security through a lightweight Python blockchain integrated with Cisco Packet Tracer, bridging simulation and analytical evaluation.

1.3. Research objectives

The main reason for this study is to design and produce a lightweight blockchain-based security framework that strengthens IoT-enabled smart homes against different cyber threats, with a focus on data-driven statistical standards. To achieve this goal, the research is directed by the following objectives:

Objective 1: Examine the security challenges of IoT in smart homes and their constraints:

The first step is to carefully look into the main threats to IoT-based smart homes. These threats include MITM attacks on gateways, unauthorized access to devices, RFID card cloning, and social engineering attempts.

The study deeply checks how well the current and proposed system works. This study will show the need of decentralized system.

Objective 2: Evaluate the existing framework for attack prevention and detection:

The aim is to analyse current solutions and identify gaps in those solutions. The objective is to evaluate the positive and negative aspects of each solution, such as cryptographic evaluations or intrusion detection systems. This will help address the problems associated with these traditional frameworks.

Objective 3: Propose the BIoTC framework: The introduction of the framework BIoTC, a blockchain lightweight in nature, implemented using modular Python programs, is the unique feature of this solution. The framework also follows blockchain features such as immutability, transparency, decentralized validation, and consensus algorithms such as PoA. Moreover, BIoTC guarantees secure device authentication, immutable access logs, and trustworthy IoT event validation.

BIoTC presumes that all authenticated IoT devices in the smart-home network are preregistered and recognized as trusted participants. Two reliable nodes—the home gateway and an authorized smartphone—will function as validators under a lightweight PoA mechanism to verify and record transactions. The adversary is modeled as a local attacker capable of device cloning, unauthorized access, or message interception but without control over validator credentials. These assumptions define the security boundary within which BIoTC ensures integrity and decentralized validation of IoT events.

Objective 4: Validate and statistically analyze the BIoTC framework: The final objective is to rigorously validate the proposed framework against simulated attack scenarios. Comparative experiments are conducted before and after blockchain integration, and the results are quantified using mathematical and statistical metrics such as ASP, BVR, and CI. This ensures that validation is evidence-based, reproducible, and analytically sound.

The framework's performance is evaluated using three quantitative metrics such as ASP, BVR, and CI as defined in the *Mathematical and Analytical Validation* section. These metrics are derived from experimental logs generated during multiple attack scenarios (MITM = 12, RFID = 6, unauthorized = 1, social engineering = 1), ensuring consistency between the statistical analysis and the results discussed later in the paper.

2. Literature Review

In the paper "Statistical Analysis of Remote Health Monitoring Based IoT Security Models & Deployments From a Pragmatic Perspective," Ashok and Gopikrishnan [10] assessed statistical analysis of IoT security models in remote health monitoring systems. This work includes the identification of different attacks and the comparison of different security methods and modules. It is specifically designed for remote healthcare modeling. The paper uses success rate and vulnerability scores to achieve its target. The study also includes advanced techniques and models such as machine learning (ML), blockchain, and software-defined networking to show their effectiveness in scalability and latency in

the field of IoT healthcare. The study is now giving any new technique but guiding researchers for future work. In a similar context, Almarri and Aljughaiman [11] conducted a deep research work on IoT that includes blockchain-based trust and security mechanisms. The main goal of the study is to demonstrate the role of blockchain in preventing data manipulation, and it shows positive results in various aspects such as authentication and transparent transactions, which are the main features of blockchain. The study also emphasizes scalability, energy-efficient consensus, and resilient trust protocols as key directions for future research. In another work, Selvarajan et al. [12] proposed the DIDLT-BC model, which integrates blockchain with Rabin's digital signature to enhance IoT security and privacy. The model achieved 98 % secure-transaction validation accuracy under simulated cloud–IoT conditions, with reduced execution time (150 ms) and mining latency (0.98 s), thereby outperforming existing approaches in security, cost, and throughput. It enables protected data storage and retrieval in heterogeneous IoT–cloud environments while mitigating scalability and processing constraints. Almuqren et al. [13] evaluated their hybrid deep learning intrusion detection system (IDS) using the NSL-KDD benchmark; we note that NSL-KDD is a general IDS dataset (widely used for classifier comparisons) rather than an IoT-specific corpus, so their results demonstrate classifier performance in benchmark conditions but do not by themselves prove smart-home traffic fidelity. Mathur S. et al. [14] compare various approaches, including a private blockchain-based smart-home network with an IDS, Unmanned Aerial Vehicles (UAVs) for surveillance, supply chain and logistics, and ML-based framework for smart cities. The review also references deep learning–based anomaly detection techniques, which could be applied to analyze BIoTC event logs in future work for identifying anomalous device behavior, as well as a permission-based blockchain scheme to secure IoT devices. Other works cited include distributed ML-oriented IDSs, a blockchain-enabled IDS using a deep stacked network, and a hybrid optimization model for detecting Distributed Denial-of-Service (DDoS) attacks. Overall, the reviewed literature points to the use of blockchain and various ML and deep learning models to address the security and privacy challenges in smart home and IoT environments. Overall, the reviewed literature points to the use of blockchain and various ML and deep learning models to address the security and privacy challenges in smart home and IoT environments; however, most prior studies remain conceptual and lack real-time blockchain-based event validation and cross-device verification, which this work addresses through the BIoTC framework. The study "Generative AI, IoT, and Blockchain in Healthcare: Application, Issues, and Solutions" by Mazhar et al. [15] demonstrates how blockchain ensures secure data management, while Artificial Intelligence (AI) enhances decision-making within a sensitive IoT environment. Although focused on healthcare, its architectural insights—such as the integration of blockchain for data integrity and AI for adaptive learning—are equally applicable to smart-home security systems. These parallels underline that cross-domain frameworks combining intelligence and immutability can strengthen IoT ecosystems against data manipulation and privacy breaches. Hızal et al. [16] proposed a blockchain-based IDS research center that decentralizes security intelligence sharing among research nodes using blockchain immutability. While their focus is on collaborative DDoS detection in large-scale IoT networks, the underlying architecture—where full nodes validate IDS model updates and light nodes access validated security data—illustrates a transferable mechanism of decentralized validation. In a smart-home context, similar principles can be adapted so that the gateway and authorized devices act as validators, enabling real-time detection sharing and immutable logging of anomaly events. Similarly in "Privacy-Preserving Security of IoT Networks: A Comparative Analysis of Methods and Applications" [17], Wakili and Bakkali compare privacy-preserving security methods for IoT networks, evaluating cryptography (symmetric such as Advanced Encryption Standard (AES), asymmetric such as Elliptic Curve Cryptography (ECC)/Rivest–Shamir–Adleman (RSA), lightweight options such as PRESENT, and emerging quantum-resistant algorithms), blockchain (decentralized authentication, smart contracts, consensus mechanisms such as PoW/PoS, and advanced integrations such as Hyperledger Fabric), ML (supervised with SVM/RF/DT/Naive Bayes for intrusion/malware detection, unsupervised with KNN/clustering for anomalies, reinforcement with Q-Learning for adaptive responses, and deep learning with Convolutional Neural Network (CNN)/Recurrent Neural Network (RNN) for pattern recognition), and fog/edge computing (IDS systems, decentralized architectures, secure data processing, and virtualization technologies) against metrics such as scalability, efficiency, robustness, and usability. It highlights cryptography's strong security but high overhead, blockchain's decentralization but energy demands, ML's adaptability with privacy risks, and fog/edge's low latency with management challenges, addressing IoT issues such as resource constraints, interoperability, and threats like DDoS. The findings advocate for a hybrid approach to leverage strengths, offering guidance for academia, industry, and policymakers, with future research directed toward integrated and quantum-resistant solutions. There is another research study done by Bhatia and Charul [18]. The target of this work was to study IoT security research published between 2017 and 2024. A dataset of 1881 Scopus-indexed papers was analyzed using Citespace and VOS viewer. It basically focuses on new technologies such as AI, ML, blockchain, etc. It also discussed major security approaches such as cyber deception technology and Quantum-inspired security. The study promoted the shift toward a decentralized approach with an intelligent security framework. It says that there is a need for scalability and lightweight models. In a similar manner, Zrelli and Rejeb [19] conducted a bibliometric analysis of 2680 Scopus-indexed publications (2000–2023). It traverses different IoT applications in the field of supply-chain management and logistics. Their outcome shows how IoT, blockchain, and intelligent systems can increase data integrity, transparency, and trust across distributed environments. Although centered on logistics, the mechanisms identified, such as blockchain-based traceability, integrity, and AI-driven automation, are directly transferable to smart-home IoT security, where similar decentralized validation and data-integrity principles can strengthen trust among connected devices.

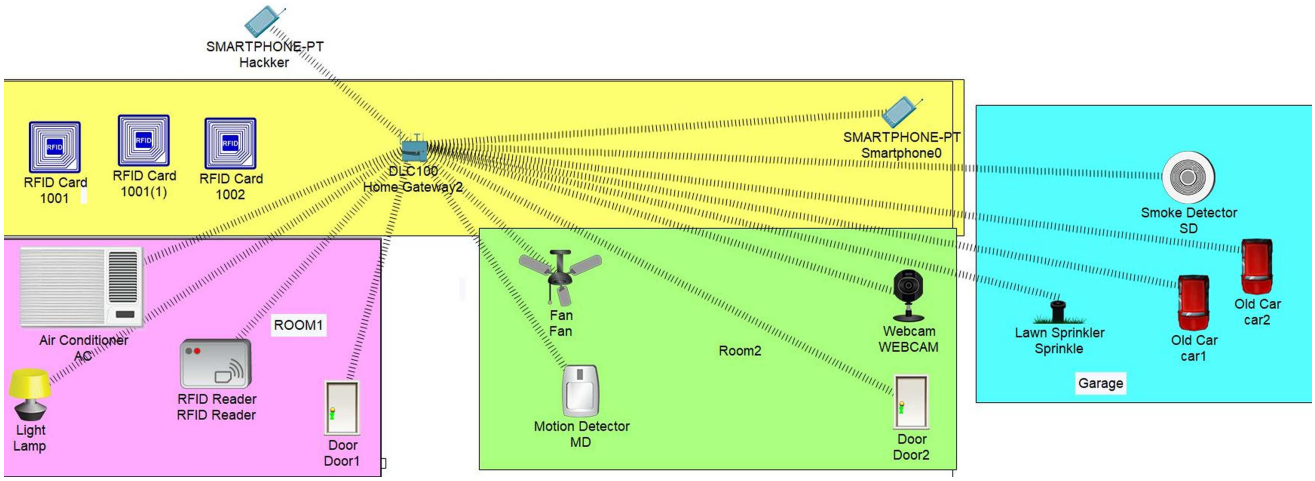
3. Methodology and System Design

The proposed framework was simulated and validated with two different environments. This involves Cisco Packet Tracer and Python-based blockchain modules. This part explains the smart-home simulation and the mapping of attacks on these simulations. In addition, blockchain-based Python modules are described and illustrated with supporting Figures.

3.1. Smart-home simulation in Cisco Packet Tracer

Figure 1 shows a smart-home simulation on Cisco Packet Tracer. To enhance the reproducibility, an IoT-based smart home is simulated on Cisco Packet Tracer [20]. It has two different rooms

Figure 1
Smart-home simulation



and one garage; all these parts have their own electronic devices that are connected to a central IoT gateway. The description of these devices is as follows:

Room 1 has RFID reader, smart lock, and air conditioner smart lamp.

Room 2 has smart lock, fan, motion detector, and webcam.

Garage has IoT-enabled cars, smoke detector, and lawn sprinkler.

An authorized smartphone was also configured as the controller, while an unauthorized smartphone with similar privileges was introduced to simulate attack attempts. This setup provides a reproducible environment for both normal operations and malicious activities.

3.2. Attack scenarios simulated

Figure 2 shows the vulnerabilities in smart homes. To evaluate the security posture of the smart home, four representative attack scenarios were executed:

1) RFID Cloning: Exploiting cloned RFID credentials to unlock smart locks.

2) Man-in-the-Middle (MITM): Intercepting and altering communication between devices and the gateway.

3) Unauthorized Access: Exploiting weak/default authentication credentials to bypass access control.

4) Social Engineering: Manipulating legitimate users to grant malicious access or perform unsafe actions.

These scenarios were chosen because they reflect both technical vulnerabilities and human-centric threats, ensuring a holistic coverage of the smart-home attack surface.

3.3. Lightweight blockchain integration (Python modules)

Figure 3 shows one of the Python modules that is used to integrate all components into one platform. The blockchain integration [21, 22] for BIoTC is realized through a lightweight Python framework consisting of seven coordinated modules, each responsible for a specific function in the simulation and validation pipeline.

1) Smart-Home Simulation: Models IoT devices (locks, webcams, fans, AC) as Python classes with attributes such as IP, MAC, authentication, and state.

2) Attack Simulation: Recreates threats such as RFID cloning, MITM, unauthorized access, and social engineering, generating logs of successful and failed attempts.

Figure 2
Attack flow in smart homes

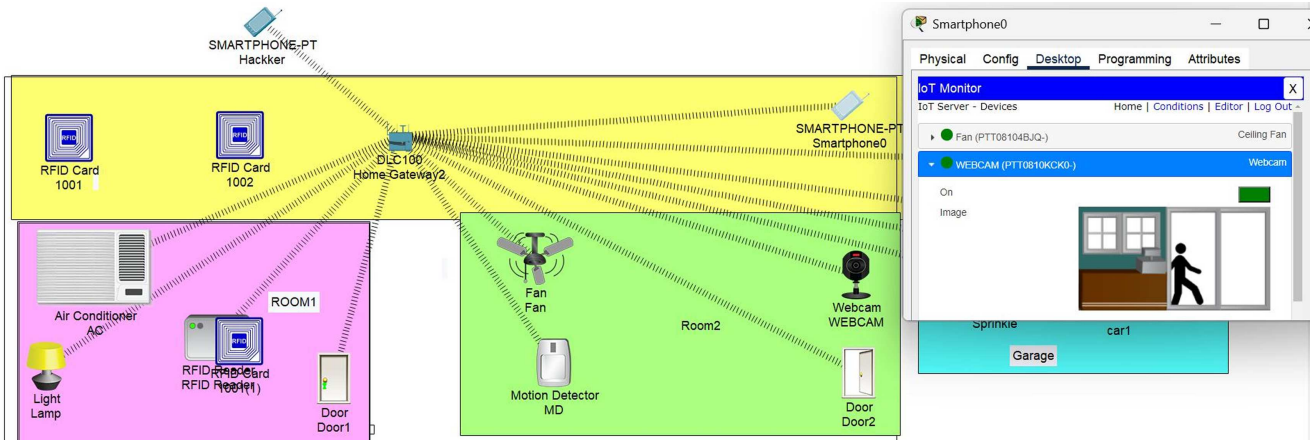


Figure 3
Python module of the BIoTC framework

```
=== BIOT SMART HOME RESEARCH MENU ===
1 Smart Home Details > press 1
2 Attack Simulation > press 2
3 Blockchain Simulation > press 3
4 Testing & Validation > press 4
5 Visualization > press 5
6 Smart Home with Blockchain > press 6
Run All: press 7
Exit: press 0

Enter your choices:
```

3) Blockchain Simulation: Implements a Python-based blockchain with block creation, nonce, mining, and SHA-256 hashing to demonstrate immutability and transparency.

4) Blockchain–Smart Home Integration: Links device actions with blockchain validation. Unauthorized devices are blocked, and validation uses PoA [23] with the smartphone and gateway as validator nodes.

5) Validation and Metrics: Analyzes authentication logs before and after blockchain integration, computing metrics such as block creation time, security breach rates, and detection accuracy.

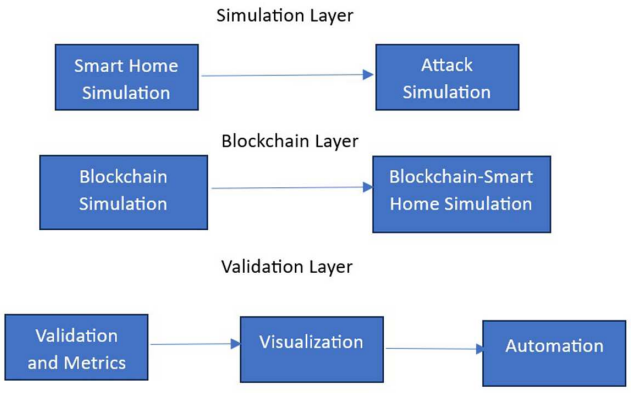
6) Visualization: It produces bar charts, pie charts, and line plots to illustrate access patterns, block times, and attack mitigation effectiveness.

7) Automation: Orchestrates all modules sequentially, ensuring reproducibility by simulation, attack (automatic), blockchain, validation, and visualization stages.

This modular design ensures that BIoTC is lightweight, reproducible, and adaptable. Each module directly contributes to the overall workflow, enabling the framework to both simulate real-world attacks and validate the blockchain's security benefits.

Figure 4 illustrates the three operational layers—Simulation, Blockchain, and Validation—where the Simulation Layer models IoT and attack behavior, the Blockchain Layer records and verifies events through a lightweight Python blockchain, and the Validation Layer performs metric analysis and visualization for performance assessment.

Figure 4
Layered architecture of the BIoTC framework



3.4. Observation of events

This section explains how the attacks were managed with or without blockchain. Multiple attack attempts were executed, with each attack treated as an independent event. It has nothing to do with previous outcomes and any previous state. Every trial is totally independent. The reported sample sizes of attacks were 12 for MITM, 6 for RFID cloning, 1 for unauthorized access, and 1 for social engineering [24]. These attacks were designed to demonstrate the consistency of the framework. Even the events were observed in the simulation output. The output includes the number of attack attempts per scenario and the success or failure status of each attempt. It was also checked by the system whether the blockchain validation blocked or allowed each attempt.

These observations formed the primary dataset and were subsequently translated into the statistical quantities defined in Section 4 (Mathematical and Analytical Validation), namely, ASP, BVR, and CI. By emphasizing direct observation rather than synthetic collection, the methodology ensures that the results are reproducible and faithfully represent the simulated IoT environment.

4. Mathematical and Analytical Validation

There are different ways to evaluate the system. Some systems are based only on qualitative analysis, but for a perfect and reliable system, the process should also be quantitative. This part shows that the security parameter is evaluated on both parameters. The mathematical model of the framework validates its effectiveness. It is directly mapped to the results produced by simulations. This section defines the core metrics, explains how they are computed, and demonstrates how blockchain integration changes the security posture of the system.

4.1. Rationale for mathematical validation

Traditional IoT security studies often present attack–defense scenarios without a rigorous statistical foundation. In such works, it is unclear how much security has been improved or whether improvements are consistent and reproducible. In contrast, the BIoTC framework uses event logs as the basis for formulas that measure attack success, detection probability, and blockchain reliability. This approach ensures that every claim of improvement is tied to observable quantities rather than assumptions. In other words, the validation is not a theoretical exercise but a statistical [25] reflection of experimental results.

4.2. Notation and data linkage

For each attack type (MITM, UNAUTH, RFID, SOCENG), the following quantities are taken directly from the simulation logs:

$N_{att}(A)$: total attempts of attack.

$N_{succ,\ raw(}(A)$: successful attempts in the baseline run (BIoTC disabled).

$N_{blk}(A)$: attempts blocked by BIoTC in BIoTC-enabled runs.

$N_{succ,biotc}(A)$: successful attempts under BIoTC.

$N_{ver}(A)$: number of events sent to blockchain for verification.

$N_{rej}(A)$: number of events rejected by blockchain rules.

Assumptions used here**:** (1) All events in BIoTC runs are verified on chain, so $N_{ver}=N_{att}$, and (2) blocked events are indicated in red in the logs.

1) Comparative Improvement (CI): CI is based on the standard concept of relative performance improvement [25, 26].

Percentage reduction in attack success due to BIoTC:

$CI(A)= ((ASP_{raw}(A)-ASP_{obs}(A)) *100)/ (ASP_{raw(}A))$

2) Attack Success Probability (ASP): ASP is directly derived from empirical probability [27], where each "attempt" corresponds to an independent attack execution as described in Section 3.4.

Baseline (no blockchain):

$ASP_{raw}(A) =N_{succ,\ raw}(A) / N_{att}(A)$ (/ = division)

Observed with BIoTC:

$ASP_{obs}(A)=N_{succ,\ biotc}(A) / N_{att}(A)$

3) Blockchain Verification Reliability (BVR): It shows how effective the blockchain policy is at filtering malicious inputs.

Fraction of verified events that are rejected by blockchain policy:

$BVR(A)= N_{rej}(A) / N_{ver}(A)$

With our assumption $N_{ver}=N_{att}$

Numeric results after execution:

MITM (gateway):

$N_{att}=12, N_{succ,raw}=10, N_{blk}=12, N_{succ,biotc}=0$

Unauthorized access**:**

$N_{att}=1, N_{succ,raw}=1, N_{blk}=1, N_{succ,biotc}=0$

RFID cloning (Room1**):**

$N_{att}=6, N_{succ,raw}=2, N_{blk}=2, N_{succ,biotc}=0$

Social engineering (Room 2):

$N_{att}=1, N_{succ,raw}=1, N_{blk}=1, N_{succ,biotc}=0$

MITM:

$ASP_{raw}=10/12=83.3\%., ASP_{obs}=0/12=0\%, CI=100\%$ $BVR=12/12=1.00.$

Unauthorized:

$ASP_{raw}=1/1=100\%, ASP_{obs}=0\%$ $CI=100\%.$ $BVR=1.00$

RFID cloning:

$ASP_{raw}=2/6=33.3\%., ASP_{obs}=0\%$ASP.$CI=100\%$ $BVR=2/6=33.3\%$

Social engineering:

$ASP_{raw}=1/1=100\%, ASP_{obs}=0\%, CI=100\%$ $BVR=1.00$BVR

4.3. Interpretation

Strong defensive effect**:** Across all simulated attack types, BIoTC reduced observed success to zero in these runs. The effect is strongest for MITM, where baseline vulnerability was high (83.3% success), indicating that message anchoring and gateway validation are effective against interception and injection attacks in the simulated topology.

RFID nuance**:** RFID cloning had a lower baseline success rate (33.3%) because only a subset of attempted cards was valid, yet BIoTC removed the residual risk by validating tag registrations on chain. Note that BVR for RFID is 33.3% because only two of six attempts were rejected—this reflects the composition of your RFID tests.

Human factor**:** Social engineering and single unauthorized attempts were successful in baseline runs. In the simulation, BIoTC's policy enforcement and audit logging prevented those single attempts from completing, showing that combining on-chain policy checks with forensics can help mitigate socio-technical attacks. However, these attacks had small sample sizes (N = 1); therefore, results must be presented with caution.

5. Results and Discussion

The current part explains the result of the simulation work. It identifies the meaningful outcomes. Discussion around these outcomes will take the research to broader implications such as security and privacy and scalability. All these things are executed around those four attack scenarios that were discussed before. These attacks were simulated on Cisco Packet Tracer and then secured through the Python-based framework BIoTC.

The first performance parameter is the ASP. This measurement directly relates to the vulnerabilities of the IoT smart-home system. The result shows the clear difference between before and after the integration of blockchain with the system. For the first security issue, MITM, the ASP decreases from 83.3% to 0%.

The confidence interval was moderate and showed clear improvement after blockchain integration. The other two issues—unauthorized access and social engineering—both had ASP = 100% for single testing. Here, the sample size is small, but the results are positive as the ASP dropped to 0% after blockchain implementation. There was also an issue of cloning, so for RFID cloning, ASP dropped from 33.3% to 0%. The baseline confidence interval was broad due to six attempts, but after the blockchain introduction, the system cloning issue was completely eliminated. The confidence interval reached to 100% for all specified attacks. This shows that blockchain is effective in neutralizing the attacks. The attack success rate is zero in each attempt.

BVR evaluates the effectiveness of blockchain integration in preventing unauthorised access. It indicates whether harmful access attempts are successfully blocked. The matric is attack specific and it reflects the frequency of attacks and ability to discriminate legitimate and malicious activities. In this experiment, the MITM, unauthorized, and social engineering achieved BVR = 1.00. This means that all malicious attempts were rejected. RFID achieved BVR = 0.333. It shows only two of the six total attempts.

These result shows the reliability and effectiveness of the system.

5.1. Practical implications

In practical terms, the BIoTC framework has shown notable effectiveness across different layers of IoT security. This study uses an event-driven simulation environment (Cisco Packet Tracer and Python) focused on functional and logic-level validation; therefore, device-level resource profiling (CPU, RAM) and end-to-end network latency measurements were not directly recorded in the present experiments.

In the smart home simulation, the gateway provided strong resilience against MITM attacks, underscoring how immutability and blockchain anchoring can secure packet level communication. Beyond network-level threats, it also addressed human-factor risks, as blockchain based validation and auditing mechanism successfully mitigated social engineering attempts, offering forensic traceability and deterrence. In addition, the RFID cloning experiments highlighted the framework's ability to preserve credential integrity by reliably distinguishing genuine identities from cloned ones, even under the constraints of low-resource IoT devices. In BIoTC, after merging blockchain with IoT, the framework shows significant changes in security. The next two figure shows few results after the blockchain was implemented. Both are the results of different inputs but show flexibility accordingly.

Figure 5 explains the time taken to generate blocks. It shows noticeable fluctuations across different block indices. The early stages exhibit higher variability, with some blocks requiring significantly longer processing time than others, which can be attributed to the computational overhead of handling initial transactions and cryptographic hashing.

Figure 5
Block creation time comparison

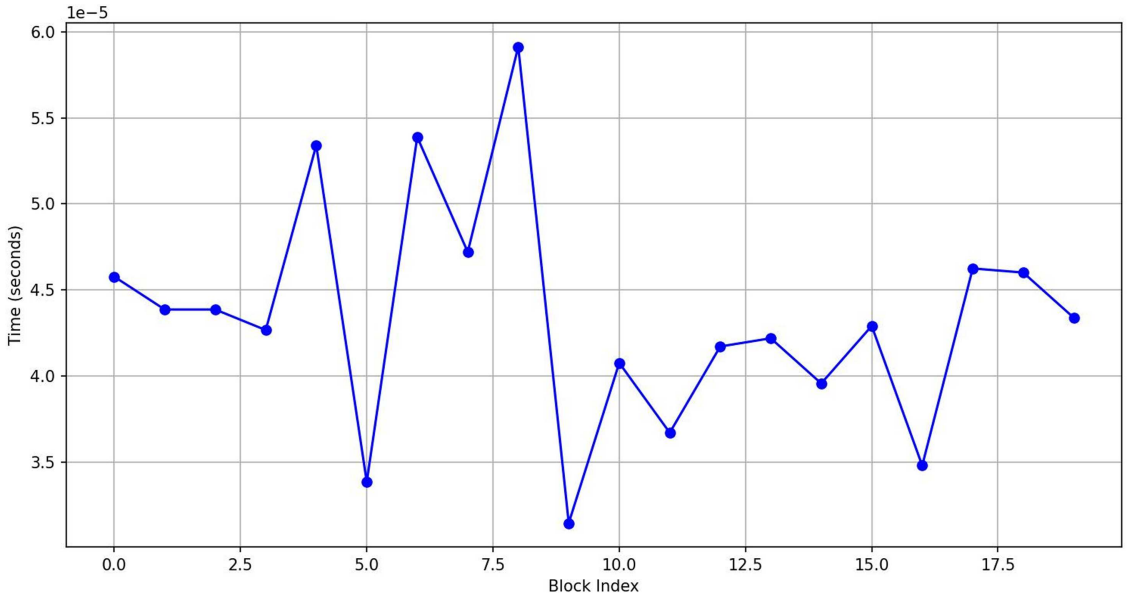


Figure 6
Device authentication and energy consumption

```
Block 1 created in 0.00005 seconds
Device: AC [Authorized]
Energy Consumed: 39 units
Hash: 62718e07bdfc2e9eb643f4f221cddab3d9568e588ae3f2c037976a017c15dd05
Previous Hash: f814a40417d5c3224d589e10f80cd82a3e36c8f18dfb3096b83bc3979c17c340

Block 2 created in 0.00004 seconds
Device: 1001(1) [Unauthorized]
Energy Consumed: 83 units
Hash: 582dc5bed7e5b87843c67d613100a8fe1c5f8cb76fbef0ae5217d300a4824f13
Previous Hash: 62718e07bdfc2e9eb643f4f221cddab3d9568e588ae3f2c037976a017c15dd05

Block 3 created in 0.00004 seconds
Device: Home Gateway2 [Authorized]
Energy Consumed: 27 units
Hash: 15cf47be331997c34af854f15ff1f107406f8235fd9ada300b9e91d60fd6e1c9
Previous Hash: 582dc5bed7e5b87843c67d613100a8fe1c5f8cb76fbef0ae5217d300a4824f13

Block 4 created in 0.00004 seconds
Device: Doorl [Authorized]
Energy Consumed: 13 units
Hash: 2791ad3461f889c6ddf39fac46a6d6f7a2bc1292de183e51184f3f01f746469a
Previous Hash: 15cf47be331997c34af854f15ff1f107406f8235fd9ada300b9e91d60fd6e1c9

Block 5 created in 0.00005 seconds
Device: Door2 [Authorized]
Energy Consumed: 25 units
Hash: 487486978248a6e0685059027224944848fdee94ec9221c9706f90d5b36a963a
Previous Hash: 2791ad3461f889c6ddf39fac46a6d6f7a2bc1292de183e51184f3f01f746469a
```

Figure 6 illustrates how the blockchain responds to both authorized and unauthorized device activities within the smart-home network. Each block records critical parameters, including the device identity, transaction legitimacy, energy consumed, and the cryptographic hash linking it to the previous block. For authorized devices such as the AC, home gateway, and door, the block creation time is extremely low, and the energy consumption remains within a consistent range, reflecting efficient validation and seamless integration into the chain.

5.2. Limitations of the study

Current research work has some weak points that should be kept in mind while interpreting the results. The main and first problem is the number of tests. MITM and RFID cloning had 12 and 6 trials, respectively, but unauthorized access and social engineering were tested only once. The study requires more experiments to rely on the results and to achieve a better conclusion. One more limitation is the lack of performance measurements. It should have more quantitative evaluation methods and records of resource utilization. For future work, it will definitely have parameters such as anomaly detection probability [28], detailed system statistics, and computational cost. For better integrated performance analysis, the collection of these parameters is important. Lastly, there are a few factors one cannot simulate on virtual world such as background noise and environmental inferences. Even human mistakes or behavior may influence the system's outcomes.

6. Conclusion and Future Scope

This work focuses mainly on security issues related to smart-home automation systems. The study proposed a blockchain-based framework, BIoTC, as a solution. The whole system has two major parts: first, the smart-home simulation on Cisco Packet Tracer, and second, blockchain-based Python modules. Four major threats were systematically simulated and observed.

The result shows that IoT environments are highly insecure, with the ASP being around 33–100%. The ASP totally depends on the type of attack. But after introducing blockchain as a possible best solution, the ASP drops to zero. The proposed framework demonstrates a CI of 100% in all tested cases. It shows complete mitigation of the target vulnerability. All these results show that blockchain is the perfect solution for IoT security. Its features such as immutability, transparency, and smart contact play an important role in providing privacy. The solution is equally effective in technical [29] and nontechnical attacks.

The main feature of this paper is its mathematical calculations and their validation. The utilization of concepts such as ASP, BVR, and CI is helping to prove the effectiveness of this framework quantitatively. The visual results show that the blockchain integration provides better security for the system. This approach shows that it is not only conceptually strong but also more effective in real life. The proposed framework has some limitations as well. Few attacks are tested with a small sample, so this will have a reliability issue. Moreover, there is a lack of advanced performance indicators. These issues will be fixed in our future work.

This work is very useful for the future. First, the same solution can be tested with more diverse data for stronger validation of the framework, which will support its real-life implementation. Second, the introduction of smart algorithms, such as isolation forest, can give external support to blockchain for analyzing strange behavior. This framework is currently working only on one area of IoT, but in the future, this idea can do wonders beyond just smart homes.

In conclusion, this research work proposes BIoTC as the best robust, blockchain-driven framework for IoT security. The framework's behavior is observed and validated through systematic simulation of the IoT environment andmathematical analysis. By reducing the attack success rate and its probability, the framework demonstrates its effectiveness and establishes foundation for scalable, trust-enhancing architectures in next-generation IoT deployments.

Acknowledgment

This work was significantly supported by the mentorship of Prof. (Dr.) Sarvesh Tanwar and Prof. (Dr.) Pankaj Kumar Sharma. The authors are grateful for their continuous support, intellectual contributions, and constructive suggestions provided during the research work, which greatly improved the quality of the final manuscript. Their guidance was instrumental in shaping the direction of this research.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Gaurav Vats: Conceptualization, Methodology, Software, Formal analysis, Investigation, Writing – original draft, Visualization. **Sarvesh Tanwar:** Validation, Investigation, Resources, Writing – review & editing, Visualization, Supervision, Project administration. **Pankaj Kumar Sharma:** Resources, Data curation, Supervision.

References

[1] Sengupta, S. (2024). IoT-based flood detection and management systems in urban areas. *Risk Assessment and Management Decisions*, *1*(2), 301–313. https://doi.org/10.48314/ramd.v1i2.53

[2] Vaigandla, K. K. (2025). An extensive examination on IoT and industrial IoT: Attacks, security, detection methods, blockchain solutions and challenges. *Babylonian Journal of Internet of Things*, *2025*, 89–100. https://doi.org/10.58496/BJIoT/2025/004

[3] Amoo, O. O., Osasona, F., Atadoga, A., Ayinla, B. S., Farayola, O. A., & Abrahams, T. O. (2024). Cybersecurity threats in the age of IoT: A review of protective measures. *International Journal of Science and Research Archive*, *11*(1), 1304–1310. https://doi.org/10.30574/ijsra.2024.11.1.0217

[4] Vats, G., & Sharma, P. K. (2023). An exhaustive analysis on security issues concerning IoT using blockchain. In *2023 International Conference on Disruptive Technologies*, 1–7. https://doi.org/10.1109/ICDT57929.2023.10150747

[5] Feng, Y., Huang, W., Wang, S., Zhang, Y., & Jiang, S. (2021). Detection of RFID cloning attacks: A spatiotemporal trajectory data stream-based practical approach. *Computer Networks*, *189*, 107922. https://doi.org/10.1016/j.comnet.2021.107922

[6] Sivasankari, N., & Kamalakkannan, S. (2022). Detection and prevention of man-in-the-middle attack in IoT network using regression modeling. *Advances in Engineering Software*, *169*, 103126. https://doi.org/10.1016/j.advengsoft.2022.103126

[7] Vats, G., Tanwar, S., & Sharma, P. K. (2024). A simulation-based analysis of IoT security architecture in smart homes. In *2024 International Conference on Computing, Sciences and Communications*, 1–4. https://doi.org/10.1109/ICCSC62048.2024.10830301

[8] Ahmed, O. G. (2025). Smart building systems: A confluence of architecture and technology. *KHWARIZMIA*, *2025*, 11–22. https://doi.org/10.70470/KHWARIZMIA/2025/002

[9] Al Barazanchi, I. I., & Hashim, W. (2023). Enhancing IoT device security through blockchain technology: A decentralized approach. *SHIFRA*, *2023*, 10–16. https://doi.org/10.70470/SHIFRA/2023/002

[10] Ashok, K., & Gopikrishnan, S. (2023). Statistical analysis of remote health monitoring-based IoT security models and

deployments from a pragmatic perspective. *IEEE Access*, *11*, 2621–2651. https://doi.org/10.1109/ACCESS.2023.3234632

[11] 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

[12] Selvarajan, S., Shankar, A., Uddin, M., Alqahtani, A. S., Al-Shehari, T., & Viriyasitavat, W. (2025). A smart decentralized identifiable distributed ledger technology-based blockchain (DIDLT-BC) model for cloud-IoT security. *Expert Systems*, *42*(1), e13544. https://doi.org/10.1111/exsy.13544

[13] Almuqren, L., Mahmood, K., Aljameel, S. S., Salama, A. S., Mohammed, G. P., & Alneil, A. A. (2023). Blockchain-assisted secure smart home network using gradient-based optimizer with hybrid deep learning model. *IEEE Access*, *11*, 86999–87008. https://doi.org/10.1109/ACCESS.2023.3303087

[14] Mathur, S., Kalla, A., Gür, G., Bohra, M. K., & Liyanage, M. (2023). A survey on role of blockchain for IoT: Applications and technical aspects. *Computer Networks*, *227*, 109726. https://doi.org/10.1016/j.comnet.2023.109726

[15] Mazhar, T., Khan, S., Shahzad, T., Khan, M. A., Saeed, M. M., Awotunde, J. B., & Hamam, H. (2025). Generative AI, IoT, and blockchain in healthcare: Application, issues, and solutions. *Discover Internet of Things*, *5*(1), 5. https://doi.org/10.1007/s43926-025-00095-8

[16] 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

[17] Wakili, A., & Bakkali, S. (2025). Privacy-preserving security of IoT networks: A comparative analysis of methods and applications. *Cyber Security and Applications*, *3*, 100084. https://doi.org/10.1016/j.csa.2025.100084

[18] Bhatia, M., & Charul, K. M. (2025). IoT security through the scientometric lens: Emerging techniques and research trends. *IEEE Internet of Things Journal*, *12*(16), 32796–32820. https://doi.org/10.1109/JIOT.2025.3585573

[19] Zrelli, I., & Rejeb, A. (2024). A bibliometric analysis of IoT applications in logistics and supply chain management. *Heliyon*, *10*(16), e36578. https://doi.org/10.1016/j.heliyon.2024.e36578

[20] Cisco Networking Academy. (2025). *Cisco Packet Tracer*. (Version 8.2.1, Build 103) [Computer software]. Cisco NetAcad https://www.netacad.com/cisco-packet-tracer

[21] Addula, S. R., & Ali, A. (2025). A novel permissioned blockchain approach for scalable and privacy-preserving IoT authentication. *Journal of Cyber Security and Risk Auditing*, *2025*(4), 222–237. https://doi.org/10.63180/jcsra.thestap.2025.4.3

[22] Shanshool, A. M. (2023). Exploring the role of blockchain in IoT-driven healthcare solutions. *Babylonian Journal of Networking*, *2023*, 82–88. https://doi.org/10.58496/BJN/2023/010

[23] Manolache, M. A., Manolache, S., & Tapus, N. (2022). Decision making using the blockchain proof of authority consensus. *Procedia Computer Science*, *199*, 580–588. https://doi.org/10.1016/j.procs.2022.01.071

[24] Aijaz, M., & Nazir, M. (2024). Modelling and analysis of social engineering threats using the attack tree and the Markov model. *International Journal of Information Technology*, *16*(2), 1231–1238. https://doi.org/10.1007/s41870-023-01540-z

[25] Gopalrao, K. B., Baban, A. B., & Ashok, D. R. (2023). Use of probability in statistics: A study. *International Journal of Advanced Research in Science, Communication and Technology*, *3*(1), 257–261. https://doi.org/10.48175/IJARSCT-12441

[26] Montgomery, D. C., & Runger, G. C. (2014). *Applied statistics and probability for engineers* (6th ed.). USA: Wiley.

[27] Berberyan, T., Nguyen, T., & Swan, A. (2025). *4.1: Empirical probability*. LibreTexts Statistics. Retrieved from: https://stats.libretexts.org/Courses/Citrus_College/Statistics_C1000%3A_Introduction_to_Statistics/04%3A_Probability_and_Combinatorics/4.01%3A_Empirical_Probability

[28] Entezami, A., Sarmadi, H., Behkamal, B., & Mariani, S. (2025). Early warning of structural damage via manifold learning-aided data clustering and non-parametric probabilistic anomaly detection. *Mechanical Systems and Signal Processing*, *224*, 111984. https://doi.org/10.1016/j.ymssp.2024.111984

[29] Singha, R. (2024). IoT-based disaster detection and response in urban areas. *Risk Assessment and Management Decisions*, *1*(2), 252–259. https://doi.org/10.48314/ramd.v1i2.49

How to Cite: Vats, G., Tanwar, S., & Sharma, P. K. (2026). Performance Analysis of Block–Internet of Things–Chain (BIoTC) Framework for Smart Home. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewJCCE62027670