Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 3, pp. 1950–1962, DOI 10.12694/scpe.v25i3.2686

BLOCKFOG: A BLOCKCHAIN-BASED FRAMEWORK FOR INTRUSION DEFENSE IN IOT FOG COMPUTING

VG PRASUNA,[*] B. RAVINDRA BABU,[†] AND BHASHA PYDALA[‡]

Abstract. In the rapidly evolving domain of the Internet of Things (IoT) and fog computing, maintaining security, scalability, and efficient operation poses significant challenges. Addressing these issues, this study introduces "BlockFog," a novel blockchain-based framework designed to bolster intrusion defense in IoT fog computing environments. The core objective of BlockFog is to counteract the vulnerabilities inherent in decentralized IoT ecosystems by leveraging blockchain technology for enhanced security and transparency. The framework's innovative design integrates crucial components such as Device Onboarding & Identity Management, Data Integrity & Logging, Smart Contract-Driven Intrusion Detection, Automated Blockchain Responses, Secure Peer-to-Peer Communication, and a Lightweight Consensus Mechanism. These elements work collectively to ensure the security and functionality of IoT devices within the fog computing paradigm. BlockFog stands out for its meticulous approach to handling high transaction volumes with off-chain computations and layer-2 solutions, ensuring data integrity and facilitating seamless audit processes. The framework's resilience is further demonstrated through its robust response to evolving cyber threats, incorporating Over-the-Air (OTA) updates and advanced data protection mechanisms like zero-knowledge proofs. A comparative analysis highlights BlockFog's superior performance against existing models. The results reveal BlockFog's lower latency rates in normal, high traffic, and attack scenarios, its higher throughput efficiency, and its more effective resource utilization in terms of CPU, memory, and bandwidth usage. Moreover, BlockFog exhibits an enhanced ability to detect and respond to malicious activities, including DDoS attacks, with significantly higher accuracy than its counterparts. These findings underscore BlockFog's potential in redefining security and operational paradigms in IoT fog computing, making it a robust, agile, and transparent framework suitable for the current digital landscape.

Key words: BlockFog, Internet of Things, blockchain, fog computing, Hybridchain-IDS .

1. Introduction.

In the digital age, transformative technologies are redefining possibilities. The Internet of Things (IoT), which imagines a world where every object, from the commonplace to the crucial, is connected and interactive, is driving this technological renaissance. The vastness of IoT is complemented by fog computing, which decentralizes data processing closer to data sources. Theirs is the basis for smarter homes, cities, and industries [1]. There are problems with efficiency, scalability, and security in this digital paradise. Particularly in decentralized systems, existing IoT frameworks struggle to strike a balance between security, scalability, and efficiency [2]. These systems are susceptible to device manipulation and data breaches. How do we keep the connected future of IoT from turning into a cybersecurity nightmare?

This paper introduces a comprehensive framework that tackles the aforementioned problems and establishes a new benchmark for IoT fog computing solutions in response to this conundrum. We created and developed "BlockFog," an intrusion defense framework for Internet of Things fog computing that is based on blockchain. BlockFog integrates blockchain technology, which is renowned for its security and transparency, to provide an IoT fog computing solution that is safe, scalable, and efficient.

Some new features of the BlockFog model are as follows. Every element, from smart contract-driven intrusion detection to cryptographic device onboarding, is thoughtfully designed to address challenges within the IoT ecosystem. BlockFog's importance is justified for two reasons. By utilizing blockchain technology, it introduces an unchangeable, transparent, decentralized ledger system that guarantees data integrity and trust. Second, its scalable architecture effectively manages the enormous volumes of transactions generated by IoT.

[*] Professor, Department of CSE, Satya Institute of Technology and Management, Vizianagaram, Andhra Pradesh (Corresponding author, prasunavg@gmail.com)

[†] Faculty of ICT Department, FDRE TVTI, Addis Ababa, Ethiopia (ravindrababu4u@yahoo.com).

[‡] Assistant Professor, Department of Data Science, Mohan Babu University (Erstwhile Sree Vidyanikethan Engineering College), Tirupati-517 102,A.P. India (basha.chanti@gmail.com).

Innovative blockchain applications and cryptographic principles were used in the development of BlockFog. These techniques were selected following a careful examination of blockchain and IoT best practices and trends. The integration with the BlockFog framework demonstrates our commitment to a reliable, long-lasting solution.

Following this introduction, related research covers the review of contemporary literature. Further section 2 go over the architecture and significance of BlockFog. A comprehensive experimental study in section 3 contrasts the performance of BlockFog with contemporary models. Further, section 4 concludes the study's findings.

In today's digital world, device communication and data sharing have been transformed by the Internet of Things (IoT). But in order to make these massive networks resistant to changing cyber threats, it is necessary to address the inherent security vulnerabilities of IoT as it expands. Modern research on blockchain's contribution to the revolution in IoT security is reviewed in this review. The in-depth analysis of 25 foundational works will show how researchers and technologists are reinforcing IoT system defenses with the help of blockchain's decentralized ledger and sophisticated cryptography techniques.

Mathew et al. [3] explored the merger of blockchain and collaborative intrusion detection for secure data transactions in industrial IoT. They pinpointed the challenges of multi-layered networks with varied protocol standards, suggesting the integration of collaborative IDS and blockchain as a promising solution. Babu et al. [4] emphasized on safeguarding urban IoT data against DDoS attacks using a permissioned blockchain, introducing the arbiter PUF model for IoT device security.

Li, Wenjuan, Yu Wang et al. [5] presented a blockchain-based filtration mechanism integrated with a collaborative intrusion detection network for IoT security. Their focus was on curbing attacks like DDoS and ensuring efficient traffic management using blockchain and IPFS. Saravanan, V., M. Madiajagan et al. [6] brought forward a Blockchain-based African Buffalo scheme integrated with a Recurrent Neural Network model to enhance cloud-based intrusion detection.

Abou El Houda et al. [7] introduced FedIoT, combining Explainable AI techniques and blockchain to secure Federated Learning-based Intrusion Detection Systems in IoT. Douiba, Maryam et al. [8] addressed security in the healthcare industry, emphasizing the significance of Internet of Health Things. Their solution was a collaborative fog-based intrusion detection system bolstered by blockchain and machine learning.

Siddamsetti, Swapna et al. [9] highlighted a machine blockchain framework for distributed intrusion detection in IoT networks, emphasizing the importance of smart contracts. Meanwhile, Aburas et al. [10] underscored the need for green IoT, discussing how blockchain can bolster its security. Osama Alkadi et al. [11] focused on shared cloud infrastructure and IoT security, presenting a deep blockchain framework.

Hafsa Benaddi et al. [12] emphasized the need for sophisticated IoT intrusion detection systems that can adapt to new attack types, with blockchain integration seen as a potential solution. M. Praveen Kumar et al. [13] highlighted IoT vulnerabilities, proposing blockchain-based solutions with Zero-Knowledge proof techniques for added data protection. Rajesh Kumar Sharma et al. [14] discussed the dangers of malicious attacks in IoT networks and how blockchain can be leveraged for better protection.

Omkar Shende et al. [15] introduced the Collaborative Ensemble Blockchain Model for effective IoT intrusion traffic analysis, employing an ensemble of machine learning models. Eman Ashraf et al. [16] proposed FIDChain, which combines lightweight artificial neural networks and blockchain for healthcare IoT security.

Randhir Kumar et al. [17] put forth a fog computing solution to detect DDoS attacks in blockchain-enabled IoT networks, achieving efficient detection compared to traditional methods. Mohanad Sarhan et al. [18] proposed a hierarchical blockchain-based federated learning framework for IoT intrusion detection, ensuring enhanced security while maintaining data integrity.

Rezvan MAHMOUDIE et al. [19] highlighted the security challenges of decentralized IoT devices, introducing a private blockchain model for IoT intrusion detection that optimizes scalability and minimizes overhead. Salaheddine Kably et al. [20] highlighted the integration of blockchain technology with intrusion detection systems to protect IoT nodes.

Mamunur et al. [21] explored the concept of Federated Learning for IoT security and how it can be boosted using blockchain technology. Jawad Hassan et al. [22] provided a comprehensive overview of blockchain-based intrusion detection for IoT, emphasizing blockchain's potential to redefine IoT security.

Reda Salama et al. [23] proposed the BXAI-IDCUCS model, integrating blockchain with Explainable Artificial Intelligence for IoT security. AHMED A. M. SHARADQH et al. [24] emphasized HybridChain-IDS, a model that combines blockchain, trusted execution environments, and machine learning for advanced IoT network security.

Hayam Alamro et al. [25] put forward FIDANN, a Federated Artificial Intelligence System of Intrusion Detection for IoT Healthcare System using blockchain. The model leverages machine learning, blockchain technology, and edge computing for efficient intrusion detection. Finally, Priyanka Tyagi et al. [26] addressed the security concerns of IoT-based healthcare systems, proposing FIDANN to enhance intrusion detection mechanisms.

The Internet of Things (IoT) has quickly become known as a challenging field with enormous potential. But there are a lot of security problems as a result of this quick growth. These vulnerabilities are brought to light and the necessity for strong, decentralized, and scalable security solutions is emphasized by recent studies, such as Mathew et al. [3] and Salaheddine Kably et al. [20]. The scholarly contributions underscore the potential of blockchain technology to fortify Internet of Things networks. The decentralized ledger of blockchain is well-known. Every device touchpoint has transparent logging and authentication. Research suggests integrating blockchain to safeguard IoT networks from various cyber threats in light of these advantages.

Industrial IoT was thoroughly examined by Mathew et al. [3]. The need for improved security in intricate, multi-layered networks is highlighted by their research. Network defenses could be completely transformed by fusing blockchain technology with Collaborative Intrusion Detection Systems (CIDS). The threat posed by DDoS attacks on IoT networks is highlighted by parallel research conducted by Babu et al. [4] and Li et al. [5]. Their research shows how successful collaborative detection systems are at stopping these kinds of crimes, particularly when paired with the robust security of blockchain technology. The advantages of blockchain and machine learning algorithms for security are emphasized by Saravanan et al. [6] and Siddamsetti et al. [9]. They claim that harmonizing these can increase the effectiveness and precision of IoT intrusion detection. Aburas et al. [10] and Douiba et al. [8] have pushed blockchain-based solutions for green IoT and healthcare. Their arguments focus on these areas' particular vulnerabilities and the requirement for tailored, efficient security solutions.

The need for BlockFog is highlighted by this research. BlockFog gives hope as blockchain-integrated Internet of Things solutions are discussed. It stands out for its distinct take on blockchain in IoT fog computing and Smart Contract-Driven Intrusion Detection. Its Device Onboarding & Identity Management feature further strengthens its position as the industry leader in IoT security solutions. BlockFog is contrasted with other models, specifically AHMED A. M. SHARADQH [24] and Salaheddine Kably et al. [20]. The performance and potential of BlockFog in IoT security have been evaluated with the aid of these and other references. BlockFog's superiority and innovation in IoT security are highlighted by the contrast between its architecture and empirical performance when compared to these models.

2. Methods and Materials. Navigating the intricate crossroads of the burgeoning realms of the Internet of Things (IoT) and fog computing, it becomes clear that a delicate balance between security, scalability, and streamlined operation is paramount. Enter "BlockFog," a framework birthed precisely at this juncture. It melds blockchain technology seamlessly into the heart of IoT fog computing, marking a significant stride in countering both existing and anticipated challenges of decentralized IoT ecosystems. By strengthening the very peripherals of our digital infrastructures, BlockFog heralds an era of robust, transparent, and agile frameworks for a new wave of interconnected devices. In response to the vastness of the IoT universe, BlockFog is meticulously designed for scale and agility. By harnessing off-chain computations and leveraging layer-2 solutions, it manages to process high transaction volumes with finesse. True to its commitment to transparency, every step—from a device's initial registration to its critical alerts—is intricately logged onto the blockchain. This approach not only fosters trust but also streamlines audit processes. Moreover, as the cyber threat landscape constantly evolves, BlockFog remains ahead, offering timely security enhancements via Over-the-Air (OTA) updates [27]. While the framework's transparency is evident, it is equally dedicated to safeguarding sensitive data, implementing sophisticated mechanisms like zero-knowledge proofs to ensure certain transaction specifics remain confidential. The "BlockFog Framework," its components, and how they relate to IoT devices and the blockchain are depicted in the figure 2.1. Security and functionality are guaranteed by the "Device Onboarding & Identity Management,"[28], "Data Integrity & Logging," [29] and "Smart Contract-Driven Intrusion Detection" modules of the BlockFog framework. Through the framework, IoT devices register, transmit data, and are

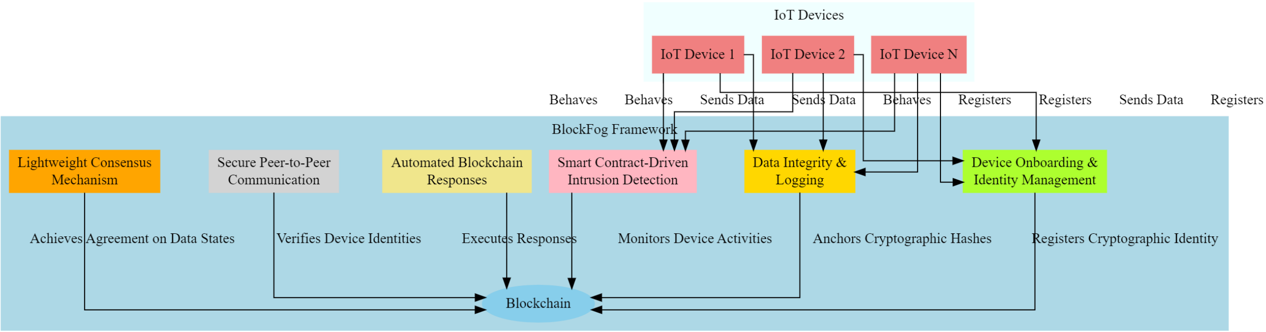
IoT Devices
IoT Device 1
IoT Device 2
IoT Device N
Behaves
Behaves
Sends Data
Sends Data
Behaves
Registers
Registers
Sends Data
Registers
BlockFog Framework
Lightweight Consensus Mechanism
Secure Peer-to-Peer Communication
Automated Blockchain Responses
Smart Contract-Driven Intrusion Detection
Data Integrity & Logging
Device Onboarding & Identity Management
Achieves Agreement on Data States
Verifies Device Identities
Executes Responses
Monitors Device Activities
Anchors Cryptographic Hashes
Registers Cryptographic Identity
Blockchain

Fig. 2.1: Architecture diagram of the BlockFog

watched over. In order to register device identities, store data hashes, and verify blockchain contracts, these components communicate with a centralized blockchain database. The diagram demonstrates the robustness and complexity of the framework by clearly illustrating the interaction between IoT devices, BlockFog components, and the blockchain.

Diving deeper into BlockFog's architectural design, it's evident that a series of core components work in harmony to fortify IoT fog computing. Central to its framework is the Device Onboarding & Identity Management system, bestowing upon each device a unique and verifiable cryptographic identity registered on the blockchain. This core strength is further amplified by the Data Integrity & Logging mechanism, ensuring every piece of data is securely anchored. Proactive security measures, such as the Smart Contract-Driven Intrusion Detection, continuously monitor and rectify anomalous behaviors. Alongside, Automated Blockchain Responses tackle emerging threats, and protocols like Secure Peer-to-Peer Communication [30] and the Lightweight Consensus Mechanism [31] enrich the framework, ensuring both security and efficient functionality tailored to IoT's unique demands. Detailed description of each of these core components is presented in following.

2.1. Device Onboarding & Identity Management. In the BlockFog ecosystem, each IoT device is uniquely identified using a cryptographic digital identity registered on the blockchain. This two-pronged identity system utilizes a public key as the device's ID, while its private counterpart facilitates secure data authentication and signing. This meticulous onboarding ensures not only device authenticity but also establishes a secure foundation for all subsequent interactions. The mathematical model of this component follows.

Notation:

G**:** Generator point of the elliptic curve.
n**:** Order of the elliptic curve.
d**:** Device's private key.
Q**:** Device's public key (corresponding to private key d).
k**:** Random nonce used during signing.
CA_d**:** CA's private key.
CA_Q**:** CA's public key.
$H(\cdot)$**:** Cryptographic hash function.

Preliminary Setup:

a. Curve Selection: Choose an elliptic curve over a finite field, e.g., one of the NIST recommended curves.

Device Onboarding:

a. Key Generation: Randomly select an integer d from $[1, n-1]$ and then compute $Q = d \times G$.

b. Device Registration (device → RA/CA): Send device's public key Q and metadata M (like device type, model) to RA or CA.

Device Identity Verification & Certificate Issuance (RA/CA):

a. Verification: Verify device's metadata M through whatever means necessary (manual, automated checks, database cross-reference).

b. Certificate Creation: Form a certificate information CI comprising Q, M, expiration date E, and other relevant data. And then Compute the hash of the certificate information: $h = H(CI)$.

c. Certificate Signing using ECDSA: Randomly choose a nonce k from $[1, n-1]$, calculate point $R = k \times G$ and let r be the x-coordinate of R mod n, compute $s = k^{-1}(h + r \times CA_d) \mod n$. The signature (r, s) is the CA's signature on the certificate information.

d. Certificate Issuance: Send the signed certificate $(CI, (r, s))$ back to the device.

Secure Authentication:

a. Device presents certificate: When authenticating, the device presents its certificate $(CI, (r, s))$ to another entity.

b. Certificate Verification:

- Extract CI from the certificate and compute $h = H(CI)$.
- Calculate $w = s^{-1} \mod n$.
- Compute $u_1 = h \times w \mod n$ and $u_2 = r \times w \mod n$.
- Calculate point $R' = u_1 \times G + u_2 \times Q$.
- The certificate is valid if the x-coordinate of R' is congruent to r mod n.

2.2. Data Integrity & Logging. Data is the lifeblood of IoT, and BlockFog ensures its sanctity. While devices produce vast data streams, the framework accentuates data integrity by endorsing every piece of data with a device-specific private key signature. To strike a balance between storage efficiency and tamper resistance, cryptographic hashes of this data are periodically anchored to the blockchain, certifying its originality. The mathematical model of this component follows.

Notation:

D_i**:** Data block/item i from an IoT device.
$H(\cdot)$**:** Cryptographic hash function.
d**:** Device's private key.
M**:** Merkle tree.
MR**:** Root of the Merkle tree.
k**:** Random nonce used during signing for ECDSA.

Data Collection: Gather a set of data items from the IoT device, $\{D_1, D_2, \ldots, D_n\}$.

Data Integrity using Merkle Trees [32]:

a. Leaf Node Creation: For each data item D_i: Compute its hash: $h_i = H(D_i)$.

b. Merkle Tree Construction:

- Start with n leaf nodes, each holding one h_i.
- Group the hashes in pairs and compute the hash for each pair: $h_{ij} = H(h_i \| h_j)$, where $\|$ denotes concatenation.
- Repeat the process layer by layer, using the newly computed hashes, until reaching a single hash value, the Merkle root MR.

Data Signing using ECDSA for Logging:

a. Generate Signature on Merkle Root:

- Compute the hash of the Merkle root: $h = H(MR)$.
- Randomly choose a nonce k from $[1, n-1]$, where n is the order of the elliptic curve.
- Calculate point $R = k \times G$ and let r be the x-coordinate of R mod n.
- Compute $s = k^{-1}(h + r \times d) \mod n$.
- The signature (r, s) becomes the device's authentication of the data integrity.
- *Logging Data and Signature:* Store the Merkle root MR and the signature (r, s) in the log or on the blockchain.

Optionally, depending on storage and needs, store the entire Merkle tree M to allow for granular verification later.

Data Verification:

a. *Retrieve Data and Merkle Path:* To verify a specific data item D_i, retrieve the D_i, the data item itself and the path in the Merkle tree leading to D_i, which consists of a subset of hashes from M.

b. *Recompute Merkle Root:* Start with $h_i = H(D_i)$ and traverse the Merkle path, recomputing parent hashes using the retrieved hashes and the computed hashes from the previous step. If the computed Merkle root matches the stored MR, data integrity for D_i is verified.

c. *Verify Signature:* Using the device's public key, verify the ECDSA signature (r, s) on MR to ensure the data's authenticity.

2.3. Smart Contract-Driven Intrusion Detection. BlockFog's security acumen is exemplified by its integration of smart contracts. These autonomous blockchain programs are vigilantly on the lookout for any device behavior anomalies. By juxtaposing device activity with predefined intrusion patterns, these smart contracts serve as the ecosystem's ever-watchful sentinels, ready to identify and react to threats. The mathematical model of this component follows.

Notation:

T**:** Transaction or interaction with an IoT device.
P**:** Profile or behavior pattern of an IoT device under normal operation.
$H(\cdot)$**:** Cryptographic hash function.
SC**:** Smart Contract.

Profile Learning Phase:

a. *Data Collection & Profiling:* Monitor IoT devices' activities for a specific duration to understand their normal behaviors. Then aggregate these behaviors into a profile P that represents the device's typical operations.

b. *Profile Commitment:* Compute $h_P = H(P)$ and then deploy a smart contract SC or use an existing one and store h_P within SC. This hash represents the device's normal behavioral fingerprint.

Transaction Monitoring:

a. *Monitor Device Transactions* For every transaction T (interaction or data transmission) involving an IoT device:
   - Compute $h_T = H(T)$.
   - Send h_T to SC for validation.

Smart Contract-Driven Intrusion Detection:

- *Transaction Validation (within SC):* Compare the received h_T with the stored profile hash h_P and other historical transaction hashes to identify potential anomalies or deviations.
- *Pattern Analysis & Anomaly Detection (within SC):* Use pre-defined logic in the smart contract to detect potential intrusions based on deviations from P or other known safe patterns.
- *Alerts & Responses:* If an anomaly is detected, the smart contract can trigger specific actions:
  - Emit an alert event that stakeholders can listen to.
  - If integrated with other systems, initiate a response like isolating the IoT device, notifying administrators, or updating a threat database.

Continuous Learning:

a. *Update Profile Periodically:* Over time, the behavior of IoT devices may change due to software updates, changed usage patterns, etc. Periodically or under specific conditions, the profile P can be recalculated and the hash h_p updated in the smart contract.

b. *Community Feedback (for a network of IoT devices):* Allow other IoT devices or nodes in the network to provide feedback on detected anomalies. If multiple nodes report similar deviations, the smart contract might adjust its parameters or update the reference profile, enhancing the detection mechanism's accuracy and reducing false positives.

2.4. Automated Blockchain Responses. Proactive defense is a hallmark of BlockFog. Upon detecting a security breach or anomaly, the framework's smart contracts swing into action. The range of these automated responses varies, from issuing alerts to network administrators to initiating protocols that restrict or revoke access for compromised devices, ensuring real-time defense against potential threats. The mathematical model of this component follows.

Notation:

A**:** Detected anomaly or breach.
SC**:** Smart Contract.
R**:** Blockchain-driven response action.
N**:** Network nodes or IoT devices.
V**:** Validation criteria or thresholds for triggering a response.
S**:** State of an IoT device or network node.
T**:** Transaction triggering the response.

Anomaly Detection:

a. *Monitor for Anomalies:* Watch for emitted events or logs from the Intrusion Detection Smart Contract (or equivalent). Capture detected anomaly A and associated data, e.g., IoT device ID, type of anomaly, timestamp, etc.

Automated Blockchain Response Smart Contract (BRSC) Initialization:

a. *Define Response Logic:* Codify in SC the logic that dictates what responses R are appropriate for each type of detected anomaly A.

b. *Set Validation Criteria:* Define V, thresholds or conditions under which SC will trigger a response. This could include consensus mechanisms, anomaly severity levels, etc.

Anomaly Validation & Response Determination:

a. *Analyze Anomaly Data (within SC):* Compare the detected anomaly A against the defined criteria V to determine the validity and severity of the anomaly.

b. *Determine Appropriate Response:* Based on the anomaly data and validation, use the predefined logic in SC to choose an appropriate response R.

Execute Blockchain Response:

a. *Transaction Creation:* Formulate a transaction T that triggers the desired response R and pushes it to the blockchain.

b. *Transaction Verification & Execution (by network nodes N):* Nodes N in the blockchain network will validate and execute T. Once the transaction is verified and added to the blockchain, the prescribed action R is executed, e.g., isolating a compromised IoT device, notifying administrators, etc.

State Update & Logging:

a. *Update State:* After executing R, update the state S of the associated IoT device or network node on the blockchain to reflect the new condition.

b. *Logging:* Record details of the anomaly A, the response R, and any subsequent state changes S in the blockchain. This ensures a transparent and tamper-proof record of all events and actions.

Continuous Feedback & Learning:

a. *Feedback Loop:* Allow nodes N or other stakeholders to provide feedback on the executed responses. Then, gather insights and adjust the logic in SC as necessary to optimize response mechanisms.

Periodic Review: Periodically review logged anomalies and responses to refine the response mechanisms and reduce false positives or unnecessary actions.

2.5. Secure Peer-to-Peer Communication. Within BlockFog, the sanctity of communication channels is paramount. End-to-end encryption safeguards all device interactions, ensuring data integrity and confidentiality. The framework's inherent design permits only devices with blockchain-verified identities to engage in exchanges, ensuring both data security and device authenticity. The mathematical model of this component follows.

Notation:

M**:** Message to be sent.
$E(\cdot)$**:** Encryption function.
$D(\cdot)$**:** Decryption function.
$S(\cdot)$**:** Digital signature function.
$V(\cdot)$**:** Signature verification function.

$K_{\mathbf{pub}}$**:** Public key.
$K_{\mathbf{priv}}$**:** Private key.
$K_{\mathbf{sym}}$**:** Symmetric key.
ID**:** Device or node identifier.
$H(\cdot)$**:** Cryptographic hash function.
R**:** Random nonce or value for key agreement or challenge.

Key Establishment for Secure Communication:

a. *Retrieve Peer Public Key:* Query the blockchain for the public key K_{pub} associated with the peer's ID. This ensures the authenticity of the retrieved key.

b. *Key Agreement (e.g., Diffie-Hellman):* Generate a temporary key pair and compute the shared secret. Then derive K_{sym} from the shared secret for symmetric encryption during the session.

Message Encryption & Signature:

a. *Message Encryption:* Encrypt the message M using the derived symmetric key K_{sym}: $C = E_{K_{\text{sym}}}(M)$.

b. *Message Signing:* Generate a hash of the message: $h_M = H(M)$ and Sign the hash using the sender's private key K_{priv}: $S_{K_{\text{priv}}}(h_M)$.

Message Transmission:

a. *Package for Sending:* Package the encrypted message C and the signature together.

b. *Send Package:* Use the P2P protocol to send the package to the intended recipient.

Message Reception & Verification:

a. *Decrypt Message:* On receiving the package, decrypt C using K_{sym} to retrieve the original message M.

b. *Signature Verification:* Compute $h_M = H(M)$. Use the sender's K_{pub} retrieved from the blockchain to verify the signature: $V_{K_{\text{pub}}}(h_M)$. If valid, the message is authentic and hasn't been tampered with.

Challenge-Response for Continuous Authentication:

a. *Challenge Creation:* A device can send a random challenge R to its peer.

b. *Response Generation:* The receiving peer computes $h_R = H(R||K_{\text{sym}})$ and sends it back.

c. *Verification:* The initiating device verifies the response by comparing it with its own computation. If they match, the peer's presence and the session's security are reaffirmed.

Session Termination & Key Disposal:

a. *End Session:* Once communication is completed, or after a pre-defined time, the session is terminated.

b. *Key Disposal:* For security, discard or overwrite K_{sym} to prevent its reuse or compromise.

2.6. Lightweight Consensus Mechanism [31]. Understanding that IoT devices often grapple with resource constraints, BlockFog employs a lightweight consensus mechanism. This judicious choice guarantees that devices reach agreement on data states without being bogged down by computationally intensive tasks, striking a balance between security and efficiency. The mathematical model of this component follows.

In the enhanced BlockFog process shown in figure 2.2, each stage of the workflow is vividly represented with distinct colors to improve clarity and visual differentiation. The process begins at the 'Start' node, colored green for initiation, and flows into 'Device Registration', shaded light blue, indicating a decision point where the path diverges based on whether a new device is registering. Positive paths, such as successful registration or anomaly detection, are marked in blue, while negative outcomes, like the absence of a new device, are highlighted in red and lead to the process's termination at the grey-colored 'End' node. The 'Device Validation' stage is in yellow, transitioning into 'Data Transmission' in orange, followed by a 'Data Integrity Check' in light green. The critical decision point, 'Anomaly Detection', is pink, leading either to 'Alert Generation' in red for detected anomalies or looping back in green to 'Data Transmission' for continuous operation. The process is designed for iterative monitoring, as indicated by the dashed purple line looping back from 'End' to 'Device Registration', underscoring the framework's ongoing vigilance.

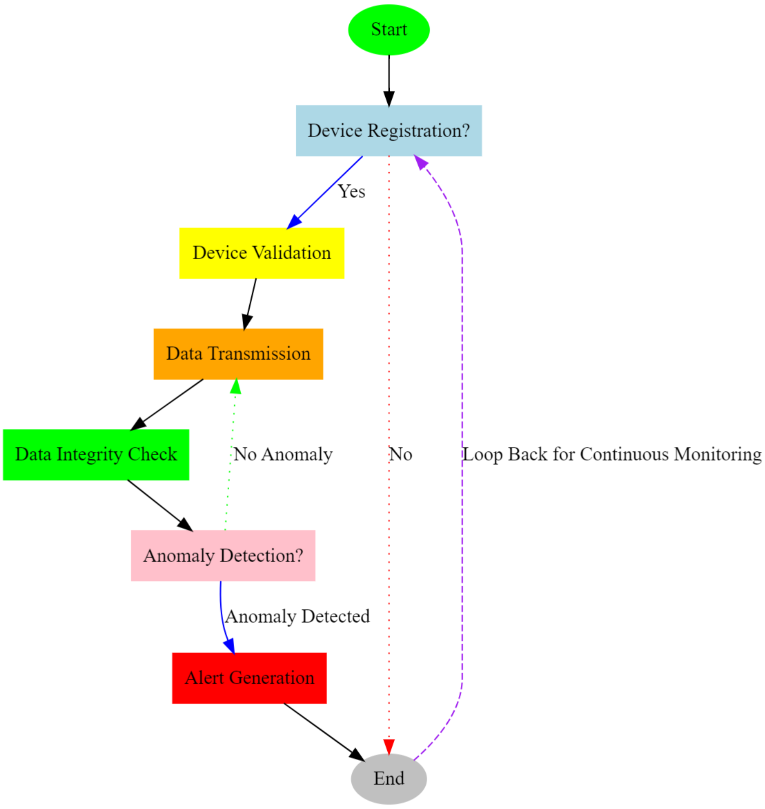

Fig. 2.2: The flowdiagram representation of the RF-RFE

3. Experimental Study. In a meticulously designed study, the performance of the BlockFog framework was evaluated using a simulated network environment comprising varied IoT and fog devices, realized through the fogsim [33] and blocksim [34] simulators, with Python serving as the foundational programming language. The assessment was amplified by introducing different traffic patterns, encapsulating both regular transmissions and deliberate malicious activities. Performance metrics were concentrated on four pillars: transaction latency within the blockchain, throughput capabilities, resource consumption metrics including CPU, memory, and bandwidth, and the framework's proficiency in detecting security threats.

To ensure a well-rounded evaluation, the study embraced several testing scenarios. The baseline performance was first analyzed under standard operations, followed by probing the system's resilience during high traffic loads. The real challenge emerged when BlockFog was subjected to various cyber threats, such as DDoS and Sybil attacks, to gauge its defensive mechanisms. Additionally, by simulating network failures and disconnections, the robustness and reliability of BlockFog were put to the test. Concluding the study, a comparative lens was employed as BlockFog's performance was juxtaposed against two contemporary models, Hybridchain-IDS [24] and MZWB [20], highlighting its potential strengths and areas of refinement in the vast realm of IoT fog computing.

3.1. Comparative Analysis. This section contrasts the performance metrics of BlockFog, Hybridchain-IDS, and MZWB, shedding light on their significant metrics. The latency and security capabilities of these systems are summarized in the following figures and narratives. With every metric, BlockFog's resilience and effectiveness in IoT fog computing are demonstrated. This section highlights the architecture and performance of BlockFog and highlights data-driven evaluations.

BlockFog's processing efficiency with latency data can be found in figure 3.1. In the Normal, High Traffic,

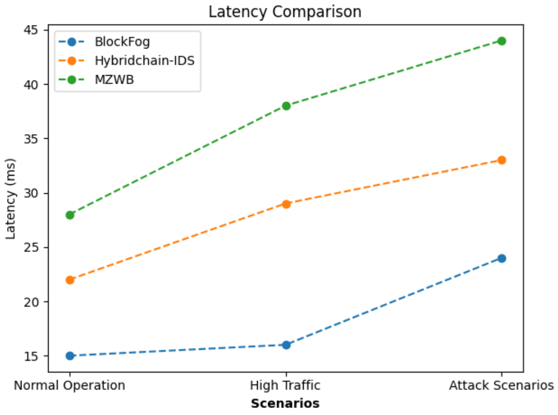

Fig. 3.1: Comparative analysis of Latency observed for BlockFog, Hybridchain-IDS, and MZWB

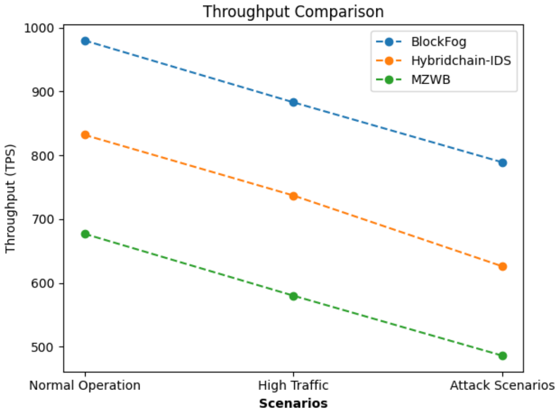

Fig. 3.2: Comparative analysis of throughput observed for BlockFog, Hybridchain-IDS, and MZWB

and Attack scenarios, BlockFog had the lowest values (15 ms, 16 ms, and 24 ms). In normal operations, BlockFog performed better than Hybridchain-IDS by 31.8% and MZWB by 46.4%. The pattern continues in attack scenarios and high traffic areas. The notable difference in latency demonstrates how BlockFog optimizes both transaction propagation and validation.

Transactional volume handling capability of a system is measured by throughput. According to figure 3.2, In normal conditions, BlockFog processed 980 TPS, 17.7% and 44.8% faster than Hybridchain-IDS and MZWB, demonstrating superior performance. Attacks and heavy traffic did not deter BlockFog from leading. This suggests both superior hardware capability and effective network protocols and algorithms that avoid bottlenecks and guarantee steady data flow.

Ensuring sustainability requires effective resource use. As shown in figure 3.3, during normal operations, BlockFog consumed 11.5% and 17.7% less CPU than Hybridchain-IDS and MZWB, respectively. high traffic with a consistent pattern. BlockFog utilized 21.2% less memory than MZWB in situations with high traffic. During normal operations, BlockFog has superior bandwidth, but during system traffic, the systems converge. The information suggests that BlockFog's resource efficiency is high, ensuring less wear and a longer device lifespan.

The ability of a system to identify malicious activity is critical due to digital threats. As presented in figure

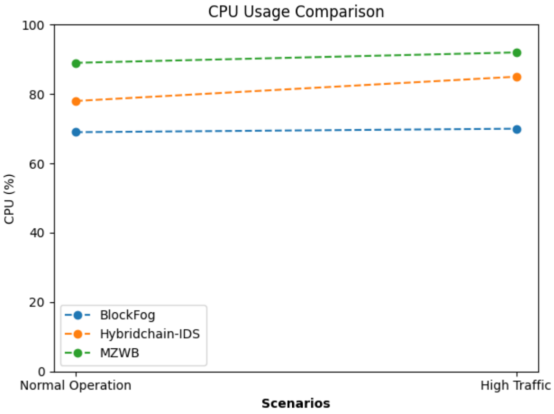

Fig. 3.3: Comparative analysis of resource utilization observed for BlockFog, Hybridchain-IDS, and MZWB

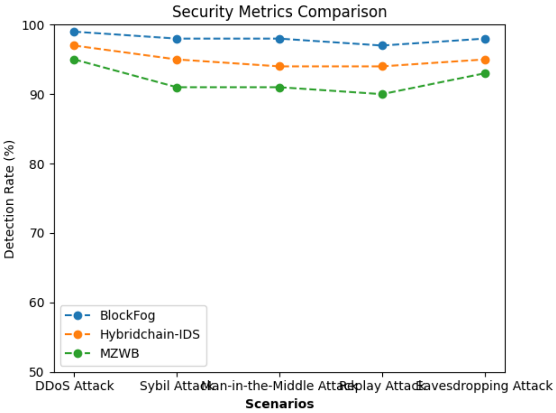

Fig. 3.4: Comparative analysis of Attack Detection Accuracy observed for BlockFog, Hybridchain-IDS, and MZWB

3.4, BlockFog detects DDoS attacks at a rate of 99%, which is 2% higher than Hybridchain-IDS and 4% higher than MZWB. Compared to Hybridchain-IDS and MZWB, BlockFog identified threats 3.6% and 7.4% better, respectively. BlockFog's extensive security protocols are reinforced by threat intelligence and updates.

The statistics demonstrate how well BlockFog performs across the board. BlockFog is a formidable IoT fog computing competitor thanks to its quick transaction processing, effective resource usage, and robust security measures.

4. Conclusion. The Internet of Things (IoT) and fog computing have made it possible for devices to connect to each other, which has created new opportunities and challenges. We require strong, scalable, and effective frameworks as we use these technologies more frequently. This paper presented ”BlockFog” as an innovation and examined IoT fog computing. BlockFog has raised the bar for decentralized IoT ecosystems with its clever use of blockchain technology. The discussion demonstrated how the specifics of BlockFog's architecture, such as the use of smart contracts for intrusion detection and the onboarding of cryptographic devices, made the system stronger against both new and existing threats. The ability of blockchain to handle high transaction volumes without compromising speed, data integrity, or transparency showed the technology's potential to redefine the security and operational paradigms of IoT. A comparative study revealed BlockFog's advantages.

In every case, BlockFog performed better than MZWB and Hybridchain-IDS. BlockFog's leadership can be attributed to its transaction processing agility, resource efficiency, and resolute posture against cyber threats, all of which demonstrate their preparedness for practical implementations. The rapidly evolving field of IoT fog computing presents numerous opportunities for future research to advance and adjust to due to BlockFog. Its integration with new technologies such as edge computing, 5G, and artificial intelligence (AI) is a key priority to boost its performance and applicability across multiple sectors. The increasing number of IoT devices may require refining consensus mechanisms and off-chain calculations, so scalability and efficiency must be optimized.

REFERENCES

[1] Y. A. Thakare, P. P. Deshmukh, R. A. Meshram, K. R. Hole, R. A. Gulhane, and N. A. Deshmukh, "A review: The Internet of Things using fog computing," *International Research Journal of Engineering and Technology*, vol. 4, no. 3, pp. 711-715, 2017.

[2] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors*, vol. 19, no. 8, art. 1788, 2019.

[3] S. S. Mathew, K. Hayawi, N. A. Dawit, I. Taleb, and Z. Trabelsi, "Integration of blockchain and collaborative intrusion detection for secure data transactions in industrial IoT: a survey," *Cluster Computing*, vol. 25, no. 6, pp. 4129-4149, 2022.

[4] E. S. Babu, B. K. N. SrinivasaRao, S. R. Nayak, A. Verma, F. Alqahtani, A. Tolba, and A. Mukherjee, "Blockchain-based Intrusion Detection System of IoT urban data with device authentication against DDoS attacks," *Computers and Electrical Engineering*, vol. 103, art. 108287, 2022.

[5] W. Li, Y. Wang, and J. Li, "Enhancing blockchain-based filtration mechanism via IPFS for collaborative intrusion detection in IoT networks," *Journal of Systems Architecture*, vol. 127, art. 102510, 2022.

[6] V. Saravanan, M. Madiajagan, S. M. Rafee, P. Sanju, T. B. Rehman, and B. Pattanaik, "IoT-based blockchain intrusion detection using optimized recurrent neural network," *Multimedia Tools and Applications*, 2023.

[7] Z. Abou El Houda, H. Moudoud, B. Brik, and L. Khoukhi, "Securing Federated Learning through Blockchain and Explainable AI for Robust Intrusion Detection in IoT Networks," in *IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2023.

[8] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "A Collaborative Fog-Based Healthcare Intrusion Detection Security Using Blockchain and Machine Learning," in *The International Conference on Artificial Intelligence and Smart Environment*, Cham: Springer International Publishing, 2022.

[9] S. Siddamsetti and M. Srivenkatesh, "Implementation of Blockchain with Machine Learning Intrusion Detection System for Defending IoT Botnet and Cloud Networks," *Ingénierie des Systèmes d'Information*, vol. 27, no. 6, 2022.

[10] A. A. Aburas and H. A. Afolabi, "Securing Green IoT Infrastructure Using Blockchain Based Machine Learning Intrusion detection system," *Turkish Online Journal of Qualitative Inquiry*, vol. 12, no. 6, 2021.

[11] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9463-9472, 2020.

[12] H. Benaddi and K. Ibrahimi, "A review: Collaborative intrusion detection for IoT integrating the blockchain technologies," in *2020 8th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, IEEE, 2020, pp. 1-6.

[13] M. P. Kumar and T. Swarnalatha, "Implementation Of Iot System Using Blockchain Security Analysis For Malicious Attack And Intrusion Prevention," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 11, no. 3, pp. 2227-2236, 2020.

[14] R. K. Sharma and R. S. Pippal, "Malicious Attack and Intrusion Prevention in IoT Network Using Blockchain Based Security Analysis," in *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)*, IEEE, 2020, pp. 380-385.

[15] O. Shende, R. K. Pateriya, P. Verma, and A. Jain, "CEBM: Collaborative Ensemble Blockchain Model for Intrusion Detection in IoT Environment," 2021.

[16] E. Ashraf, N. F. F. Areed, H. Salem, E. H. Abdelhay, and A. Farouk, "Fidchain: Federated intrusion detection system for blockchain-enabled iot healthcare applications," in *Healthcare*, vol. 10, no. 6, MDPI, 2022, p. 1110.

[17] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55-68, 2022.

[18] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection," *Computers and Electrical Engineering*, vol. 103, art. 108379, 2022.

[19] R. Mahmoudie, S. Parsa, and A. Rahman, "Presenting a method to detect intrusion in IoT through private blockchain," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 30, no. 6, pp. 2355-2372, 2022.

[20] S. Kably, T. Benbarrad, N. Alaoui, and M. Arioua, "Multi-Zone-Wise Blockchain Based Intrusion Detection and Prevention System for IoT Environment," *Computers, Materials & Continua*, vol. 75, no. 1, 2023.

[21] M. Rashid Md. Mamunur, "A Novel Intrusion Detection System in IoT Networks Leveraging Blockchain-Enabled Federated Learning," PhD diss., , 2023.

[22] J. Hassan, M. K. Abid, A. Ghulam, M. S. Fakhar, and M. Asif, "A Survey on Blockchain-based Intrusion Detection Systems for IoT," 2023.

[23] R. Salama and M. Ragab, “Blockchain with Explainable Artificial Intelligence Driven Intrusion Detection for Clustered IoT Driven Ubiquitous Computing System,” *Computer Systems Science & Engineering*, vol. 46, no. 3, 2023.

[24] A. A. M. Sharadqh, H. A. M. Hatamleh, S. S. Saloum, and T. A. Alawneh, “Hybrid Chain: Blockchain Enabled Framework for Bi-Level Intrusion Detection and Graph-Based Mitigation for Security Provisioning in Edge Assisted IoT Environment,” *IEEE Access*, vol. 11, pp. 27433-27449, 2023.

[25] H. Alamro, R. Marzouk, N. Alruwais, N. Negm, S. S. Aljameel, M. Khalid, M. A. Hamza, and M. I. Alsaid, “Modelling of Blockchain Assisted Intrusion Detection on IoT Healthcare System using Ant Lion Optimizer with Hybrid Deep Learning,” *IEEE Access*, 2023.

[26] P. Tyagi and S. K. M. Bargavi, “Using federated artificial intelligence system of intrusion detection for IOT healthcare system based on Blockchain,” *International Journal of Data Informatics and Intelligent Computing*, vol. 2, no. 1, pp. 1-10, 2023.

[27] X. He, S. Alqahtani, R. Gamble, and M. Papa, “Securing over-the-air IoT firmware updates using blockchain,” in *Proceedings of the International Conference on Omni-Layer Intelligent Systems*, 2019, pp. 164-171.

[28] S. Kesavan, J. Senthilkumar, Y. Suresh, and V. Mohanraj, “IoT Device Onboarding, Monitoring, and Management: Approaches, Challenges, and Future,” in *Challenges and Opportunities for the Convergence of IoT, Big Data, and Cloud Computing*, IGI Global, 2021, pp. 196-224.

[29] J. H. Park, J. Y. Park, and E. N. Huh, “Block chain based data logging and integrity management system for cloud forensics,” *Computer Science & Information Technology*, vol. 149, 2017.

[30] K. Khacef and G. Pujolle, “Secure Peer-to-Peer communication based on Blockchain,” in *Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 33rd International Conference on Advanced Information Networking and Applications (WAINA-2019)*, Springer International Publishing, 2019, pp. 662-672.

[31] N. Andola, S. Venkatesan, and S. Verma, “PoEWAL: A lightweight consensus mechanism for blockchain in IoT,” *Pervasive and Mobile Computing*, vol. 69, art. 101291, 2020.

[32] J. Mao, Y. Zhang, P. Li, T. Li, Q. Wu, and J. Liu, “A position-aware Merkle tree for dynamic cloud data integrity verification,” *Soft Computing*, vol. 21, pp. 2151-2164, 2017.

[33] M. Garcia, P. Fuentes, M. Odriozola, E. Vallejo, and R. Beivide, “FOGSim interconnection network simulator,” *University of Cantabria*, 2014.

[34] C. Faria and M. Correia, “BlockSim: Blockchain Simulator,” in *2019 IEEE International Conference on Blockchain*, IEEE, 2019, pp. 439-446.

Edited by: Anil Kumar Budati
Special issue on: Soft Computing and Artificial Intelligence for wire/wireless Human-Machine Interface
Received: Oct 12, 2023
Accepted: Jan 28, 2024