



Article

Decentralized Blockchain Network for Resisting Side-Channel Attacks in Mobility-Based IoT

Rashidah Funke Olanrewaju ¹, Burhan Ul Islam Khan ^{1,*} , Miss Laiha Mat Kiah ², Nor Aniza Abdullah ² and Khang Wen Goh ^{3,*} 

¹ Department of Electrical and Computer Engineering, Kulliyah of Engineering, International Islamic University Malaysia (IIUM), Kuala Lumpur 50728, Malaysia

² Department of Computer System & Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia

³ Faculty of Data Science and Information Technology, INTI International University, Nilai 71800, Malaysia

* Correspondence: burhan.iium@gmail.com (B.U.I.K.); khangwen.goh@newinti.edu.my (K.W.G.)

Abstract: The inclusion of mobility-based Internet-of-Things (IoT) devices accelerates the data transmission process, thereby catering to IoT users' demands; however, securing the data transmission in mobility-based IoT is one complex and challenging concern. The adoption of unified security architecture has been identified to prevent side-channel attacks in the IoT, which has been discussed extensively in developing security solutions. Despite blockchain's apparent superiority in withstanding a wide range of security threats, a careful examination of the relevant literature reveals that some common pitfalls are associated with these methods. Therefore, the proposed scheme introduces a novel computational security framework wherein a branched and decentralized blockchain network is formulated to facilitate coverage from different variants of side-channel IoT attacks that are yet to be adequately reported. A unique blockchain-based authentication approach is designed to secure communication among mobile IoT devices using multiple stages of security implementation with Smart Agreement and physically unclonable functions. Analytical modeling with lightweight finite field encryption is used to create this framework in Python. The study's benchmark results show that the proposed scheme offers 4% less processing time, 5% less computational overhead, 1% more throughput, 12% less latency, and 30% less energy consumption compared to existing blockchain methods.

Keywords: mobility; Internet-of-Things; secure data transmission; blockchain; Ethereum; side-channel attack; smart agreement; physical unclonable function



Citation: Olanrewaju, R.F.; Khan, B.U.I.; Kiah, M.L.M.; Abdullah, N.A.; Goh, K.W. Decentralized Blockchain Network for Resisting Side-Channel Attacks in Mobility-Based IoT.

Electronics **2022**, *11*, 3982.
<https://doi.org/10.3390/electronics11233982>

Academic Editor: Juan M. Corchado

Received: 11 October 2022

Accepted: 28 November 2022

Published: 1 December 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Internet-of-Things (IoT) has evolved as a technological advancement toward communication systems and data analytics in the present era [1]. It consists of interconnected physical objects, also called “things”, in the form of various technologies, softwares, and sensors, essentially [2]. The core agenda of IoT is to offer a more extensive deployment of connected devices or machines for facilitating the exchange of data over the internet [3]. With the increasing adoption of smart appliances, IoT enables efficient process automation [4–7]. However, it is still in the beginning stage of commercial practices in the form of applications or smart cities, apart from various ongoing research work toward multiple application forms [8]. One of the biggest concerns about IoT is its security issue owing to its broader set of heterogeneous devices connected over a vulnerable internet connection. To date, various dedicated research works have addressed security problems in IoT. At the same time, some are proven effective in resisting specific threats, while the majority still have limitations [9,10]. It has been noted that the majority of the attacks in IoT are associated with applications/software, communication channels, and devices [11,12]. Some of the attacks that have been widely studied are related to physical tampering, distributed

denial-of-service, firmware hijacking, injection of malicious nodes, eavesdropping, etc. However, less robust solutions are seen among research communities associated with side-channel attacks. The prime origination point of a side-channel attack is the leakage of information related to power, light, sound, electromagnetic signal, and timing [13,14]. Being a passive attack, such an attack can break through the potential security system even if it is secured by brute force [15]. It is also noted that various studies are being carried out to address this form of threat. However, these studies are pretty specific to the case of side-channel attacks. One significant fact is that there are various types of such forms of attack—viz. (i) acoustic attack, (ii) differential fault attack, (iii) cache attack, (iv) timing attack, (v) electromagnetic attack, (vi) power-based attacks—that are further classified to correlation power analysis, differential power analysis, and simple power analysis [16,17].

Although the methodology and strategy of all these attacks are discrete, the vulnerability point is that one attack could eventually weaken the system in the network enough to introduce another form of side-channel attack. From a global problem perspective, there is no generalized solution for securing comprehensive threats in side-channel attacks, especially in the case of an extensive network of IoT. In search of a practical solution, it has been found that blockchain is capable of securing communication in IoT [18]. Blockchain adoption in IoT offers extensive security to sensitive data, higher flexibility, reliability, etc. [19]. Based on existing trends of research work in blockchain towards securing IoT and this study's result, it is understood that private networks constructed by blockchain can be effectively used for transmitting data via the internet using IoT devices [20–23]. This operation is claimed to offer better tamper resistance to its data. Therefore, the proposed scheme introduces a scalable framework of decentralized blockchain networks for resisting different variants of threats in side-channel attacks in IoT.

The contributions of the proposed scheme are as follows:

1. The proposed method introduces multiple stages of secure network implementation in IoT, where a novel communication model is built over mobile IoT devices;
2. A novel blockchain network is constructed to verify and authorize data related to mobile IoT devices, access points, and smart agreements;
3. The mobile IoT devices are configured to play the role of the requestor, worker, and supporter in the blockchain network in a branched form for facilitating a faster transaction with the least overhead and higher scalability;
4. The complete operation of the proposed blockchain network is carried out by constructing an algorithm for permission rights, verification of adjacent nodes, data transmission, and assessment of candidate IoT nodes;
5. Ethereum blockchain is implemented with an extensive test environment benchmarked by comparing with frequently used blockchain models to exhibit a better balance between securing multiple variants of side-channel attacks and communication efficiency.

The rest of this paper is organized as follows: Section 2 discusses frequently used methodologies for securing side-channel attacks and different variants of blockchain-based security approaches in IoT. Section 3 highlights the research problem, and the methodology is discussed in Section 4. Section 5 illustrates algorithm implementation, and the result is discussed in Section 6, while the conclusion is highlighted in Section 7.

2. Existing Approaches

At present, there are various studies with unique methodologies for resisting side-channel attacks in different forms of networks. The security model presented by Kwon et al. [24] used a deep learning approach to identify the presence of side-channel attacks that are non-profiled. The work carried out by Le et al. [25] presents a security model for resisting cache attacks using a neural network. The adoption of a convolution neural network is reported in the work of Mukhtar et al. [26] towards addressing dual problems of side-channel attack and dimensional reduction. A hardware-based realization technique for identifying power attacks was deployed by Moini et al. [27]. The authors have used cloud-

based gate arrays to investigate the vulnerabilities using a Bayesian neural network. A study on power attacks has also been carried out by Ghandali et al. [28] using a combination of asymmetric encryption and a deep learning approach. The technique used asymmetric encryption via hardware implementation, wherein the Boltzmann learning technique is used for learning the probability of intrusion. Work in a similar direction was also carried out by Ng et al. [29].

Vuppala et al. [30] presented a security technique for resisting electromagnetic attacks. Furthermore, the study model emphasizes controlling overhead using the rekeying mechanism. A study on fighting electromagnetic attacks was also presented by Ghosh et al. [31] and Jevtic [32] using a hardware prototyping approach. The model is also claimed to resist fault-injection attacks. Liu et al. [33] developed a model for strengthening physical unclonable functions by integrating a set of challenges and responses with information from the side channel. Further, a softmax function with a feed-forward neural network is implemented to perform classification. Ensan et al. [34] conducted a study to prove that architecture using in-memory computation is highly vulnerable to side-channel attacks. Kim and Shin [35] have presented another unique study to resist thermal attacks. The core intrusion indicator is constructed based on the distinction between memory access and cache hit aimed at the loading process using thermal sensors. Antognazza et al. [36] developed a security framework for resisting electromagnetic and power attacks. In their work [37], Ha et al. put forward a defense model to secure cloud storage from side-channel attacks and privacy leakage. Kulow et al. [38] designed a learning-based model to ward off side-channel attacks in asymmetric encryption. Apart from the studies mentioned earlier on side-channel attacks, exploration has also been carried out towards studying blockchain-based methodologies for resisting various security threats [39–48]. The dominant usage of learning-based techniques is reported in blockchain-based security approaches [39,49–58], while some are implemented using game theory [59–64]. The following section outlines the research problems identified from existing security methodologies.

3. Research Problem

Existing methodologies have considered addressing unique case studies of intrusion associated with side-channel attacks on various forms of the network system. To a large extent, the claimed accomplishment is proven to resist the identified threat; however, open-end issues must be addressed. The identified research problems are as follows:

1. Narrowed focus on side-channel attack—All the variants of side-channel attacks are potentially linked. Hence, addressing one security problem will leave another set of related issues unsolved. A minor vulnerability in the secret key will affect both power and differential attacks and, to some extent, other variants of side-channel attacks. Hence, existing approaches offer a local solution that is not applicable when exposed to an extensive and distributed network;
2. Less novelty in blockchain network—The majority of existing approaches are more focused on block formation than formulating a secure network. Encrypting with sophisticated secret keys will only increase delay and significantly affect the quality of service, especially in extensive networks like IoT. Even if it is deployed over many transactions, it will give rise to scalability issues that have not been addressed;
3. Non-inclusion of mobility—Existing studies do not report the possible impact of mobile nodes on blockchains in extensive networks. Constructing the block, performing authentication, and updating data are challenging in a vast network with many connected devices. Even if a blockchain network is developed, authenticating all the mobile nodes joining and leaving the network will require dependency on many network devices and increased computational resources;
4. Lack of realization of adversary strength—A side-channel attack can adopt a varied strategy to initiate an attack. A closer look into existing studies shows increasing adoption of the learning-based model for identifying the adversary. However, none of

- these schemes have reported a secure learning model that could be compromised by such an attacker and thereby grows more intelligent capabilities to introduce attackers;
5. Lack of adoption of scalability—In the presence of a vast network, there will be an increasing demand for identifiers of mobile devices as well as certificates associated with network authentication. Further, adopting public key encryption makes the adversary formulate a more straightforward strategy to intrude into the network. Hence, existing encryption-based blockchains are also vulnerable to side-channel attacks.

Based on the above-stated problems, it can be stated that resisting side-channel attacks with blockchain is yet an open-end problem in large-scale network deployment. The following section outlines a solution to address this problem.

4. Materials and Methods

The prime aim of the proposed work is to construct a secure blockchain-based communication scheme to resist different variants of side-channel attacks. The deployment environment of the proposed system is considered to be Internet-of-Things (IoT), where the communication media is termed a mobile IoT device. The agenda is to offer multi-layer security to the communication process along with adherence to scalability toward the secure communication process. The proposed system shown in Figure 1 considers this deployment in three security stages: primary, secondary, and ternary. In the *primary* implementation stage, multiple mobile IoT devices initiate communication with the Local Access Point (LAP) and a centralized structure of all mobile nodes in complete IoT. Therefore, the centralized structured node is called the core IoT node, which retains information on the locations of all mobile nodes before communication using blockchain. From the viewpoint of blockchain, the miner's role is played by LAP and the core IoT node, which frames up in the *secondary* implementation stage.

In contrast, the *ternary* implementation stage concerns cloud and core IoT node operation storage hosting services. The LAP carries out the centralized communication via the proposed approach with the condition that the centralized structure only communicates with the local blockchain, core IoT node, and LAP. Hence, all these nodes communicate with each other in both primary and secondary stages of implementation.

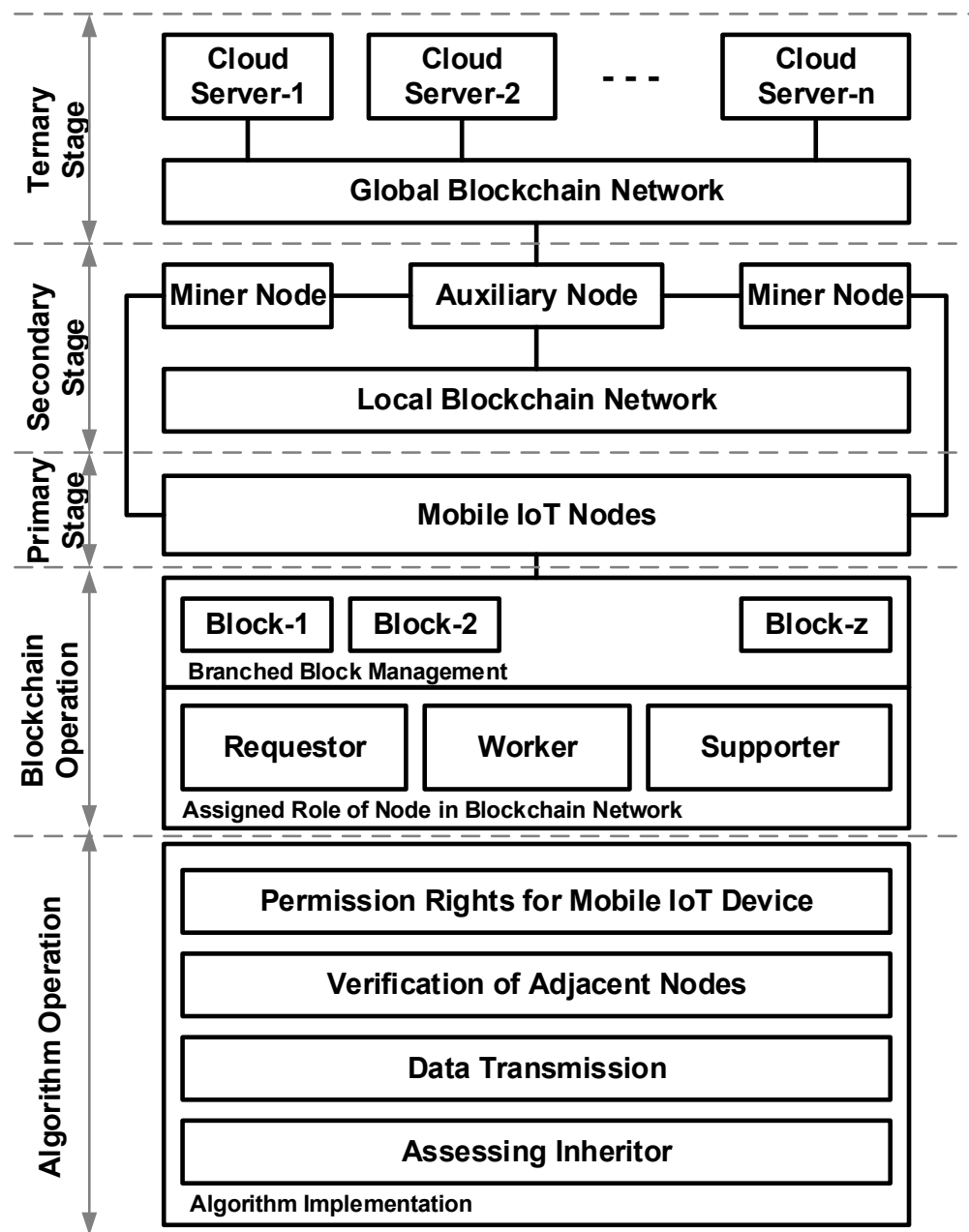


Figure 1. Proposed architecture.

4.1. Primary Stage

This implementation stage is associated with the communication scheme of mobile IoT nodes with respect to all networking devices deployed in the IoT environment. Group-based communication is deployed within the simulation area where LAP plays the role of the core IoT node. All the mobile IoT devices initiate their communication with the LAP before carrying out authorization in a centralized manner. However, this is just a one-time process that instantly transforms itself using blockchain in a decentralized way to offer more scalable and secure communication in IoT. The proposed scheme uses a distributed data storage mechanism using a hash tree to construct the blockchain network. It harnesses the beneficial features of branched blockchain, which ensure a lighter version of data exchange with efficient control over any possible overhead. One of the security advantages of this usage is that its accessibility is limited to only its branch, which restricts other mobile IoT nodes from joining the network directly. After constructing the first primary block, an integrated blockchain results from merging the core IoT device.

All these blocks in a highly branched form help classify the mobile IoT nodes into passive and active blocks storing all sorts of transactional records. It should be noted that such a large chain of mobile IoT devices will also call for using extensive resources. Hence, a branched blockchain can address this problem by storing only the updated block, thus saving much processing memory. Unlike existing blockchain methods [39–48], the proposed scheme is independent of any demand for mining processing for a sophisticated hashing algorithm. In the communication scenario, all the mobile IoT devices are connected with the LAP using the internet. The LAP acts as a core IoT device in a defined geographical region. The authentication of the hardware with respect to its integrated circuits in this mobile IoT device can be carried out by verifying responses obtained from challenges using a physical unclonable function. Further, the proposed scheme considers the security configuration among the IoT devices to be carried out offline before the deployment of the communication scenario. The complete mechanism of authentication is carried out using three variants of secure control messages, as follows:

- msg_a —This control message is forwarded by the mobile IoT node to the LAP, where the prime fields of the message consist of a random nonce and identification number of the mobile IoT device;
- msg_b —This control message is generated by the cloud server when the LAP either accepts or denies the identity of the mobile IoT device based on a physical unclonable function. The denial flag is generated only when the identity information of the mobile IoT device is not found within the device's memory by LAP. Using another random number, this message is further ciphered in case of its presence. A unique code is appended with this message to ensure integrity;
- msg_c —With the aid of a physical unclonable function, a response is generated by the mobile IoT device. A secret arbitrary integer value is obtained by this mobile IoT device using its response to verify the integrity and freshness of the message. The consecutive iteration of the random secret number is further used in increasing the count to generate a set of challenges by the mobile IoT device. This message is therefore used to ensure that the newly generated response and the arbitrary number are forwarded to the cloud server using the first random number. The computation of the received information is carried out by a cloud server using the first arbitrary secret number.

4.2. Secondary Stage

The proposed scheme uses blockchain to manage the trusted authority for rendering the availability of data specific to mobile IoT nodes by a distributed ledger. Owing to strict restrictions on accessibility, all the data retained within the distributed ledger are highly secured from any tampering attempt. As a part of the primary implementation stage, the proposed scheme secures all mobile IoT devices using a physical unclonable function, resisting the possibilities of different variants of side-channel attacks. As it is quite difficult to synchronize blockchain with mobile IoT devices, it is necessary for all mobile IoT devices to communicate with the LAP using centralized infrastructure in the primary stage of implementation. However, the secondary implementation stage calls for the communication of all LAP with other auxiliary nodes using LAP, where the latter (i.e., LAP) acts as a core IoT device. An auxiliary node is a specific LAP role characterized by extensive computing capabilities, which communicates with the distributed cloud storage units and plays a trusted authority role in the IoT environment.

The auxiliary node and LAP carry out the block generation after the broadcasting of blocks is accomplished. These nodes also perform the verification and voting process for selecting devices in IoT communication. The proposed scheme uses a blockchain platform for managing the second stage of operation, which uses a modular architecture for application development. The scheme uses all transmission via the blockchain approach in a decentralized manner instead of using the physical layer of the mobile IoT devices, which is known to increase the demands of computational resources. This part of the implementation

also introduces multiple secondary roles into the nodes to carry out blockchain operations for secure data management, as follows:

- *Requestor*—This mobile IoT node is responsible for understanding the task and placing a request to process a new task. To carry out this operation, the scalability is maintained by recommending multiple numbers of block allocation support by this node to the blockchain;
- *Worker*—This is a specific set of mobile IoT devices that receives the request for new tasks subjected to the blockchain process. Hence, such a node whose details are managed and updated by a distributed ledger accepts all the transaction blocks. The ledger stores the copy of the block of transaction that is altered by the other mobile IoT device after being authenticated;
- *Supporter*—This is the third role of the mobile IoT device, which is essentially meant to support services for all transactions using Smart Agreement (SA). The details of this SA are digitally signed with an encryption signature by the supporter node and transmitted to the original client.

Apart from the above-mentioned node functionalities, this scheme also introduces a *super-ledger* node responsible for the overall monitoring of the network's operation and offering authentication services. Notably, all the *data blocks* differ from the *transactional blocks* in the proposed blockchain. The former maintain all data transactions from aggregated data from multiple communicating nodes. At the same time, the latter are constructed by requesting services followed by a forwarding mechanism for all the control messages. It is also necessary to realize that the assignment of the specific role for the mobile IoT node (supporter or worker) maintained in adherence to the blockchain network is potentially impacted by the network topology. Furthermore, the network state and the verification task are required to be initially carried out to add a block of data by the worker node. After successfully transmitting a digitally encrypted signature, the role of the mobile IoT device is declared in the current state of the network.

4.3. Ternary Stage

In this implementation stage, an auxiliary node performs the supervision of the specific LAP. The auxiliary node carries out the data and device management and query processing. Finite field encryption is used to strengthen the blockchain for better data integrity. The secure communication between the cloud and auxiliary node is facilitated using blockchain incorporated with the certificates, while SA maintains all the distribution operation of certificates. This operation controls the secure communication among all mobile IoT nodes. Another significant contribution is the non-dependency of any domain tag or constant address by the LAP to perform communication with the cloud or operate SA. This implementation stage also calls for verifying all the adjacent mobile IoT devices via each target node in order to enrich the updating information to the blockchain network. Further, the probability of a mobile node being intruded is computed, followed by assessing the physically unclonable function every time.

Therefore, the proposed system performs all three stages of implementation to ensure the seamless connectivity of mobile IoT nodes in a highly secure manner. The following section outlines the algorithm's implementation.

5. Algorithm Implementation

The prior section notes that the proposed system has various levels of operation to resist side-channel attacks in the large deployment environment of a mobile IoT system. One essential point of information from the implementation is that the proposed scheme focuses on fighting all the variants of side-channel attacks by emphasizing vulnerability identification. This is further followed by resisting the participation of such adversaries in data propagation in IoT. This section discusses different algorithms that carry out a discrete set of security operations toward accomplishing the agenda.

5.1. Permission Rights for Mobile IoT

The proposed system considers that all the mobile IoT devices communicate with each other based on their Smart Agreement (SA). It also believes that all mobile IoT devices have an individual blockchain account. Unlike any existing scheme, the proposed system maintains a mirror of the blockchain on every Local Access Point (LAP) connected in a synchronized manner. This is the first phase of algorithmic implementation, denoted as Algorithm 1, which is responsible for constructing permission rights for all mobile IoT devices. The newly introduced mobile IoT devices will be provided with a nonce and a route discovery beacon by the core IoT device. Further, the implementation is directed towards the secure distribution of time-bound session keys, followed by updating it. The proposed system generates this distribution key from mobile and core IoT devices.

Algorithm 1 Permission Rights for Mobile IoT Device

Input: m (mobile IoT device)
Output: Declaration of Accept/Reject
Start
 1. Obtain $((\text{'beacon'} \parallel C_{non}), C)$
 2. **For** $K_{dis} = 1$
 3. Obtain $(ID_m, ID_{req}, non_c, non_m, K_{dis})$
 4. Obtain $(non, K_{ses}[], K_{dis})^C$
 5. **Else**
 6. Obtain $(ID_m, ID_{req}, non_c, non_m, K_c)$
 7. Obtain $(non, K_{ses}[], K_{dis})^C$
 8. Obtain $(K_{dis}, K_c, K_m)^C$
 9. Config $(K_{ses}[m] = 1, C)$
 10. $lu(ID_{creq}, ID_{sk}(m), non_c, non_m, K_{dis})$
 11. **If** $ID_{creq} = 1$
 12. Obtain $(non_c, non_m, K_{ses}[])$
 13. Declare *Accept*
 14. **Else**
 15. Declare *Reject*
End

According to this technique, to resist the evolution of *differential fault attacks* and all the variants of *power-based attacks* in side-channel adversaries, the system forwards the aggregated keys along with a message consisting of public key information of both mobile and core IoT devices. This is followed up by appending these keys to the authorized mobile IoT nodes. The mobile IoT device forwards a request beacon if it does not acquire this session key. This time-bound session key is used for appending along with the encrypted message to be forwarded. The operation of the algorithmic steps is discussed as follows: The algorithm initially extracts a *beacon* in the form of a route discovery message along with nonce C_{non} generated by the core IoT node, i.e., C (Line-1). Considering the presence of keys for distribution K_{dis} (Line-2), the algorithm further obtains multiple information points from the mobile IoT node m , i.e., the identity of mobile IoT device ID_m , the identity of the request generated for key ID_{req} , the nonce generated by core IoT device non_c , the nonce generated by the mobile IoT device non_m , and keys for distribution K_{dis} (Line-3). The algorithm also extracts the nonce generated by the mobile IoT device non_m , K_{dis} , and the array for storing the key $K_{ses}[]$ extracted from the core IoT node C (Line-4). However, suppose no keys are found for distribution (Line 5). In that case, the algorithm obtains further information just as in Line-3, except for substituting the K_{dis} variable with the key of the core IoT node, i.e., K_c (Line-6).

Furthermore, it obtains information similar to Line-4 in Line-7 and Line-8 with a new inclusion of variables, i.e., the public key of core IoT node K_c and the mobile node, i.e., K_m , along with K_{dis} (Line-8). The next part of algorithm implementation is configuring the key $K_{ses}[m]$ for the mobile IoT node with the core node whose information is obtained from the authorized mobile IoT node m (Line-9). Further, a lookup function $lu()$ is constructed

that searches for the identity of the communication request ID_{creq} , the identity of the session key ID_{sk} , the nonce of mobile IoT node non_m , and K_{dis} (Line-10). In the presence of a communication request (Line-11), the algorithm obtains information associated with the nonce information and the session key array from an authorized mobile IoT node (Line-12). Based on this information, the algorithm declares *Accept*, signifying authorized communication (Line-13), or else declares *Reject* for unauthorized communication (Line-15).

5.2. Verification of Adjacent Node in Blockchain

This algorithm is responsible for verifying the adjacent mobile nodes in IoT, where all the nodes maintained in the form of a blockchain retain a set of all adjacent nodes for each mobile IoT device. This part of the algorithm emphasizes a possible mitigation strategy for the *Timing attack* based on the difference in execution time. To resist this possible attack, the algorithm computes the primary instantaneous event of communication considering all the mobile IoT devices (Line-1). The construction of the Algorithm 2 is carried out based on the pair of mobile IoT devices where the i th device communicates with the j th device. To offer better scalability in performance, an empty matrix of adjacent nodes $\beta(i)$ is constructed (Line-2). To initiate data transmission, the transmitting mobile node must assess the window of time needed to resist timing attacks in IoT. However, this assessment must be carried out by receiving node j , unlike any existing system, where such assessment is continued only for transmitting nodes. In such a way, both the communicating nodes, i.e., i and j , will perform the computation of probability until they accomplish a higher probability *Prob* (Line-6, 8, 11, 12) for both duration and distance.

Algorithm 2 Verifying Adjacent Nodes

Input: m (regular node of blockchain)

Output: β (verified adjacent nodes)

Start

1. **For** $i = 1:m$
 2. Construct $\beta(i) = []$
 3. **For** $j = 1:m$
 4. Compute $d^{\alpha}_{(i,j)}$
 5. **If** $d^{\alpha}_{(i,j)} = d^{\alpha_{max}}_{(i,j)} \ \&\& \ D_{\gamma i} = D_{\gamma j}$
 6. $\text{Prob}(d)_{ij} = 1$
 7. $j \rightarrow \beta_i$
 8. $\text{Prob}\theta_i = \text{Prob}\theta_j$
 9. $D_{ij} = D_{i-1,j-1}$
 10. **Else**
 11. $\text{Prob}\beta_{ij}(d) = 0$
 12. $\text{Prob}\theta_i = \text{Prob}\theta_j$
 13. $D\beta_{ij} = D\beta_{i-1,j-1}$
 14. **Return** $\beta(m)$
 15. **End**
 16. **End**
- End**
-

For this purpose, the algorithm computes the instantaneous duration for the complete blockchain network, i.e., $d^{\alpha}_{(i,j)}$ for both participating nodes (Line-4). Concerning the conditional logic associated with duration d from α to α_{max} (Line-5), the proposed scheme represents this condition to state a favorable condition to resist the threat posed by mobile IoT devices. In such a situation, the instantaneous probability factor is set to the maximum limit, i.e., 1 (Line-6). During this security assessment, the algorithm will keep adding the identified regular mobile IoT device to the matrix that maintains adjacent nodes, i.e., β (Line-7). In this process, the algorithm also ensures that no adversary can misuse the stale information of probability. Hence, the whole probability-based matrix *Prob* must be updated with a new set of mobile IoT nodes in sequence concerning the mathematical coefficient θ (Line-8 and Line-9).

However, if the situation is different (Line-10), the algorithm configures the probability value $\text{Prob}\beta_{ij}(d)$ to be minimal, i.e., 0 (Line-11). This allocation of a reduced probability value is carried out towards mitigating timing attacks with the adjacent mobile IoT devices sequentially without altering the internal probability allocation (Line-12). It will eventually mean that such sorted nodes will not be included for participation in the communication process, and therefore the success rate of the probability matrix remains unchanged (Line-12). Thus, with the defined computed and updated instantaneous time scale of D , the interaction of the adjacent mobile IoT devices is carried out considering the lowest duration score during the leaving index of nodes by establishing Smart Agreement among themselves (Line-13). This processing will lead to the generation of all verified lists of adjacent nodes in the form of matrix $\beta(m)$ (Line-14). Once this operation is successfully over, the algorithm will proceed further toward the interaction of the nodes with the blockchain network. This is one of the innovative features that permit the blockchain network to authenticate almost all the connected nodes before participating in the data transmission system in IoT.

5.3. Data Transmission and Inheritor Assessment

This is the next part of the algorithmic implementation, which emphasizes the data transmission and the assessment of the inheritor node within the blockchain network are presented in Algorithm 3. The algorithmic steps and discussion are as follows:

Algorithm 3 Data Transmission

Input: m_1 (transmitting node), m_2 (receiving node)

Output: ψ (blockchain)

Start

1. For $i = 1: s$
2. init D, ψ
3. For $j = 1: D$
4. For $k = 1: \psi$
5. $m_1 \rightarrow m_2$
6. $\psi(k) \rightarrow \psi_{up}$
7. **End**
8. **End**
9. Verify ψ_{up} on m_2
10. Assign ψ_{up} from m_2 to ψ
11. **End**

End

The algorithm mentioned above is used for performing data transmission considering m_1 transmitting and m_2 receiving mobile IoT nodes, which yields the ψ blockchain of an updated form upon processing. Considering all the s simulation rounds (Line-1), the algorithm performs the initialization of temporal factor D and blockchain ψ (Line-2). Regarding the deployment of the duration counter j (Line-3) and the blockchain counter k (Line-4), the algorithm performs the transmission of data from m_1 to m_2 (Line-5). Further, the algorithm constructs a sub-matrix of blockchain $\psi(k)$ with all its updated information and finally stores it back in the blockchain's main matrix, i.e., ψ_{up} (Line-6). The process is carried out until it covers all the data blocks over the duration while the algorithm further verifies the updated block over the receiving node m_2 (Line-9). Finally, all the updated blocks ψ_{up} obtained from the receiving node are assigned to the main blockchain matrix, i.e., ψ (Line-10). The contribution of this algorithm is that it amends the mechanism of storage and the accessibility of data from the blockchain, and offers a dual layer of security for each generated block. This phenomenon assists in mitigating all forms of *power attacks* (especially the simple power analysis where the block cipher is quite vulnerable) and mitigates *cache attacks* and *differential fault attackers* in proposed blockchain-based security aimed at side-channel attacks. Including temporal factors also ensures its resistance to

timing attacks when several mobile nodes are deployed in an IoT environment. Hence, this is one of the more innovative constructs presented by the proposed scheme, whereby it can resist multiple variants of side-channel attacks and other forms of related vulnerable characteristics. The algorithm contributes to increasing the scope of security strength of mobile IoT devices with more resistance capabilities.

The next part of algorithm implementation presented as Algorithm 4 is associated with assessing the unique role of a mobile IoT device called an *inheritor*. Essentially, the inheritor is a new mobile IoT device that some are currently seeking to incorporate into the data forwarding process in the current LAP. The inheritor could be some old regular mobile IoT device that was previously a part of one specific LAP. While dependent on mobility, it could have traveled to the communication region of the new LAP. For such nodes, the identity and other information could be accessible from the SA, accessed via LAP. However, the inheritor could also be a new mobile IoT device that was never part of any old network of IoT. For such nodes, the initial registration process considering identity information is carried out, followed by assigning a unique identification number based on trust. The inheritor node is essential to assigning the data forwarding task, where the data must be forwarded to the next eligible node to play the role of the inheritor. However, it is always challenging to ascertain their complete legitimacy, and hence the proposed system deploys a mechanism to assess this form of node. The algorithmic steps are briefed as follows:

Algorithm 4 Assessing Inheritor

Input: ID (identity attribute)

Output: σ (*inheritor*)

Start

1. **For** $i = 1:s$
 2. **If** $ID \subseteq (m, \sigma)$
 3. Return σ
 4. **Else**
 5. **For** $j = m_o:1$
 6. **If** $string[j] \subseteq (m, ID)$
 7. Return $string[j], m$
 8. **End**
 9. **End**
 10. **End**
- End**
-

The above-stated algorithm takes the input of the ID identity attribute, which yields an outcome of the σ inheritor node upon processing. Considering all s simulation rounds (Line-1), the algorithm constructs a conditional logic by choosing the identity ID, which belongs to both the existing mobile IoT device m and the candidate inheritor node σ (Line-2). In a positive match, the algorithm confirms the candidate node to the final inheritor node σ (Line-3). Irrespective of multiple candidate nodes, this algorithm verifies their legitimacy to confirm them as inheritor nodes. The algorithm looks for all the mobile nodes with name tags, considering probability (Line-5). If the string value of the name tags of the candidate is found to be present within the mobile IoT device m and its respective matrix of identity ID (Line-6), the algorithm returns the string value of the name with the definite identity of the mobile IoT device. Therefore, this algorithm contributes to resisting cache attacks and differential power attacks explicitly in an extensive network system, offering another layer of security apart from the blockchain.

After assessing the inheritor node, the next part of the implementation is to initialize the mobile IoT nodes, construct the first block in the blockchain network, and allocate this block to the mobile IoT device authorized for communication. It should be noted that this authorization is only allocated when the mobile IoT device is proven to have similar key K_{ses} . In the complete process, the communication within the mobile IoT device is carried out with the SA. At the same time, the information retained within the SA is used for

further interaction with the blockchain using LAP. The proposed scheme initially ensures that the mobile IoT device obtains the rights to generate the data. Based on the usage of account addresses by the proposed blockchain, the proposed method can perform both enrollments and the deletion of the mobile IoT nodes. Therefore, this scheme maintains the proper accountability of all authorized mobile IoT devices carried in the blockchain. A closer look into all the algorithms formulated for the proposed blockchain shows that it bears all the characteristics of a physical unclonable function that retains all mobile device transactional information. Apart from this, LAP also plays the certificate authority role and monitors all the issued certificates of the mobile IoT nodes. Further, the algorithm performs a verification process to ascertain the status of its assigned authority, while the mobile IoT device generates the data over the communication channel.

The presented algorithm also checks for mobile IoT device names on the list of authorized nodes. Upon finding its existence, the algorithm forwards a challenge that, upon acceptance by the mobile IoT device, formulates a network of local blockchains. The whole mobile IoT device is then furnished with a certificate by the LAP that is deployed for authentication. It will eventually mean that after receiving the certificate, the system does not demand a mobile IoT device to carry out this assessment; hence, this is one essential layer of security against every possible form of side-channel attack on the blockchain. The certificate allocated to the mobile IoT device is said to be valid until it is configured with the security rights maintained by the blockchain. The system revokes the certificate for the mobile IoT device, which does not retain any authority information. Such revoked mobile IoT devices are required to forward a request for obtaining security rights from the blockchain network and the certificate from the beginning. The mechanism also assists in updating the blockchain network based on any anomalies that could arise from side-channel attacks.

Therefore, the proposed scheme implements a unique mechanism for resisting different variants of side-channel attacks. The prime contribution of the proposed method is the highest degree of security for constructing the blockchain network, which maintains privacy, non-repudiation, availability, and integrity as the core standards of security. The following section discusses the results.

6. Results

This section discusses the outcome obtained after implementing the algorithms involved in the proposed blockchain-based security system for resisting side-channel attacks. This discussion is presented with respect to the adopted simulation parameters and the accomplished outcome of the system.

6.1. Simulation Environment

The simulation model is constructed in three stages of implementation, as per the discussion carried out in the adopted methodology section. In the primary stage of simulation implementation, the scheme emphasizes designing the enrollment process for new mobile IoT devices and performing authorization based on physical unclonable functions. The secondary stage of simulation implementation is associated with configuring the network elements, viz., the auxiliary node and LAP, with the blockchain network in a decentralized form. The tertiary layer consists of the Ethereum blockchain over the global deployment in a simulation study. The proposed scheme is implemented in a standard i5 processor with an Nvidia GeForce GTX processor with 4 GB RAM. The scripting of the proposed logic is carried out using Python, where the Ethereum protocol is implemented using Py-EVM that supports both legacy and updated specifications of Ethereum in private and public blockchains.

Table 1 highlights the simulation parameter and associated values used for capturing the outcome presented in this section. A Python script is crafted for initiating different variants of side-channel attacks. A challenging scenario is constructed by generating a block consisting of malicious transactional information by the auxiliary node, which is quite unlikely per the proposed scheme. However, this is the worst possibility, assum-

ing the attacker is quite capable and smart enough to introduce an intruding strategy. The side-channel attack is successful if it cannot identify the malicious block within the LAP or auxiliary node observed over the initial simulation round. The overall outcome exhibited significant control of the proposed Ethereum blockchain towards resisting side-channel attacks. A further discussion of the results in quantified form is presented in the following subsection.

Table 1. Simulation parameter.

Parameter	Values
Simulation area	1000 × 1100 m ²
No. of Mobile IoT device (<i>m</i>)	500–1000
Communication range of <i>m</i>	200 m
Communication range of LAP	800 m
Speed of <i>m</i>	10–40 kmph
Duration of simulation	1200 s
Rate of data transmission	27–54 Mbps
Channel capacity	10–20 MHz
Initialized energy	80 J

6.2. Accomplished Outcome

The proposed scheme chooses the data transmission rate (Table 1) based on the IEEE standard 802.11 p family due to the inclusion of mobility in the proposed IoT environment. This assists in benchmarking, as such standards are frequently reported in vehicular applications in IoT [65,66]. The assessment of the proposed scheme is carried out concerning multiple performance metrics, which have a stronger suitability for studying the impact of side-channel attacks. Further, the proposed method is compared with other current studies of blockchain reported in Section 2 of this paper. Table 2 highlights the numerical result derived when the existing blockchain approaches are subjected to a similar simulation environment of IoT and exposed to side-channel attacks.

Table 2. Numerical outcomes of comparative analysis.

Approaches	Energy (J)	Latency (s)	Throughput (bps)	Processing Time (s)	Computational Overhead (s)
Liu et al., 2020 [39]	63.02	8.02	2251	8.4408	6.0282
Hasan et al., 2022 [40]	62.21	14.02	2751	6.5521	5.7503
Rodrigues and Rocha, 2021 [41]	67.56	16.78	2301	6.9832	5.2108
Zhou et al., 2022 [42]	59.86	16.72	1973	7.5691	5.6662
Ren et al., 2022 [43]	75.66	11.82	1836	9.7701	7.0471
Xu et al., 2022 [44]	71.02	8.06	1750	11.781	8.6115
Alrubei et al., 2020 [45]	72.87	29.82	1800	6.192	3.7605
Hao et al., 2022 [46]	59.46	23.76	1982	9.162	5.8766
Whaiduzzaman et al., 2021 [47]	69.03	9.087	2506	7.5917	2.9878
Ullah et al., 2022 [48]	47.76	10.76	2197	7.451	2.8703
Proposed	35.27	2.8871	4211	3.673	0.2771

The proposed scheme implements a first-order radio energy model [67] to initialize the energy of 10 J, where 50 nj is required to propagate 1 bit of information from one node to another. With an observation carried out over a specified simulation round, a trend of comparative outcomes is obtained, as exhibited in Figure 2.

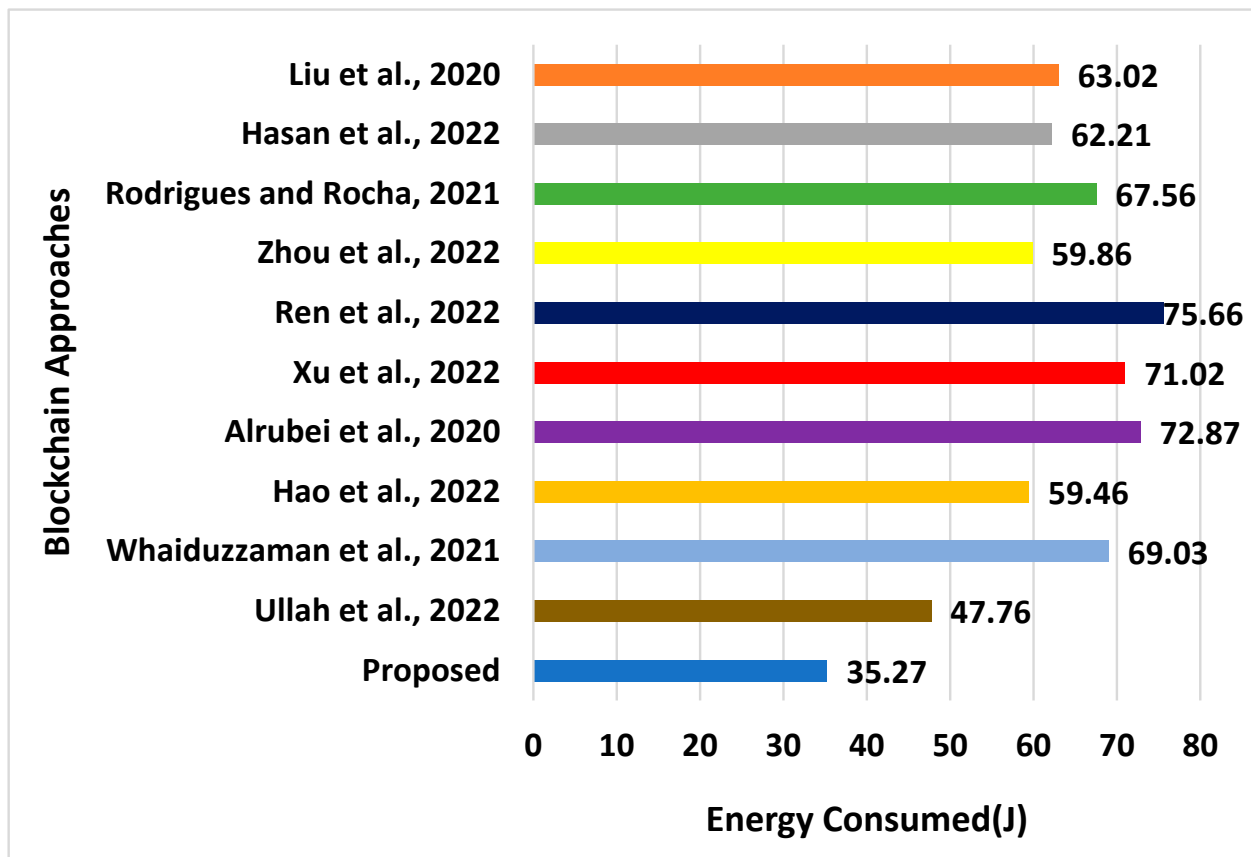


Figure 2. Analysis of energy consumption [39–48].

The outcome in Figure 2 highlights that the proposed scheme offers much-reduced energy consumption in contrast to existing approaches. Since the IoT devices are sensory, the proposed system uses a standard first-order radio energy model to perform energy computation [67]. This model assigns an initial energy of 80 J, which consumes 50 nj/bit for every transmission. The consumption increases with an increase in distance between two communicating nodes, traffic assigned, and the density of nodes in a specific mobility zone. The overall observed outcome of computed energy is shown in Figure 2. The prime justification is that the proposed system provides a comprehensive branched blockchain network in a decentralized form. With a novel algorithm for communication models over an inheritor node, the path of transmitting data is formulated more quickly owing to the faster blockchain management. This results in the availability of multiple options with higher accuracy, and there are no reported retransmission attempts resulting in significant energy conservation. Moreover, the distributed blockchain operation further contributes towards significant energy reduction, which is not often seen in existing blockchain-based studies, where the iteration is quite sophisticated and demands higher resources every time when performing block maintenance.

The next part of the analysis concerns the latency score (mean), wherein the proposed scheme shows much better performance. It is necessary to achieve reduced latency due to the inclusion of a timing attack in the side channel. Figure 3 shows the outcome of latency.

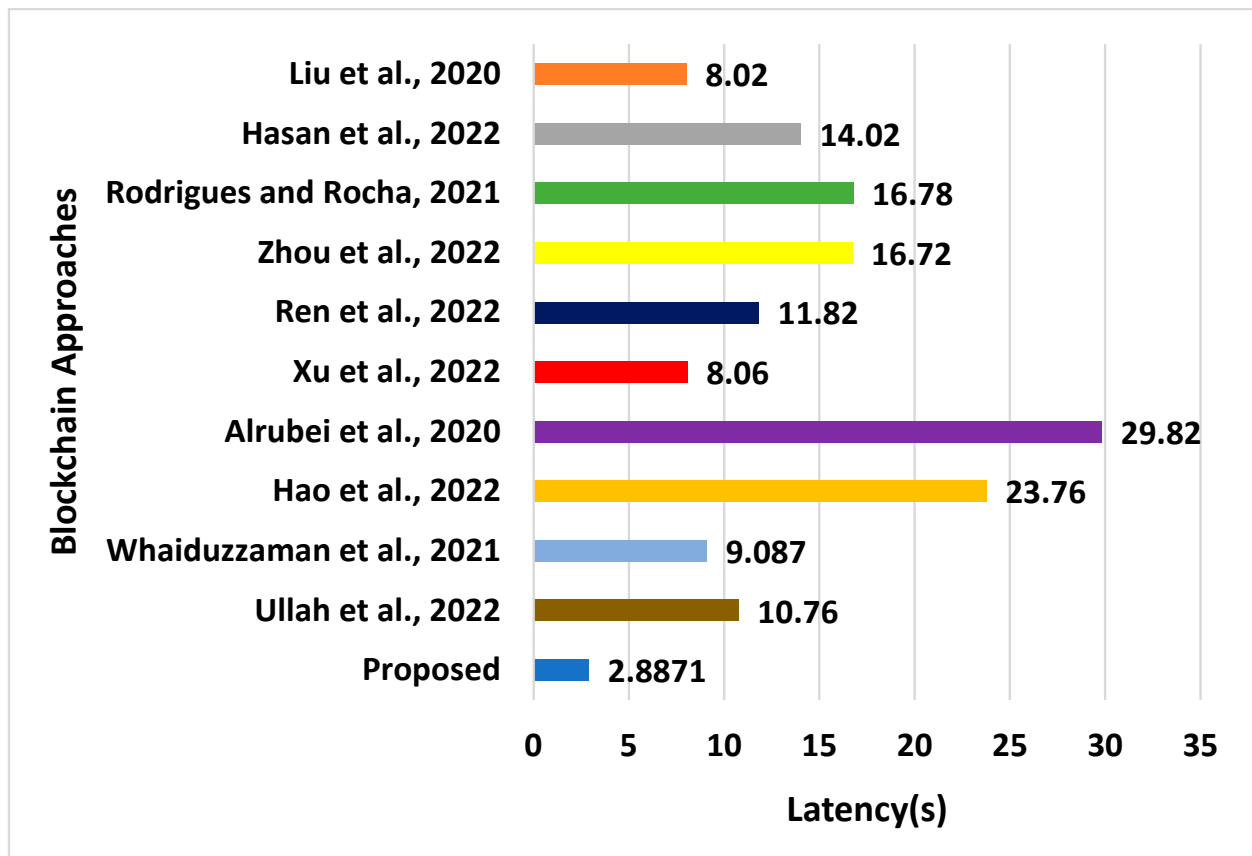


Figure 3. Analysis of latency [39–48].

The latency computation in the outcome of Figure 3 is carried out by assessing the time between forwarding requests and obtaining a response in the blockchain network. The justification of the outcome of Figure 3 is that the branched blockchain is maintained in the proposed scheme using mainly the third and second stages of implementation, corresponding to global and local block management schemes. This operation is distinct from existing blockchain architecture as it facilitates blockchain management for ongoing data transmission in a decentralized form. Apart from this, the operation carried out by the supporter node over this distributed environment is fast enough to perform authentication based on a physical unclonable function. This contributes to reduced latency for the proposed scheme. On the other hand, the existing blockchain scheme is more about the centralized structure, which requires more time to manage and update. The latency further increases in the presence of different attacks in the existing scheme of blockchains.

The third performance metric is the throughput capability of the mobile IoT node. An ideal security scheme should offer better throughput performance in the presence of an adversary. Exploring better scores of throughputs will also indirectly mean the allocation of resources, the consumption of time, the management of a complete topology, and the definition of the right propagation path are correctly structured. Figure 4 highlights the analysis of throughput obtained from the transmission of the test data of 5000 bits in a similar assessment environment.

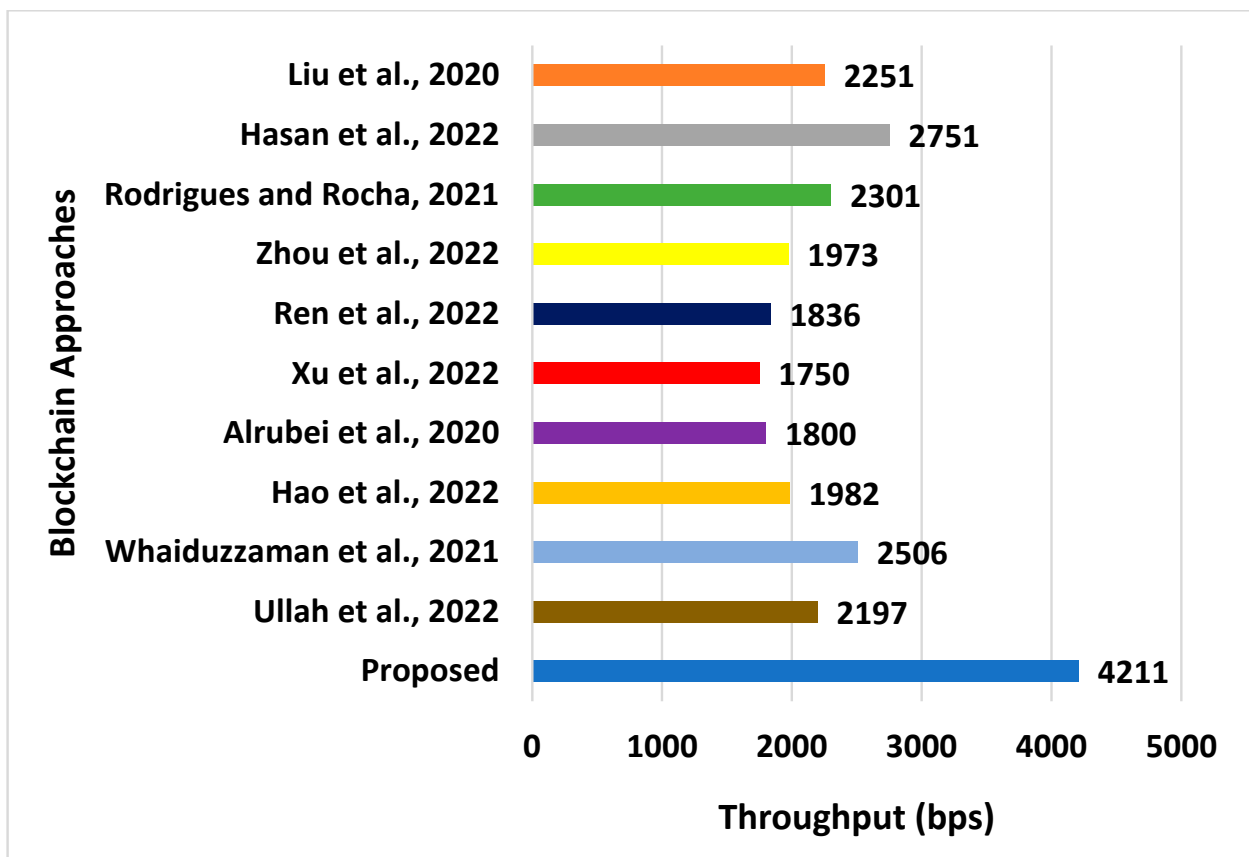


Figure 4. Analysis of throughput [39–48].

The throughput computation is carried out by calculating the quantity of data that has successfully reached the destination mobile IoT device at a specified time. The outcome exhibited in Figure 4 shows a higher throughput score for the proposed scheme compared to the existing system. This outcome is closely related to blockchain security. It should be noted that the proposed method uses a fingerprint of a physical unclonable function to produce the sets of both private and public secret keys. This operation results in the generation of a validation certificate to verify the device's legitimacy. This further results in a faster connection of all the mobile IoT nodes synchronizing with LAPs. The authenticated nodes receive a session key from LAP that acts as a core IoT node. Encryption is carried out using this key, securing all possible communications. Due to the incorporation of validity duration and a unique identifier, this key is generated faster and offers higher security. Further, by synching with the blockchain network, this key is distributed over an extensive network, which increases the number of safe routes made available in the least time.

The following line of analysis is associated with the computational overhead, which is the effective duration of time required to process a data packet. At the same time, a mobile IoT node carries and transmits it to another node. A reduced computation overhead in an IoT environment calls for a highly structured and synchronized data management process, from storing in the blockchain to query processing from the requestor node. This value must be reduced for a maximum number of mobile IoT nodes, as the computational overhead can be exponentially increased in highly interconnected networks, primarily if they work in a distributed mode of blockchain operation. The outcome of computational overhead is shown in Figure 5.

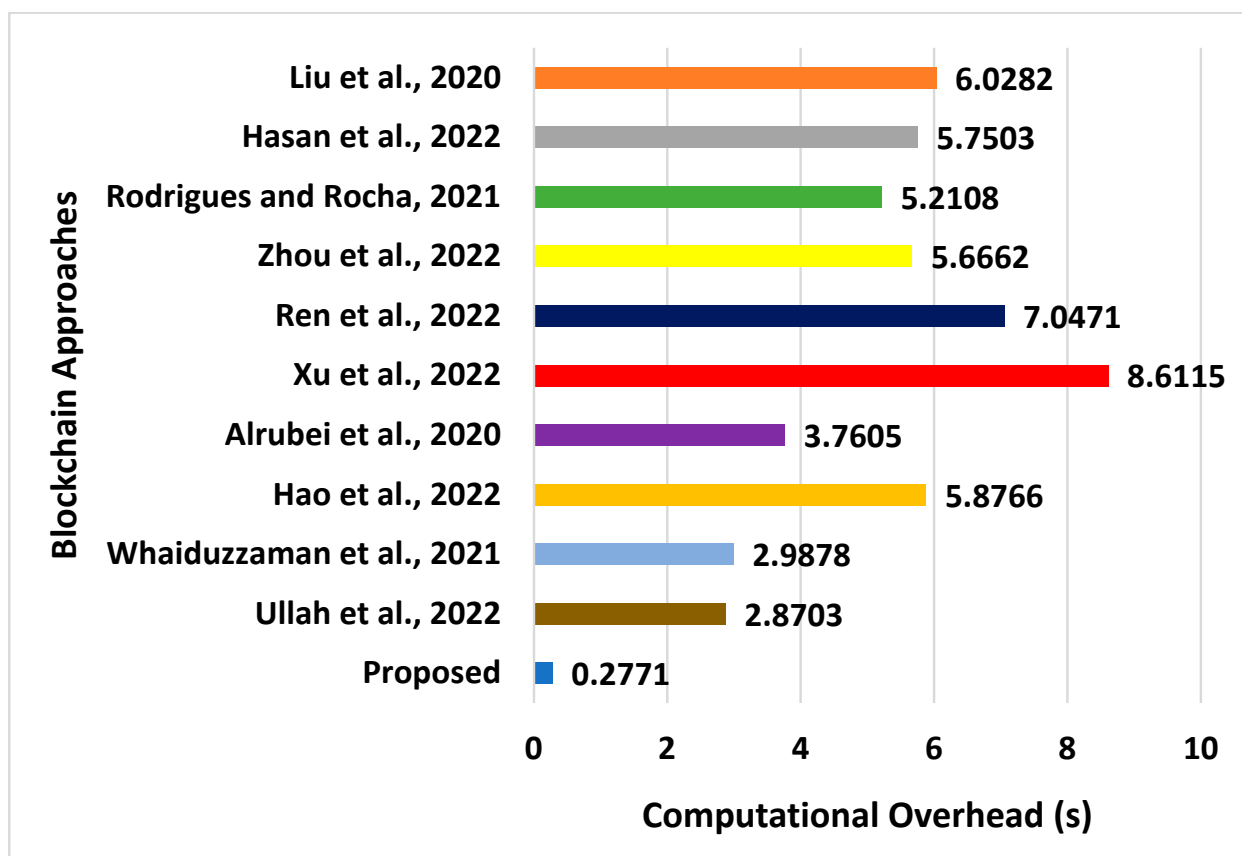


Figure 5. Analysis of computational overhead [39–48].

The computational overhead is evaluated by assessing the time consumed in processing blockchain data. The prime justification of the computational overhead outcome exhibited in Figure 5 is as follows: All the peer mobile IoT devices carry out the accountable transaction with the assistance of a distributed ledger. Further, a mobile IoT device simultaneously plays the roles of both workers and supporters, effectively distributing the computational burden. Additionally, the proposed scheme develops a matrix-based operation that finally constructs a decentralized structure for node authentication, assessing the legitimacy of certificates and checking all certificates issued in a distributed manner. This task significantly reduces the computational burden even in the presence of more traffic.

The final performance parameter to assess is the overall processing time, which depicts the possible associated computational complexity. Figure 6 highlights the trend of the comparative analysis for processing time, which is the total time required to execute the proposed algorithm.

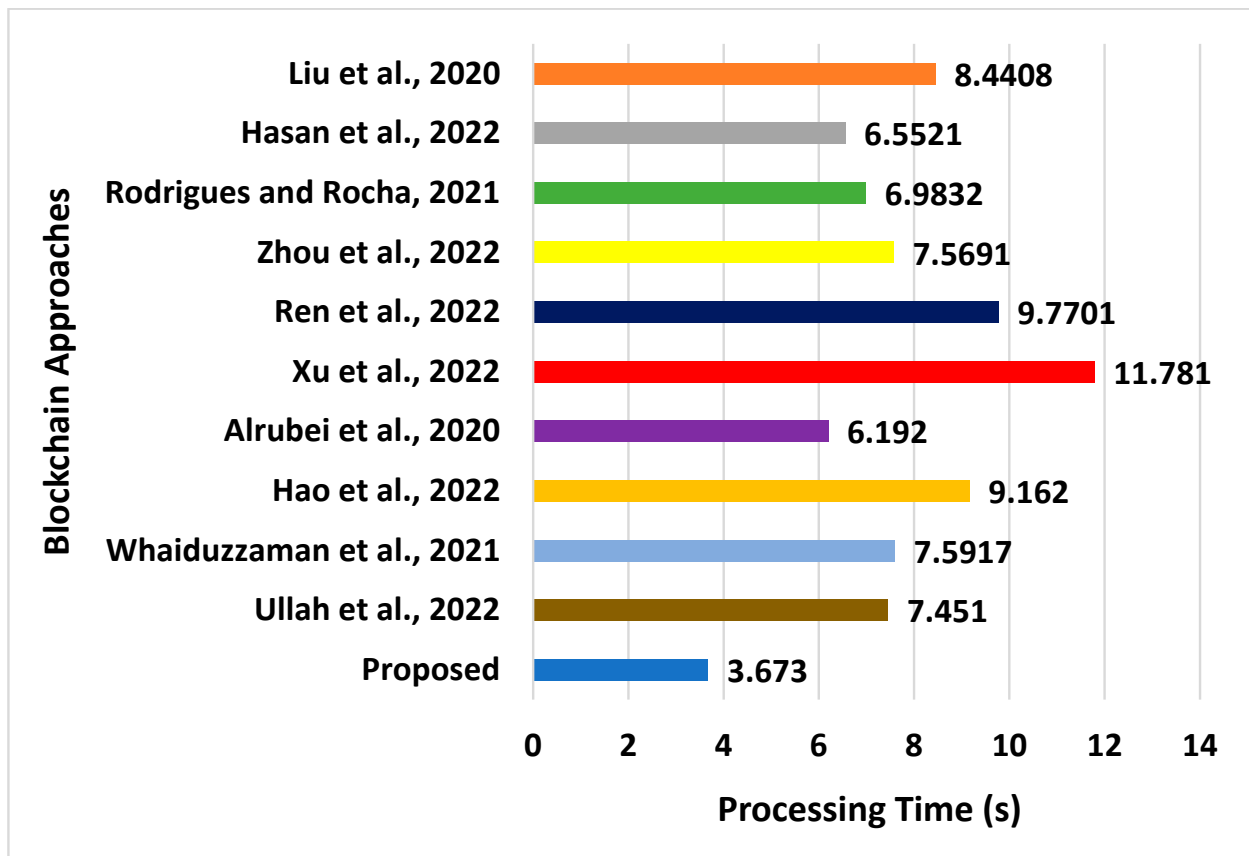


Figure 6. Analysis of processing time [39–48].

According to Figure 6, the proposed scheme offers reduced processing time compared to existing blockchain operations. It can be justified by seeking the inclusion of highly iterative and sophisticated blockchain operations in existing schemes. Such schemes have higher supportability in a centralized form, which increases the processing capacity when exposed to an extensive network.

Based on the obtained outcomes, the innovative features that are introduced in the proposed scheme to overcome the pitfalls of existing schemes are as follows.

(i) The proposed model has constructed a novel blockchain network using local and global parameters, which increases the operational security features against side-channel attacks in a more effective way compared to the existing research studies in blockchain that suffer from the pitfall of restricted security features [19]. (ii) The proposed scheme introduces a new node role called an auxiliary node, which acts as a bridge of communication between the global and local blockchain, considering direct access from the miner node. This facilitates a greater availability of data, as well as promoting secure data accessibility, leading to a scalable performance, unlike the existing blockchain scheme [39–48] that still suffers from the pitfalls of optimal scalable performance. (iii) The proposed scheme facilitates the verification of adjacent nodes as well as all other actors in a non-iterative way, which acts as a dual layer of security and increases the frequency of authentication suitable for an extensive dynamic network, unlike the existing approaches [39–64], which assess only single target nodes. (iv) The proposed scheme is capable of resisting differential fault attacks, power-based attacks, timing attacks and cache attacks, which opens up many opportunities for fighting multiple variants of side-channel attacks, whereas existing approaches [24–38] are reported to resist only singular forms of attack.

7. Conclusions

This study considers a use case of mobility inclusion within an IoT environment deploying secure data transmission using a decentralized Ethereum blockchain. From the study, it is clear that mobility inclusion in a large-scale network offers faster transmission, while it also invites a higher severity of threats from side-channel attacks. The environment becomes equivalent to a case study of heterogeneous multi-attacker circumstances with different variants of side-channel attacks in IoT. A review of existing approaches showcases security solution methodologies mainly targeting one specific variant of side-channel attack. Such deployment works well for small-scale networks, but not extensive ones, as the existing algorithm design is highly specific to attacks. Hence, the proposed system offers a novel solution that addresses this problem while balancing security and communication performance. The novel features exhibited by the proposed study model are as follows: (i) the proposed scheme offers extensive security coverage against identifying and resisting different types of power attacks, timing attacks, cache attacks, and differential attacks in the side channel in IoT; (ii) a branched and decentralized blockchain network is formulated, which maintains seamless and secure communication among mobile IoT devices and LAP with the assistance of three stages of security implementation of blockchain; (iii) the proposed system introduces an auxiliary node as well as LAP, which is capable of supervising the deployment and management of certification and authorization in an interoperable manner, unlike any existing blockchain scheme; (iv) the quantified outcome of the simulation study shows that the proposed scheme offers approximately 30% reduced energy consumption, 12% reduced latency, 21% increased throughput, 5% reduced computational overhead, and 4% reduced processing time in comparison to existing blockchain techniques.

The implications of the work could be further developed in the future towards accomplishing more gains in resisting more threats. One possible way to achieve this will be to develop a novel game model of unknown and heterogeneous adversaries. The problem's solution could be developed by developing a novel incentive scheme that could be computed using a discrete bio-inspired optimization principle. The outcome might further compensate for the computational burden and increase in security features using blockchain.

Author Contributions: Conceptualization, methodology, validation, writing review, and editing: B.U.I.K., R.F.O., K.W.G. and M.L.B.M.K.; formal analysis, investigation: K.W.G. and N.A.A.; writing—original draft preparation: B.U.I.K. and R.F.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been supported by the Ministry of Higher Education Malaysia through its Fundamental Research Grant Scheme under Grant ID FP071-2019A.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors express their appreciation for the efforts of Binyamin Adeniyi Ajayi, Zuriati Janin and M. Wajahat Hussain in proofreading and editing the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hassanien, A.E.; Dey, N.; Mahalle, P.N.; Shafi, P.M.; Kimabahune, V.V. *Internet of Things, Smart Computing and Technology: A Roadmap Ahead*; Springer International Publishing: Cham, Switzerland, 2020.
2. Kumar, A.; Balamurugan, B.; Chatterjee, J.M.; Raj, P. *Internet of Things Use Cases for the Healthcare Industry*; Springer International Publishing: Cham, Switzerland, 2020.
3. Murugesan, S.; Jain, S. *Smart Connected World-Technologies and Applications Shaping the Future*; Springer International Publishing: Cham, Switzerland, 2021.
4. Ismail, Y. *Internet of Things (IoT) for Automated and Smart Applications*; IntechOpen: London, UK, 2019.
5. Sun, J.; Han, G.; Wang, Y.; Liu, P. Memristor-based neural network circuit of emotion congruent memory with mental fatigue and emotion inhibition. *IEEE Trans. Biomed. Circuits Syst.* **2021**, *15*, 606–616. [[CrossRef](#)] [[PubMed](#)]

6. Sun, J.; Han, G.; Zeng, Z.; Wang, Y. Memristor-based neural network circuit of full-function Pavlov associative memory with time delay and variable learning rate. *IEEE Trans. Cybern.* **2020**, *50*, 2935–2945. [[CrossRef](#)] [[PubMed](#)]
7. Sun, J.; Wang, Y.; Liu, P.; Wen, S.; Wang, Y. Memristor-based neural network circuit with multimode generalization and differentiation on Pavlov associative memory. *IEEE Trans. Cybern.* **2022**, 1–12. [[CrossRef](#)] [[PubMed](#)]
8. Ghazal, T.M.; Hasan, M.K.; Alshurideh, M.T.; Alzoubi, H.M.; Ahmad, M.; Akbar, S.S.; Al Kurdi, B.; Akour, I.A. IoT for smart cities: Machine learning approaches in smart healthcare—A review. *Future Internet* **2021**, *13*, 218. [[CrossRef](#)]
9. Staddon, E.; Loscri, V.; Mitton, N. Attack categorisation for IoT applications in critical infrastructures, a survey. *Appl. Sci.* **2021**, *11*, 7228. [[CrossRef](#)]
10. Balogh, S.; Gallo, O.; PLoSzek, R.; Špaček, P.; Zajac, P. IoT security challenges: Cloud and blockchain, postquantum cryptography, and evolutionary techniques. *Electronics* **2021**, *10*, 2647. [[CrossRef](#)]
11. Sharma, G.; Vidalis, S.; Anand, N.; Menon, C.; Kumar, S. A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open-issues. *Electronics* **2021**, *10*, 2365. [[CrossRef](#)]
12. Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. Cyber threats to industrial IoT: A survey on attacks and countermeasures. *IoT* **2021**, *2*, 9. [[CrossRef](#)]
13. Méndez Real, M.; Salvador, R. Physical side-channel attacks on embedded neural networks: A survey. *Appl. Sci.* **2021**, *11*, 6790. [[CrossRef](#)]
14. Hong, S. *Side Channel Attacks*; MDPI Books: Basel, Switzerland, 2019.
15. Dogruluk, E.; Macedo, J.; Costa, A. A countermeasure approach for Brute-Force timing attacks on cache privacy in named data networking architectures. *Electronics* **2022**, *11*, 1265. [[CrossRef](#)]
16. Randolph, M.; Diehl, W. Power side-channel attack analysis: A review of 20 years of study for the layman. *Cryptography* **2020**, *4*, 15. [[CrossRef](#)]
17. Lo, O.; Buchanan, W.J.; Carson, D. Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA). *J. Cyber Secur. Technol.* **2016**, *1*, 88–107. [[CrossRef](#)]
18. Azizi, N.; Malekzadeh, H.; Akhavan, P.; Haass, O.; Saremi, S.; Mirjalili, S. IoT–Blockchain: Harnessing the power of Internet of Thing and blockchain for smart supply chain. *Sensors* **2021**, *21*, 6048. [[CrossRef](#)] [[PubMed](#)]
19. Shahbazi, Z.; Byun, Y.C. Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. *Sensors* **2021**, *21*, 1467. [[CrossRef](#)]
20. Gardas, B.B.; Heidari, A.; Navimipour, N.J.; Unal, M. A fuzzy-based method for objects selection in blockchain-enabled edge-IoT platforms using a hybrid multi-criteria decision-making model. *Appl. Sci.* **2022**, *12*, 8906. [[CrossRef](#)]
21. Heidari, A.; Jabrael Jamali, M.A.; Jafari Navimipour, N.; Akbarpour, S. Deep Q-learning technique for offloading offline/online computation in Blockchain-enabled green IoT-edge scenarios. *Appl. Sci.* **2022**, *12*, 8232. [[CrossRef](#)]
22. Jafar, U.; Aziz, M.J.A.; Shukur, Z. Blockchain for electronic voting system—Review and open research challenges. *Sensors* **2021**, *21*, 5874. [[CrossRef](#)]
23. Srinivasu, P.N.; Bhoi, A.K.; Nayak, S.R.; Bhutta, M.R.; Woźniak, M. Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network. *Electronics* **2021**, *10*, 1437. [[CrossRef](#)]
24. Kwon, D.; Hong, S.; Kim, H. Optimizing implementations of non-profiled deep learning-based side-channel attacks. *IEEE Access* **2021**, *10*, 5957–5967. [[CrossRef](#)]
25. Le, A.T.; Hoang, T.T.; Dao, B.A.; Tsukamoto, A.; Suzuki, K.; Pham, C.K. A real-time cache side-channel attack detection system on RISC-V out-of-order processor. *IEEE Access* **2021**, *9*, 164597–164612. [[CrossRef](#)]
26. Mukhtar, N.; Fournaris, A.P.; Khan, T.M.; Dimopoulos, C.; Kong, Y. Improved hybrid approach for side-channel analysis using efficient convolutional neural network and dimensionality reduction. *IEEE Access* **2020**, *8*, 184298–184311. [[CrossRef](#)]
27. Moini, S.; Tian, S.; Holcomb, D.; Szefer, J.; Tessier, R. Power side-channel attacks on BNN accelerators in remote FPGAs. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2021**, *11*, 357–370. [[CrossRef](#)]
28. Ghandali, S.; Ghandali, S.; Tehranipoor, S. Deep K-TSVM: A novel profiled power side-channel attack on AES-128. *IEEE Access* **2021**, *9*, 136448–136458. [[CrossRef](#)]
29. Ng, J.S.; Chen, J.; Chong, K.S.; Chang, J.S.; Gwee, B.H. A highly secure FPGA-based dual-hiding asynchronous-logic AES accelerator against side-channel attacks. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2022**, *30*, 1144–1157. [[CrossRef](#)]
30. Vuppala, S.; Mady, A.E.D.; Kuenzi, A. Moving target defense mechanism for side-channel attacks. *IEEE Syst. J.* **2019**, *14*, 1810–1819. [[CrossRef](#)]
31. Ghosh, A.; Nath, M.; Das, D.; Ghosh, S.; Sen, S. Electromagnetic analysis of integrated on-chip sensing loop for side-channel and fault-injection attack detection. *IEEE Microw. Wirel. Compon. Lett.* **2022**, *32*, 784–787. [[CrossRef](#)]
32. Jevtic, R.; Otero, M.G. Methodology for complete decorrelation of power supply EM side-channel signal and sensitive data. *IEEE Trans. Circuits Syst. II Express Briefs* **2022**, *69*, 2256–2260. [[CrossRef](#)]
33. Liu, W.; Wang, R.; Qi, X.; Jiang, L.; Jing, J. Multiclass classification-based side-channel hybrid attacks on strong PUFs. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 924–937. [[CrossRef](#)]
34. Ensan, S.S.; Nagarajan, K.; Khan, M.N.I.; Ghosh, S. SCARE: Side Channel Attack on In-Memory Computing for Reverse Engineering. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2021**, *29*, 2040–2051. [[CrossRef](#)]
35. Kim, T.; Shin, Y. ThermalBleed: A practical thermal side-channel attack. *IEEE Access* **2022**, *10*, 25718–25731. [[CrossRef](#)]

36. Antognazza, F.; Barenghi, A.; Pelosi, G. Metis: An integrated morphing engine CPU to protect against side channel attacks. *IEEE Access* **2021**, *9*, 69210–69225. [[CrossRef](#)]
37. Ha, G.; Chen, H.; Jia, C.; Li, M. Threat model and defense scheme for side-channel attacks in client-side deduplication. *Tsinghua Sci. Technol.* **2023**, *28*, 1–12. [[CrossRef](#)]
38. Kulow, A.; Schamberger, T.; Tebelmann, L.; Sigl, G. Finding the needle in the haystack: Metrics for best trace selection in unsupervised side-channel attacks on blinded RSA. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3254–3268. [[CrossRef](#)]
39. Liu, H.; Han, D.; Li, D. Fabric-IoT: A blockchain-based access control system in IoT. *IEEE Access* **2020**, *8*, 18207–18218. [[CrossRef](#)]
40. Hasan, H.R.; Salah, K.; Yaqoob, I.; Jayaraman, R.; Pesic, S.; Omar, M. Trustworthy IoT data streaming using blockchain and IPFS. *IEEE Access* **2022**, *10*, 17707–17721. [[CrossRef](#)]
41. Rodrigues, C.K.D.S.; Rocha, V. Towards blockchain for suitable efficiency and data integrity of IoT ecosystem transactions. *IEEE Lat. Am. Trans.* **2021**, *19*, 1199–1206. [[CrossRef](#)]
42. Zhou, J.; Feng, G.; Wang, Y. Optimal deployment mechanism of blockchain in resource-constrained IoT systems. *IEEE Internet Things J.* **2022**, *9*, 8168–8177. [[CrossRef](#)]
43. Ren, J.; Li, J.; Liu, H.; Qin, T. Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. *Tsinghua Sci. Technol.* **2022**, *27*, 760–776. [[CrossRef](#)]
44. Xu, C.; Qu, Y.; Luan, T.H.; Eklund, P.W.; Xiang, Y.; Gao, L. A lightweight and attack-proof bidirectional blockchain paradigm for Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 4371–4384. [[CrossRef](#)]
45. Alrubei, S.M.; Ball, E.; Rigelsford, J.M. A secure blockchain platform for supporting AI-enabled IoT applications at the Edge layer. *IEEE Access* **2020**, *10*, 18583–18595. [[CrossRef](#)]
46. Hao, X.; Yeoh, P.L.; Ji, Z.; Yu, Y.; Vucetic, B.; Li, Y. Stochastic analysis of double blockchain architecture in IoT communication networks. *IEEE Internet Things J.* **2022**, *9*, 9700–9711. [[CrossRef](#)]
47. Whaiduzzaman, M.; Mahi, M.J.N.; Barros, A.; Khalil, M.I.; Fidge, C.; Buyya, R. BFIM: Performance measurement of a blockchain based hierarchical tree layered fog-IoT microservice architecture. *IEEE Access* **2021**, *9*, 106655–106674. [[CrossRef](#)]
48. Ullah, Z.; Raza, B.; Shah, H.; Khan, S.; Waheed, A. Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment. *IEEE Access* **2022**, *10*, 36978–36994. [[CrossRef](#)]
49. Qu, Y.; Pokhrel, S.R.; Garg, S.; Gao, L.; Xiang, Y. A blockchained federated learning framework for cognitive computing in Industry 4.0 networks. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2964–2973. [[CrossRef](#)]
50. Qiu, C.; Wang, X.; Yao, H.; Du, J.; Yu, F.R.; Guo, S. Networking integrated cloud–edge–end in IoT: A blockchain-assisted collective Q-learning approach. *IEEE Internet Things J.* **2021**, *8*, 12694–12704. [[CrossRef](#)]
51. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Dehghantanha, A.; Choo, K.K.R. FabricFL: Blockchain-in-the-Loop Federated Learning for trusted decentralized systems. *IEEE Syst. J.* **2022**, *16*, 3711–3722. [[CrossRef](#)]
52. Miao, Y.; Liu, Z.; Li, H.; Choo, K.K.T.; Deng, R.H. Privacy-preserving Byzantine-robust federated learning via blockchain systems. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 2848–2861. [[CrossRef](#)]
53. Weng, J.; Weng, J.; Zhang, J.; Li, M.; Zhang, Y.; Luo, W. DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 2438–2455. [[CrossRef](#)]
54. Qin, Z.; Ye, J.; Meng, J.; Lu, B.; Wang, L. Privacy-preserving blockchain-based federated learning for marine Internet of Things. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 159–173. [[CrossRef](#)]
55. Shahbazi, Z.; Byun, Y.C. Blockchain-based event detection and trust verification using natural language processing and machine learning. *IEEE Access* **2022**, *10*, 5790–5800. [[CrossRef](#)]
56. Peng, Z. VFChain: Enabling verifiable and auditable federated learning via blockchain systems. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 173–186. [[CrossRef](#)]
57. Sun, J.; Wu, Y.; Wang, S.; Fu, Y.; Chang, X. Permissioned blockchain frame for secure federated learning. *IEEE Commun. Lett.* **2022**, *26*, 13–17. [[CrossRef](#)]
58. Ayaz, F.; Sheng, Z.; Tian, D.; Guan, Y.L. A blockchain-based federated learning for message dissemination in vehicular networks. *IEEE Trans. Veh. Technol.* **2022**, *71*, 1927–1940. [[CrossRef](#)]
59. Li, J.; Niyato, D.; Hong, C.S.; Park, K.-J.; Wang, L.; Han, Z. Cyber insurance design for validator rotation in sharded blockchain networks: A hierarchical game-based approach. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 3092–3106. [[CrossRef](#)]
60. Feng, S.; Wang, W.; Xiong, Z.; Niyato, D.; Wang, P.; Wang, S.S. On cyber risk management of blockchain networks: A game theoretic approach. *IEEE Trans. Serv. Comput.* **2021**, *14*, 1492–1504. [[CrossRef](#)]
61. Guo, S.; Dai, Y.; Guo, S.; Qiu, X.; Qi, F. Blockchain meets edge computing: Stackelberg game and double auction based task offloading for mobile blockchain. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5549–5561. [[CrossRef](#)]
62. Kruminis, E.; Navaie, K. Game-theoretic analysis of an exclusively transaction-fee reward blockchain system. *IEEE Access* **2022**, *10*, 5002–5011. [[CrossRef](#)]
63. Zhang, M.; Eliassen, F.; Taherkordi, A.; Jacobsen, H.A.; Chung, H.-M.; Zhang, Y. Demand–response games for peer-to-peer energy trading with the Hyperledger blockchain. *IEEE Trans. Syst. Man Cybern. Syst.* **2022**, *52*, 19–31. [[CrossRef](#)]
64. Jiang, S.; Li, X.; Wu, J. Multi-leader multi-follower Stackelberg game in mobile blockchain mining. *IEEE Trans. Mob. Comput.* **2022**, *21*, 2058–2071. [[CrossRef](#)]
65. Arena, F.; Pau, G.; Severino, A. A review on IEEE 802.11p for intelligent transportation systems. *J. Sens. Actuator Netw.* **2020**, *9*, 22. [[CrossRef](#)]

-
66. Ahn, J.; Kim, Y.Y.; Kim, R.Y. A novel WLAN Vehicle-To-Anything (V2X) channel access scheme for IEEE 802.11p-based next-generation connected car networks. *Appl. Sci.* **2018**, *8*, 2112. [[CrossRef](#)]
 67. Zanaj, E.; Caso, G.; Nardis, L.D.; Mohammadpour, A.; Alay, O.; Benedetto, M.G.D. Energy efficiency in short and wide-area IoT technologies—A survey. *Technologies* **2021**, *9*, 22. [[CrossRef](#)]