Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

ICASET
2024

Research Article
Collection: Intelligent Computing of Applied Sciences and Emerging Trends

Architecting Secure, Scalable, Lightweight Block Chains for IoT-Driven Smart Buildings using Direct Acyclic Graphs and Smart Contracts

Syed Irfan Raza Naqvi[1*], Zheng Jiang Bin[1], Ahmad Mohsin[2], Muhammad Pervaz Akhter[3], and Ali Mustafa[4]

[1]School of Software, Northwestern Polytechnical University, Xian, China.
[2]Cyber Security research Institute, Edith Cowan University, Australia.
[3]Deparment of Computer Science, National University of Modern Languages (NUML), Faisalabad, Pakistan.
[4]Department of Computer Science, Air University, Pakistan.
[*]Corresponding Author: Syed Irfan Raza Naqvi. Email: irfanrazanaqvi9@gmail.com

Academic Editor: Salman Qadri **Published:** April 01, 2024

Abstract: Connected Smart Buildings (SBDs) in distributed networks with the Internet of Things (IoT) provide automated building monitoring, and control. However, IoT offers distinct security and scalability issues. IoT systems with centralized client-server architectures may have scalability and privacy vulnerabilities owing to increased interactions and dependencies. Distributed Ledger Technology DLT can be incorporated across architectural layers to solve these problems. Block Chain Technology (BCT), like Bitcoin (BTC) and Ethereum, can solve numerous IoT issues. IoT device's computing capabilities are too low for resource-intensive block chain consensus; scalability, security, and transaction costs must be improved in blockchain solutions. IOTA, a distributed ledger based on Direct Acyclic Graph technology, is emerging as a potential solution. However, current IOTA Blockchain-based techniques have limitations to address these challenges. To optimize IoT systems further, we introduce the scalable, lightweight distributed blockchain for IoTs (SLDBI) approach, which harnesses the DAG-based Tangle and implements a lightweight message data model. The SLDBI approach addresses IoT device limitations and streamlines integration across diverse domains. It improves system security with enhanced access controls, energy efficiency, and scalability within IoT ecosystems. This is achieved by employing the Masked Authentication Message (MAM) protocol and the IOTA Smart Contract Protocol (ISCP). Our technique introduces an energy-efficient proof-of-work (PoW) computation approach throughout the entire node. Using a case study approach for Smart Building Devices (SBDs), we conducted experiments and analysis that proved the effectiveness of the SLDBI approach. This approach offers improved security and scalability while maintaining energy efficiency. With SLDBI, granular user access control can be easily managed, and the system can seamlessly scale across expansive networks, encompassing smart buildings comprising numerous IoT nodes.

Keywords: Direct Acyclic Graph (DAG); Blockchain; Internet of Things; Intelligent Buildings; Scalability; Privacy.

1. Introduction

IoT-based intelligent systems have advanced in manufacturing, AI-driven commercial systems, supply chain optimization, asset tracking, smart city infrastructure, digital agriculture, and daily life [1]. By 2030, the number of active IoT devices is expected to reach 25.4 billion, according to forecasts [2]. The billions of connections between these gad- gets will generate 180 zettabytes of world data annually. IoT is also changing smart buildings (SBDs) connectivity that al- lows HVAC, waste management, lighting, and everyday job automation to be controlled and monitored. However, these heterogeneous developments of IoTs-based SBDs introduce substantial challenges. Traditional architectural approaches and technologies are inadequate to address these challenges. Utilizing a centralized architecture model in IoT systems raises privacy concerns, including unauthorized access and authentication issues. Ensuring security in SBDs involves several crucial aspects. One of the critical concerns is the presence of a Single Point of Failure (SPoF), where a central server manages all the processing and communication among multiple IoT devices. The failure of such a central server can significantly affect the availability and quality ofservice [3].

Storing all data in one place can increase the risk of security breaches. Moreover, the growing numberof IoT devices, particularly in SBDs, highlights the limitations of the centralized architecture model in terms of scalability and performance [4]. Despite these challenges, finding a solution to these issues while ensuring data security remains a top priority. When designing resource-constrained SDBs, operational issues can arise if importantquality attributes like scalability and security are not considered early on. There are various techniques to tackle these challenges, but integrating a Blockchain-based solution into IoTs appears to hold promise. Distributed Ledger Technology (DLT), particularly Blockchain, has displayed itspotential in IoT applications such as artificial intelligence, energy grids, intelligent transport systems, drug supply chains, e-healthcare, innovative vehicles, and parking systems [5]. Blockchain can effectively address security, accesscontrol, and data integrity issues within the IoT landscape. However, the success of a Blockchain-enabled IoT system depends heavily on its underlying consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS) [6].

Traditional Blockchain consensus mechanisms come with computational overheads, highlighted by the staggering annual electricity consumption of 70TWh by Bitcoin (BTC) miners worldwide. This makes them impractical for IoTdevices with limited resources. Additionally, existing IoT systems suffer from scalability and user access management issues due to their client-server architecture, traditionalBlockchain transparency, slow block generation rates, and complex consensus procedures. The emergence of IOTA Tangle, a third-generation DLT, has created new and optimized blockchain techniques, particularly for IoT and blockchain integrations in complexsystems. IOTA Tangle utilizes a revolutionary block less, tree-based architecture based on the Direct Acyclic Graph (DAG) structure. This architecture is specially designed to overcome the limitations of traditional blockchain technology. This innovative design stores transactions within a DAG, simplifying verification by involving just two prior transactions and a modest computational effort. This unique approach allows for parallel execution and attachment at any point within Tangle [7].

This results in a system that eliminates confirmation delays and scalability bottlenecks, making it highly efficient and scalable. Our research article introduces a new energy-efficient architectural innovation called" Scalable Lightweight DAG-based Blockchain Design for Intelligent IoT Systems" (SLDBI). To enhance SLDBI's security in managing access within IoT contexts, we introduce a lightweight message data model that optimizes Masked Authenticated Messaging (MAM) and IOTA Smart Contract Protocol (ISCP) with a consensus approach. To evaluateits effectiveness within the IOTA Tangle framework, weanalyze the impact of network load on achieving DAG consensus among nodes using a Markov chain model (MCMC). In this paper, we present a proof-of-concept case study highlighting the potential of SLDBI to improve scalability inIoT applications, such as SBDs. Our study revealed that the SLDBI approach stands out regarding access management efficiency, system scalability, and resource utilization. This results in a significant enhancement of system performance and security. To summarize, the main contributions of this paper are:

- A DAG-based blockchain architecture deploys a lightweight message model and IOTA Smart Control Protocol (ISCP) for SBDs, optimizing IoT resources and enhancing access control.

- Incorporating highly distributed IoT sensors, connected via scalable technology, to optimize energy consumption with an improved proof-of-work mechanism in IOTA Tangle.
- Improving overall system performance and security of SDBs using lightweight IOTA algorithm with an improved version of underlying intelligent smart con- tracts development.

Our innovation combines DAG Blockchain to achievescalability and security goals while IOTA nodes efficiently manage and optimize IoT energy. The paper is structured as follows: we discuss the foundational DLTs such as Blockchain and IOTA. Then, we conduct an extensive literature review and delve into the DLT Tangle, coveringtransaction mechanisms and security techniques. Our main contribution is developing the SLDBI technique, which we describe in detail. This includes an examination of its underlying architecture, constituent components, design ofnew algorithms, and their applicability in the context of smartbuildings. We present a carefully designed case study,results, and insightful analysis to validate our approach. Finally, we acknowledge limitations and suggest potential avenues for future research, providing a comprehensiveconclusion to the paper.

2. Preliminaries

This section provides an overview of the concepts related to Distributed Ledger Blockchain Technology used in the paper. We also discuss the challenges of integrating Blockchain with IoTs and explore how DAG blockchain technologies can enhance IoT architecture to improve security and performance. Distributed Ledger Technology (DLT) has attracted alot of attention from researchers due to its decentralized, tamper-proof, and publicly verifiable features. DLTs are preferred over centralized systems because they prevent SPoFand privacy issues. Depending on the data structure, there are primarily three types of DLT: Blockchain, IOTA Tangle (DAG), and Hash graph [8]. Blockchain is a fundamental protocol for cryptocurrencies like Bitcoin (BTC), initially suggested by Satoshi Nakamoto in 2008 as the first practicable application [3] [7]. The blocks are connected by referencing the preceding block, creating a chain.

The blockchainensures accurate and secure transactions by using consensus algorithms and smart contracts to prevent unauthorized users from mining. Its key features include decentralization, immutability, consensus process, smart contracts, and cryptography. There are three types of blockchains categorized by their applications and requirements [4] [9]: Public, Private, and Hybrid Blockchain.

2.1. Challenges and Motivation: Integrating IoT and Block Chain:

When incorporating Blockchain into IoT, several obstacles arise, including scalability, interoperability, compatibility, developments in quantum computing, user identity tracking, and energy efficiency [9]. Here are some challenges thatcome up when integrating IoT with Blockchain technology:

- **Scalability:** The growing size of the Blockchain as moredevices connect can pose a challenge for IoT networks. Additionally, current Blockchain implementations may not be able to process enough transactions per second,creating a bottleneck for the IoT.
- **Security and Privacy:** The 51 percent attack is a typicalsecurity threat to the Bitcoin protocol, where a participant controls more than 51 percent of mining power, allowing them to manipulate the network's consensus [7]. Double spending attacks and high mining fees are well-known drawbacks of using blockchain in IoT.
- **Limited throughput:** The Traditional Blockchain structures are single chains based on sequential ledgers where each block is added one after another. Single block generation rate causes limited throughput and an increase in conformation delay [9] [10]. The throughput of Blockchain describes the number of published transitions per second (TPS) that would be limited to a dozen, e.g., 7-8 TPS in Bitcoin, and Ethereum has 20-30 TPS [11].
- **Consensus and resource utilization**: IoT devices have limited computing abilities and low power consumption, making complex consensus mechanisms inappropriate for their scenarios [3]. Resources must be carefully allocated to reach an agreement in these situations.

- **Trustworthiness:** Collecting various data from diverse networks in an IoT setup poses challenges in ensuring trustworthy data and device operations, such as data aggregation and processing [1]. It is essential to have measures in place to manage and coordinate the trust- worthiness of data for users.

Table 1. IoT Integration Blockchain Challenges

Challenges	**IoT**	**Blockchain**
Scalability	IoT contains a Billion devices	Scale Poorly with large Network
Energy consumption	Limited Resources	Resource Consuming heavyweight consensus
Bandwidth and Latency	Demand low Latency and Limited Bandwidth	Block Mining is time- consuming
Access control	Lack of access management	Ensures access control

Table 1 summarizes the challenges of integrating blockchain with IoT. Despite these challenges, a team of researchers and developers are working to unleash the full potential of blockchain technology in IoT.

2.2. Internet-of-Things Association (IOTA)

IOTA is a third-generation DLT that utilizes a Directed Acyclic Graph (DAG) to depict transactions rather than a Blockchain. It is constructed on a foundational data structure known as Tangle. IOTA was created in 2015 by David Sonstebo, Serguei Popov, Sergey Ivancheglo, and Dominik Schiener [12]. IOTA transactions are stored in a DAG by attaching some computational work and verifying two previous transactions, thus eliminating the confirmation time limit and scalability issues [8]. It uses light proof of workto prevent network spamming rather than securing transactions. As a result, proof of work is no longer a computation race and is not energy-intensive [2].

2.2.1 The DAG (Direct Acyclic Graph) Structure

In the Directed Acyclic Graph (DAG) design, user transactions are considered a site within the tangle graph. These transactions store important details like timestamps, digital signatures, hash values, and message payloads. The transactions are propagated through the nodes. A new transaction that has not been confirmed yet is called a"tip" [10]. During each round, a transaction can establish one or moreunconfirmed transactions by choosing two parents within the DAG. When a transaction is directly approved by its parents, it is confirmed. If a multi-hop path exists between two transactions, indirect confirmation is considered.

InFigure1, each transaction has a weight in the lower right cornerand a cumulative weight in the upper left corner. The weightof transactions F and G are 3 and 1, respectively, indicating that the node initiating transaction F has a more excellent PoW than the node initiating transaction H. Transaction F has a cumulative weight of 14, which is calculated by adding the consequences of all the transactions that reference it either directly or indirectly.

For example, transaction G is directly referenced once by transactions A and E and indirectly referenced once by transaction D and twice by transactions B and C. The cumulative weight represents the trust of the entire network in the transaction. When a transaction's cumulative weight is high enough, it can be confirmed with a high probability.

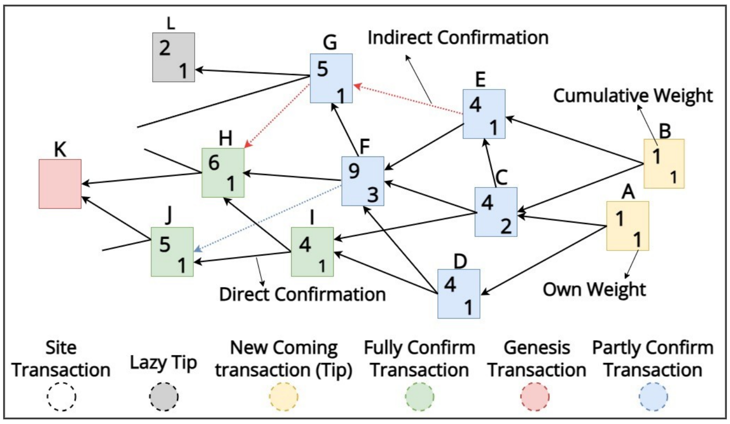


Figure 1. DAG Consensus mechanism with weight assignments before and after a newly coming transaction A and B. (boxes represent transactions)

The Markov Chain Monte Carlo (MCMC) tip selection algorithm (TSA) is an essentialelement of the Tangle [13]. It ensures that new transactions are selected over previously approved ones when attached to the Tangle graph, facilitating timely approval of non- approved transactions.

3. Related Work

We conducted a literature review on DAG-based DLT for privacy and scalability, analyzing various proposed blockchain-based methods and their pros and cons for IoT applications and SBDs.

Recent research papers have been published due to the increasing popularity of blockchain in smart homes. DAG- based distributed ledger technology, with its high concurrency of the graph structure, is the most promising solution for improving blockchain scalability. Different approaches for achieving consensus and system security in DAG-based blockchain paradigms exist. For instance, in Tangle, Proof of Work (PoW) is used for consensus, while the Markov chain Monte Carlo (MCMC) algorithm selects parent nodes for new transactions and forms the DAG. Byte ball, on the other hand, relies on witnesses elected by the community and acting as marshals to enforce the main chain rule for consensus and system security. Hash graph, proposed by Baird in 2016, employs a different mechanism using RGP forcommunication and virtual voting to achieve asynchronousByzantine fault tolerance (ABFT) consensus.

Denis et al. [2], an attribute-based usage control, demonstrates DLT advantages for IoT, including cost reduction, network distribution, and DAG-based DLTs with cost- effective transactions, high throughput, and disintermediation benefits. Lang li et al. [14], DBAG proposes an efficientDAG blockchain architecture. It uses a tree-based gossip protocol (TBGP) to improve consensus efficiency and reduce message redundancy. However, the number of events in DBAG is fixed and does not increase. S. Wang et al. [15], a new solution is presented for managing the identities of IoTdevices and authorizing large-scale data access. Unlike the current PKI and Blockchain-based schemes with scalabilityand single-point failure concerns, the proposed solutionutilizes DAG-based distributed ledger technology, specifically IOTA. This offers improved identity management and authorization for accessing IoT devices. Nakanishi et al. [16] provide a revolutionary access control and privacy system that uses IOTA, a technology that enables quick and cost-free micro transactions. Access rights are encrypted using Cipher text-Policy Attribute-Based Encryption (CP- ABE) and stored on IOTA's Tangle distributed ledger to allow flexible and granular access control. However, the scalability of the suggested system may be assessed with more nodes. Mohanty et al. [17] introduce a model called Efficient and Lightweight Integrated Blockchain (ELIB) for IoT systems. The model incorporates blockchain, cloud storage, and smart contracts, and was tested in smart homes to evaluate its performance. Although ELIB successfully decreased the time required to process transactions and performed well, it also resulted in an overall increase in the system's cost. In a paper Lee et al, [18] present a smart home solution based on the Ethereum blockchain. This solution aims to tackle confidentiality, integrity, and authentication issues that arise with IoT devices. The pro-posed design also addresses concerns around centralized gateways. However, it does not fully address the additional computational complexities that blockchain technology cancreate. Fan et al, [19] a comprehensive DAG-based solutionto creating scalable and approved transaction spaces within smart communities has been presented. However, there is room to increase decentralization and throughput.

It is worth mentioning that a blockchain-based platform can efficiently handle various issues. By using the DAG blockchain, we can take a step forward in building a robustdistributed secure, and lightweight system that can over- come many of the challenges associated with centralized SBDs. These challenges include a single entity calculating access control policies, access rights, and scalability. In the following section, we will explain how the DAG feature of the blockchain addresses these IoT security and privacy issues.

4. SLDBI: A Scalable, Lightweight DAG- Based Blockchain Design for Intelligent IOT Systems

We aim to develop an efficient and scalable system that utilizes IOTA Tangle and smart contracts in the SLDBI approach. In Section 4.1, we provide an overview of the SLDBI architecture. Section 4.2 delves into the MAM consensus mechanism and message model design using ISCP, while section 4.3 explains the access control management mode.Finally, section 4.4 covers the security procedures and goals.

4.1. SLDBI: System Architecture

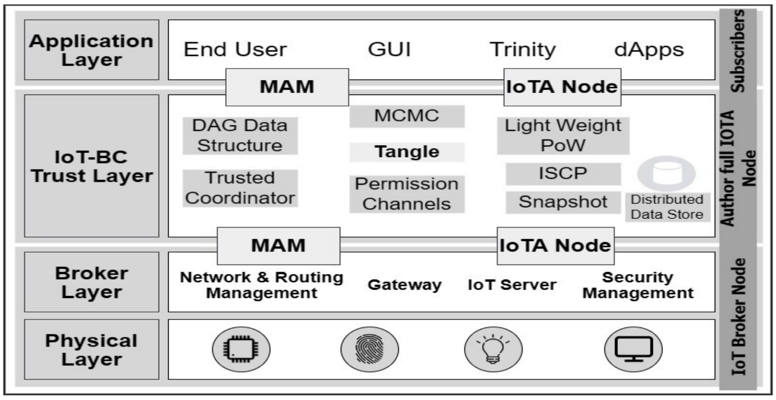


Figure 2. Proposed SLDBI Layered Architecture design for IoTs

Figure 3 displays the SLDBI module's suggested design. Four distinct levels in this design allow for the simple addition or replacement of modules without changing the overall structure. Sensors, zero-level IoT devices, and data providers are all part of the physical layer. Both power usage and data storage capacity are constrained in this tier. A smart device or single-board computer controls the Broker layer, handling security and communication. It uses theMAM and IoTA nodes to interface with the higher layer. TheTangle DAG-based DLT, MAM protocol, PoW consensus, Trusted Coordinator, TSA, and IOTA smart contract protocol(ISCP) are among the standard services the IoT-Blockchaintrust layer arranges. A local or remote PC linked to the entire IOTA node sends and receives all data. The client libraries and API interface show off the capabilities of the IOTA network. The web interface is accessible and controllable bythe client application layer. Subscribers or data consumers access public data from Tangle, most of which is encrypted for protection. Authorized access is necessary to decode the data.

4.2. Bundle Message Format and Data Model

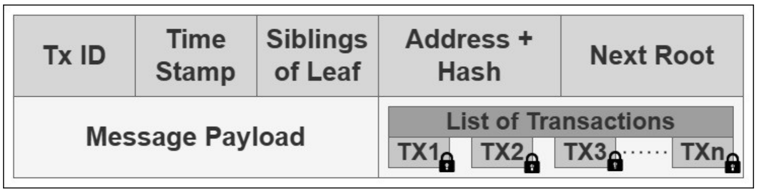


Figure 3. SLDBI Bundle Message Format

As shown in Figure 3, a whole MAM transaction bundle is divided into the MM (masked message) and MSS (Merkle signature scheme). A Masked Message comprises raw data, such as the message payload (payload$_m$) that must be communicated, the index of the selected leaf with its siblings, the Timestamp, and the following root address. While the transaction direction of *n* ‑1 ppriormessageq is unclear, MM must transfer and link to the succeeding message where each transaction n has a pointer *n* 1 pfuturemessageq [20].

4.2.1 Message Data Model

We assume that there are two main participants in every Message model, which are as follows:

- Data author utilizing subscript utilizing pDaq publish its data through the MAM channel modes pCiDq.
- Data Subscribers pDrq are interested receivers, through the specific channel to get authorized data access by utilizing permission key pPKq such as for encryption key pPKeq and decryption key qPKdq respectively.

1) ppayloadmq " pTdq | | pSdq | | pAdq
2) pTdq " pTidq | | pAuthoridq | | pSubscriberidq
3) pSdq " pSidq | | pCidq | | pDeviceidq | | timestamp

4) pAdq ” pCidq | | pSrc, time, Dtnidq | | pEidq | |p Optfield q

The raw data referred to here as the message payload p$Payload_m$q consists of transaction data pT_d q, sensor data pS_dq , and author data pA_dq as shown in equation.1. Transaction data T_d consist of transaction detailed information as described in equation.2. Whereas equation.3 refers to Sensor data pS_dq with sensor ID p*Sid*q allocated to each sensor, Channel ID p*Cid*q publishing the sensor data such as temperature and humidity including pDeviceidq and timestamp. We utilize this message model (eq2 andeq3) in data published by the author in Algorithm 2. Dataretrieved by subscribers is detailed in section 5.3a as explained in Algorithm 3 of section 5.3b. IOTA smart contractprotocol (ISCP) is proposed to allow authorized data accessto subscribers for a limited time, as algorithum.1 of section 4.3 explains.

4.3. Message Data Model

Table 2. SLDBI permission and Access Control Management

Permission access control	Address	Write	Join and Read	Ownership verification
Permission less	Root(Channel Id)	Author (owner)	Any	Any
Permissions	Hash (root)	Author (owner)	Private	Private
Restricted	Hash (root+ pk)	Author (owner)	Authorized	Authorized

IOTA transactions are condensed into Masked Authentication Messages (MAM) using the Merkle Signature Scheme (MSS) and One-Time Signature (OTS). MAM facilitates data exchange, cryptography, and authorized data flow. It uses three access management modes: Permission-less, Permissioned, and Restricted as explained in table 2. In permission less mode, any user with an address containing thesame root channel ID can access public announcements. Permissioned mode is used for a higher level of security, allowing only the seed owner to access messages [21]. Restricted mode requires root and permission keys; only the source and permission key can access messages.

4.3.1. Message Data Model

Smart contracts using ISCP can enhance privacy between IoT nodes, manage access control in SBDs, and automate permission rules. This helps save time and money, but the implementation method is offline, regardless, and limited to a small number of nodes [21]. This implementation is necessary for the IoT industry and does not strain the rest of the network.

Access policy (AP) using Smart Contract: The author node has two primary responsibilities. Firstly, it sets up the sub- scriber access policy. Secondly, it keeps Tangle updated. To verify the author’s identity and decrypt the private key, the policy contract relies on the public key known as promise ().

Moreover, a smart contract automatically denies subscriber authorization after a certain amount of time. The model forsubscriber access and control policy follows this structure:

- **Policy p P q:** It reflects a strategy of assigned ownership of entry. Three elements are included in this set: SA, PA, and T. Policy pPq “SA, PA, T.
- **Subscriber (SA):** It reflects subscriber attributes and consists of two types: rootaddress pCidq and decryptionkey pPkdq, which the author gives.
- **Permission (PA):** This field shows if the subscriber can access the source. 1 allows access, and 0 denies it. The default is 1. Admins can set AP to 0 during initialization to revoke access. Permission (PA) = {1=allow, 0=deny}.
- **Time*(T)*:** In the masked message data model, time is represented by start time, end time, and De-vice ID. The end time attribute represents the policy expiration time. Access is only granted to authorize IDs and blocked for IPs outside the network segment. $Timestamp$ pT q ʺ{$startTime$pT_sq, $endTime$pT_eq, $Device$pd_{id}q}.

Algorithm 1. Permission access policy

Input: access request

```
**Output:** allow or deny
1:  p SA, PA, T q Đ Query Policy  p P q
2:   for isOK = Allowed do
3:   for Value in SA do:
4:   ifvalue Cid, Pkd then
5:   isOK = Deny
6:   If end
7:  if Val p PA q! =1 or 0 isOK = Deny
8:   If end
9:   for Value in T do:
10:  ifvalue Ts, Te, Did, then
11:  isOK = Deny
12:  If end
13:  If for
14:  return isOK
```

Algorithm 1 describes the operation of the ISCP, whichis designed for interacting with IoT nodes. When an access request is received from an IoT node, a signal is sent to approve or deny access. The first phase of the algorithm includes embedding information about policy, authorization, and time, while the second step uses flags to confirm permission. Steps 3 through 7 involve iterative operations that check keys for permissions and steps 8 through 11 illustrate access controls for permissions. Time-based access verification is completed in steps 12 through 16 and is contained in a smart contract with the ID of each IoT node.In a recent webinar, it was explained how to construct and manage DAG-based Blockchain-oriented systems to guarantee a variety of system functional and non-functional attributes at runtime. The following section will discuss important system aspects like scalability, performance, and energy efficiency.

4.4. Security Goals

The DAG-based Blockchain system uses virtual voting for security and efficient algorithm execution. Using the gossip protocol, MAM offers an encrypted data stream on the tangle through channel functions. SLDBI system uses MSS and TSA for safe access control management and to protect against double-spending attacks. It leverages the IOTA tangle and DAG consensus method.

- **Decentralization:** The SLDBI architecture's trusted coordinator mechanism selects the distributed IOTA full nodes randomly receiving milestones. This ensures that the con- sensual regulations are maintained [10]. Other nodes create milestones to validate the transactions in a node failure or crash. This scalable distributed architecture improves the system's resilience to unexpected failures and cyberattacksby reducing the probability of centralization and SPOF.
- **Access control rights:** A robust message model and ISCP implementation are crucial to maintaining access to **future** messages. Data should be distributed incrementally. We will discuss our recommended approach and the benefits ofIOTA Tangle for IoTs, particularly in SBDs.
- **Data integrity and confidentiality:** When transmitting data, ensuring that the transaction remains intact and secure is crucial. One way to achieve this is by encrypting the data exchange, which helps prevent competitors from accessingsensitive information. Furthermore, the IOTA network per- forms a synchronized snapshot, which saves the balance of every address with tokens greater than zero. After a certain period, Tangle data is cleared to maintain the network's efficiency [22] [18].

5. Implementing Proposed Approach: IOT-Driven SBDS as a Case Study

Our paper comprehensively explains our proposed approach for automating the control of indoor air quality (IAQ) and HVAC systems. Section 5.1 describes the requirednetwork model, software, and hardware configuration to implement our approach. Sections 5.2 and 5.3 elaborate on the deployment structure of the experimental SBDs and thealgorithms used for transaction execution, data permission access, and control management.

5.1. System Network Interface and Architectural Configuration

We have implemented a Pub-Sub architecture for IoT node interaction using the IOTA Devnet to prove the viability of our solution.

Publisher-Subscriber Network model: The pub-sub design pattern comprises three main components: publishers (authors), brokers, and subscribers (end-users). In this design, the author node publishes messages to the Tangle network after receiving an issuing certificate without any knowledge of the subscriber. Tangle is a data management layer that efficiently stores and processes data. The broker node man- ages and processes transactions between the author node and the subscribers. End-users will only receive messages from the channels they have subscribed to. This concept is illustrated in Figure 4.

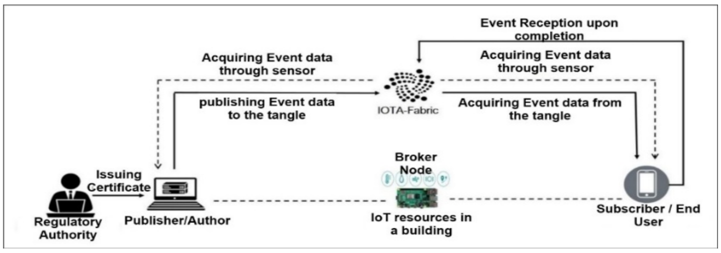

Event Reception upon completion
Acquiring Event data through sensor
Acquiring Event data through sensor
publishing Event data to the tangle
IOTA-Fabric
Acquiring Event data from the tangle
Broker Node
Issuing Certificate
Regulatory Authority
Publisher/Author
IoT resources in a building
Subscriber / End User

Figure 4. Pub-Sub Network model illustrating for a trade event

5.1.1. System deployment structure and functionalities:

The SLDBI architecture comprises three primary components: the Author IOTA node, Broker node, and subscriber node. An IoT broker node is a management point to ensureeffective data transfer. (See Figure 5.)

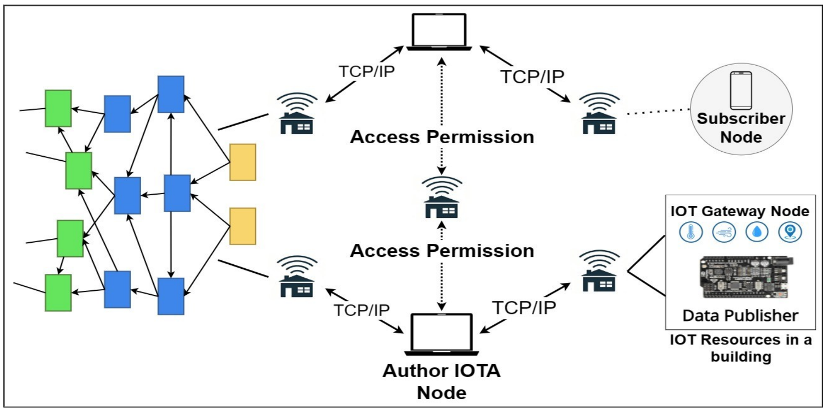


Figure 5. SLDBI for SBDSs utilizing Tangle Blockchain with the author IOTA and IoT broker nodes.

1) Author-IOTA node: The author manages the distributed IOTA tangle infrastructure and operates the broker node program. Transactions are received from the building's broker nodes and stored in a Scylla cluster. The author provides subscribers access certificates, identifies neighbors, and communicates with buildings. Approved basic activities are:

- In SBDs, the author manages access control policies for each house. They use a Proof of Work (PoW)enabled server to perform computations for other IoT devices.
- The IoT building data is managed on nodes. This protocol ensures that access to real-time and historical resources is granted only with proper authorization by the ISCP.

2) IoT-broker node: IoT sensors connected to a Raspberry Pi broker node generate real-time environmental data.Each building has an IoT broker node paired with a distributed author IOTA node. The broker node uses the MAM data stream relay to encrypt and transmit sensor data with the Tangle securely.

3) Subscriber node: The end-user can only access data from the tangle after authorized permission from the author node. To subscribe to the channel, the subscriber must be connected to the IOTA node but can use any device.

Note: The IOTA network prioritizes user protection while allowing anonymous data sharing. MAM encrypts and signs data streams, ensuring secure access for authorized users.

5.2. System Workflow

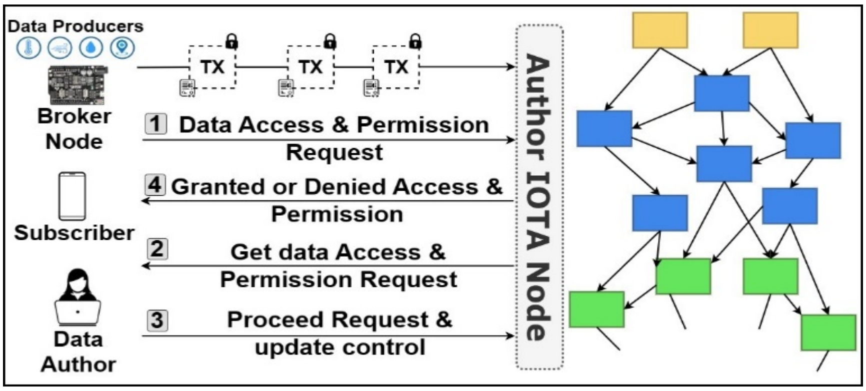

Data Producers
Broker Node
TX
TX
TX
1 Data Access & Permission Request
4 Granted or Denied Access & Permission
Subscriber
2 Get data Access & Permission Request
3 Proceed Request & update control
Data Author
Author IOTA Node

Figure 6. Sequence diagram of Transaction execution and data access authorization in SLDBI

This section explains the transaction workflow in each partof the process, as depicted in Figure 6. To participate in theSBDs, the data author must create a seed. From this seed, addresses and private keys are generated during transactions. For instance, data producers can publish real-time garbage monitoring (GM) data on MAM-restricted channels,while garbage collectors (GC) can subscribe to that data stream. The IoT Broker node, installed in each building andpaired with the author IOTA node, signs and encrypts the time-stamped data bundle, performs PoW, implements the channel stream where the data is allocated, and stores the required MAM transaction bundle (message payload) gradually. Each sensor data is transferred by utilizing the Merkle root address and encryption permission key open key p Pk_e q into the Tangle. The author publishes building resources de-scribed in section 5.3(a) through Algorithm.2. The sequenceof transaction execution is described below:

- Subscribers (GC) intending to access GM data in SBDSs must first seek an access permission request, including their action on the resource(s).
- The data author determines the local authorization conditions (promises) upon receiving the request before granting access approval. These requirements can be maintained on the Tangle in the SLDBI framework by the SBDs author node by ISCP.
- Upon successful authorization, a request and secure transmission channel have been defined among the author and subscriber. To update permission access for a specific time, channel address p Root q and permission decryption key p Pkd q are shared with the subscriber.
- Authorized subscribers with the correct root address and permission key can access author resources by decrypting the message payload in section 5.3(b) algorithm. If the signature verification fails, access is denied. The author can modify the permission key to prevent subscriber access at any time.

5.3. Data Permission and Access Control Management

MAM-restricted access enables fine-grained data permission and control comes with an effort to revoke access of a single subscriber and update the new permission key (PK) to other subscribers of that channel [23]. We implement MSS based on MHT and verify multiple OTS using one public verification key to overcome this issue.

- The author publishes data to the Tangle: After receiving time-stamped sensor data accurately, an encrypted message payload is created by utilizing the Merkle root and encryption permission key pPkeq. Finally, selecting the channel function, level of security, and secret, the MAM protocol publishes the pmaskedpayloadeq into the tangle as Algorithm 2 depicts data publication steps. Steps 1 and 2 of Algorithm 2 show the MAM initial state and change modes, while step 3 describes the MAM message flow with payloads. Message decoding in IoT nodes is described in step 4, attaching the MAM message to the destination node as the last step. Details about the masked message payload design for the proposed system are available in section 4.2.
- Subscriber Retriever data from Tangle: The user must connect with the IOTA network and subscribe to the publisher channel to access the author data for message payload decryption. The subscriber would be capable of retrieving published data pmaskedpayloadaq based on Merkle Root p MR q and decryption permission key p Pkd q as shown in Algorithm 3. The inputs for Algorithm 3 are root and

decryption permission keys, while the output is the masked payload of IoT nodes. Steps 1 and 2 describe the MAM message initially and change states with parameters. Step 3 depicts the current state, while Step 4 shows the message payload with a decryption key.

Algorithm 2. Publish p **maskedpayloade** q to the Tangle

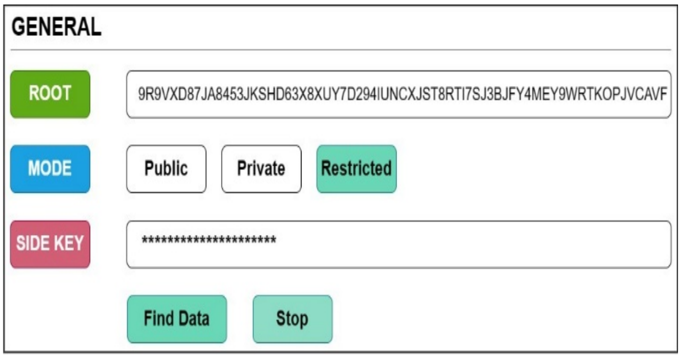
```
Input: root, seed, encryption permission_key pPkeq
Output: Masked payload e
   maskedPayload e
1:  mam.state  Ð mam.init p message, seed, levelofsecurity q
2:  mam.state     Ð mam.Change Mode p mam State,mode, encryptionpermissionkeyPke q
      //for instance, the restricted mode needs an encryption permission key (Pke) to message payload encryption.
3:  mam. Message Mam. Create (mam. State, message payload)
      //after converting asci to tires, create the MAMbundle that contains the message payload of sensor data.
4:  mam.decode Mam. Decode (message payload, root, encryption permission key (Pke)
      //Decode messagepayload.
5: mam. Attach MAM. Publish (address, message payload)
      //Message payload attaches to the IOTA Tangle.
```

Algorithm 3. Retrieval p *maskedpayloade* q from the Tangle

```
Input: root, seed, encryption permission_key pPkdq
Output: Masked payload d
   maskedPayload d
1:  mam.state  mam.init (message, seed, levelofsecurity)
2:  mam.state     mam.Change Mode (mam State,mode, encryptionpermissionkeyPkd q)
      //for instance, the restricted mode needs a decryption permission key (Pkd) for message payload decryption.
3:  mam.State mam.Message.state. //Save in the new State
4:  mam. Fatach mam. Retrieve (root, mode, (decryption permission key pPkdq, call back)
// Retrieve messagepayload from the tangle
```

6. Experimental Evaluation

This section evaluates our approach to permission access, performance, and system security at various granular levels within SBDs.



GENERAL

ROOT 9R9VXD87JA8453JKSHD63X8XUY7D294IUNCXJST8RTI7SJ3BJFY4MEY9WRTKOPJVCAVF

MODE Public Private [✓ Restricted]

SIDE KEY ********************

Figure 7. An authorized subscriber granular access control to retrieve message payload from the tangle in restricted mode

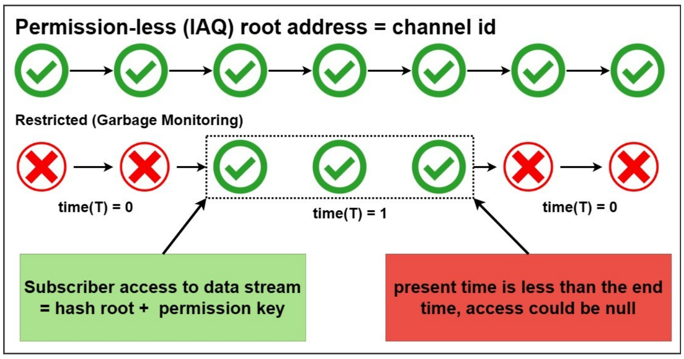

Permission-less (IAQ) root address = channel id
Restricted (Garbage Monitoring)
time(T) = 0
time(T) = 1
time(T) = 0
Subscriber access to data stream = hash root + permission key
present time is less than the end time, access could be null

Figure 8. Access control management with IOTA Smart Contract Protocol (ISCP) in restricted

6.1. SBDs Functional Setup

We use two types of sensor data - IAQ DHT-11 sensor and Ultrasonic Sensor SR04. IAQ sensor uses permission-less MAM mode, while SR04 sensor is published using restricted MAM mode and connected to Devnet full node. Author generates both seeds (root) and permission keys during data publishing. To decode the message payload, subscribersneed both root address and permission encryption key (side key), as shown in Figure 7. We can see the permission-less mode, which allows any subscriber to access the message payload by matching the root address with the channel address, In Figure 8. To enable access to the real-time and historical data stream for a limited period, the author only needs to share the address and permission key with the subscriber once. However, in restricted mode with ISCP, subscriber access may be null at time (T) =0. The author could revoke any subscription to access without changing the side key.

6.2. Discussion

We examine how our proposed approach enhances performance and security by evaluating quality attributes of IoT nodes during runtime based on SBDs functional scenarios.

6.2.1. Performance Analysis

The performance of the SBDs system is evaluated by considering the following attributes:

1) *PoW (PoW is related to the Energy Efficiency use case)*
2) *Scalability*
3) *Throughput*

PoW for SBDs IoT Nodes: We conducted using local PoW and IoT nodes to gather various metrics. Unlike other blockchains such as Bitcoin (BTC) and Ethereum, PoW computation on IOTA does not compete for block incentives. Our findings revealed that there was no noticeable difference in the computing times for posting data to the Tangle between the two data modes. However, the message sizes and encryption techniques used by the two were different. The maximum message size for transactions on the IOTA network is 1650 bytes [13]. If the message is smaller than this limit, the processing time for data broadcast on the same node will be the same. According to the test connecting encrypted messages from IoT devices to the Tangle can take between milliseconds to seconds. Creating permission keys in limited mode takes longer than permission-less mode. Table 3 shows the time it takes to broadcast two types of sensor data to the Tangle. The cumulative time to link encrypted data to the Tangle does not affect the granularity of data. No additional PoW is needed to retrieve data from the IOTA Tangle network, making it faster to create authorization keys when retrieving data.

Scalability: Figures 9 and 10 show the TPS/CTPS results with varying numbers of nodes. As the number ofnodes increases, both TPS/CTPS transaction speeds also increase. For instance, when 50 nodes publish transactionswith MWM=13, the proposed solution reaches 1.91 tx/sand 1.53 tx/s for TPS and CTPS respectively. On the other hand, with MWM=9, the TPS/CTPS reaches 2.56 tx/s and 2.29 tx/s respectively. This indicates that transaction speedscales linearly with the increasing number of publishers. It is important to note that scalability is not limited to transaction speed but is also driven by system throughput.

Throughput: In terms of load tests, it is evident thatour proposed approach has relatively high efficiency in transaction processing. For example, when 150 nodes are publishing with MWM= 13, the average TPS is 2.74 tx/s, CTPS is 2.13 tx/s nearly and MWM=9, the TPS is 4.53 tx/s and CTPS 4.38 tx/s nearly. That is due to the efficient consensus process and DAG-based data structure.

Table 3. Comparative Evaluation Results Computation time for data publishing and retrieving over the Tangle, using MAM in IoT devices.

MAM Modes	**Avg. Publish Time(ms)**			**Retrieve time (ms)**		
	Min	Mix	Avg.	Min	Max	Avg.
Restricted Mode (GM)	79.10	129.17	99.72	68.28	117.51	86.46
Permission-less (IAQ)	53.81	95.41	79.57	48.53	84.63	65.97

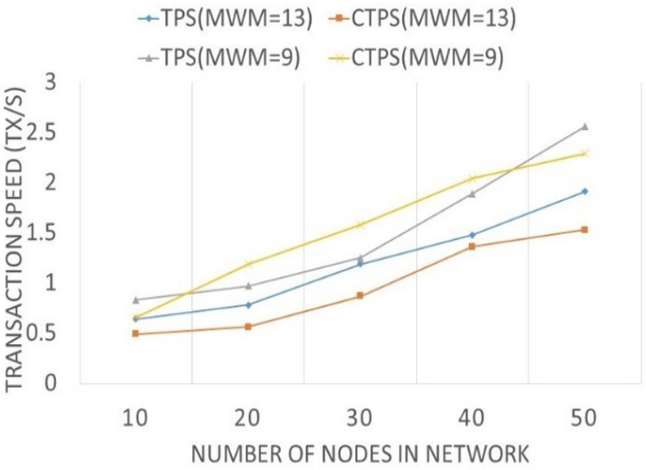


Figure 9. Network Scalability in 50 Nodes

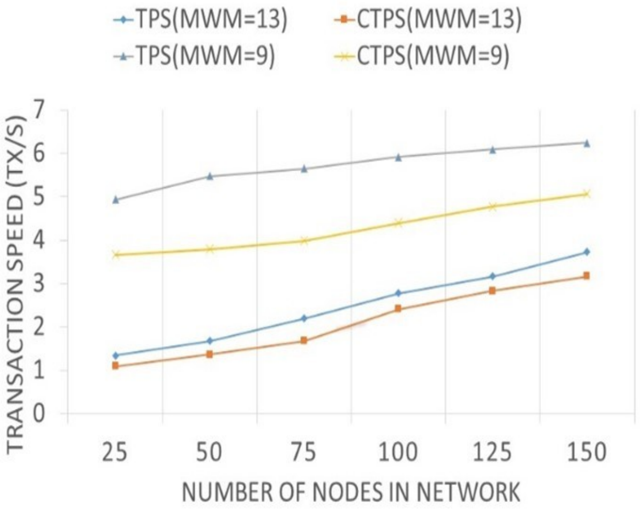


Figure 10. Network scalability in 150 nodes

6.2.2 Decentralization and Energy Efficiency

This subsection discusses how the SLDBI approach improves system energy efficiency by capitalizing on performance and underlying decentralization.

Decentralization: In the proposed approach, each IoT device has a specific number of computational resources. Multiple decentralized coordinators are chosen randomly using MCMC from the involved parties and verify transactions independently. In the transaction process, there are no mediators; as a result, our solution is decentralized.

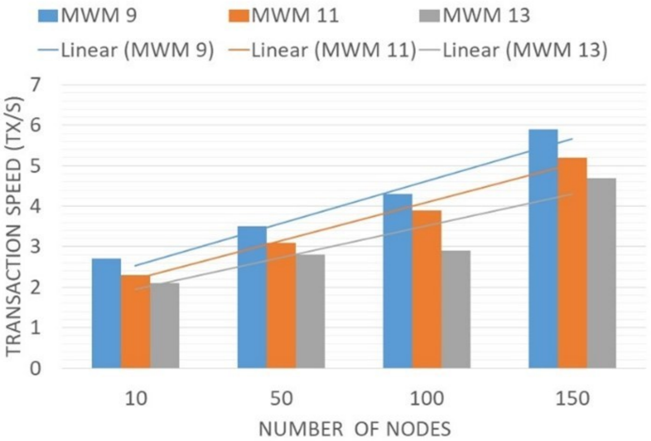


Figure 11. Network Performance with 150 Nodes

Energy Efficiency: In DAG-based DLT, all decentralized nodes are validators and must contribute their computing power to keep the network running. The nodes involved in executing PoW have an impact on power consumption. As a result, offloading saves energy and improves transaction processing speed. MWM impacts the computational load required for PoW calculation, and coordinators are responsible for all the PoW. To verify if MWM influenced TPS and CTPS, we set the MWM to 9, 11, and 13 with 150 nodes in the test. TPS is affected by the usage of different MWMs, as seen in Figure11, where it nearly hits 4.721 tx/s when set to 13 and almost reaches 5.931 tx/s when set to 9. Figure 11, straight lines suggest that increasing messages would also increase transaction speed and network performance. Tangle DLT offers a way to process many nodes with multiple transactions at the same time effectively and consumes fewer resources.

6.2.3 SBDs Security Analysis

Overall, the system security of SBDs is enhanced with improved system resilience and trustworthiness by employing the unique architectural approach of SLDBI for IoT systems. This subsection analyzes the security of SBDs using the proposed approach. Since the SBDs IoT nodes are vulnerable to various cyber security attacks, the SBDs system uses multiple steps to enhance the system's security posture. Enhancing IoT system reliability improves overall system resilience, catering to unexpected data breaches/information loss dueto cyber-attacks. With the high reliability of IoT nodes within SBDS infrastructure, system availability is ensured concerning the Confidentiality, Integrity, and Availability (CIA) tirade. For this, we build a security scenario wherean attacker (X) can take control of SBD using various attackvectors.

Attack Scenario: In an IoT-based smart building, robust access control mechanisms and identity management systems are in place to safeguard the premises. However, this system has specific attack vectors with underlying system vulnerabilities that an adversary can exploit. Anattacker X, with a deep understanding of the building's IoT infrastructure, decides to exploit vulnerabilities targeting the access control system. He aims to compromise access control, integrity, and identity management within the smart building using various tactics; refer to Table 9 for attack tactics. Compromised data integrity can lead to potential data loss, system malfunctions, and operational disruptions.

6.2.4 Security of SBDs using SLDBI

The integration of lightweight blockchains with DAGs and smart contracts brings forth a multitude of cybersecurity use cases and remarkable improvements for the resilience and security of SBDs as follows:

Node to Node Identity Management: The implementation of the IOTA Smart Contract Protocol (ISCP) using the algorithm specified in previous sections, significantly enhances access and identity management within smart building systems based on IoTs.

Granular Access and Identity Management: ISCP introduces granular access control through Algorithm 3, enabling fine-grained permissions based on the identity and specific permissions of each IoT device. This approach minimizes the risk of unauthorized access, ensuring that only authenticated and authorized de- vices can interact with sensitive areas or data within the smart building. Moreover, ISCP incorporates time- based access control from Algorithm 3, allowing administrators to schedule access permissions according to specific intervals, aligning access with the building's operational needs at runtime.

Immutable Security: Smart contracts optimized through ISCP, as outlined in Algorithm 1 and Algorithm 2, create an immutable security system that prevents unauthorized changes to access policies, enhancing security. Additionally, ISCP operates efficiently and is implemented by a select group of nodes, ensuring re- source efficiency across the broader IoT network. Thisapproach enhances not only identity and access management but also overall control and efficiency within smart building systems.

Access Authorization: Access provision of interacting IoT nodes in SBDs is restricted via secure smart contracts. ISCP based node contracts regularly update access policy into author nodes enhancing authorization controls at run-time. Multiple access control contracts are enforced with publisher and subscriber nodes restricting access through the automated authorization of participating IoT nodes. It uses decentralized consensus mechanisms for identity verification. Instead of relying on a central authority for identityvalidation, the smart contract can cross-verify identity data across multiple nodes in a decentralized manner, making it more resilient to identity spoofing attempts.

1) *Dynamic Access Management:* The ISCP's integration with the DAG-based blockchain enables real-time adjustments of access permissions. As tenants, visitors, oremployees' roles change or as specific access requirements evolve, the system can swiftly and securely modify permissions, ensuring that access control remains aligned with the building's operational needs.
2) *Building Users/Visitors Access Data:* The proposedlightweight blockchain securely stores visitor data, while smart contracts generate unique identifiers for each visitor in the building areas. These identifiers,when used at the building entrance, are swiftly validated by smart contracts, granting access for the scheduled visit duration. This ISCP-based access mechanism not only simplifies visitor management but also reduces administrative burdens, ultimately enhancing security by ensuring that only authorized individuals gain entry.
3) *Resilience to SPFs:* DAGs are inherently resilient to single points of failure. Unlike traditional centralized systems, where compromising a central server can have catastrophic consequences, a DAG-based system distributes control and data across multiple nodes in the SBD security system. This decentralized architecture makesit more challenging for an attacker to compromise the entire system in one go.
4) *Immutable Audit Tracking:* The immutable audit trail maintained by the lightweight blockchain ensures compliance with regulations and offers invaluable insights.Once audit data is published on the IOTA Tangle using Algorithm 1, it becomes immutable. It cannot be alteredor deleted, providing a tamper-proof record of access- related events.

A summary of attacker tactics and countermeasures applicable through SLDBI-based security measures is described in Table 4 below.

These countermeasures, integrated with smart contracts ISCP using lightweight DAG blockchains, enhance security, access control, and identity management while mitigating various attacker actions in an intelligent building context. The integration of lightweight blockchains with DAGs and smart contracts brings forth a multitude of cyber- security use cases and remarkable improvements for the resilience and security of SBDs as follows:

Table 4. Summary of countermeasures to attacker tactics using SLDBI

Attacker Tactics	**SLDBI based Attackers Tactics Counter Measures**
Unauthorized Data Access	Utilize Algorithm 2 to publish masked data payloads.

Unauthorized Message Retrieval	Use Algorithm 3 to retrieve masked payloads from the Tangle, Restrict access with decryption permission key as described in Algorithms 2 and 3.
Tampering with Access Control Policies	Implement Algorithm 3 for permission access policy. Verify access requests against the policy for authorization.
Identity Spoofing	Apply Algorithm 3 to check and validate subscriber attributes. Ensure only authorized identity attributes are accepted.
Data Tampering	Use Algorithms 1 and 2 for data publication and retrieval. Maintain data integrity through the decryption method.
Access control Violation	Implement the IOTA Smart Contract Protocol (ISCP). Ensure that policies are enforced off-Tangle by specific nodes. Implement reward-less ISCP to prevent unwanted incentives

7. Conclusion and Future Work

SLDBI provides robust security and resilience for smart buildings with limited resources. It outperforms conventional ledgers and is scalable. We'll continue enhancing it to create cutting-edge IoT infrastructure. SLDBI fortifies smart buildings against threats, ensuring the integrity and confidentiality of IoT data streams. It incorporates DLT andan advanced access control system to offer robust protection and resilience for smart buildings with limited resources.

7.1 Limitations

We understand that there is still room for improvement, and we are committed to refining our infrastructure to meet the evolving requirements of IoT systems. Notably, we needto consider the impact of distributed author IOTA nodes on future technological exploitation and cost-effectiveness, as highlighted [22] [21]. To improve efficiency, sensor datacan be published directly from IoT devices to the Tangle, enabling real-time machine-to-machine interaction. Implementing a local snapshot function helps in managing data storage, allowing author IOTA nodes to remove outdated transactions and maintain a streamlined database. Depending on specific circumstances, perm anode and local snap- shot functionalities may be integrated into IoT systems.While MAM is proficient in one-way communication, the IOTA Foundation is actively working on improving bidirectional communication through MAM. However, a significant concern is the centralization introduced by IOTA's Coordinator, which can affect scalability and decentralization, as pointed out [24]. This element serves as a Single Pointof Failure (SPOF) and influences transaction prioritization, asset freezing, and oversight.

7.2 Future work

Our solution utilizes the Distributed IOTA Tangle technology to provide enhanced security and scalability for intelligent buildings. This innovative approach allows IoT nodes and users to share information, promoting trust and confidentiality securely. Our architecture prioritizes energy efficiency and resource optimization and has been success- fully demonstrated on a single-board computer. However, we continuously strive to improve it based on changing design and system requirements.

In the future, we plan to develop smart building prototypes and integrate lightweight contract reasoning with Machine Learning (ML) and Artificial Intelligence (AI) using edge and cloud computing. By utilizing AI and ML, we can optimize and secure IoT-based block chains and add intelligence to them, making them more efficient and valuablein various applications. Additionally, we aim to seamlessly integrate our system with other DLTs, such as hyper ledger fabric to establish a robust and reliable identity frameworkfor distributed IoT systems and their participating nodes.

References

1. Y. Liu, J. Wang, Z. Yan, Z. Wan, and R. Ja¨ntti, "A survey on blockchain-based trust management for Internet of Things," IEEE Internet of Things Journal, vol. 10, no. 7, pp. 5898–5922, 2023.
2. N. Denis, M. Laurent, and S. Chabridon, "Integrating usage control into distributed ledger technology for internet of things privacy," IEEE Internet of Things Journal, 2023.
3. H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A review of blockchain in internet of things and ai," Big Data and Cognitive Computing, vol. 4, no. 4, p. 28, 2020.
4. G. C. Sekhar and R. Aruna, "An integrated secure scalable blockchain framework for iot communications," 2023.
5. S. Mathur, A. Kalla, G. Gu¨ r, M. K. Bohra, and M. Liyanage, "A survey on role of blockchain for iot: Applications and technical aspects," Computer Networks, vol. 227, p. 109726, 2023.
6. X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms: mechanism, design and applications," Science China Information Sciences, vol. 64, pp. 1–15, 2021.
7. Cullen, P. Ferraro, C. King, and R. Shorten, "Distributed ledger technology for iot: Parasite chain attacks," arXiv preprint arXiv: 1904.00996, 2019.
8. T. Alsboui, Y. Qin, R. Hill, and H. Al-Aqrabi, "Towards a scalable iota tangle-based distributed intelligence approach for the internet of things," in Intelligent Computing: Proceedings of the 2020 Comput- ing Conference, Volume 2, pp. 487–501, Springer, 2020.
9. Alrehaili, A. Namoun, and A. Tufail, "A comparative analysis of scalability issues within blockchain-based solutions in the internet of things," International Journal of Advanced Computer Science and Applications, vol. 12, no. 9, 2021.
10. Fan, S. Ghaemi, H. Khazaei, Y. Chen, and P. Musilek, "Perfor- mance analysis of the iota dag-based distributed ledger," ACM Transactions on Modeling and Performance Evaluation of Computing Systems, vol. 6, no. 3, pp. 1–20, 2021.
11. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li, "Performance analysis and comparison of pow, pos and dag based blockchains," Digital Communications and Networks, vol. 6, no. 4, pp. 480–485, 2020.
12. N. Zivic, C. Ruland, and J. Sassmannshausen, "Distributed ledger technologies for m2m communications," in 2019 International Con- ference on Information Networking (ICOIN), pp. 301–306, IEEE, 2019.
13. B. Kusmierz, W. Sanders, A. Penzkofer, A. Capossele, and A. Gal, "Properties of the tangle for uniform random and random walk tip selection," in 2019 IEEE International Conference on Blockchain (Blockchain), pp. 228–236, IEEE, 2019.
14. L. Li, D. Huang, and C. Zhang, "An efficient dag blockchain architecture for iot," IEEE Internet of Things Journal, vol. 10, no. 2, pp. 1286–1296, 2022.
15. S. Wang, H. Li, J. Chen, J. Wang, and Y. Deng, "Dag blockchain- based lightweight authentication and authorization scheme for iot devices," Journal of Information Security and Applications, vol. 66, p. 103134, 2022.
16. R. Nakanishi, Y. Zhang, M. Sasabe, and S. Kasahara, "Iota-based access control framework for the internet of things," in 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pp. 87–95, IEEE, 2020.
17. S. N. Mohanty, K. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. Lakshmanaprabu, and A. Khanna, "An efficient lightweight integrated blockchain (elib) model for iot security and privacy," Future Generation Computer Systems, vol. 102, pp. 1027–1037, 2020.
18. Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," Human-centric Computing and Information Sciences, vol. 10, no. 1, pp. 1–14, 2020.
19. C. Fan, H. Khazaei, Y. Chen, and P. Musilek, "Towards a scalable dag-based distributed ledger for smart communities," in 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), pp. 177–182, Ieee, 2019.
20. X. Zheng, S. Sun, R. R. Mukkamala, R. Vatrapu, and J. Ordieres- Mere´, "Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies," Journal of medical Internet research, vol. 21, no. 6, p. e13583, 2019.
21. S. Suhail, R. Hussain, A. Khan, and C. S. Hong, "Orchestrating product provenance story: When iota ecosystem meets electronics supply chain space," Computers in Industry, vol. 123, p. 103334, 2020.
22. S. Abdullah, J. Arshad, M. M. Khan, M. Alazab, and K. Salah, "Prised tangle: A privacy-aware framework for smart healthcare data sharing using iota tangle," Complex & Intelligent Systems, vol. 9, no. 3, pp. 3023–3041, 2023.
23. M. Lu¨ cking, R. Manke, M. Schinle, L. Kohout, S. Nickel, and W. Stork, "Decentralized patient-centric data management for sharing iot data streams," in 2020 International Conference on Omni- layer Intelligent Systems (COINS), pp. 1–6, IEEE, 2020.
24. W. F. Silvano and R. Marcelino, "Iota tangle: A cryptocurrency to communicate internet-of-things data," Future generation computer systems, vol. 112, pp. 307–319, 2020.