Using Direct Acyclic Graph (DAG) based Distributed Ledger for a secure and scalable Internet of Things (IoT) architecture.

A. Author[1], Syed Irfan Raza Naqvi
B. Author[2], Zheng Jiang Bin
C.Author[3], Ahmad Mosin
D.Author[4], M. Mueez-ur-Rehman
E.Author[5], S.M Ali Zain ul Abidin

[1]School of Software,
Northwestern Polytechnical University, Xian, China
email1@irfanrazanaqvi9@gmail.com

[2]School of Software,
Northwestern Polytechnical University, Xian, China
email 2@zhengjb@nwpu.edu.cn

[3]Cyber Security Research Institute,
Edith Cowan University, Australia
email 3@a.mohsin@ecu.edu.au

[4]Department of Computer Science,
Air University Multan Campus, Multan, Pakistan
email chaudarymueez@gmail.com

[5]Department of Computer Science,
Air University Multan Campus, Multan, Pakistan
email alizainnaqvi911@gmail.com

ABSTRACT

The Internet of Things (IoT) system is rapidly growing, but it has some vulnerabilities due to its centralized architecture, including scalability, security, and access control. To address these issues, Distributed Ledger Technology (DLT) has become increasingly important in providing a secure and scalable infrastructure for IoT. However, traditional DLT systems, such as Bitcoin and Ethereum, are unsuitable for IoT devices with limited resources due to their inefficiency, scalability problems, and high transaction fees. Our research proposes a solution to this problem using a Directed Acyclic Graph (DAG) based DLT that is scalable and secure. IOTA, a distributed ledger based on DAG, has shown promise in addressing the problems in the IoT domain. Our proposed architecture utilizes the DAG-based Tangle and implements a lightweight Masked Authentication Message (MAM) message data model to overcome the limitations of IoT. This allows for easy integration new IoT devices across various domains using the protocol and IOTA. Furthermore, our experiments have shown energy-efficient proof-of-work (PoW) computation on the entire node, leading to efficient resource utilization. These findings indicate secure user access control management at different granularity levels and the ability to scale massive networks with numerous IoT nodes in IoT systems. In conclusion, the proposed DAG-based

distributed ledger is a feasible solution for building a scalable access control infrastructure for IoT.

Keywords: Distributed Ledger Technology (DLT), Blockchain, Internet of Things (IoTs), Direct Acyclic Graphs (DAG), Scalability

1. INTRODUCTION

By 2030, the number of IoT-connected devices is expected to reach 25.4 billion,[1] leading to increased devices and connections per household and Internet user. The data generated is expected to reach 180 zettabytes (180 trillion gigabytes) by 2025. Due to massive data volumes, IoT networks require scalability, cybersecurity, and data privacy. In existing IoT networks, security management and node connection are done using a centralized architecture [2]. The current IoT system's centralized architecture leads to a single point of failure (SPoF), lack of security, privacy, scalability, and data integrity. Obstacles in IoT application development must be overcome.

Decentralizing IoT transactions is the answer to the problems described. Distributed Ledger Technology (DLT) enables decentralized security privacy and allows users to share or sell sensor data without intermediaries [3]. Blockchain is among the most prevalent and well-known distributed ledger technologies. Blockchain is a decentralized database that uses a peer-to-peer network to immutable block transactions. There are numerous benefits to utilizing the IoTs in combination with Blockchain technology. Bitcoin and Ethereum, which are traditional blockchain systems, are mainly intended for trading cryptocurrencies [4]. The limited use of Blockchain technology in IoT applications is due to its high energy consumption during mining and its consensus algorithms and linear ledger structure, which can limit transaction speeds. The primary concern with the existing Blockchain technology for IoT systems is that it requires a lot of computational energy, which can be challenging for resource-limited IoT devices. However, a more efficient type of DLT could be suitable for IoT environments where a large amount of data is generated continuously.

Recently, directed acyclic graph (DAG) based distributed ledger technology (DLT) has been proposed to address the scalability and security issues of conventional DLTs in IoT systems. One DLT is the IOTA Tangle, which utilizes a blockless and tree-like data structure based on a direct DAG. This approach resolves the challenges associated with traditional blockchain technologies. Tangle is the underlying technology of IOTA, a minor-less cryptocurrency designed for the IoT industry that can improve performance by minimizing unnecessary communication, computation, and storage needs [5]. This paper aims to propose a secure and intelligent Internet of Things architecture that is lightweight and scalable based on DAG. We utilize a lightweight permission mode and POW to improve energy efficacy regarding secure access mechanisms in IoTs. We use Masked Authenticated Messaging (MAM) for

confidential flow information distribution with restricted data retrieval and flexible data accessibility with limited resources. To summarize, the main contributions of this paper are as follows:

- We discuss the evolution of IoT systems, including their transition from legacy to DLT. Incorporating IoT sensors connected via secure and scalable DAG-based IoT architecture, enabling energy-efficient PoW on full author IOTA nodes.
- Improved system performance and security of smart IoT using lightweight IOTA algorithm by utilizing Masked authentication Message (MAM) Modes.

1.1Paper organization:

We'll examine DLTs like Blockchain and IOTA, review the literature, analyze the Tangle, discuss proposed architecture and its implementation, summarize results, and suggest future research.

2. PRELIMINARY

In this section, we will discuss the integration challenges of Blockchain and IoT, the IOTA tangle's fundamental design principles, and its underlying structure.

2.1 Blockchain Distributed Ledger

Blockchain is a fundamental protocol for cryptocurrencies like Bitcoin (BTC), initially suggested by Satoshi Nakamoto in 2008 as the first practicable application [3][8]. The blocks are connected by referencing the preceding block, creating a chain. The blockchain ensures accurate and secure transactions by using consensus algorithms and smart contracts to prevent unauthorized users from invalid 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 [6] [10]: Public, Private, and Hybrid Blockchains.

2.1.1 Challenges and Motivation: Integrating IoT and Blockchain

It is essential to understand that incorporating Blockchain into the IoT presents several obstacles, including scalability, interoperability, compatibility, developments in quantum computing, user identity tracking, and energy efficiency [10] [13]. Challenges that arise from integrating IoT with Blockchain technology include:

- Scalability: The growing size of the Blockchain as more devices 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% attack is a typical security threat to the Bitcoin protocol, where a participant controls more than 51% of mining power, allowing them to manipulate the network's consensus [8]. Double spending attacks and high mining fees are well-known drawbacks of using blockchain in IoT.

- 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.

- 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 [11]. 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 [14].

Despite these challenges, researchers and developers are working diligently to overcome these issues and unlock the full potential of Blockchain-based IoT.

2.2 Internet-of-Things Association (IOTA) Distributed Ledger

IOTA, the latest DLT, uses a DAG to represent transactions instead of a traditional Blockchain. Its foundation is built upon a data structure called Tangle. The creators of IOTA are David Sonstebo, Serguei Popov, Sergey Ivancheglo, and Dominik Schiener, first introduced in 2015 [15]. Transactions that can execute parallel and link to any point on the Tangle [10], eliminating confirmation time limits and scalability issues. Lightweight proof of work prevents network spamming instead of securing transactions, making proof of work less energy-intensive [1]. Integrating IOTA into IoT infrastructure has numerous benefits and motivations. The key advantages include scalability, M2M feeless transactions, security, privacy, and decentralization.

2.2.1 Direct Acyclic Graph (DAG) Structure

In the DAG design, user transactions are organized into a set on the tangle graph. This set acts as a ledger and contains important transaction details such as time stamps, digital signatures, hash values, and message payloads. The nodes then propagate these transactions. A new or unconfirmed transaction in the tangle graph is called a "tip" [7]. In the Tangle system, each transaction must have two parents selected from the DAG. When a transaction is confirmed, it is represented by an edge that connects it to its approving parents. If there exists an indirect path with multi-hops, it represents indirect confirmation. For example, in Figure 1, if transaction F confirms transaction J, it is a direct confirmation. If there is no direct edge between transactions E and H, but there is an indirect path (G), then E indirectly confirms H. The genesis site or transaction in the Tangle is unique and has no parents. This single transaction can be confirmed multiple times, directly or indirectly, by all other sites.

To ensure that all non-approved transactions are approved on time, the Markov Chain Monte Carlo (MCMC) tip selection algorithm (TSA) plays a crucial role in the Tangle system. It selects new transactions to be attached to the Tangle graph, rather than previously approved ones. To achieve this, a random walk is performed twice, selecting tips along the timeline from the genesis transaction graph and moving along the Tangle, including its edges [8].

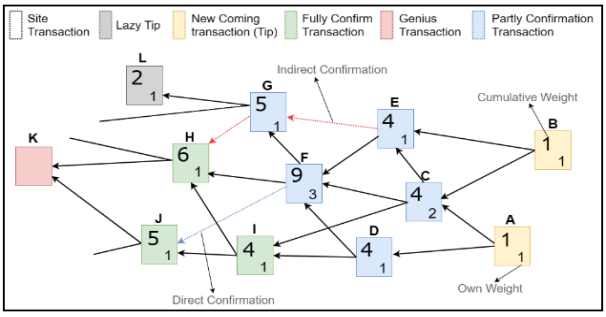

Figure 1. DAG base transaction Conformation (boxes represent transactions)

3. RELATED WORK

This section reviewed DAG-based DLT for IoT access control and scalability. We will evaluate their methods for IoTs, weighing their pros and cons.

Bitcoin and Ethereum are successful DLTs based on blockchain technology [18], where Transactions are stored in blocks and chained together in single chain by hash pointers. Several solutions have been proposed for managing secure IoT and scalability using BCT [9][19]. N. Denis et al. [1] proposed that DLT can benefit IoT by reducing costs and expanding network coverage. Attribute-based usage control and DAG-based distributed ledgers offer affordable transactions, high capacity, and no intermediaries. S. Akbulut *et al.* [10], present a decentralized system that utilizes IOTA Tangle to secure patient medical records in IoT medical devices. Additionally, the system includes an access management feature that enables patients to manage their medical records through smart contracts. S. wang at al. [11] suggest to create a secure environment for the Internet of Things (IoT), it is important to design a lightweight authentication and authorization scheme using various technologies like IOTA, IPFS, and fog computing. This scheme should be cost-effective, consume less energy and have the capability to scale. Moreover, it is recommended to use fog nodes instead of IoT devices for localization calculation and verification, which can help reduce latency. Alsboui at al. [12] Proposed MADIT - Mobile Agent Distributed Intelligence Tangle-based approach for the Internet of Things (IoT) to improve scalability. MADIT enables local interactions between IoT devices and reduces energy consumption by offloading computation to resource-rich devices. C. Fan at al. [13] proposed IoT infrastructure design for smart communities incorporates IOTA's Tangle technology. However, there is still room for improvement in terms of decentralized optimization and security verification.

We researched IoT DAGs, comparing approaches for scalability, privacy, access control, devices, and delay. Scalability was a major challenge, so we developed a mechanism with a single-board computer for the DAG and multiple agents. This created a secure, distributed and highly scalable solution.

4. PROPOSED APPROACH

This section discusses the proposed architecture in Section 4.1. Sections 4.2-4.5 cover MAM, data permission, transaction flow, and access control respectively.

4.1 System architecture

Figure 2 shows a diagram that explains how to create a framework for IoT applications using DAG. The modular design consists of four layers that can be easily modified or replaced. The Physical layer has data producers and sensors, while the Broker layer ensures secure communication. The IoT-Blockchain trust layer manages standard services, and the client Application layer controls authorized access to encrypted data through a web interface. IoT devices utilize MAM protocols to connect with nearby nodes and interact with the Tangle through transactions. Although these devices handle and process transactions, a PoW-enabled server with ample resources performs costly computations for other IoT devices.

Tangle serves as an efficient data management layer for processing and storing data.

4.2 Masked Authenticated Massaging (MAM)

IOTA transactions use MAM to summarize messages. MAM uses MSS built on MHT with OTS to sign encryption cipher digest [14]. MHT generates a new Merkle tree with a user seed, and the MAM root address is used for each message. The seed owner can generate MHT for subsequent messages. A related Merkle tree is created and signed with private keys when a new message is published. The root becomes the MAM channel ID. Subscribers validate statements by validating Merkle root siblings' signatures. The message will be validated if the Merkle root matches the channel ID. Utilize MAM protocol for secure data exchange with access management modes: Permissionless, Permissioned, and Restricted.

1. **Permission-less:** *address= (root):* Public announcements in permission-less mode allow any user with an address containing the same root channel ID to decrypt the message, providing data transparency and audibility.

2. **Permissioned:** *address= hash(root):* Private communication is restricted to the owner with a secure hash address and added security measures. With permissioned access, private communication is kept safe for the seed owner. An additional layer of protection is in place to prevent unauthorized access.

3. **Restricted:** *address= hash (root + side key):* The root and permission keys (pk) are used to encrypt and decrypt messages in the channel address. Only the source and the permission key (side key) can access messages in restricted mode [15].

4.3 Security Mechanism

A comprehensive MAM transaction bundle is split into the MSS (Merkle signature scheme) and MM (masked message), as represented in Figure 3. MSS is generated from one of the private keys corresponding to one of the leaves [16] and outperforms security models, as explained in figure 3. A Masked Message consists of raw data, including the message payload $(payload_m)$ that needs to be shared, the following root for MHT, and the index of the chosen leaf with its siblings. MM must transfer and link to the subsequent message where each transaction n has a pointer n+1(future message), although the transaction direction n−1 (previous message) is unknown[16] [17].

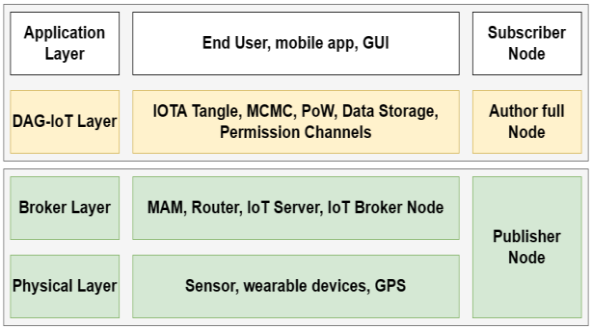

Figure 2. Proposed Layered Architecture Design for IoTs

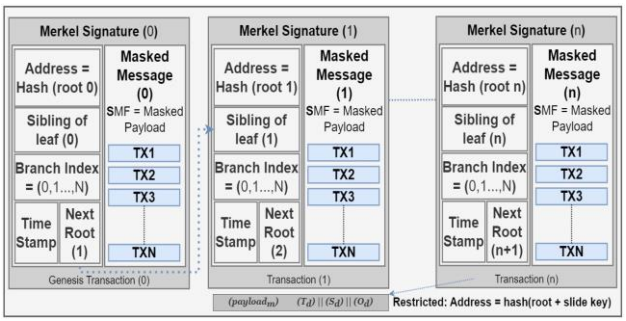

Figure 3. Bundle Message Format

4.4 Transaction Workflow

We will explain the transaction workflow for each node involved as shown in figure 4. For example, Data producers use MAM to share real-time garbage monitoring (GM) data on restricted channels. Garbage collectors (GC) can subscribe to this data. The IoT Broker node connects with the author IOTA node to produce signed, encrypted, and time-stamped data bundles. Each sensor data is transferred to the Tangle using the Merkle root address and encryption permission key (openkey). The author publishes IoT data using 4.5(a) Algorithm.1. Subscribers (GC) who want to access GM data on the network must request access permission and specify their intended actions on the resource(s).

1. The data author sets local authorization requirements before granting access approval, which can be stored on the Tangle framework by the author node. After successful authorization, the author and subscriber establish a secure transmission channel. To update permission access for the specific period, channel address (Root), and permission decryption key shared with the subscriber.

2. To access author resources, only the authorized subscriber with the correct root address and permission key can decrypt the message payload, as explained in section 4.5(b) algorithm.2. Access will be denied if the signature verification fails. The author can revoke the subscriber's access to the channel by modifying the permission key at any time.

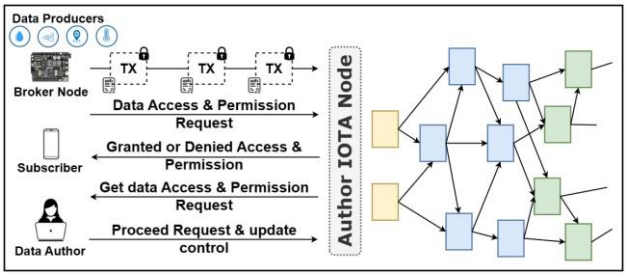

Figure 4. Transaction execution and data access authorization

4.5 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 [18]. We implement MSS based on MHT and verify multiple OTS using one public verification key to overcome this issue.

1. 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$^{(Pk_e)}$. Finally, selecting the channel function, level of security, and secret, the MAM protocol publishes the ($^{\text{masked } payload_e)}$ into the Tangle as Algorithm 1 depicting data publication steps. Steps 1 and 2 of Algorithm 1 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.

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$^{(masked\ payload_d)}$ based on Merkle Root (MR) and decryption permission key

(Pk_d)as shown in Algorithm 2. The inputs for Algorithm 2 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.

Algorithm1: Publish $\boldsymbol{masked\ payload_e}$ *to the Tangle*
Input: $root, seed$, encryption permission key (Pk_e)
Output: $Masked\ payload_e$
1: mam-state ← Mam. Init (message, seed, level of security)
2: Mam-state ← Mam. Change-Mode (mam-State, mode, encryption permission key Pk_e) // The restricted mode needs an encryption permission key for message payload encryption.
3: mamMessage ← Mam. Create (mamState, message payload) / after converting asci to tires, Create MAM bundle that contains message payload of sensor data
4: mam.decode ← Mam. Decode (message payload, $root$ encryption permission key (Pk_e) //Decode message payload
5: Mam. Attach (address, message payload) //Message payload attaches to the IOTA Tangle.

Algorithm 2: Retrieve $\boldsymbol{Masked\ payload_d}$ *from the Tangle*
Input: $root$*, decryption permission key* (Pk_d)
Output: $Masked\ Payload_d$
1: mam-state ← *Mam. Init (message, seed, level of security)*
2: mamstate ← *Mam.changeMode (mamState, mode, Permission Key* (Pk_e) *//for instance, restricted channel mode needs a decryption permission key*(Pk_e) *to decrypt message*
3: mamState ← *mamMessage.state //save in the new state*
4: Mam.fetch (root, mode, decryption permission key (Pk_d)*, call back) //Retrieve message*

5. EXPERIMENTAL EVALUATION

In This section we implement our approach to ensure permission access and performance at different levels of granularity, including scalability, energy efficiency, and system security.

5.1 System implementation Environment Setup

We have installed the IOTA Horneti on a Raspberry Pi as a Publisher Node and install at each building, set up a local server as an Author Node for Proof of Work (PoW) operations. Our implementation adheres to the IOTA network specifications and uses the official Java build, including the Java API library for the IOTA Distributed Ledger. This library manages IOTA addresses, transactions, broadcasting, routing, and multi-signatures. We've created a network with different numbers of IOTA participant nodes to mimic real-world situations.

5.2 Security Goals:

The DAG-based IoT system utilizes a virtual voting mechanism to ensure efficient algorithm operation and high security in an asynchronous environment. The proposed method uses MAM with a gossip protocol to deliver encrypted data

through the IOTA tangle and DAG consensus. It also employs MSS and TSA for secure access control in IoT environments.

Decentralization: The proposed architecture uses a trusted coordinator to randomly select IOTA full nodes for issuing milestones, ensuring no violation of consensus rules. Nodes create milestones to verify transactions when one malfunctions, lowering the risk of centralization and making the system more dependable against failures and cyberattacks. Maintaining subscriber access without changing permission keys or channel addresses is essential. Sharing only a portion of data is possible.

Data integrity and confidentiality: Keep data accurate and secure by encrypting it when sharing. IOTA network synchronizes snapshots to save a balance of addresses with tokens greater than zero and erases Tangle data after a set time to protect sensitive information from competitors.

Secure Access Management: We monitor home inside air quality using the DHT-11 sensor and publish data through MAM permissionless mode. Garbage Monitoring (GM) is done with the Ultrasonic Sensor SR04, and data is published through restricted MAM mode. Authors create seeds and permission keys to start publishing data streams. Subscribers need the root address and side key to access the message payload as shown in figure 5. Access is limited for a specific period, and restricted mode allows subscription revocation without side key fundamental changes, as shown in figure 6.

Figure 5. Subscriber Secure Access Management to retrieve message payload from the Tangle in restricted mode.

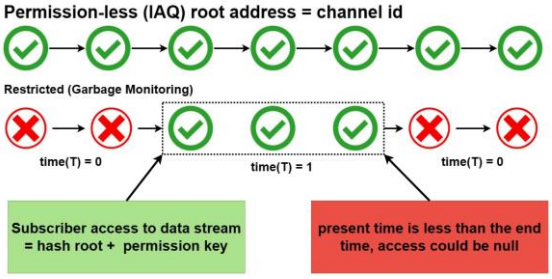

Figure 6. Access control management in permissionless and restricted mode

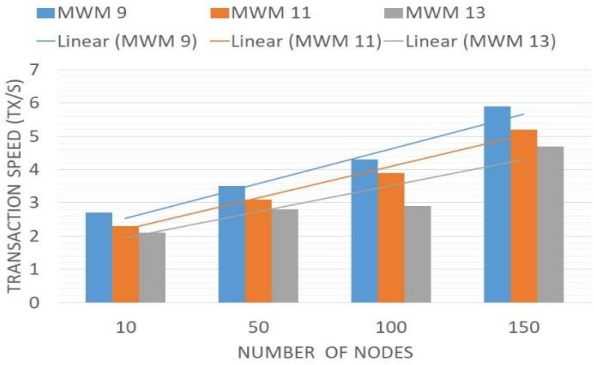

Figure 9. Network Performance in 150 Nodes

5.2 Performance Analysis

We assessed the effectiveness of the DAG-IoT system based on its Scalability, Throughput, and PoW (which relates to Energy Efficiency). To do this, we tested the system using different Minimum Weight Magnitudes (MWMs) such as 9 and 13. We chose different MWMs because they impact the Transaction Per Second (TPS) measure. A higher MWM means it takes longer to attach transactions, reducing the chances of others selecting them as tips.

Adding more nodes to the system increases transaction speed, as seen in Figures 9. The proposed solution

improves TPS/CTPS, almost doubling with each new node. In Addition, a DAG-based DLT system, nodes validate transactions and contribute computing power. Offloading computation can save energy and speed up transactions. MWM affects PoW load, and coordinators handle all PoW. We tested MWM values of 9, 11, and 13 with 150 nodes on local machine and found different values impact TPS, with a maximum of 5.931 tx/s at MWM 9 and 4.721 tx/s at MWM 13.

6. CONCLUSION AND FUTURE WORK

Our approach is a reliable and efficient choice for IoT applications, with strong TPS/CTPS and access control management. Transaction approval is faster with more connected nodes, but performance can still be improved.

There are concerns that IOTA's Tangle technology, despite claims of being fully decentralized, still has some central control. However, IOTA has implemented measures to improve scalability and decentralization, such as the coordinator, which helps prevent double-spending attacks. These efforts aim to make the network more mature and secure [19]. IOTA created CORDICIDE to eliminate the need for a coordinator and prevent a single point of failure in their transaction prioritization and asset-freezing tool. GoShimmer supports the IOTA Smart Contract Protocol, improving security and decentralization. Our solution uses the IOTA Tangle for data scalability and encrypted sharing with Merkle hash trees. It's energy-efficient and requires fewer resources when implemented on a single-board computer. We plan to enhance it by using ISCP for secure access management and developing e-health records prototypes.

7. REFERENCES

[1] N. Denis, M. Laurent, and S. Chabridon, “Integrating Usage Control into Distributed Ledger Technology for Internet of Things Privacy,” *IEEE Internet Things J.*, pp. 1–24, 2023, doi: 10.1109/JIOT.2023.3283300.

[2] S. Pal, A. Dorri, and R. Jurdak, “Blockchain for IoT access control: Recent trends and future research directions,” *J. Netw. Comput. Appl.*, vol. 203, no. March, p. 103371, 2022, doi: 10.1016/j.jnca.2022.103371.

[3] F. Restuccia, S. D. andSalil S. Kanhere, T. Melodia, and S. K. Das, “Blockchain for the Internet of Things: Present and Future,” vol. 1, no. 1, pp. 1–8, 2019, [Online]. Available: http://arxiv.org/abs/1903.07448

[4] S. R. Cherupally, S. Boga, P. Podili, and K. Kataoka, “Lightweight and Scalable DAG based distributed ledger for verifying IoT data integrity,” *Int. Conf. Inf. Netw.*, vol. 2021-Janua, pp. 267–272, 2021, doi: 10.1109/ICOIN50884.2021.9334000.

[5] Q. Wang, J. Yu, S. Chen, and Y. Xiang, “SoK: DAG-based Blockchain Systems,” *ACM Comput. Surv.*, vol. 55, no. 12, 2023, doi: 10.1145/3576899.

[6] G. C. Sekhar and R. Aruna, “An Integrated Secure Scalable Blockchain Framework for IoT Communications,” *J. Sci. Ind. Res. (India).*, vol. 82, no. 1, pp. 50–62, 2023, doi: 10.56042/jsir.v82i1.69929.

[7] C. Fan, Y. Chen, P. Musilek, S. Ghaemi, and H. Khazaei, “Performance Analysis of the IOTA DAG-based Distributed Ledger,” *ACM Trans. Model. Perform. Eval. Comput. Syst*, no. September, p. 21, 2021, [Online]. Available: https://doi.org/10.1145/1122445.

1122456

[8] N. Zivic, E. Kadusic, and K. Kadusic, "Directed Acyclic Graph as Hashgraph: An Alternative DLT to Blockchains and Tangles," *2020 19th Int. Symp. INFOTEH-JAHORINA, INFOTEH 2020 - Proc.*, pp. 2019–2021, 2020, doi: 10.1109/INFOTEH48170.2020.9066312.

[9] M. Al-Shabi and A. Al-Qarafi, "Improving blockchain security for the internet of things: challenges and solutions," *Int. J. Electr. Comput. Eng.*, vol. 12, no. 5, pp. 5619–5629, 2022, doi: 10.11591/ijece.v12i5.pp5619-5629.

[10] S. Akbulut *et al.*, "Designing a Private and Secure Personal Health Records Access Management System: A Solution Based on IOTA Distributed Ledger Technology," *Sensors*, vol. 23, no. 11, 2023, doi: 10.3390/s23115174.

[11] S. Wang, H. Li, J. Chen, J. Wang, and Y. Deng, "DAG blockchain-based lightweight authentication and authorization scheme for IoT devices," *J. Inf. Secur. Appl.*, vol. 66, no. March, p. 103134, 2022, doi: 10.1016/j.jisa.2022.103134.

[12] T. Alsboui, Y. Qin, R. Hill, and H. Al-Aqrabi, "Enabling distributed intelligence for the Internet of Things with IOTA and mobile agents," *Computing*, vol. 102, no. 6, pp. 1345–1363, 2020, doi: 10.1007/s00607-020-00806-9.

[13] C. Fan, H. Khazaei, Y. Chen, and P. Musilek, "Towards a scalable dag-based distributed ledger for smart communities," *IEEE 5th World Forum Internet Things, WF-IoT 2019 - Conf. Proc.*, pp. 177–182, 2019, doi: 10.1109/WF-IoT.2019.8767342.

[14] N. Zivic *et al.*, "Directed Acyclic Graph as Hashgraph: An Alternative DLT to Blockchains and Tangles," *2020 19th Int. Symp. INFOTEH-JAHORINA, INFOTEH 2020 - Proc.*, vol. 21, no. 6, pp. 2019–2021, 2020, doi: 10.1109/WF-IoT.2019.8767342.

[15] S. Suhail, C. S. Hong, and A. Khan, "Orchestrating product provenance story: When IOTA ECOSYSTEM meets the electronics supply chain space," *arXiv*, 2019.

[16] X. Zheng, S. Sun, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Meré, "Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies," *J. Med. Internet Res.*, vol. 21, no. 6, Jun. 2019, doi: 10.2196/13583.

[17] A. . Mushi, "Masked Authenticated Massage." https://iota-news.com/iota-mam-eloquently-explained/ (accessed Nov. 15, 2020).

[18] M. Lucking, R. Manke, M. Schinle, L. Kohout, S. Nickel, and W. Stork, "Decentralized patient-centric data management for sharing IoT data streams," *2020 Int. Conf. Omni-Layer Intell. Syst. COINS 2020*, 2020, doi: 10.1109/COINS49042.2020.9191653.

[19] W. F. Silvano and R. Marcelino, "Iota Tangle: A cryptocurrency to communicate Internet-of-Things data," *Futur. Gener. Comput. Syst.*, vol. 112, pp. 307–319, Nov. 2020, doi: 10.1016/j.future.2020.05.047.

[i] https://github.com/iotaledger/hornet