A Scalable Decentralized and Lightweight Access Control Framework Using IOTA Tangle for the Internet of Things

Tariq Alsboui[1], Muhammad Hussain[1], Hussain Al-Aqrabi[2], Richard Hill[1] and Mohammad Hijjawi[3]
[1]*University of Huddersfield, U.K.*
[2]*Higher Colleges of Technology, U.A.E.*
[3]*Applied Science Private University, Jordan*

Keywords: Internet of Things (IoT), Access Control, IOTA Tangle, Masked Authenticated Messaging (MAM), Restricted Mode.

Abstract: With the vast development of Internet-of-Things (IoT) ecosystem, various types of information, such as healthcare records and physical resources, are integrated for different types of applications. Due to the sheer number of connected IoT devices, which generate a large amount of data, Distributed Ledger Technology, such as Blockchain and IOTA have been recently applied in developing access control models, yet they involve significant energy due to mining, low throughput, non-scalable, and computational overhead that is not acceptable for IoT resource-constrained devices. In this paper, we propose a Scalable Decentralized and Lightweight Access Control framework (SDAC) by using the IOTA platform. IOTA is an emerging distributed ledger technology that has significant features for IoT, such as zero fees transactions, scalability, security and energy efficiency. The proposed SDAC aims to improve security, authorize, and authenticate users when accessing data by using the IOTA Masked Authenticated Messaging (MAM) protocol. MAM ensures access control by encrypting and granting permission to only authorized users. The experimental results indicate that IOTA MAM is a feasible solution that can be used for managing authorization in the IoT domain.

1 INTRODUCTION

Over the last few years, various branches of Artificial Intelligence, have been widely adopted for delivering services across numerous domains, from industrial defect detection (Hussain et al., 2022c), healthcare (Hussain et al., 2022d) renewable energy (Hussain et al., 2022a), intelligent transportation (Perera et al., 2017; Sumalee and Ho, 2018) and preservation of food quality (Hussain et al., 2022b). Internet of Things (IoT) interconnects heterogeneous devices with diverse functionalities to meet the evolving requirements of the earlier mentioned domains (Al-Fuqaha et al., 2015). IoT devices are characterised by limited resources, such as power consumption, memory and processing (Alsboui et al., 2021a). Research reports estimate the rapid growth of IoT; in the order of 125 billion devices connected to the Internet in 2030 (Cisco, 2016; Gartner, 2013; Research, 2013). Consequently, this presents many challenges with regards to data that comes in greater volume, velocity and variety, timely processing, privacy and scalability (Al-Aqrabi et al., 2019; Alsboui et al., 2020).

IoT devices, in particular sensors are usually deployed without careful security consideration. This results in critical security issues. It has been reported that one issue related to security is unauthorized access to the IoT resources, which has been extensively studied in (Neshenko et al., 2019). As IoT data contains personal information and IoT devices equipped with sensors are often deployed in close proximity to human bodies, without providing an appropriate *access control* mechanism to the IoT resources, our data and safety would be significantly threatened.

Authorization and access control are fundamental challenge determining the successful implementation of many IoT applications. Authorization can be defined as the process of enabling the right access to authorized users. Access control is considered as the backbone technology to ensure information security. It provides the opportunities to overcome some of the IoT technical challenges. It can be defined as a technique that restricts access to resources (i.e., objects) to only the authorized users (i.e., subjects). Access control will ultimately monitor the access of resources and prevent the unauthorized flow of informa-

Alsboui, T., Hussain, M., Al-Aqrabi, H., Hill, R. and Hijjawi, M.
A Scalable Decentralized and Lightweight Access Control Framework Using IOTA Tangle for the Internet of Things.
DOI: 10.5220/0011963600003482
In *Proceedings of the 8th International Conference on Internet of Things, Big Data and Security (IoTBDS 2023)*, pages 178-185
ISBN: 978-989-758-643-9; ISSN: 2184-4976

tion. However, traditional access control methods and techniques cannot fully solve the access control problems faced by the IoT due to centralization, which represents a single point of failure (Qiu et al., 2020).

Distributed Ledger Technology (DLT) is an emerging development that shares data among different participants deployed over various locations all over the world. This technology provides several benefits to various IoT applications. Literature reveals a growing interest of relevant research community in DLT, considering it one possible solution to address some of the IoT related challenges, such as scalability, access control, security and privacy. (Alsboui et al., 2020; Fan et al., 2019).

Most recently, IOTA technology, a paradigm shift, is changing the infrastructure for the major application areas of IoT by enabling a decentralized environment with anonymous and trustful transactions. The combination of IoT and IOTA technology brings many benefits including less operational cost, decentralized resource management, scalability, and robustness against attacks. This indicates that the convergence of IoT and IOTA technology will ultimately overcome the significant challenges identified in the IoT domain.

In this paper, we propose a Scalable Decentralized and Lightweight Access Control framework by using the IOTA Masked Authenticated Messaging (MAM) (See Section 2 for Further Details) as a suitable solution to tackle the scalability, and authorization issues for IoT applications. MAM is a second layer data communication protocol that is used to authenticate, and encrypt data streams via the use of a set of operations, such as public, private, and restricted.

Contributions. In this paper, we propose a system architecture for IoT, called Scalable Decentralized and Lightweight Access Control framework (SDAC). This framework addresses access control issues in IoT, whilst supporting the popular proof-of-work (PoW) mechanism in an energy-efficient way. The key contributions can be summarized as follows:

- A Scalable decentralized and lightweight access control framework that ensures scalability and efficiency in authorizing access to data by using the IOTA MAM protocol with a set of operations.
- Evaluation of an existing Proof of Work (PoW) offloading mechanism for efficacy with regard to energy efficiency and transaction throughput.
- Preliminary experimental results to verify the effectiveness and scalability of the proposed framework.

The rest of this paper is organized as follows: Section 2 presents an overview of the IOTA platform and a detailed description of the masked authenticated messaging. Section 3 presents the recent research efforts in access control models in the IoT domain. In Section 4, we describe our scalable decentralized and lightweight access control framework. Section 5 presents an implementation of the proposed framework and analysis of the results. Finally, in Section 6, we conclude the paper and discuss future work.

2 IOTA PLATFORM: AN OVERVIEW

Currently, IOTA is scheduled to undergo a two-part protocol upgrade, IOTA 1.5 (Chrysalis), which is the current network and IOTA 2.0 (Coordicide), aimed at implementing a series of major DLT technology advancements to improve network functionality and achieve greater decentralization. The IOTA 1.5 introduces a protocol enhancements that enable smart contract functionality, tokenized assets and stable coins, which could enable new use cases for consumer and enterprise IoT applications, an implementation of product features including: reusable addresses, UTXO, new Firefly wallet, and new libraries and Application Programming Interface (APIs) for an improved developer experience. The IOTA 2.0, implements a new consensus mechanism that aims to improve IOTA's scalability, security, and decentralization by removing the centralized Coordinator node.

The architecture of the IOTA tangle is an evolving DLT platform aimed at addressing transaction costs, mining and scalability issues (in the context of Blockchain technology) (Zhang and Jacobsen, 2018), that are related to IoT. The architecture of a *Tangle* (Serguei, 2017), which is central to IOTA, a DAG that offers a potentially scalable IoT-enabled applications. *Tangle* can be used to build IoT applications. However, tangle has the advantages of being intuitively understandable.

IOTA technology offers the necessary data access authorization for IoT applications. In the context of transactions, IOTA may promote IoT interactions. This approach radically changes the overall design, development, implementation and management process of IoT systems.

2.1 The Tangle

The IOTA Tangle was developed to cope with the requirements of IoT applications such as privacy, and security. Tangle is built upon a Directed Acyclic Graph (DAG), which is considered to be the ledger that stores transactions. The Tangle is the data

structure that consists of a collection of sites and edges (Serguei, 2017) as shown in Fig. 1. In order to issue a transaction by a node, the node should work to approve two previous transactions. Choosing the two previous transactions is done by using the tip selection technique whereby default is the Markov Chain Monte Carlo (MCMC) technique (Serguei, 2017). Fig. 1 shows that the green boxes represent confirmed transactions, while the red boxes are unconfirmed transactions and the grey boxes represent tips without any validation. The main aim of the Tangle network is to make all the transactions to be confirmed and to make all the unconfirmed transactions to confirmed transactions. The MCMC technique is executed n number of times Genesis is the first transaction of the network, which is approved directly or indirectly by the other transactions.

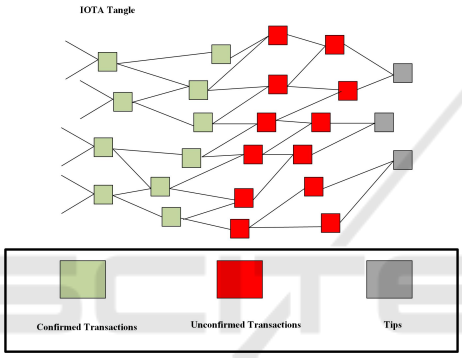

Figure 1: IOTA Tangle is based on a Directed Acyclic Graph (DAG).

The IOTA Tangle is designed in a way to enable transactional settlement to be more scalable, more the transactions made more secure and efficient the tangle gets (Serguei, 2017).

2.2 Masked Authentication Messaging

IOTA developed a second layer data communication protocol, called Masked Authenticating Messaging (MAM) (Handy, 2017), which is responsible for masking, authenticating, and encrypting data streams. Consequently, data streams are broadcasted and retrieved through the Tangle as zero fee transactions. Given these properties, MAM fulfills an important need in which integrity and access control are required.

Every MAM data transaction is linked with an address in which a user can refer to the transaction. Data transactions would be transmitted using the MAM protocol at any point in time, but a small amount of Proof of Work (PoW) is needed in order to broadcast data streams to the IOTA network. Transaction data broadcasted using MAM are linked together in chronological order. Furthermore, a signature of the user is attached to all MAM data streams. This ensures that subscribers are required to verify the authenticity of the user. By adopting MAM, users will certainly ensure safety when exchanging data to the Tangle.

MAM transactions can be broadcasted and fetched from the IOTA Tangle, by communicating with a fully functional node. This indicates that an IoT device will be able to transmit encrypted data streams using the IOTA MAM protocol.

2.2.1 MAM Privacy and Encryption Operations

MAM enables encryption to occur through several operations including: public, private, and restricted. In public operation, the user uses the tree's root as the address of the transaction that the message is published to. A user will be able to decode it by using the address of the message. Public operation enables any user to read the content of the data, but it adds immutability and data integrity.

In the case of private operation, there is an added level of security that controls the access in order to be able to read the content of the transaction data. It enables access to users who have only the hash of the channel key. The users would request the tangle for the hash of the channel key. Then, it would enable them to decode the transaction data by using the channel key.

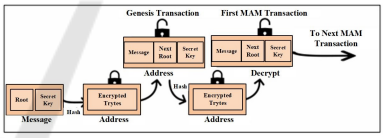

Figure 2: The process of publishing transaction using restricted operation.

In the case of restricted operation, it adds an authorization key to the private operation. The address used to attach to the network is the hash of the authorization key and the Merkle root. It also offers granular access to users who have the secret key. Therefore, access would be revoked from users if needed. If the secret key change, the new authorized key is required and should be distributed to the users that needs to gain access to the data. Fig. 2 describes the process of sending data using the restricted operation.

3 RELATED WORK

There has been sustained research into access control models for IoT over the last few years. In a recent

publication (Ravidas et al., 2019), the authors classified access control models into six categories including: Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-based Access Control (RBAC), Organization-Based Access Control (OrBAC), Attribute-based Access Control (ABAC), and Usage Control (UCON). For a comprehensive and recent literature review, we refer the interested readers to (Ravidas et al., 2019) and the references therein. Such research efforts focused on developing access control models for IoT. However, there has been little attention on how to manage the scalable IoT infrastructure.

Recently, the authors in (Shafeeq et al., 2019) introduced a new decentralized access control system based on the Tangle. The system empowers the users to dictate the access to their resource. The proposed decentralized access control model allows the policies and access rights to be published on the Tangle. Therefore, it guarantees distributed auditability and prevents the user from fraudulently denying the granted access rights. The proposed system is scalable, introduces low delays, and has zero transaction fees. However, resource constraints of IoT devices such as power consumption is not taken into consideration.

In (Nakanishi et al., 2020), a novel access control framework based on IOTA and the Ciphertext Policy Attribute-based Encryption (CP-ABE) CP-ABE technology is proposed. The framework works according to three phases including: token structure, access right authorization, and access right verification. In token structure, a token contains a unique ID, the issuer, the address it is linked with on the Tangle, the policy that must be satisfied to decrypt the token, and a list of access rights. In the authorization phase, the object owner first decides the policy embedded into the token and the corresponding access rights to specify which group of subjects can perform what actions to the object. Finally, the access right verification After successfully decrypting the token, a subject can send the object owner an access request. The request is also encrypted using CP-ABE and there is no need to establish a secure communication channel between the subject and the object owner. The proposed system is scalable and has zero transaction fees. However, the system does not take into consideration the limited energy consumption and computation of IoT devices.

Similarly, an access control mechanism called, Decentralized Capability-Based Access Control framework (DCACI) is introduced in (Pinjala and Sivalingam, 2019). The DCACI framework enables complete privacy and integrity of the capability tokens using IOTA's Masked Authenticated Messaging (MAM) protocol. It enables device owners and users to Grant, Update, Delegate and Revoke the capability tokens. The proposed DCACI framework is scalable, requires less delay, provides fine-grained access control mechanism for IoT networks and has zero transaction fees. However, the framework does not take into consideration the limited energy consumption and computation of IoT devices.

Different from the above is the work proposed in (Maesa et al., 2017) in which a new approach based on blockchain technology to publish the policies expressing the right to access a resource and to allow the distributed transfer of such right among users. The proposed system uses the policies and the rights exchanges, which are publicly visible on the blockchain. The proposed solution allows distributed auditability, preventing a party from fraudulently denying the rights granted by an enforceable policy. However, the system lacks scalability and is not specifically designed for constrained IoT devices.

In (Andersen et al., 2017) the authors propose WAVE an authorization scheme based on Ethereum Smart Contracts. Wave uses Delegations of Trust (DoTs) and Identity-Based Encryption (IBE). The DoTs together form a global permission graph which spans different trust domains. A proof of authorization is a chain of DoTs. WAVE enables the relevant parties to look up such proofs of delegation efficiently. The IBE allows a party to encrypt a message using a global public key and the identity of the receiver instead of that receiver's public key. In order to decrypt, the receiver must be granted a secret key for his identity by a global trusted entity. The Wave approach provides a powerful means of federating networks of embedded networks and supporting the life cycles of devices, services, smart environments, infrastructures, and individuals. However, it lacks support for resource constrained IoT devices.

4 PROPOSED APPROACH

Fig. 3 presents an abstract view of the system architecture of the proposed Scalable Decentralized and Lightweight Access Control Framework (SDAC). It shows all relevant components including IoT devices, transaction data flow, Node JS with MAM, Gateway, and PoW computation offloading server. The IoT devices are mainly responsible for transmitting transaction data using MAM client and sends transaction data to a receiver, which is the gateway. The gateway is connected to the internet and transmits transactions data to a server, which runs the Node JS Masked

Authenticated Messaging (MAM) application. The Node JS MAM is responsible for transmitting transaction data to the IOTA Tangle. For example, the transaction data flow from IoT devices (e.g., dash lines) represents the way how transaction data is transmitted to the IOTA Tangle using MAM.

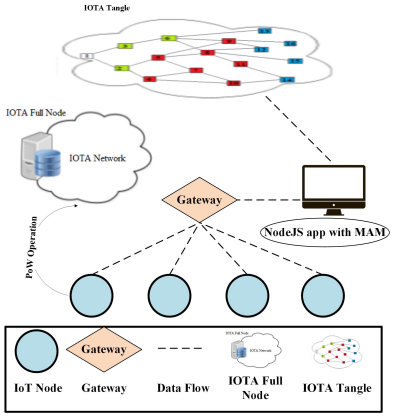

Figure 3: The proposed scalable decentralized and lightweight access control framework (SDAC).

The PoW enabled server is concerned with performing heavy computation tasks on behalf of constrained IoT devices.

The flowchart of the proposed SDAC framework is shown in Fig. 4. First, the MAM state is initialized using the main Tangle provider. After MAM state is initialized, its patched with the Proof of Work (PoW) for performing the PoW, which patches MAM sate with the PoW Provider. Then, the channel mode is set to restricted on the MAM state. Once this step is completed, the payload is created and prepared to be transferred to the main Tangle. Then, the PoW is performed on the PoW provider. Once the PoW is completed, the payload will be attached to the main Tangle. In order for users to be able to access healthcare records, the root ID and the correct secret key should be provided. Therefore, If the correct secret key is provided, grant access to that user otherwise deny access.

4.1 PoW Offloading

There are two types of offloading including: data offloading and computation offloading. Data offloading refers to the use of novel network techniques to transmit mobile data originally planned for transferring via cellular networks, while computation offloading refers to offloading heavy computation tasks to reserve resources (Zheng et al., 2020). Fig. 5 illustrates the PoW computation offloading mechanism used in the SDAC framework. It shows how constrained IoT

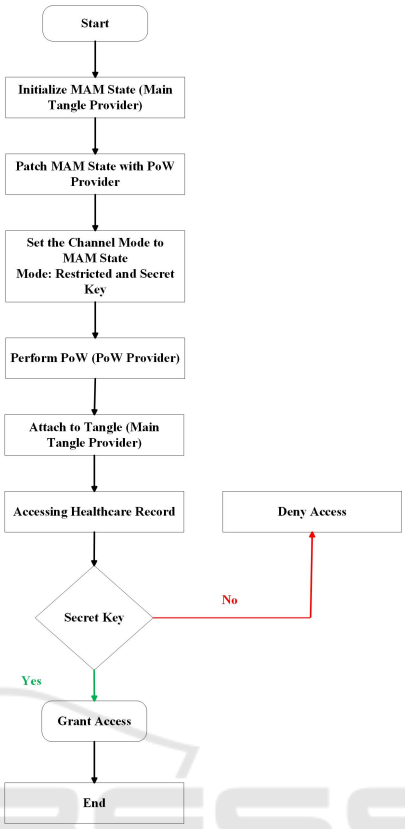

Figure 4: Flowchart of the basic SDAC framework.

devices in terms of power are able to offload the PoW computation to a node with higher resources. The selected node is an IOTA full node, which is responsible for performing the PoW as described in Fig. 5.

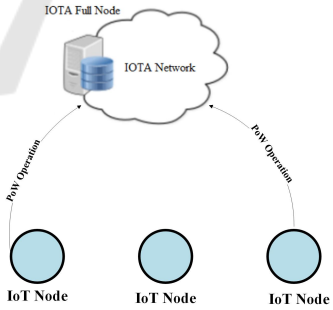

Figure 5: PoW Computation Offloading in SDAC framework.

5 IMPLEMENTATION, RESULTS AND ANALYSIS

In this section, we report the preliminary experimental findings of our proposed SDAC framework, which indicate its effectiveness in terms of access control,

authorization, and scalability for IoT healthcare application. Furthermore, we provide analysis and discussion of the results

5.1 Environment Setup

The implementation of our proposed SDAC framework is based on Node JS. The functionality related to IOTA addresses, transactions, broadcasting, and multi-signatures has been implemented using iota.lib.js (Foundation, 2018), the official JavaScript library of the IOTA MAM Distributed Ledger Techology, which allows issuing and fetching MAM transactions. We simulated a network using the IOTA devnet [1] as clients, which in turn interacts with an IOTA full node to issue and fetch data using MAM. In addition, another IOTA full node was deployed on a local server dedicated for performing the Proof of Work (PoW) operation.

The implementation focuses on the public and restricted operations of MAM. Public operation is utilized to ensure authenticity, and data integrity, while restricted operation enables users to control access to healthcare records using the secret key. This is particularly useful for healthcare applications where permissions is required in order to gain access to sensitive data.

5.2 Results and Analysis

Fig. 6 shows the result of sending transaction data to the Tangle using public operation. It also shows the output of fetching masked transaction data in which the user would only require the root, which is the encryption and decryption key. The transaction data sent using public operation ensures authenticity and data integrity i.e., confirming that the data is coming from a particular IoT device. The public operation uses the root as the address of the transaction that contains the MAM message (channel ID). Consequently, any user can find and decrypt the message in a public operation by using the address.

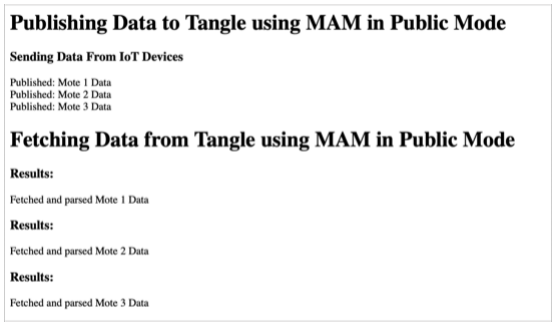

Figure 6: Publishing transaction data from IoT devices using Public Operation.

[1] https://nodes.devnet.iota.org

Sending Transactions with Restricted Operation. Fig. 7 shows the result of publishing transactions data using the restricted operation.

Figure 7: Publishing transactions from IoT devices using Restricted operation.

Access Right Authorization. Restricted operation enables granular access control to transaction data and provides authorization to the transaction data stored on the Tangle. It only allows participants who have the secret key to decode the transaction data. Fig. 8 demonstrates the granular access control over the transaction data stored on the Tangle. It also shows that when a user fetches transaction data, access will be authorized, and a user is allowed to decrypt the transaction data by having the secret key. Therefore, access will be authorized.

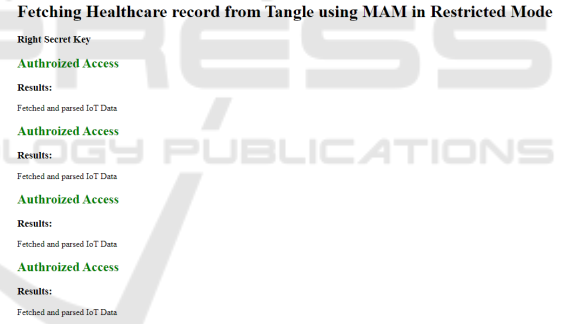

Figure 8: Accessing transaction data with right secret key (Authorized Access).

Unauthorized Access. Fig. 9 demonstrates the use of restricted operation with the wrong secret key. A user who has the wrong secret key will be unable to access the transaction data stored on the Tangle. It also shows that when a user is attempting to fetch the transaction data by having the wrong secret key, access will be unauthorized. This is in turn useful in IoT healthcare application in which users will have the ability to control who can gain access to their healthcare records.

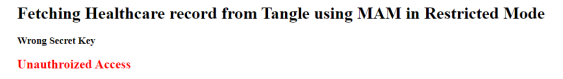

Figure 9: Accessing transaction data with wrong secret key (Unauthorized Access).

PoW Execution Time. Fig 10 shows the result of the execution time when offloading the PoW compared to the baseline. As it can be seen from Fig 10 that when the number of sent transactions are 100, the execution time of the PoW reaches 1177.5 second and the baseline reaches 1440.1 second. This is because the PoW is being offloaded to a dedicated node with higher resources, while in the baseline the PoW is computed on the same IoT device.

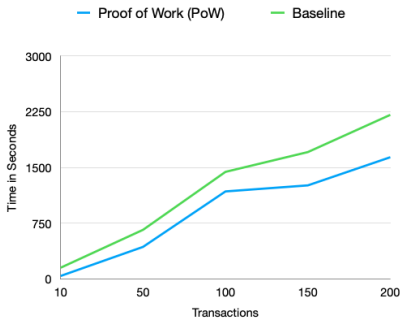

Figure 10: PoW execution time compared to the baseline.

Scalability. Fig 11 shows the result of the SDAC framework in terms of scalability with different Minimum Weight Magnitude (MWM) settings, and different number of nodes. it is clear that as the number of nodes increases, the Transaction Per Second (TPS) transaction speed increases linearly. Consequently, the transaction speed has a good linear scalability when the number of nodes increases. Also, its clear that when 100 nodes are sending transactions, the average TPS reaches 1.543 tx/s when the MWM is set to 14, while the average TPS reaches 1.764 tx/s when the MWM is set to 9.

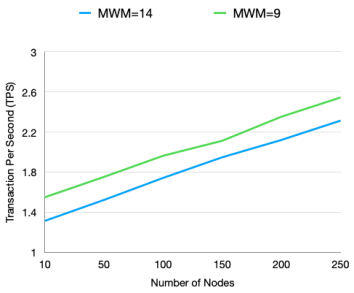

Figure 11: Scalability in Tangle with 250 nodes.

6 CONCLUSION AND FUTURE WORK

In this paper, we have addressed the issue of access control in IoT by using the IOTA distributed ledger technology. Specifically, we have employed the IOTA MAM protocol using a set of operations, such as public and restricted, to grant granular access to data. In order to achieve access control and ensure scalability, a scalable decentralized and lightweight access control framework, called SDAC, has been proposed.

There are a number of interesting directions for future work. We plan to thoroughly investigate the reduction in energy consumption and improve the scalability of the proposed approach by looking into processing access requests per unit time that measures the execution time of various processes such as, attach, encrypt, and decrypt. Then, we plan to develop an interactive model that enables the users to enter the secret key to be able to access the data.

Finally, we plan to introduce the concept of mobile agent (Alsboui et al., 2016), in particular multi-mobile agent with a *dynamic* multi-mobile agent itinerary planning mechanism (Alsboui et al., 2021b) for data collection from healthcare sensors and employ techniques of information extraction (Alsbouí et al., 2011) in order to further improve the performance of the proposed SDAC framework.

REFERENCES

Al-Aqrabi, H., Pulikkakudi Johnson, A., Hill, R., Lane, P., and Liu, L. (2019). A multi-layer security model for 5g-enabled industrial internet of things. In *7th International Conference on Smart City and Informatization (iSCI 2019), Guangzhou, China, November 12-15, 2019*, Lecture Notes in Computer Science, Switzerland. Springer International Publishing AG.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376.

Alsboui, T., Alrifaee, M., Etaywi, R., and Jawad, M. A. (2016). Mobile agent itinerary planning approaches in wireless sensor networks- state of the art and current challenges. volume 188, pages 143–153.

Alsbouí, T., Hammoudeh, M., Bandar, Z., and Nisbet, A. (2011). An overview and classification of approaches to information extraction in wireless sensor networks.

Alsboui, T., Qin, Y., Hill, R., and Al-Aqrabi, H. (2020). Enabling distributed intelligence in the internet of things with iota and mobile agents. *Computing*, xx.

Alsboui, T., Qin, Y., Hill, R., and Al-Aqrabi, H. (2021a). Distributed intelligence in the internet of things: Challenges and opportunities. *SN Comput. Sci.*, 2(4):277.

Alsboui, T., Qin, Y., Hill, R., and Al-Aqrabi, H. (2021b). An energy efficient multi-mobile agent itinerary planning approach in wireless sensor networks. *Computing*, 103(9):2093–2113.

Andersen, M. P., Kolb, J., Chen, K., Fierro, G., Culler, D. E., and Popa, R. A. (2017). Wave: A decentralized authorization system for iot via blockchain smart

contracts. *University of California at Berkeley, Tech. Rep*.

Cisco (2016). Internet of things at a glance. (1).

Fan, C., Khazaei, H., Chen, Y., and Musilek, P. (2019). Towards a scalable dag-based distributed ledger for smart communities. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pages 177–182.

Foundation, I. (2018). Iota javascript api library. (visited on 1-08-2021).

Gartner (2013). Gartner says the internet of things installed base will grow to 26 billion units by 2020. (1).

Handy, P. (2017). Introducing masked authenticated messaging. (1). (visited on 31-07-2021).

Hussain, M., Al-Aqrabi, H., and Hill, R. (2022a). Pv-cracknet architecture for filter induced augmentation and micro-cracks detection within a photovoltaic manufacturing facility. *Energies*, 15(22).

Hussain, M., Al-Aqrabi, H., Munawar, M., and Hill, R. (2022b). Feature mapping for rice leaf defect detection based on a custom convolutional architecture. *Foods*, 11(23).

Hussain, M., Al-Aqrabi, H., Munawar, M., Hill, R., and Alsboui, T. (2022c). Domain feature mapping with yolov7 for automated edge-based pallet racking inspections. *Sensors*, 22(18).

Hussain, M., Al-Aqrabi, H., Munawar, M., Hill, R., and Parkinson, S. (2022d). Exudate regeneration for automated exudate detection in retinal fundus images. *IEEE Access*.

Maesa, D., Mori, P., and Ricci, L. (2017). Blockchain based access control. pages 206–220.

Nakanishi, R., Zhang, Y., Sasabe, M., and Kasahara, S. (2020). Iota-based access control framework for the internet of things. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 87–95.

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., and Ghani, N. (2019). Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. *IEEE Communications Surveys & Tutorials*, 21(3):2702–2733.

Perera, C., Qin, Y., Estrella, J. C., Reiff-Marganiec, S., and Vasilakos, A. V. (2017). Fog computing for sustainable smart cities: A survey. *ACM Comput. Surv.*, 50(3):32:1–32:43.

Pinjala, S. K. and Sivalingam, K. M. (2019). Dcaci: A decentralized lightweight capability based access control framework using iota for internet of things. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pages 13–18.

Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., and Fang, B. (2020). A survey on access control in the age of internet of things. *IEEE Internet of Things Journal*, 7(6):4682–4696.

Ravidas, S., Lekidis, A., Paci, F., and Zannone, N. (2019). Access control in internet-of-things: A survey. *Journal of Network and Computer Applications*, 144:79–101.

Research, A. (2013). More than 30 billion devices will wirelessly connect to the internet of everything in 2020. (1).

Serguei, P. (2017). The tangle. (1).

Shafeeq, S., Alam, M., and Khan, A. (2019). Privacy aware decentralized access control system. *Future Generation Computer Systems*, 101:420–433.

Sumalee, A. and Ho, H. W. (2018). Smarter and more connected: Future intelligent transportation system. *IATSS Research*, 42(2):67–71.

Zhang, K. and Jacobsen, H. (2018). Towards dependable, scalable, and pervasive distributed ledgers with blockchains. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, pages 1337–1346.

Zheng, T., Wan, J., Zhang, J., Jiang, C., and Jia, G. (2020). A survey of computation offloading in edge computing. In *2020 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pages 1–6.