DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data

Hafida Saidi, Nabila Labraoui, Ado Adamou Abba Ari, Leandros A Maglaras, Joel Herve Mboussam Emati

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data

Hafida Saidi[1,*], Nabila Labraoui[2], Ado Adamou Abba Ari[3,4], Leandros Maglaras[5,*], And Joel Herve Mboussam Emati[4]

[1] STIC Lab, University of Abou Bekr Belkaid, Chetouane Tlemcen 13000, Algeria
[2] LRI Lab, University of Abou Bekr Belkaid, Tlemcen 13000, Algeria
[3] DAVID Lab, Université Paris-Saclay, University of Versailles Saint-Quentin-en-Yvelines, 45 Avenue des États-Unis, 78000, Versailles, France
[4] Department of Computer Science, University of Maroua, Maroua P.O. Box 814, Cameroon
[5] School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK

Corresponding author: Hafida Saidi (hafida.saidi@univ-tlemcen.dz), Leandros Maglaras(leandros.maglaras@dmu.ac.uk)

ABSTRACT In recent years, the interest in using wireless communication technologies and mobile devices in the healthcare environment has increased. However, despite increased attention to the security of electronic health records, patient privacy is still at risk for data breaches. Thus, it is quite a challenge to involve an access control system especially if the patients' medical data are accessible by users who have diverse privileges in different situations. Blockchain is a new technology that can be adopted for decentralized access control management issues. Nevertheless, different scalability, security, and privacy challenges affect this technology. To address these issues, we suggest a novel Decentralized Self-Management of data Access Control (DSMAC) system using a blockchain-based Self-Sovereign Identity (SSI) model for privacy-preserving medical data, empowering patients with mechanisms to preserve control over their personal information and allowing them to self-grant access rights to their medical data. DSMAC leverages smart contracts to conduct Role-based Access Control policies and adopts the implementation of decentralized identifiers and verifiable credentials to describe advanced access control techniques for emergency cases. Finally, by evaluating performance and comparing analyses with other schemes, DSMAC can satisfy the privacy requirements of medical systems in terms of privacy, scalability, and sustainability, and offers a new approach for emergency cases.

INDEX TERMS Blockchain, data privacy, decentralized access control, decentralized IDentifier (DID), IoMT sensors, Self Sovereign Identity (SSI), smart contract, verifiable credential (VC).

I. INTRODUCTION

Over the past few decades, the world has become more connected with the wide adoption of networking and wireless communication technologies, and mobile devices. This evolution let the healthcare organizations and researchers think about benefiting from these technologies to solve the current challenges that the medical technologies are facing, by transforming unsustainable healthcare systems into sustainable ones [1] [2].

Patients are increasingly exploiting mobile devices for their medical needs to promote the availability of their medical data and to help avoid repeated examinations. However, the sharing and the privacy of medical data represent major technological, legal, and operational challenges [3]. Likewise, the identification of the patient is of critical importance for performing transactions with different healthcare organizations [4]. But by using different identifiers, patients find themselves having to maintain or memorize many combinations of accounts, and they may get interoperability issues, identity loss/theft, and privacy issues. To improve the user identity model, we are considering the concept of Self Sovereign Identity (SSI) [5]. SSI is a new model for digital identity. It helps to prove who we are and establish trusted relationships to access information [6]. SSI can also facilitate the linking of patients' health records from multiple healthcare organizations for research and medical purposes. Lacity and Carmel have used SSI technology for designing digital staff passports for the United Kingdom National Health Service [7]. SSI has also been introduced for birth registration in Kenya by Freytsis [8].

Subsequently, the patients' medical data are accessible by individuals who have diverse privileges under different situations. Indeed, the deployment of an access control model took part in this area. Traditional access control mechanisms, like the Role-based Access Control (RBAC)

[9] and the Attribute-based Access Control (ABAC) [10], have been frequently utilized in the Internet of Medical Things (IoMT) systems. However, they adopt a centralized architecture by outsourcing the data's control to trusted third parties and preventing the patient from controlling his data. Unfortunately, these access control models are suffering several issues due to the third party's interference, and the patients' privacy that may be seriously breached if no safety measures were been taken. In addition, these access control mechanisms are unable to provide a manageable, scalable, and efficient solution to address new issues caused by IoMT networks. Likewise, the IoMT devices generally have constrained resources in regards to their low computation power, limited battery life, small size, and small memory.

The aforementioned issues will need an evaluation of access control technologies and the suggestion of a new access control model that assures decentralized authentication and authorization techniques in untrusted environments. In addition, the IoMT devices need cryptographic solutions to meet the security, privacy and trust requirements. Hence, one of the practical solutions is to securely outsource the computations to an external and more powerful device to reduce the computational cost of cryptographic computations and maintain data confidentiality [aa].

Proposing a blockchain technology in that situation can be more beneficial for the healthcare requirements in terms of immutability, decentralization, traceability, transparency, and data security and privacy [11], [12], [13], [21]. Notably, several researches have been conducted on blockchain-based decentralized access control system [12], [13], [14], [15], [16]. However, they do not provide solutions for emergency cases in which the patient is unable to grant access to doctors. To address these issues, the combination of blockchain and SSI technologies will lead to good effects.

Therefore, this paper proposes a novel Decentralized Self-Management of data Access Control (DSMAC) system using a blockchain-based Self-Sovereign Identity (SSI) model for privacy-preserving medical data, empowering patients with mechanisms to preserve control over their personal information and allowing them to self-grant access rights to their medical data.

DSMAC is distinct from the works discussed in the literature by integrating a hybrid level of the decentralized access control model which considers both the "role" concept and the "attributes" as important topics. By utilizing the smart contract, we integrate RBAC model into blockchain which is a better fit for IoMT than other access control systems. Additionally, ABAC is a model that can provide expressive fine-grained access control in an emergency case.

In the experiments, we use the hyperledger indy [17], an open-source version of permissioned blockchain, to create and evaluate our decentralized access control mechanism. Experimental results based on low-latency, and privacy-preserving medical records demonstrate the effectiveness of the DSMAC scheme.

In brief, our main contributions are as follows:

1. We implement a decentralized access control model based on role and attribute models.
2. We use smart contract functionalities to issue or modify the role-based access control policies.
3. An SSI-based decentralized access control system is integrated to preserve data privacy.
4. We formulate an attribute-based access control mechanism by using DID document.
5. Protect patient's medical data via encryption security algorithms.
6. The simulation results show that our proposed scheme gives better results in execution time as well as transaction throughput and latency.

The remainder of this paper is organized as follows: In Section 2, we review and discuss existing techniques to address the problem of decentralized access control for healthcare systems. In Section 3, we provide background knowledge. We formally define the models and security requirements in Section 4, followed by our proposed decentralized access control scheme in Section 5. Security and privacy analysis are described in Section 6. We report and discuss evaluation results in Section 7. Finally, we conclude the paper.

II. RELATED WORK

In this section, we have introduced a brief review related to decentralized access control systems in the healthcare environment. Further, these works have been divided into two sections. The first one represents the blockchain-based access control research in the healthcare environment. The second one highlights a few works in decentralized access control management-based SSI systems.

A. BLOCKCHAIN-BASED ACCESS CONTROL

Smart contracts and blockchain technologies are frequently used in several domains. This section focuses on the development of access control techniques using blockchain-based healthcare systems. Yue et al. [13] suggested a Healthcare Data Gateway (HGD) system which is a decentralized platform based on blockchain for gathering, sharing, and storing patient health records. The proposed access model ensures patient owns and controls their health records. However, the issue with [13] lies in the size of the blocks. Storing all of the patient's medical records on a blockchain would dramatically increase the blockchain's size, requiring much more storage at each node.

Vora et al. [18] proposed a framework based on several contracts to enable secure Electronic Health Records (EHR) access control and protect the privacy of patients through the consensus protocol Proof of Vote

(PoV). However, the deployment of the differential privacy approach generates a large computational cost overhead in blockchain. Madine et al. [19] designed a decentralized data sharing system in which Oracle nodes' proxy re-encryption is used to grant EHRs access privileges. However, the system is useless in emergency cases where the patient is unable to grant access to doctors. Xu et al. [12] illustrated the Healthchain system which supports access control and protects privacy while storing data in the InterPlanetary File System (IPFS) storage system via a hybrid blockchain system. However, the doctor can still access the data even though the patient can revoke the permissions by providing a new IoT key to the doctor.

Kumar et al. [15] used smart contracts to construct dynamic access control policies. Dagher et al. [16] introduced Ancile, a blockchain that enables patients and other parties to access medical records. It uses advanced cryptographic methods for security and smart contracts-based blockchain to provide better access control models. However, this approach is vulnerable to DoS attacks. To address issues of the blockchain-based cloud-centric IoMT healthcare system, Egala et al. [21] proposed a decentralized Selective Ring-based Access Control mechanism (SRAC) with a blockchain-based Distributed Data Storage System (DDSS). Similarly, Zhang et al. [14] authors have proposed the block-based access control scheme (BBACS) for sharing and accessing medical data. Authors have designed a proxy layer to facilitate access control rights to the peers. However, the proposed system did not explain how to define the access control scheme for various types of peers. Tao and Ling [1] presented a practical health data sharing scheme based on blockchain and decentralized attribute-based encryption. The blockchain is used to grant authorizations and manage data. To ensure privacy and security, fine-grained access control of health data uses decentralized attribute-based encryption. However, to simplify the management of patients' health data and enhance privacy protection, the authors should use proxy re-encryption and zero-knowledge proof. Xia et al. [22] proposed a blockchain-based health data-sharing (BBDS) approach that overcomes the access control difficulties associated with medical records stored in the cloud. The scheme grants access to only approved and requested participants, and the blockchain records a log of their activities. Furthermore, the authors use smart contracts and an access control scheme [23] to successfully monitor data usage and revoke access to offending entities when permissions on data are violated. Rajput et al. [24] presented a permissioned blockchain-based emergency access control management system (EACMS) built on and powered by smart contracts. However, the privacy and authentication processes are not defined. Although, there is not any information about data storage if the medical data will be kept off-chain.

B. SSI-BASED ACCESS CONTROL

Self-sovereign identity, SSI, is a novel digital identity model, it helps to prove who we are to establish trusted relationships to access information [6]. Belchior et al. [25] proposed a Self-Sovereign Identity Based Access Control system (SSIBAC), an access control system for managing identities across organizations. SSIBAC offers decentralized authentication and centralized authorization using a traditional access control architecture with blockchain technology. Lagutin et al. [26], presented an OAuth-based method for delegating the access policy management to the authorization server, allowing systems with limited IoT devices to benefit from Decentralized ID (DID) and Verifiable Credentials (VCs). However, to determine whether DIDs are the right approach for the IoMT devices, a complete threat analysis must be performed before using DIDs for IoMT. Jung [27] proposed a decentralized access control system based on DID and explained how the proposed approach grants access privileges without a centralized authority. However, this may not be an ideal proposition against hacking as with other centralized systems. Kim et al. [28] present a DID-based ABAC to address the issue of ABAC's privacy exposure and implement it on a power transaction platform. Additionally, the privacy of the users can be preserved by using a verifiable credential verification process.

The main objective of the aforementioned articles is to establish access control systems for medical records and provide patients control over their medical data. However, the majority of the solutions cannot overcome the emergency cases issue. To address these limitations, we propose in this paper an efficient privacy-preserving decentralized access control scheme using both blockchain and self-sovereign identity (SSI) systems to provide better management of access control policies and resolve issues of emergencies. Our framework differs from the works reviewed in the literature by proposing the hybrid level of the decentralized access control model which considers both the "role" concept and the "attributes" as important topics. As a consequence, security and privacy with efficient access control policies remain a pivotal issue, and this is what we attempt to address in this study.

III. BACKGROUND KNOWLEDGE

In this section, we discuss the necessary background of our proposed system. First, we discuss the Self-sovereign identity (SSI) ecosystem. Then, we present different components of a blockchain.

A. SELF-SOVEREIGN IDENTITY (SSI)

Self-sovereign identity (SSI) is a decentralized approach for verifying credentials in online relationships. SSI aims to empower individuals to possess and control digital proofs of their credentials. Thus, SSI is a new model for digital identity. It helps to prove who we are to establish trusted relationships to access information [6]. It includes some standards like Verifiable Credential (VC) and Decentralized IDentifier (DID) [29]. Both are the twin pillars of SSI. Additionally, this ecosystem fulfills three key roles (issuer,

holder, and verifier). Credentials are created and issued to the holder by the issuer. A holder keeps and shares the received credentials with a verifier. A verifier accepts and approves credentials presented by a holder [30].

1) DECENTRALIZED IDENTIFIER (DID)

DID is a concept defined by the W3C [31], it is a string identifier of a subject (e.g., a person, organization, thing, etc.) controlled by a controller [32]. It consists of three parts [26]. The first one is a URL scheme identifier declared as *"did"*. The second is a DID method identifier that describes how a certain DID scheme can be used and resolved to DID documents. The last one is a DID method that communicates the information for the resolution [26].
For example: *"did:dac:patient1"*, *"did"* is URL scheme, *"dac"* is DID method and *"patient1"* is DID method-specific. In addition, DIDs help to authenticate users based on their Verifiable credentials VC (diploma, certificate) issued by different companies [33]. Thus, DIDs and VCs are useful for several aims such as reducing the cost of the issuing credential [34]. With DIDs, we can digitally sign documents or transactions, create persistent communication channels, send encrypted private messages, and also log in without usernames and passwords [35]. Fig. 1 illustrates the key elements of DID architecture, it displays the interactions between DID components.

2) VERIFIABLE CREDENTIAL (VC)

A verifiable credential (VC) is a digital file that includes several key-value claims of an entity (the subject), such as name, birth date, gender, etc [29]. VC is a standard method for digitally expressing credentials in a cryptographically secure way [36]. Credentials are created and signed by the issuer using its private key, enabling the third party to confirm the issuer of the VC (the DID of the issuer is typically associated with the credential). The verifier can search for the public key associated with a specific DID and a specific credential on a verifiable data registry (e.g., a public blockchain). A VC includes metadata, claims, and proofs. Proofs are used to verify a credential. These credentials can be self-issued or issued by a third-party [29].

B. BLOCKCHAIN

Blockchain is a technology for data transmission and storage that achieves decentralized self-management [23]. It is a database that records the history of all the transactions. This database is distributed and safe; it is accessed by various users, without intermediaries, enabling everyone to check the validity of the chain [38]. Peers in blockchain connect the blocks chronologically into a specific data structure in a chain manner [39]. The blockchain has been involved due to its decentralization, immutability, as well as persistence properties in the distributed peer-to-peer (P2P) network. Blockchain technology utilizes asymmetric cryptography to ensure transactions are done safely [38].

1) TRANSACTION

All the nodes of the network (issuer, owner, requester, and verifier) interact with each other via transactions [39]. Thus, the transaction is considered as a communication form between network nodes.

2) BLOCK

The blocks are used to store data permanently. A block contains many transactions that should not be included in another block and it uses a hash of the referenced block to refer to the previous block [38].

3) SMART CONTRACT

Smart contracts are programs stored on a blockchain that run when determined conditions are met. They are used to define more complex transactions with a flexible and programmable method [39]. Once a smart contract is published in the blockchain network, its contents are almost unchangeable, because each node in the network has the same copy of the smart contract. The blockchain stores and uses the execution record of the contract as a transaction. A smart contract can be called to start a transaction that links to its address [10].

4) CONSENSUS ALGORITHM

A consensus algorithm is a procedure that allows all blockchain network peers to reach a common agreement about the current state of the distributed ledger [39].

C. ZERO-KNOWLEDGE PROOF (ZKP)

Goldwasser, Micali, and Rackoff [40] proposed Zero-knowledge proof (ZKP) in 1989. ZKP is a cryptographic method where one party, termed prover, can prove to another party, termed verifier, that they know a certain value without revealing the actual value [41]. ZKP helps in making true and authorized claims by adding multiple layers of security to data [41].

IV. MODELS AND SECURITY REQUIREMENTS

We discuss the Decentralized Self-Management Access Control (DSMAC) architecture in this section. Our proposed architecture is depicted in Fig. 2. In the following subsections, we first present the main components of our system. Then, we discuss the adversary model followed by security requirements and design goals.

A. SYSTEM MODEL

DSMAC brings a novel decentralized access control scheme based on blockchain and self-sovereign identity (SSI) mechanisms [42]. Our framework is composed of three layers, namely IoMT devices layer, F2C layer, and the user layer, as presented in Fig. 2.

1) IOMT DEVICES LAYER

This layer is used to sense, collect, encrypt and upload the medical data to F2C computing [42], [43], including wireless sensors, smart bracelets, and digital wallet. The sensed data are sent to the digital wallet for aggregation and encryption purposes. Then, the data will be transmitted to

the F2C layer for processing and storage purposes [43]. Digital wallets are portable and secure digital repositories that allow users to store and manage identifiers and verifiable credentials, and also encrypt and share medical data with others [29].

2) USER LAYER

In our system, each user is identified by a DID, and he has a set of VCs, issued by trusted issuers. DSMAC allows individuals to use their mobile wallets to manage their DID and give access to their health data. Different levels of users can participate in our system, such as:

- DO (Data Owner): plays a vital role in our system. He is an entity (e.g., a patient) who owns the data to be shared, and he can specify who can access the shared data. He can manage his DID or delegate permissions to other users to manage his mobile wallet on behalf of a DID owner. For example, an elderly parent might delegate to an adult the authority to manage the parent's medical account. The DO performs data encryption, sets the access policies, and uploads ciphertext of the shared data to the F2C,.
- AR (Access Requester): is an entity that wants to access data shared by DO. An AR has different privileges in diverse situations such as a doctor, nurse, pharmacist, and researcher. Each AR must create his DID using the digital wallet, then register in the system using his DID. Upon successful registration, a corresponding DID is resolved to DID Document (DDO) and stored in the blockchain.

The AR initiates a data access request, obtains authorization and URL of data storage location from the blockchain, then downloads data ciphertext from the F2C according to the URL.

3) F2C COMPUTING LAYER

This layer is composed of two sub-layers, fog computing, and cloud computing. It combines the advantages of both, and it is detailed in our previous work [43].

Fog computing: is located close to the end-user to satisfy the low-latency and high-scalability requirements of the IoMT scenario. The main components of this sub-layer are:

- Temporary storage: represents the off-chain storage. However, health data are neither stored nor processed on-chain to avoid potential high loads, it will be stored temporarily at the fog layer to have real-time medical data access with minimal latency. Fog will send periodic data to cloud computing for permanent storage [61].
- Blockchain-based Decentralized Access Control: is composed of processing nodes responsible for mining the blocks and executing the smart contract used to ensure secure and reliable access to medical data. Also, blockchain is used to store the users' public key, decentralized policies, and the user's proof to verify the user's credentials with minimum time and cost. To increase throughput and reduce the system latency, Proof of Authority (PoA) [56] is used instead of Proof of Work (PoW).
- Authorization Management Node (AMN): acts as a gateway between the user layer and blockchain. AMN is responsible to manage the relationships between AR and permission assignment according to his role or his attributes.
- Authenticator Node (AN): verifies DID and VCs of AR and manages token-based authentication.

Cloud computing: we integrate cloud computing in our DSMAC framework because of its strong capacity for computation and storage [20]. It includes, (i) Permanent storage to store permanently the history of medical data. (ii) Complex computation to perform the complex analyzes that could not be done in fog computing.

B. ADVERSARY MODEL

In this part, we will improve the reliability, security as well as privacy-preserving medical data. We suggest some security assumptions to satisfy the goal of preserving privacy and resisting the attacks threatening access authorization. Then, we describe some attacks aimed at obtaining access authorization to medical data generated by the IoMT devices and forwarded to the fog storage node.

We assume that the end-users might be honest but curious about the health records and potentially interested to get more data than what their access privileges allow. For example, a pharmacist can be interested in obtaining patient prescriptions and learning different doctors' prescription patterns which could be useful for marketing purposes. In addition, we assume that the fog's nodes are honest but curious. They can legitimately do their assigned tasks, but are also curious about the privacy of the IoMT devices which are usually exposed to malicious attacks. Therefore, attackers may reside between the IoMT devices and the fog storage node. They try to establish a channel through which different components seem to communicate directly. They will also try to satisfy the access policies by obtaining or using attributes illegally. They can control, monitor, and modify all the data, tamper with the message, drop some packets and even replace the original message. Furthermore, all the data transmitted to the fog storage and to the blockchain through the digital wallet can be intercepted and analyzed by the adversary.

In our model, the main aim of attackers is to gain access privileges from the data owner. Thus, we are interested only in attacks threatening the access process such as:

1) REPLAY ATTACK

An attacker can observe and record some encrypted data during the transmission and reply to them in another request using the user's signature. This can be accomplished by either (i) network monitoring, or (ii) reading the blockchain. The attacker can act as a user and actively interact with the system to get the messages, or he can be a passive observer who collects the messages at the network level [44]. Therefore, this attack can help to get illegal authorization in the DSMAC framework.

2) SPOOFING ATTACK

Spoofing is an unethical process where the unauthorized user intrudes and promotes himself as an authorized user to access the system [45]. This is also known as the masquerading attack, it is the act of disguising an identity so that it appears to be associated with a trusted and authorized user. Therefore, the spoofing purpose is to gain access to health records using another user's credentials and steal the personal information related to the authorized user [45]. Therefore, the adversary forges the credentials of the data owner and tries to communicate with the system.
During this attack, we have considered the case where an attacker spoofs a user DID to gain access to medical data. Furthermore, he may change the identity of the data owner.

3) CREDENTIAL-STUFFING ATTACK

To get access to a system, attackers exploit lists of compromised user credentials. The attack is based on the assumption that many users reuse their usernames and passwords across many services. This attack is the automated injection of stolen credentials (username and password) to fraudulently gain access to user accounts [46].

C. SECURITY REQUIREMENTS AND DESIGN GOAL

The main security requirements to be satisfied in DSMAC scheme are summarized as follows.
• *Patient privacy.* It is critical to avoid any sort of illegal sharing of patients' medical records. Thus, any user who does not have enough attributes to fulfill the access policy must be prevented from accessing the patient health data.
• *Access control*. Access control is a critical problem due to the different kinds of end-users involved in the interactions between patients and the healthcare systems. Access control systems define who can access the patient's data and which part(s) of the data can be accessed, to ensure that only allowed parties can gain access to authorized data [47].

Our design goal is to propose privacy-preserving medical data based on a decentralized access control system and blockchain, using Decentralized Identifiers (DIDs) and verifiable credentials (VCs). Our framework provides the opportunity to share medical data and define access rights by the patient for giving access to different end-users without having a central authority. The following issues must be addressed:

a) How to acquire a decentralized access control system?
b) How can end-users access the medical records?
c) Can the DID approach add privacy value to the system?

V. PROPOSED DSMAC SCHEME

This section presents our DSMAC framework that integrates the concept of SSI and implements it with blockchain to ensure a decentralized self-management of the access control policies in the healthcare environment. The major idea is to achieve data privacy and sovereignty using access control policies based on blockchain, VC and DID.

A. TOWARDS A DECENTRALIZED ACCESS CONTROL SCHEME

Our model proposes a novel decentralized access control method based on the user's role, attributes, and contextual constraints. This means that our security model reuses concepts and mechanisms of Role-based access control (RBAC) [9] and Attribute-based access control (ABAC) [10], giving the owner the right to self-manage his principal policies. Hence, in a regular case, our system is instantiated with the RBAC system, and default permissions (DP) are assigned to ARs based on their roles. However, in cases where Data Owner (DO) is confronted with an emergency case, our model will be instantiated with the ABAC system, and adaptive permissions (AP) are assigned to ARs based on a set of VC's contextual attributes. Furthermore, in this way, we establish a bridge between DIDs and VCs to define users' permission policies (P):

$$P = \{DP \cup AP\} \tag{1}$$

1) ROLE-BASED DECENTRALIZED ACCESS CONTROL (RDAC)

Role-based access control (RBAC) is a security technique that allows and limits system access to different users based on their role(s). It provides secure and flexible access control policies to ensure the security and privacy of data, authorize users to access the data to fulfill their job requirements, and minimize the risk of unauthorized access [9]. RBAC can define how a user interacts with data, allowing read-only or read/write access to certain roles. In DSMAC framework, we propose the Role-based Decentralized Access Control (RDAC) model that combines the RBAC model with Blockchain. The key idea behind the RDAC approach is that users are assigned roles based on their VCs, then define the policies which contain the rules that must be followed by AR while accessing or updating medical data. Finally, we publish all access control policies according to the user-role assignments in a smart contract deployed on blockchain. Each user can be assigned to one or multiple roles. Roles are associated with default permissions (DP). Thus, the default permissions are granted to users, and they are defined by the policy decision smart contract (PDC).

Definition 1 Default Permissions (DP) represent the regular basic permissions (RP) that are defined explicitly by a smart contract based on the user's role (R).

$$DP \subseteq R \times RP \tag{2}$$

The default permissions include the patient's DID, the off-chain URL medical data stored in the F2C computing, AR's role, and authorized operation (Read, Write, and Update).

2) ATTRIBUTES-BASED DECENTRALIZED ACCESS CONTROL (ADAC)

One of the most popular access control methods is attribute-based access control (ABAC) [10], but it poses a serious threat to privacy because it defines access control policies based on user attribute values [48]. Whereas, DID is

emerging as a new alternative for preserving user privacy. In the DSMAC framework, we propose the Attribute-based Decentralized Access Control (ADAC) model that combines the ABAC with DID model to solve the problem of ABAC's privacy and apply it to emergency cases. Therefore, we implement the access control policies based on DID Document (DDO) to provide a level of adaptive security that would meet the DO needs while taking into consideration the emergency cases. The access rights are granted to users through any type of attributes such as subject's attributes, object's attributes, and environment attributes [10]. The DO can enforce the default permissions (DP) by configuring adaptive permissions (AP) based on DO's attributes, AR's attributes, and certain contextual attributes which must satisfy specific requirements to perform a specific operation. A contextual attribute defines a specific environmental characteristic whose real value changes dynamically such as date, time, location, and health status (emergency case, critical crisis, normal, etc.). Hence, AP is introduced to make and adjust decisions locally for emergency and unanticipated situations.

Likewise, to improve and enhance security and data privacy, blockchain technology is integrated with the ADAC model. The access control policies are created by the patient's wallet and stored in his DDO. Then, the wallet broadcasts the DDO as a transaction to the network; the network verifies, validates the transaction, and adds it to the blockchain. DSMAC system enables the patient to quickly modify permissions by changing contextual information.

Definition 2 Adaptive Permissions (AP) are defined to suit contextual constraints (CC) and relevant contextual conditions (CD) confronting DO (e.g. crisis, emergency, a heart attack, an allergic reaction, etc.).

$$AP \subseteq R \times CC \quad where \quad R=role,\ CC= set\ of\ CD \tag{3}$$

AP becomes active when an emergency has been declared, and a subset of the contextual conditions 'CD' is satisfied. The set of contextual conditions can be combined based on the context information and using a conjunction (∧), disjunction (∨), and negation (¬) operators.

For example, we consider the following contextual conditions (CD): 'T' denotes a request Time, 'A ' denotes a location Address and 'S' denotes a health Status. Contextual conditions are formed by making conjunctions of these elements (4).

$$CD = \{ (...,(A \wedge S),(T \wedge A),...) \ \ | cd \in CD \}, \quad e.g.: cd1 = A \wedge S \tag{4}$$

Case study: we assume that a patient suffers a serious medical emergency as a result of an accident, and he needs prompt intervention by medical professionals. The patient's digital wallet can allow users to quickly reach the emergency case, it will make access to medical records easier and faster.

Thus, according to the contextual constraints mentioned in (5), the patient or his delegate will approve the adaptive permissions for a user if the following contextual conditions are satisfied:

i) *cd1*: the doctor is not far from the 'accident scene'.
ii) *cd2*: if the patient's health status is in a 'critical' condition.

$$if\ (AR(user) \wedge role(doctor)) \wedge (cd1 \wedge cd2) \quad then\ Approve\ access \tag{5}$$

Once the doctor leaves the 'accident scene' or the patient's health status becomes 'normal' again, the adaptive permission will be deactivated.

B. DECENTRALIZED ACCESS CONTROL SCHEME BASED-SSI MODEL

In this section, we propose a security model for the privacy-preserving SSI management scheme. SSI technology can improve user authentication and authorization mechanisms [6]. It can be integrated with the healthcare systems for delivering enhanced interoperability [6].

1) DID APPROACH

DID is generated by the user (DO and AR) from the public/private key pair [49] and signed with the user's private key. The most crucial point of any DID implementation is the specification of the DID method which is composed of a method scheme and operations. The method scheme specifies the structure of the DID implementation's string identifier(s). Operations define how to create, read and verify a DID document, as well as how a DID controller can update or deactivate a DID document [31].

The method name that identifies DID in our system is *"dac"* (*D*ecentralized *A*ccess *C*ontrol). This produces a string identifier of the form "*did:dac:namespace*". All DID must begin with the following prefix: *"did:dac:"*. The remainder of the DID, after the prefix, is the Method-Specific Identifier (MSI) [31].

In the DSMAC system, each user has a minimum one of digital wallet with his DID, VCs, and private key used to sign transactions and access requests. However, the public key will be recorded in the blockchain to be accessible.

In summary, a digital wallet performs the following functions:

1) Generates DID and keys (public and private).
2) Requests the issuance of verifiable credentials, accepts the issued credentials, and stores them.
3) Receives a request from a verifier for proof of one or more credentials.
4) Data aggregation, encryption, and signature.
5) Creates AC policies.

In general, the AR must authenticate with his DID before submitting an access request to medical data. He must prove his identity and his role to access patient data using the VCs. The VCs issuance process proceeds as follows: the AR sends a signed request for issuing a new credential. When the issuer (hospital) receives the request, he checks the validity of the request by verifying the AR's signature. Once the verification is completed, the issuer agrees to the credential request and issues VC. The VC will be stored in the AR's wallet.

Now, when the AR requests authentication using his DID, the AN, which acts as a verifier, sends him a proof request to verify his identity. The AR processes the proof request and determines the necessary credentials to satisfy the proof based on ZKP [41], then he sends the response to the AN. After, the AN uses the issuer's DID and the credential definition specified in the proof response to verify the response. If the response is validated, then, token-based authentication is submitted to the AR.

The flowchart shown in Fig. 3 describes the interactions between entities, including the information exchanged with the blockchain, corresponding to the SSI's phases.

2) DID DOCUMENT (DDO) APPROACH

DID can be resolved by the digital wallet to a standard resource named DID document (DDO) without reliance on a centralized network component. DDO contains several components [35], as illustrated in Fig. 4, *"id"* denotes the DID, *"Publickey"* represents one or more public keys that authenticate the DID subject, *"Authentication"* is used to specify the method that is expected to prove that it is a DID owner, *"Service"* contains one or more service endpoints that are used to describe how to communicate with a DID owner [35], *"Timestamp"* indicates when the DDO was created or updated, and *"signature"* for verifying the integrity of the DDO [55]. These components are necessary to check the user's identity and the security of their requests. DDO can be stored and resolved with blockchain so that issuers or verifiers can easily find it.

In the DSMAC system, the DDO structure has been established as in Fig. 4. It includes a public key and service endpoints which are crucial to accomplish decentralized access control. The service endpoints can contain any information. Generally, it specifies a network address, like an HTTP URL where services act on behalf of a DID owner.

3) OUTSOURCING ENCRYPTION APPROACH

Following the Self-Sovereign paradigm, the digital identity of the user is kept in a digital and private wallet. To this end, the DSMAC framework includes a component which is a mobile app through which the user can manage the wallet and at the same time he can interact with the security of medical data using an encryption scheme and the user's SSI wallet [59]. For this purpose, a ZKP cryptography technique is adopted to address specific requirements focusing on data privacy A ZKP is a kind of cryptographic method, and its use in blockchain appears to be promising in cases where existing blockchain technologies can.

C. DECENTRALIZED ACCESS CONTROL SCHEME USING BLOCKCHAIN-BASED SSI MODEL

In the DSMAC framework, blockchain is used to store the users' public key, decentralized policies, and the user's proof to verify the credentials with minimum time and cost [11]. It is operated on the fog layer to provide low-latency decentralized access control functions [43]. Moreover, SSI is used to facilitate user authentication and authorization in regular and emergency cases.

1) RDAC-BASED POLICY DECISION SMART CONTRACT (RDAC-PDC)

The main idea of the RDAC-based smart contract is to leverage the features of the smart contract to set, manage, and store default permission policies (DP) into the blockchain network. To reach these goals, a policy decision smart contract (PDC) was developed. PDC is designed to assign user-role along with role permission, then publish the details on the blockchain.

The main features of the PDC are i) allow the hospital to verify the role of the user (by checking their credentials). ii) allow the patient to permit users to access medical data based on their associated role and credentials. iii) allow the hospital to maintain the information stored in SC. Therefore, PDC implements several functions to make the user-role assignment efficient, effective, and secure.

As well, we define the AMN as the agent who has the right to manage access transactions and interact with PDC by sending a Request Access transaction.

The Request Access transaction sequence can be processed as follows, as shown in Fig. 5:

1. After a successful authentication step, the AR sends an access request to AMN by enclosing his DID.
2. AMN sends a proof request to AR.
3. AR generates a payload based on his DID and VC protected by the ZKP proof, then, signs the payload with his private key and sends it to the AMN.
4. To verify the validity of the payload, AMN checks the signed payload with AR's public key stored in blockchain.
5. After the payload and role checking step, the AMN redirects the request to the PDC in blockchain as a transaction.
6. If the policy attributes and the AR's attributes in the PDC are similar, then the PDC will create an authorization token that includes the access permissions of the AR and the transaction will be recorded in the blockchain.

2) ADAC-BASED DID DOCUMENT (ADAC-DDO)

Defining security policies and managing medical data access becomes more critical and complex in an emergency case since the access does not only depend on the user's role but it's also attached to the contextual constraints [54]. In the DSMAC framework, the patient plays a huge role in emergency cases. It can enforce the default permissions by configuring adaptive permissions based on both end-user and patient attributes using DID Document (DDO).

DDO contains several fields like a context, an authentication mechanism, the user's digital signature, and a service definition. Each service has its id and type, as well as a service Endpoint with a URI or further properties describing the service [35]. Each service's description includes the type, DID, and URL for the service endpoint. The service endpoint URL is used for the outside service

caller, while the DID is used to identify the service itself [35].

As defined in listing 1, the services endpoint are used to express adaptive access control policies. They define the access privileges' URI based on both *"Membership"* and *"Permission"* services. The *"Membership"* service maintains a list of authorized users' DIDs. Each user must be a member of one or more of the following roles: *"doctor, pharmacist, and researcher"*. Likewise, *"Permission"* service specifies the access control policies of the user managed by the *"Membership"* service.

Therefore, access policies are composed of one or several statements; each statement includes information about single adaptive permission. The information in a statement is contained within a series of elements:

- **User** – Indicates a list of accepted user DID:
  "user" : ["did:dac:alice"],
- **Role** – Indicates a list of authorized roles:
  "role" : ["doctor"],
- **Rules** – composed of the following items:
  - *"grant": ["read", "write", "update"],*
  - *By* – Specifies user's name and role to which we would like to give access rights:
    "by": ["alice_u:doctor_r"],
  - *When* – Specifies the circumstances under which the policy grants permission:
    "When":["time= 08pm-10am", "status=emergency"],
  - *Url* – Includes the URL of health records to which the actions apply.
    "url" : ["fog.storage.patient1.emg_data"],

E.g., assuming a user, *"Alice"*, is in the *"user"* membership service, the patient or his delegate can approve read and update permissions for "Alice" if the following contextual conditions are satisfied:

1) Alice's role is *"doctor"*.
2) She is not far from the *"accident scene"*.
3) If the patient's health status is *critical"*.

To specify the user's name and role to which we would like to give access rights, the DDO policies are based on hierarchically-named attributes, where 'u' means user, 'r' means the role, and 't' means type, and attributes are separated by the ':' character. For example, the attribute *alice u:doctor r:cardiologist t* means that the user Alice must be a doctor with a cardiologist specialty.

To proceed to the DDO permissions, AMN sends an authorization request to the blockchain once receiving an alert message from the patient's wallet. So, according to the patient's DID included in the authorization request, blockchain returns the corresponding authorizations managed by the patient's DDO. Then, AMN sends an access token to users mentioned in the Membership service if and only if they fulfill the conditions.

Listing1: patient DDO structure based-adaptive permission

```
{
"id": "did:dac:patient1",
"authentication": [
{
"id": "did:dac:patient1#keys-1",
"type": "RsaVerificationKey2022",
"controller": "did:dac:patient1",
"publicKeyPem": Patient1's Public Key
}
],
"service": [
{
  "id": "did:dac:patient1# membership ",
  "type": "Membership",
  "serviceEndpoint" : https://192.168.0.100/membership/,
  "user" : ["did:dac:alice" , "did:dac: bob", "did:dac: eve"],
  "role" : ["doctor" , "nurse", "pharmacist", "researcher"]
  },
  {
  "id": "did:dac:patient1# permission ",
  "type": "Permission",
  "serviceEndpoint" : https://192.168.0.100/permission/,
  "rules":
  [ {
    "grant": ["write","update"],
    "by": ["alice_u:doctor_r"],
    "When" : ["location= accident_scene ","status=emergency"],
    "url" : ["fog.storage.patient1.emg_data"]
    },
    {
    "grant": ["read"],
    "by": ["eve_u:pharmacist_r"],
    "When" : ["time= 09pm-09am ","status=critical"],
    "url" : ["fog.storage.patient1.prescription_emerg_data"]
    }
    }
    ]
}
```

VI. EXPERIMENTS AND RESULTS

A. EXPERIMENTAL SETUP

DSMAC allows users to store their DID and VC on their digital wallets using hyperledger Indy [17] and hyperledger Aries [53]. The description of the tools used in the experiment is detailed in table 1. In the general setup of the DSMAC framework, a Docker and Docker Compose are used to build and run the system test setup. The choice for our approach is based on blockchain technologies.

To connect to the Indy network and control different nodes, we have utilized the Admin UI from the VON network repository [59]. It initiates the blockchain with the genesis block, a server, and 04 nodes.

In the DSMAC system test setup, the Von network needs to be started first, as illustrated in Fig. 11a. Once all containers are started, we can view the von network and ledger by visiting the following web page: http://localhost:9000, as shown in Fig 11b.

TABLE 1: DETAILS OF TOOLS USED IN THE EXPERIMENTATION

TOOLS	DESCRIPTION
Hyperledger indy	A permissioned blockchain, used for identity management.
Hyperledger Ethereum	a public permissionless blockchain, used for running smart contracts using solidity language.
Hyperledger aries	It serves as the infrastructure for transaction interactions, it provides tools to store, transmit and verify digital credentials.
Aca-py	Aries cloud agent python serves as a cloud agent interface to both the ledger and external holders.
Von-network	Verifiable Organization Network (VON) network provides a ledger browser on the Docker environment. It allows us to examine transactions and see the status of nodes locally.
Docker community edition	Used for getting all librariesand packages required for experimentation.

Then, all involved entities (issuers, holders, and verifiers) must be registered in Hyperledger Indy and provided a DID. To generate DID for our agents, we can use the ledger browser as shown in Fig 11b. Then, we use the default option "Register from seed" in the "Authenticate a New DID" section, and put "EmatiSaidi00000000000000000000002022" as the value in the "wallet seed" field. Once successful, detailed information such as Seed, DID and Verkey will be shown below the "Register DID" button, as illustrated in Fig 11c.

In the DSMAC framework, we have implemented four Aries agents (patient, doctor, nurse, and hospital), as shown in Fig. 12, that are capable of connecting to the Indy network, and generating transactions. Those agents are written in Python by using the open-source Hyperledger Aries Cloud Agent Python (ACA-Py) library. It will be also run over Docker, as shown in Fig 13. ACA-Py provides all of the core Aries functionality such as interacting with other agents and the ledger, managing secure storage, sending event notifications, and receiving instructions from the controller [59]. Thus, the ACA-PY component is necessary to securely deliver medical data from the wallet to the F2C infrastructure, and for each agent, the sender explicitly adds another layer of encryption [59].

Our simulation is based on Postman for representing digital wallets. It is organized into several collections composed of a set of actions performed by the agents, such as the Patient_Emergency case, as shown in Fig. 14, which details the process followed in the case of an emergency.

The transactions described in this paper are recorded in the domain ledger. The key transactions maintained in the domain ledger are NYM, ATTRIB, SCHEMA, and CRED_DEF. NYM transaction is used to create DID. To add an attribute value to NYM record, the domain ledger makes use of ATTRIB transaction. SCHEMA transaction generates a template with the required attributes for issuing the credentials to the user/holder. The CRED_DEF transaction defines a credential with the user-specific values inserted into the schema in the form of a public key. Fig. 15(a,b,c,d) show all 4 transactions in action.

In addition, our framework proposes a procedure for integrating Ethereum smart contract-based credential verification into hyperledger Indy. The smart contract is charged with verifying the credentials (role) presented by users and granting access according to the access policies defined by the patient. It needs the hyperledger Indy to confirm the validity of the user's credential.

B. EXPERIMENTAL ANALYSIS

The Aries infrastructure offers: (i) a blockchain interface layer, (ii) libraries to implement cryptographic wallets for secure storage of cryptographic secrets and other information, (iii) an implementation of ZKP-capable W3C verifiable credentials using the ZKP primitives found [59].

The initial idea was to create a front-end tool that uses an API to interact with ACA-Py without the need for its database. ACA-Py has support for maintaining and querying lists of schemas, credentials, connections, etc. ACA-Py maintains its keys and requires the controller application to create schemas, credential definitions, and revocation registries, as illustrated in Fig. 15 [59]. Also, the ACA-PY provides a queue to hold messages until the mobile agent requests them because the mobile wallets are not online at all times, and are not constantly polling to see if they have any incoming messages (that consumes resources, particularly data and battery, on the phone) [59].

1) PERFORMANCE EVALUATION

In our study, we focus on evaluating the performance of our system using two experiments:

- *Experiment 1:* Evaluate the performance of the Role-based Decentralized Access Control (RDAC) model using the number of submitted and executed transactions, and the number of users.
- *Experiment 2:* Evaluate the performance of the Attributes-based Decentralized Access Control (ADAC) model using DID Document.

We show the performance of our DSMAC scheme in terms of submitting and executing time which means how fast different Access Control (AC) actions can be performed. The execution time is the most important key parameter for our architectural model. In addition, the performance of our DSMAC scheme is focused on the transaction throughput and transaction latency for both experiments. Throughput is described as the number of successful transactions per second (tps). Latency is specified as the average time interval between the initialization of the transaction and the actual execution of the transaction. Also, to reduce the cost of cryptographic computations and maintain data confidentiality, the computations are securely outsourced to

a mobile device which is more powerful. Finally, we examine the transaction scalability and sustainability.

2) RESULTS AND DISCUSSION

The evaluation process was based on the performance assessment of a decentralized access control-based smart contract and SSI system.

- *Transactions time*

We evaluate the Access Control policy assignment time in both experiments. Fig. 6 shows how Access Control policy assignment time varies according to several transactions in the RDAC experiment. However, the time is almost unchanged in the ADAC experiment.

The results show that the average time to assign an AC policy using submitted and executed transactions is around 68 ms for the RDAC experiment. However, in an emergency case, the time is around 16 ms. Also, we can notice that when the number of transactions increases, the AC policy assignment time is increased in the RDAC model. Thus, the results depict that our ADAC model takes less AC assignment time as compared to the RDAC model. This confirms that the ADAC model is the best choice for emergency cases. Moreover, DSMAC performs better in terms of the level of privacy that it offers.

- *Transaction throughput*

For this analysis, we evaluated the number of access request transactions (txs) that can be executed per second for both experiments, as shown in Fig. 7. The throughput of a user u during a time between T_i and T_j can be calculated using (6).

$$Throughput_u = \frac{count\ (T_x\ in\ (T_i, T_j))}{T_j - T_i}(txs/s) \quad (6)$$

To calculate the average throughput, we can use (7).

$$Throughput = \frac{\sum u(Throughput_u)}{N}(txs/s) \quad (7)$$

The DSMAC system may generate a large volume of access requests in RDAC experiments that need to be processed and handled. We measured the transaction throughput while increasing the number of users, then we compared the transaction throughput of RDAC and ADAC experiments. Initially, the throughputs on both models are almost equal. Since the ADAC scheme did not have the credentials verification step and queries are not updating the ledger status, it has a high throughput compared to the RDAC model. Also, as the number of users increases, there is an important increase observed in the throughput of the ADAC model.

As shown in Fig. 7, we compared the transaction throughput of ADAC with RDAC. Likewise, the query transaction throughput of ADAC is higher than RDAC.

- *Cryptographic computations*

In this section, we analyzed the encryption time, CPU consumption, and memory utilization on the mobile device. The study conducted several experiments to encrypt different medical data with different sizes. The study experiment considered a ZKP encryption approach.

To compare encryption times, Fig. 9 shows the time required to encrypt different data. The encryption application process starts by permitting the DO to select data. Then the mobile application encrypts the data using the ZKP encryption algorithm.

Fig. 10 shows the current usage of CPU and memory. When the data size is increased, the CPU utilization increase gradually, this is only natural because as we increase the number of files more transactions are sent and this means more CPU computations are recorded. Whereas memory utilization remains almost constant.

It is also necessary to note in table 2 that the encryption times taken by the process proposed in this paper are faster than other encryption schemes.

TABLE 2: ENCRYPTION TIME

The method proposed by Yonata et al. [57]		The method proposed in this paper	
Data size(KB)	Time to encrypt (sec)	Data size (KB)	Time to encrypt (ms)
25.44	4	0.87	26
200	5	3.55	45
600	7	1.14	17

As a general observation, DSMAC consumed less resources compared to other systems.

- *Transaction latency*

The latency measures the time of a transaction from submission by the user until it is processed and written into the ledger. First, all the nodes of our system are deployed in fog computing for the low latency purpose [43]. Latency values for each experiment are shown in Fig. 8 using 500 users. It is noticed that there is continuous growth in the average latency as the number of users is increasing for both experiments. However, the average latency of the ADAC model is lower than the RDAC model. It is important to mention that the higher level of security, the lower the latency.

- *Scalability*

In the DSMAC framework, scalability is analyzed through transaction latency and throughput. If the throughput remains constant or increases with the increase in the number of users, then the framework is scalable. In another way, if the latency remains constant or increases with the rise in users, then also it is considered a scalable framework that can maintain stable latency in a large-scale environment.

- *Sustainability*

The goal of the DID specification is to ensure sustainability and interoperability across the different healthcare

organizations. DSMAC framework brings a sustainable decentralized access control model without the involvement of the central entity based on sustainable DID solutions. The DID technique can increase patients' ability to contribute to building long-term sustainability. Thus, achieving sustainability in health care is essential to improving the identification of health system functions. Enhancing sustainability, through DID assignment, and managing resources efficiently, will deliver better outcomes for patients, and provide economic benefits.

VII. SECURITY AND PRIVACY ANALYSIS

After explaining the process of the DSMAC model, we present the security and privacy analysis. We theoretically analyze how DSMAC can efficiently resist the attacks proposed in the adversary model (Section 4.2). Since the main goal of an attacker is to gain authorization to access the health data.

A. COMPARISON OF SECURITY PROPERTIES

Table 3 compares the security properties of our proposed scheme with i) blockchain-based access control schemes: Yue [13], Kumar [15], Dagher [16], Xu [12], Xia [22], ii) SSI based access control schemes: Belchior [25], Lagutin [26], Jung [27]. From the table, we notice that only our proposed scheme and Rajput [24] take into consideration the emergency case. Notably, almost all the schemes have the properties of scalability and data privacy, which are critical security objectives in health record sharing systems. However, no research dealt with the property of sustainability, except in our DSMAC model.

B. PRIVACY PROTECTION

Our system achieves privacy by employing several privacy-preserving techniques. The use of encryption on all medical data placed on the F2C prevents the users and other malicious parties to learn the content of the medical data, achieving both patient privacy and health data confidentiality. Furthermore, DIDs and VCs managed by the digital wallet can be used as a preliminary step to promote privacy-preserving medical data. DSMAC also achieves privacy preservation by anonymity to ensure that malicious parties cannot deduce the owners of the data. In DSMAC scheme, anonymity is achieved by utilizing the ZKP protocol [51]. During this protocol, specific aspects of a VC can be encapsulated through a ZKP method [51] which allows the owner to prove an aspect of his identity without requiring any specific information of that aspect to be disclosed to other parties. Anonymization can be performed by the patient and it is required when the identifying information needs to be hidden from certain parties [47]. These parties include researchers, pharmacists, etc. However, physicians, nurses, and emergency medical technicians should be able to view such information to carry out proper treatment.

C. ACCESS CONTROL PROTECTION

In DSMAC system, the honest but curious model is adopted. The end-users are honest since all of them need access control policies to perform their assigned tasks. However, some of them are curious since they continuously can view and store patients' information. In our framework, the RDAC approach based on smart contracts is used to solve the problem of who has access to health records. Additional mechanisms are included for emergency cases such as an ADAC approach [37]. This approach is more precise in restricting access based on the DID document and blockchain. Therefore, the immutability and integrity features of blockchain make it impossible for any entity to manipulate, replace, or falsify access control policies stored on the blockchain. In addition, each block of information contains a hash for itself and for the previous block to verify that the access control policies are not modified illegally [52]. Thus, smart contracts [60] and SSI technologies support securing the system against various security concerns such as authorization and privacy-preserving data. The advantage of eliminating the trusted third party makes the decentralized access policy scheme suitable for user privacy-oriented scenarios.

D. ATTACKS ANALYSIS

The security of DSMAC framework is also evaluated by different attacks. Therefore, the attacker could not intercept or update or retrieve the medical data in unauthorized access since our decentralized access control system plays a vital role to protect health data against unauthorized access. As proof, we present the resistance of some attacks threatening the access process such as replay attacks, spoofing attacks, and credential-stuffing attacks.

1) REPLAY ATTACK RESISTANT

DSMAC scheme can defend against the replay attack effectively. It is based on blockchain to provide better access control mechanisms. In this way, no one can alter its contents. We note that blockchain defends against transaction replay since every single transaction is embedded with nonce value and timestamps [4]. This will provide the system with a protection mechanism against replay attacks. And even each block is linked with the previous hash; hence all communications are chained together, making it impossible for replay attacks to occur.

Furthermore, to acquire authorization, the attacker can try to reply to messages using the signature. However, he will not be successful, since each user has to use a private key and DID to compute the signature. Thus, the adversary is unable to obtain any messages from the user [50]. Therefore, the proposed protocol can resist replay attacks.

2) SPOOFING ATTACK RESISTANT

Spoofing refers to the ability to steal identity information. During this attack, a malicious user presents himself to the system as an authorized user. We have considered the case where an attacker spoofs a user DID to gain access to medical data. Furthermore, he may change the identity of

the data owner. To prevent such attacks, DSMAC scheme is integrated with a mechanism that allows each user to create a unique DID based on his private key. In addition, we have employed two security primitives to protect against spoofing attacks: (i) the use of the ZKP protocol implies that viewing any transferred data does not reveal any useful information about the user, so only legitimate users whose access has been allowed can use the medical data; (ii) blockchain that holds the access control policies with the hashes generated in every block [45].

Thus, blockchain with decentralized access control policies maintains reliable and consistent data. Since an attacker cannot inject the wrong DID or address. Also, our proposal is resistant to spoofing attacks because users' DIDs are verified through a ZKP.

3) CREDENTIAL-STUFFING ATTACK RESISTANT

This attack is the injection of stolen credentials (username and password pairs) to gain unauthorized access to user accounts. In DSMAC framework, to protect against this attack, each user must authenticate with something he knows such as DID, in addition to something he has such as a mobile phone which plays the role of a digital wallet. The digital wallet contains the DID, private key as well as the VCs of the user, and each user gets a public key which is stored in blockchain. In this way, the attacker will not be able to provide a physical authentication method. This makes it harder for the attacker, which makes the credential stuffing attack not possible.

CONCLUSION AND FUTURE WORK

In this paper, DSMAC, a decentralized access control system for health data based on the combination of blockchain, RBAC, ABAC, DIDs, and VC was proposed. By adopting smart contract and self-sovereign identity (SSI) technology. The framework is implemented in a decentralized and trustless way to share medical records and preserve security and privacy at the same time.

The choice of the SSI model allows users to own and manage their identities. This makes our framework more suitable for high privacy requirements. Deploying the authorization and verification processes with smart contracts allows a decentralized access control system for users. Therefore, access control policies can be remotely updated by updating a smart contract.

DSMAC is based on different contributions aimed to provide benefits in the areas of privacy/security, scalability, and sustainability in the medical environment. Likewise, we compared DSMAC with some typical access control models and implemented a prototype of the proposed framework in regular and emergency cases. The results of the performance evaluation demonstrate that the proposed approach is highly scalable and efficient in terms of submission and execution time, throughput, cryptographic computations and latency.

For future work, we are interested in integrating the machine learning algorithms to manage EHR. Also, we can integrate the differential privacy algorithm with the DSMAC system to provide better data protection and preserve user privacy.

REFERENCES

[1] J. Tao, and L. Ling, "Practical Medical Files Sharing Scheme Based on Blockchain and Decentralized Attribute-Based Encryption," *IEEE Access*, vol. 9, pp. 118771-118781, 2021.

[2] A.A. Abba Ari, O.K. Ngangmo, C. Titouna, O. Thiare, A. Mohamadou, and A.M. Gueroui, "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges," *Appl. Comput. Inform.*, 2020.

[3] O.K. Ngangmo, A.A.A. Ari, A. Mohamadou, O. Thiare, and D.T. Kolyang, "Guarantees of Differential Privacy in Cloud of Things: A Multilevel Data Publication Scheme," *Int. J. of Eng. Res. Africa.,* vol. 56, pp. 199-212, 2021.

[4] G. Lippi, C. Mattiuzzi, C. Bovo, E.J. Favaloro, "Managing the patient identification crisis in healthcare and laboratory medicine," *Clin. Biochem.*, vol. 50, no. 10–11, pp. 562–567, 2017.

[5] G. Kondova, and J. Erbguth, "Self-sovereign identity on public blockchains and the GDPR." In *Proc. 35th ACM Symposium on Appl. Comput. (ACM SAC)*, Brno, Czech Republic, pp. 342-345, 2020.

[6] S.Y. Lim, O.B. Musa, B.A.S. Al-Rimy, and A. Almasri, "Trust Models for Blockchain-Based Self-Sovereign Identity Management: A Survey and Research Directions," in *Advances in Blockchain Technology for Cyber Physical Systems*, Internet of Things. Springer, Cham, pp. 277-302, 2022.

[7] M. Lacity, and E. Carmel, "Implementing Self-Sovereign Identity (SSI) for a digital staff passport at UK National Health Service (NHS)," *BCoE Whitepaper*, 2022.

[8] M. Freytsis, I. Barclay, S.K. Radha, A. Czajka, G.H. Siwo, I. Taylor, and S. Bucher, "Development of a Mobile, Self-Sovereign Identity Approach for Facility Birth Registration in Kenya," *Front. Blockchain*, vol. 4, pp. 631341, 2021.

[9] J.P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: Role-based access control using smart contract," *IEEE Access*, vol. 6, pp. 12240-12251, 2018.

[10] L. Song, M. Li, Z. Zhu, P. Yuan, and Y. He, "Attribute-based access control using smart contracts for the internet of things," *Procedia Comput. Sci.,* vol. 174, pp. 231-242, 2020.

[11] P. Zhang, D.C. Schmidt, J. White, and G. Lenz, "Blockchain technology use cases in healthcare." *Adv. Comput*., vol. 111, pp. 1-41, 2018.

[12] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet Things J.*, vol. 6(5), pp. 8770-8781, 2019.

[13] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst*., vol. 40(10), pp. 1-8, 2016.

[14] X. Zhang, S. Poslad, and Z. Ma, "Block-based access control for blockchain-based electronic medical records (EMRs) query in eHealth," In *proc.* IEEE Glob. Commun. Conf. *(GLO*BECOM*),* Abu Dhabi, UAE, pp. 1-7, 2018.

[15] R. Kumar, and R. Tripathi, "Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model," *J. Ambient Intell. and Humaniz. Comput*., vol. 12(2), pp. 2321-2338, 2021.

[16] G.G. Dagher, J. Mohler, M. Milojkovic, and P.B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc*., vol. 39, pp. 283-297, 2018.

[17] A. Banerjee, B. Dutta, T. Mandal, R. Chakraborty, and R. Mondal, "Blockchain in IoT and Beyond: Case Studies on Interoperability and Privacy," In *Blockchain based Internet Things*, pp. 113-138. Singapore; Springer, 2022.

[18] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N.M.S. Kumar, Obaidat, and J.J. Rodrigues, "BHEEM: A blockchain-based framework for securing electronic health records," *IEEE Glob. Commun. Conf.* (GC Wkshps), pp. 1-6, 2018.

[19] M.M. Madine, A.A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. SASA PESIC and S. Ellahham, "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193102-193115, 2020.

[20] T. Liu, J. Wu, J. Li, J. Li, and Y. Li, "Decentralized access control for secure data sharing in cloud computing," *Concurr. Comput. Pract. Exp*., e6383, 2021.

[21] B.S. Egala, A.K. Pradhan, V. Badarla, and S.P. Mohanty, "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medial things with effective access control," *IEEE Internet Things J.,* vol. 8(14), pp. 11717-11731, 2021.

[22] Q. Xia, E.B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8 (2), pp. 44, 2017.

[23] Q.I. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE access, vol.* 5, pp. 14757-14767, 2017.

[24] A.R. Rajput, Q. Li, M.T. Ahvanooey, and I. Masood, "EACMS: Emergency access control management system for personal health record based on blockchain," *IEEE Access*, vol. 7, pp. 84304-84317, 2019.

[25] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro, "SSIBAC: self-sovereign identity based access control," In *proc IEEE 19th Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Guangzhou, China pp. 1935-1943, 2020.

[26] D. Lagutin, Y. Kortesniemi, N. Fotiou, and V.A. Siris, "Enabling decentralised identifiers and verifiable credentials for constrained IoT devices using OAuth-based delegation," In *Proc. of the Workshop on Decentralized IoT Systems and Security (DISS)*, San Diego, CA, USA, vol. 24, 2019.

[27] E. Jung, "A decentralized access control model for IoT with DID," In *IT Convergence and Security*, Springer Singapore, pp. 141-148, 2021.

[28] B. Kim, W. Shin, D.Y. Hwang, and K.H. Kim, "Attribute-based access control (ABAC) with decentralized identifier in the Blockchain-based energy transaction platform," In *Proc. Int. Conf. on Information Networking (ICOIN)*, Jeju Island, Korea (South), pp. 845-848, 2021.

[29] A.M. Thomas, R. Ramaguru, and M. Sethumadhavan, "Distributed Identity and Verifiable Claims Using Ethereum Standards," In *Proc. Inventive Communication and Computational Technologies (ICICCT)*, Tamil Nadu, India, vol. 311, pp. 621-636, 2022.

[30] S. Figueroa-Lorenzo, J. Añorga Benito, and S. Arrizabalaga, "Modbus access control system based on SSI over hyperledger fabric blockchain," *Sensors,* vol. 21, no. 16, pp. 5438, 2021.

[31] D. Reed, M. Sporny, D. Longley, C. Allen, M. Sabadello, and O. Steele. (2021). *Decentralized Identifiers (DIDs) v1.0*. Accessed: Jul. 1, 2022. [Online]. Available: https://www.w3.org/TR/did-core/

[32] C. Farmer, S. Pick, and A. Hill, "Decentralized identifiers for peer-to-peer service discovery," In *Proc. 2021 IFIP Networking Conference (IFIP Networking)*, Finland:IEEE, pp. 1-6, 2021.

[33] F. Wang, and P. De Filippi, "Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion," *Front. Blockchain*, 28, 2020.

[34] P.N. Mahalle, and G.R. Shinde, "OAuth-based authorization and delegation in smart home for the elderly using decentralized identifiers and verifiable credentials," in *Security issues and privacy threats in smart ubiquitous computing*, 1st ed, Springer, Singapore, vol. 341, pp. 95-109, 2021.

[35] M. Babaghayou, N. Labraoui, A.A. Abba Ari, M.A. Ferrag, L. Maglaras, H. Janicke, "WHISPER: A Location Privacy Preserving Scheme Using Transmission Range Changing for Internet of Vehicle," *Sensors,* vol. 21, pp. 2443, 2021.

[36] M. Sporny, D. Longley, and D. Chadwick, *Verifiable Credentials Data Model v1.1.* Accessed: Jul. 1, 2022. [Online] Available: https://w3c.github.io/vc-data-model

[37] M.A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, and H. Ning, "Distributed ledger technology for eHealth identity privacy: state of the art and future perspective," *Sensors*, vol. 20(2), pp. 483. 2020.

[38] O. Mounnan, and A. Abouelkalam, "Efficient distributed access control using blockchain for big data in clouds," In *Proc. 5th Int. Conf. on Wireless and Mobile Communications (ICWMC),* 2019.

[39] X. Yang, and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," Comput. Secur. vol. 99, 102050, 2020.

[40] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," SIAM J. Comput., vol. 18(1), pp. 186-208, 1989.

[41] S. Capraz, and A. Ozsoy, "Personal Data Protection in Blockchain with Zero-Knowledge Proof," in *Blockchain Technology and Innovations in Business Processes*, 1st ed, Springer, Singapore, vol. 219, pp. 109-124, 2021.

[42] A. Saidi, M. Hadj Kacem, I. Tounsi, A. Hadj Kacem, "Adopting the Internet of Things Technology to Remotely Monitor {COVID-19}", In *Participative Urban Health and Healthy Aging in the Age of AI: 19th Int. Conf., ICOST* 2022, Paris, France, vol. 13287, pp. 166-180, 2022.

[43] H. Saidi, N. Labraoui, A.A.A. Ari, and D. Bouida, "Remote health monitoring system of elderly based on Fog to Cloud (F2C) computing," *In Proc.* IEEE *Int. Conf. intel. Syst. and Comput. Vis. (ISCV),* Morroco, pp. 1-7, 2020.

[44] [44]A. Sonnino, S. Bano, M. Al-Bassam, and G. Danezis, "Replay attacks and defenses against cross-shard consensus in sharded distributed ledgers," In *Proc. IEEE European Symposium on Security and Privacy (EuroS&P),* Italy, pp. 294-308, 2020.

[45] J. R. Van der Merwe, X. Zubizarreta, I. Lukčin, A. Rügamer, and W. Felber, "Classification of spoofing attack types," In *Proc.* IEEE *European Navigation Conference (ENC),* Sweden, pp. 91-99, 2018.

[46] S. Rees-Pullman, "Is credential stuffing the new phishing?" *Comput. Fraud Secur.,* vol. 7, pp. 16-19, 2020.

[47] M. Sookhak, R. Jabbarpour, N.S. Safa, and F.R. Yu, "Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues," *J. Netw. Comput. Appl*., vol. 178, 102950, 2021.

[48] B. Kim, W. Shin, D.Y. Hwang, and K.H. Kim, "Attribute-based access control (ABAC) with decentralized identifier in the Blockchain-based energy transaction platform," In *Proc. Int. Conf. Inf. Netw. (ICOIN) IEEE*, Korea (South), pp. 845-848, 2021.

[49] A. Ehret, E. Del Rosario, C. Schwicking, K. Gettings, and M.A. Kinsy, "Reconfigurable Hardware Root-of-Trust for Secure Edge Processing," In *Proc. IEEE High Performance Extreme Computing Conference (HPEC)*, USA, pp. 1-7, 2021.

[50] M. Naghmouchi, H.K.B. Ayed, and M. Laurent, "An automatized Identity and Access Management system for IoT combining Self-Sovereign Identity and smart contracts," In *International Symposium on Foundations and Practice of Security*, vol 13291, pp. 208-217. Springer, Cham. 2022.

[51] P. Zhang, and T.T. Kuo, "The Feasibility and Significance of Employing Blockchain-Based Identity Solutions in Health Care," In *Blockchain Technology and Innovations in Business Processes* Springer, Singapore, pp. 189-208, 2021.

[52] Y. H. Park, Y. Kim, and J. Shim, "Blockchain-Based Privacy-Preserving System for Genomic Data Management Using Local Differential Privacy," *Electronics*, vol.10 (23), pp. 3019, 2021.

[53] T. Manoj, K. Makkithaya, and V.G. Narendra, "A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records," Cogent Eng., vol. 9(1), 2035134, 2022.

[54] H. Saidi, N. Labraoui, A.A.A. Ari, I. Semahi, and B.R. Mamcha, "Real-time Aging Friendly fall detection system," In *Proc. 6th Int. Conf. on Image and Signal Processing and their Applications (ISPA), IEEE*, pp. 1-6, 2019.

[55] P.N. Mahalle, G. Shinde, and P.M. Shafi, "Rethinking decentralised identifiers and verifiable credentials for the Internet of Things," In *Internet of things, smart computing and technology: A roadmap ahead*, Springer, Cham, pp. 361-374, 2020.

[56] J. Yang, J. Dai, H.B. Gooi, H. Nguyen, and A. Paudel, "A Proof-of-Authority Blockchain Based Distributed Control System for Islanded Microgrids," *IEEE Trans. Industr. Inform.* 2022.

[57] L. Yonata, M. Nababan, O. Sihombing, S. Aisyah, D. Sitanggang, , S. Parsaoran, and Zendato, N., "File Cryptography with AES and RSA for Mobile Based on Android." In *Journal of Physics: Conference Series* (Vol. 1007, No. 1, p. 012016). IOP Publishing. 2018.

[58] Y. Dündar, I. Sertkaya, "self sovereign identity based mutual guardianship." *J. Mod. Technol. and Eng.*.; vol. 5(3), pp. 189-211, 2020.

[59] L. Boldrin, V. Daza, R. De Prisco, S. Rovira, S. Sivo, "A trust module for the interaction with virtual characters." *In Proc. 7th Int. Conf. on Systems and Informatics (ICSAI) 2021* Nov 13, pp. 1-8. IEEE.

[60] F. Tchakounté, K.A. Calvin, A.A.A. Ari, D.J.F. Mbogne, "A smart contract logic to reduce hoax propagation across social media." *J. King Saud Univ.-Comput. Inf. Sci*. 2020.

[61] H. Saidi, N. Labraoui, A.A.A. Ari, "A secure health monitoring system based on Fog to Cloud computing" *Int. J. of Medical Engineering and Informatics,* 2022.

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3207803

HAFIDA SAIDI is a Ph.D. student at the STIC Lab of the University of Tlemcen, Algeria. She received her Master in computer engineering, "Networks and Distributed Systems", from the University of Tlemcen, Algeria in 2017 and she is preparing her Ph.D. thesis in the same domain. Currently, her research is focused on Security and data privacy in the healthcare area, Blockchain, and cloud computing.

NABILA LABRAOUI is a full professor in computer engineering at the University of Tlemcen, Algeria. She received her Ph.D. in computer engineering and the HDR from the University of Tlemcen, Algeria. Her current research interests include VANETs, wireless ad hoc sensor networks, security and trust management for distributed and mobile systems, Cognitive Radio, Cloud Computing and Big data security.

ADO ADAMOU ABBA ARI is an Associate Researcher at the DAVID Lab of the Université Paris-Saclay, University of Versailles Saint-Quentin-en-Yvelines, France and Associate Professor for Computer Networks at the LaRI Lab of the University of Maroua, Cameroon. He received his Ph.D. degree in Computer Science in 2016 from Université Paris-Saclay in France with the higher honors. He also received the Master Degree of Business Administration (MBA) in 2013, the Master of Science (M.Sc.) degree in Computer Engineering in 2012 and the Bachelor of Science (B.Sc.) degree in Mathematics and Computer Science in 2010 from the University of Ngaoundéré, Cameroon. He served/serving on several journals and conferences program and reviewing committees. Moreover, he his recognized reviewer of a number of journals including IEEE Transactions on Intelligent Transportation Sensors, Electronics, Telecommunication Systems, Wireless Personal Communications, Sustainable Computing: Informatics and Systems, Journal of Ambient Intelligence and Humanized Computing, etc. His current research is focused on Wireless Networks, IoT, and Artificial Intelligence. Systems, IEEE Access, Information Sciences, Journal of Network and Computer Applications, Computer Communications, Remote Sensing,

DR. LEANDROS A. MAGLARAS is a Professor of cybersecurity in the School of Computer Science and Informatics of De Montfort University. From September 2017 to November 2019, he was the Director of the National Cyber Security Authority of Greece. He obtained a B.Sc. (M.Sc. equivalent) in Electrical and Computer Engineering from the Aristotle University of Thessaloniki, Greece in 1998, M.Sc. in Industrial Production and Management from the University of Thessaly in 2004, and M.Sc. and Ph.D. degrees in Electrical & Computer Engineering from the University of Thessaly, in 2008 and 2014 respectively. In 2018 he was awarded a Ph.D. in Intrusion Detection in SCADA systems from the University of Huddersfield He is featured in Stanford University's list of the world's Top 2% scientists. He is a Senior Member of the Institute of Electrical & Electronics Engineers (IEEE) and is an author of more than 170 papers in scientific magazines and conferences.

JOEL HERVE MBOUSSAM EMATI is a Ph.D Student at the LaRI Lab of the University of Maroua, Cameroon, He received the Master of Science (M.Sc.) degree in computer engineering in 2021 and the Engineering degree in computer science in 2020 from the University of Maroua, Cameroon. He is also interested in legal issues and received Bachelor's degree in public Law in 2016 from the University of Douala, Cameroon. His current research is focused on blockchain, IoT, Artificial Intelligence, and cryptography.

TABLE 3. COMPARISON BETWEEN RELATED WORKS AND OUR DSMAC MODEL

Models	Blockchain-based Access control	SSI-based Access control	Access control methods			Feature comparison			
			Identification	Authentication	Authorization	Scalability	Sustainability	Data privacy	Emergency case
Yue et al., 2016 [13]	✓	×	-	-	-	✓	×	✓	x
BBDS (Xia et al., 2017) [22]	✓	×	Cryptographic keys	Encryption and digital signatures	-	✓	×	✓	x
Ancile (Dagher et al., 2018) [16]	✓	×	IDs	-	Smart contract	✓	×	✓	x
EACMS (Rajput et al., 2019) [24]	✓	×	Patient ID	-	Chaincode	×	×	x	✓
Healthchain (Xu et al., 2019) [12]	✓	×	Userchain address	Public key Cryptography	-	✓	×	✓	×
Lagutin et al., 2019) [26]	×	✓	DID	Authorization Server (AS)	Authorization Server (AS)	✓	×	✓	x
Jung, 2020 [27]	×	✓	DID	Decentralized Public Key Infrastructure (DPKI)	DID and DPKI	✓	×	x	x
Kumar et al. (2020) [15]	✓	×	Secure proof of identity	-	Smart contract	✓	×	✓	x
Madine et al., 2020 [19]	✓	×	-	Ethereum address	Re-encryption key	✓	×	✓	x
SSIBAC (Belchior et al. 2020) [25]	✓	✓	DID	decentralized authentication	Smart contract	✓	×	✓	x
Kim et al., 2021 [28]	✓	✓	DID	DID + VC	-	×	×	✓	×
Our DSMAC model	✓	✓	DID	Public key +DID	Smart contract DDO	✓	✓	✓	✓

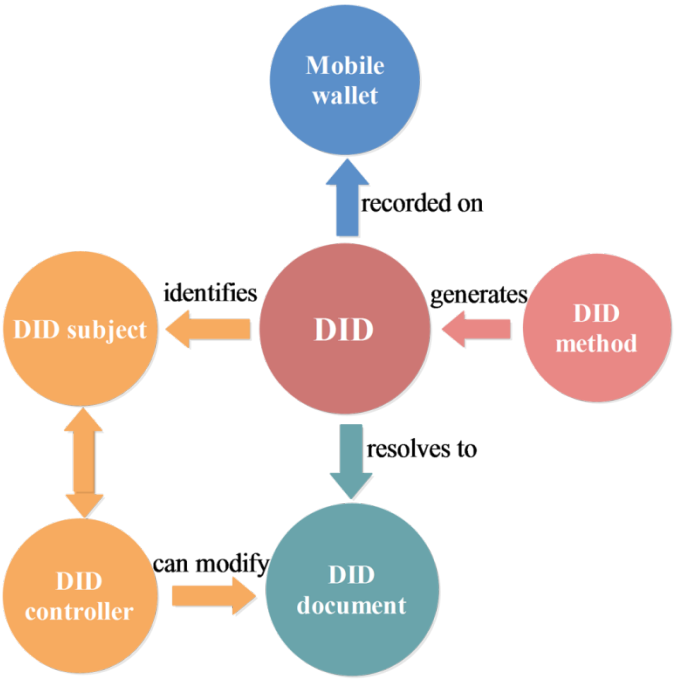


FIGURE 1. **The basic components of DID architecture. The figure displays the interaction between DID components.**

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3207803

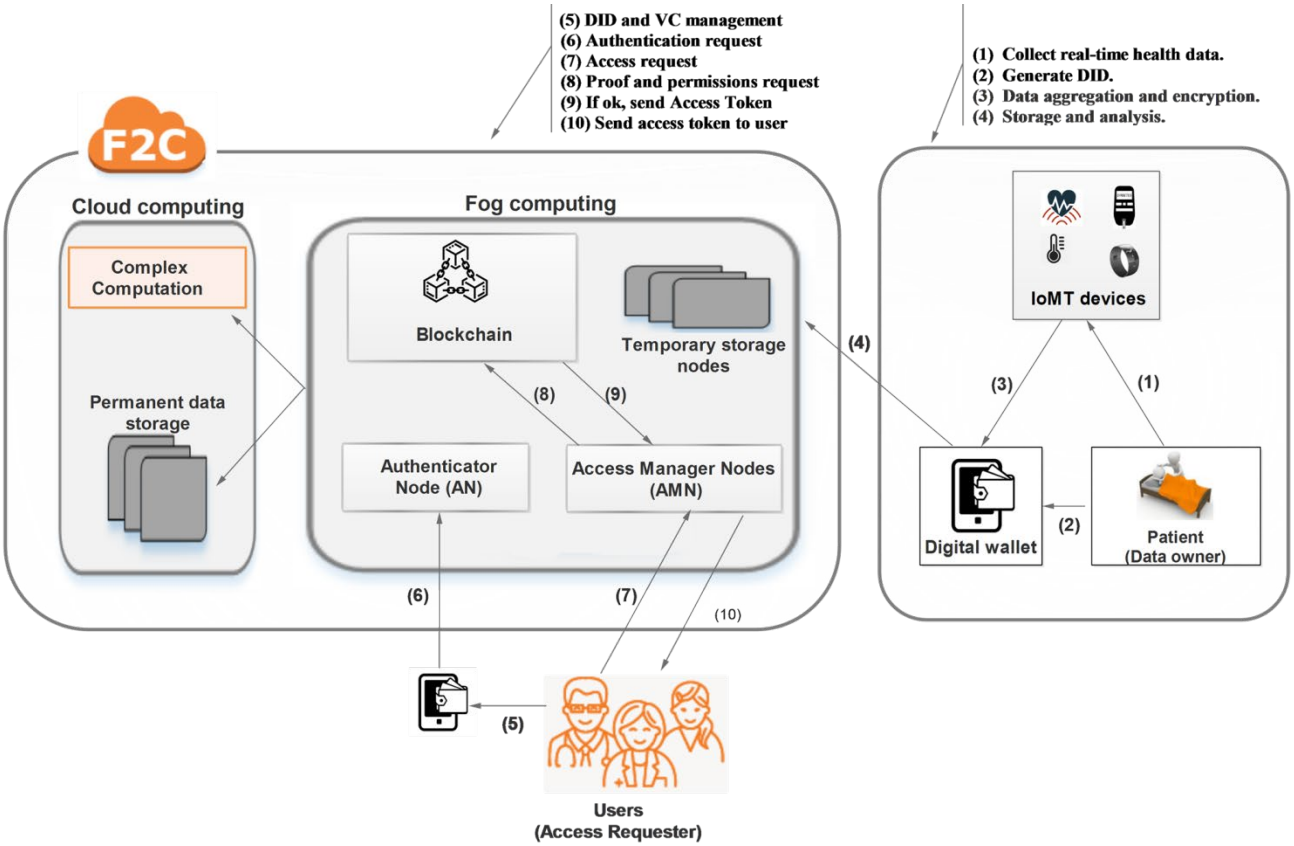


FIGURE 2. **System overview. The figure presents the main components of our framework, Decentralized Self-Management Access Control (DSMAC).**

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3207803

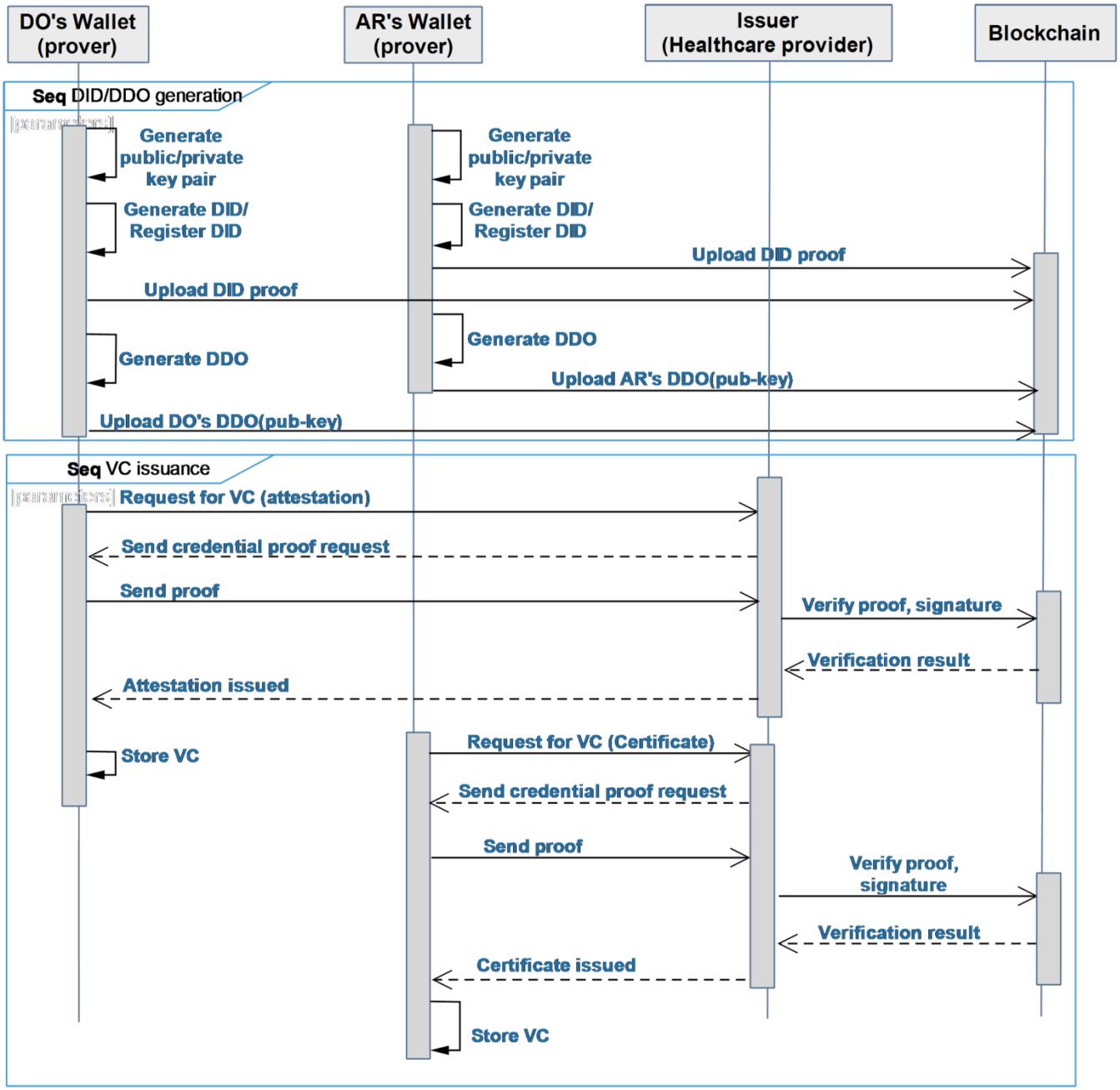


FIGURE 3. **Sequence diagram of DID generation and VC issuance operations. The flowchart describes the interaction between entities corresponding to the SSI's phases including the blockchain transactions.**

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3207803

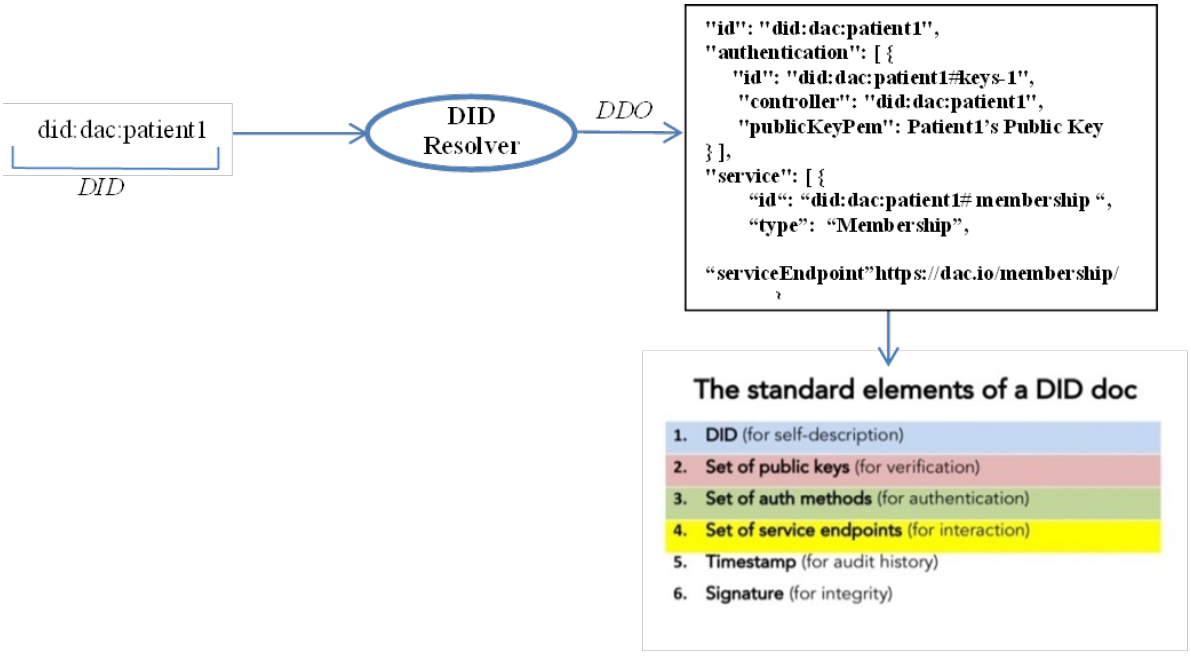


FIGURE 4. **The structure and resolution of DID Document (DDO). The crucial elements of the DDO structure are the public key and service endpoints.**

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3207803

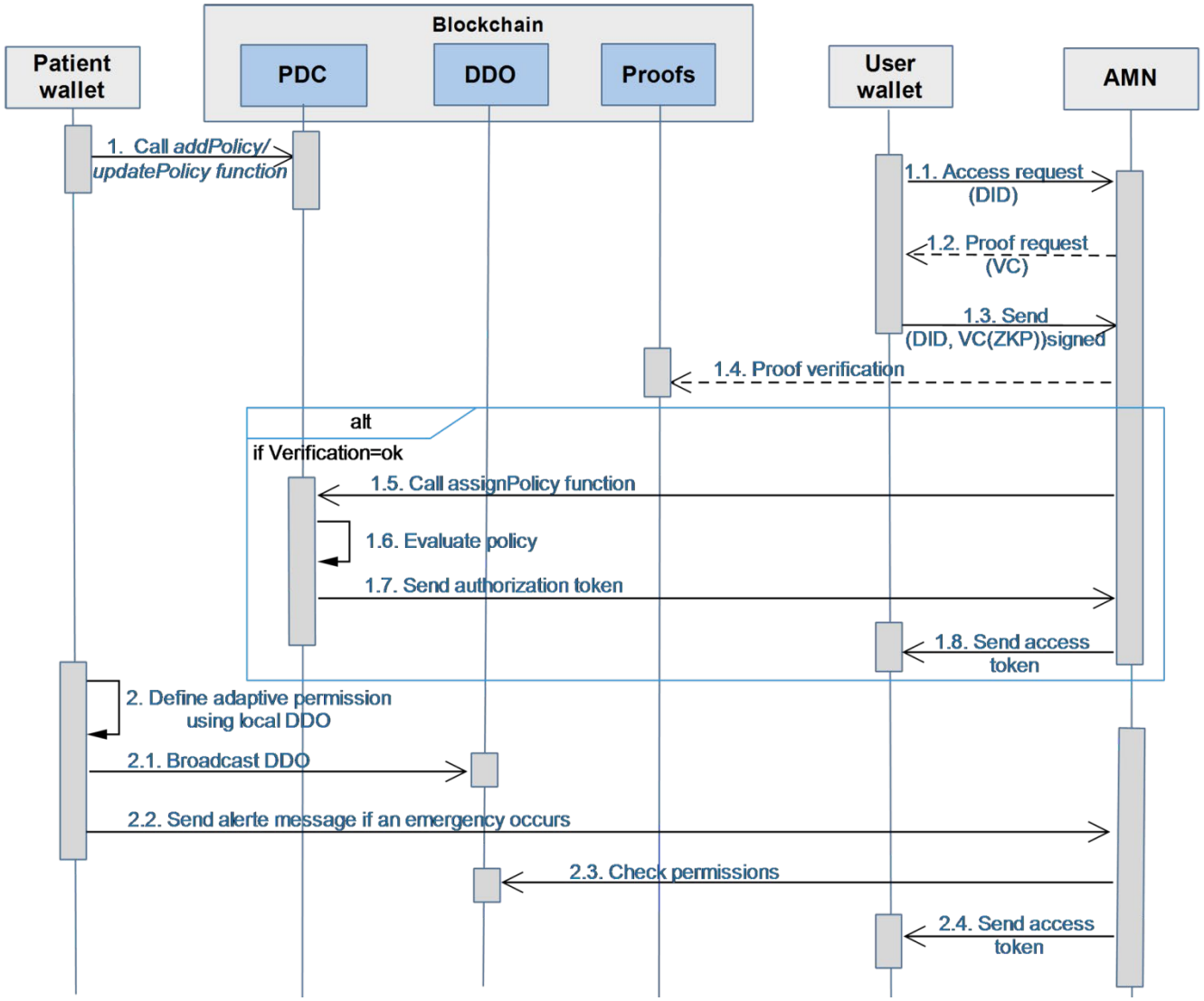


FIGURE 5. **Sequence diagram of Decentralized Access control (DAC) approach. The flowchart describes the request access transaction sequence.**

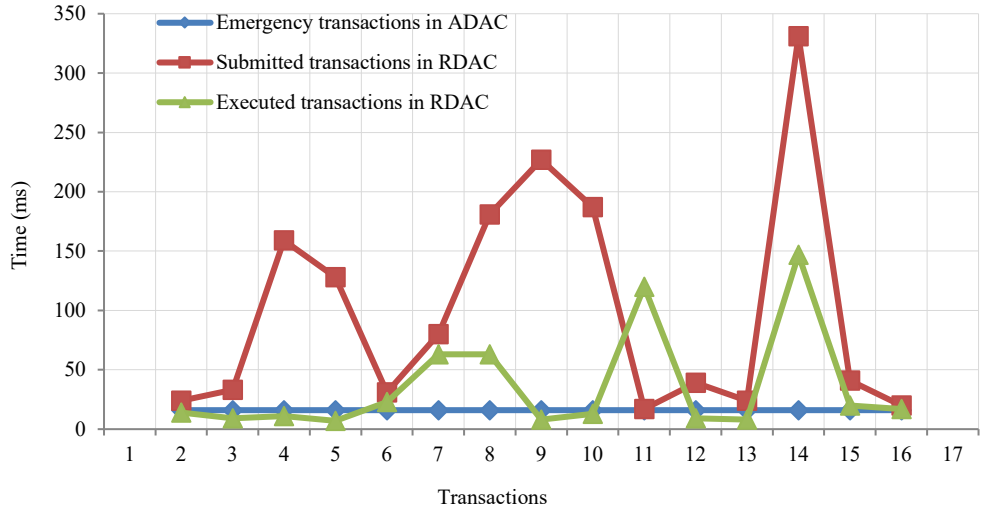


FIGURE 6. **Transaction time comparison of RDAC and ADAC models. The results depict that ADAC model takes less Access Control assignment time as compared to the RDAC model. This confirms that the ADAC model is the best choice for emergency cases.**

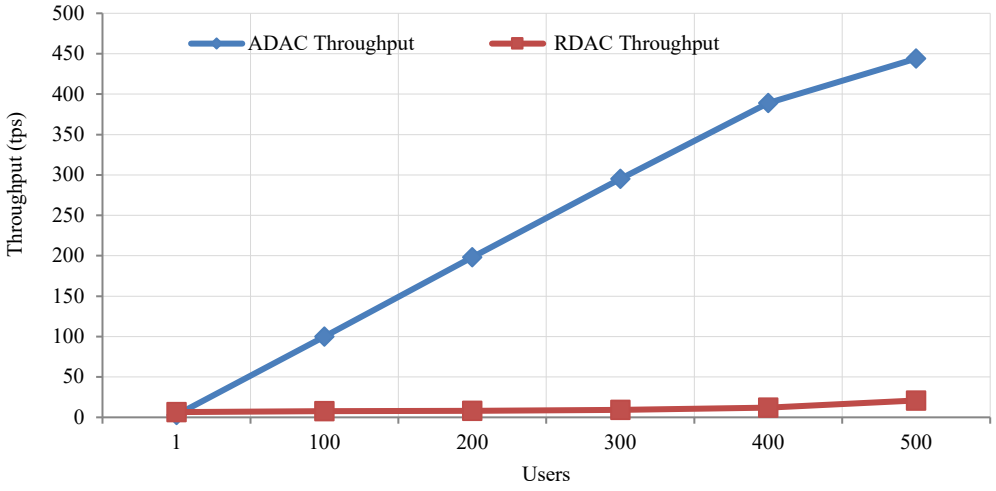


FIGURE 7. **Transaction throughput of RDAC and ADAC models. ADAC model has a high throughput compared to the RDAC model. We observe that as the number of users increases, there is an important increase observed in the throughput of the ADAC model**

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3207803

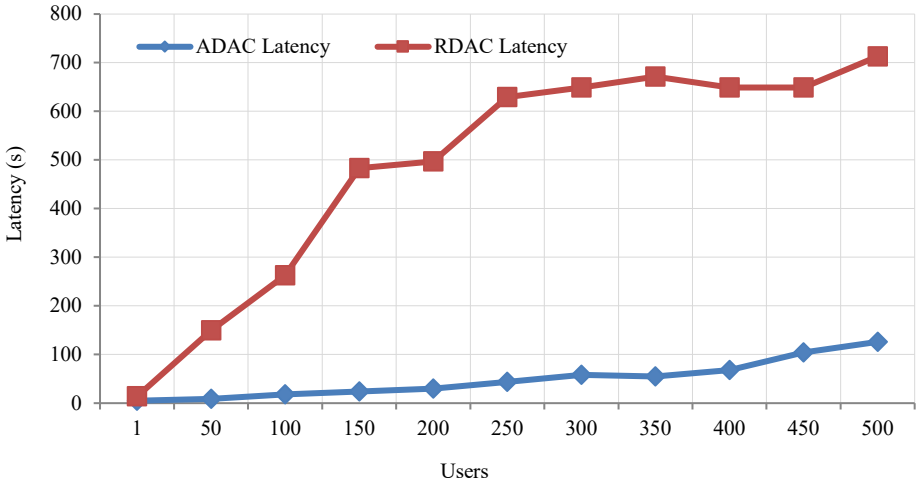


FIGURE 8. **Transaction latency of RDAC and ADAC models. It is noticed that there is a continuous growth in the average latency as the number of users is increasing for both experiments. However, the average latency of the ADAC model is lower than the RDAC model.**

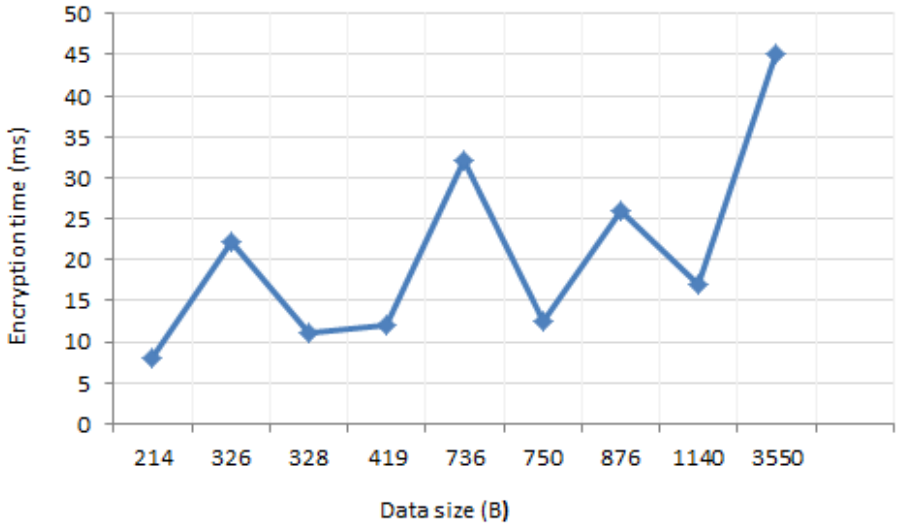


FIGURE 9. **Time while performing data encryption. It is noticed that there is a gradual growth in the encryption time as the data size is increasing.**

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3207803

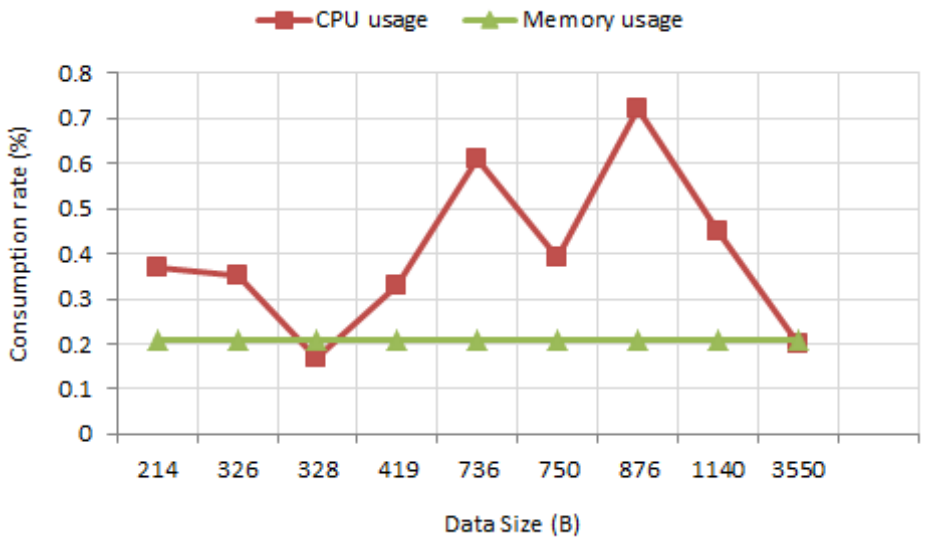
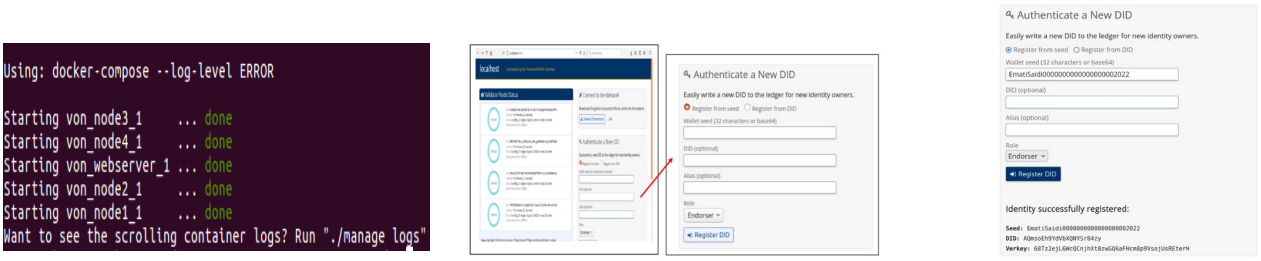


FIGURE 10. **CPU and memory usage while performing data encryption. It is noticed that when the data size is increased, the CPU utilization increase gradually. Whereas memory utilization remains almost constant.**



(a) (b) (c)

FIGURE 11. **a. Starting Von Network, b. VON network manage page and DID registration, c. Creating a public DID for patient agent.**

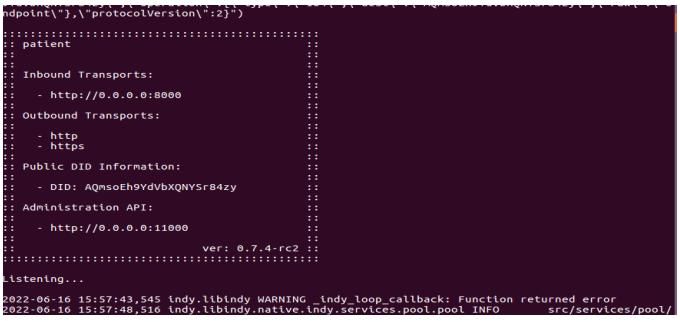


FIGURE 12. **Successfully run an ACA-Py agent as a Patient.**

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3207803

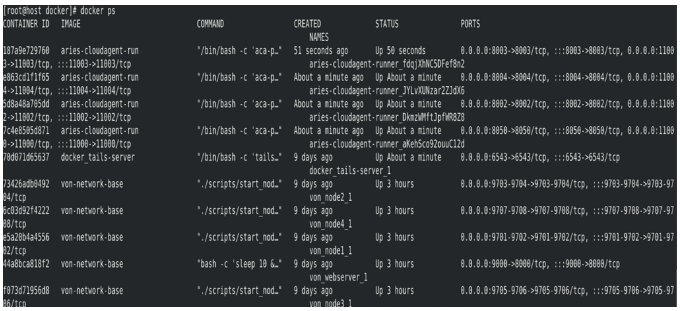
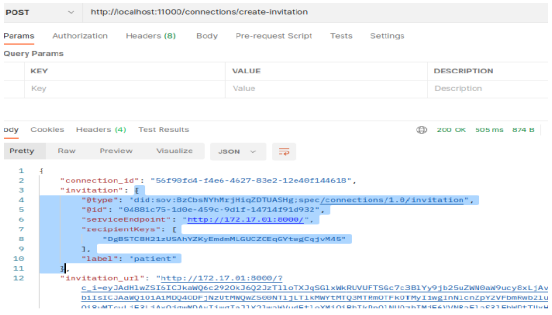
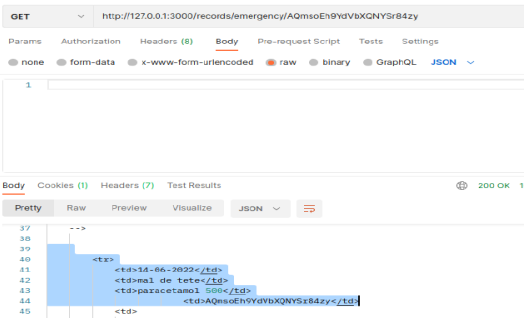


FIGURE 13. **Docker list containers.**



(a)



(b)

FIGURE 14. **a. Call create invitation API on the patient agent in an emergency case, b. API response once an emergency case is detected on the patient agent.**

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3207803

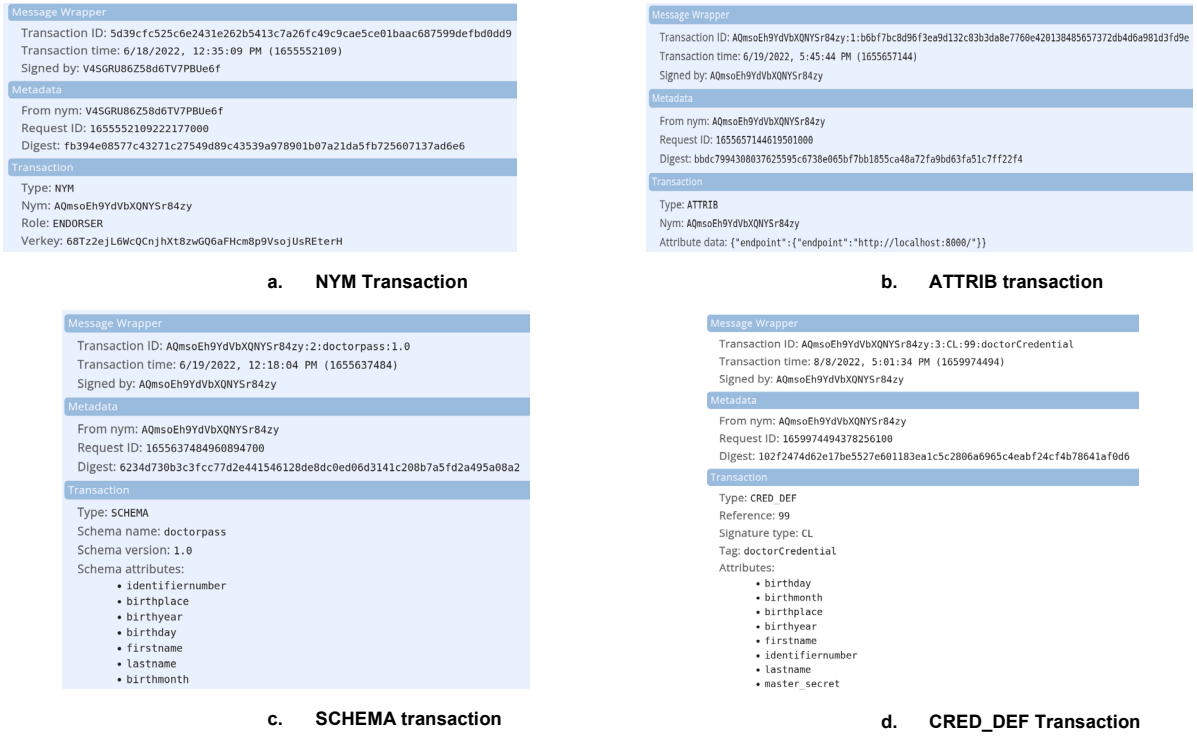


FIGURE 15. **NYM, ATTRIB, SCHEMA and CRED_DEF ledger transactions.**