Enhancing Secure Access and Authorization in Healthcare IoT through an Innovative Framework: Integrating OAuth, DIDs, and VCs

Conference Paper · November 2023

DOI: 10.1145/3625156.3625193

3 authors:

Maruf Farhan Rigan
Northumbria University
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Abdulrahman Salih
Northumbria University
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Usman Butt
Northumbria University
19 PUBLICATIONS **66** CITATIONS
SEE PROFILE

Enhancing Secure Access and Authorization in Healthcare IoT through an Innovative Framework: Integrating OAuth, DIDs, and VCs

Maruf Farhan[*]
Northumbria University, Department of Computer and Engineering
Maruf.farhan@northumbria.ac.uk

Abdulrahman Salih
Department of Computing & Engineering, Northumbria University,
Abdul.salih@ northumbria.ac.uk

Usman Javid Butt
Department of Computing & Engineering, Northumbria University
Usman.butt@northumbria.ac.uk

ABSTRACT

Protecting patient information's confidentiality is paramount considering the widespread use of Internet of Things (IoT) gadgets in medical settings. This study's subjects are decentralized identifiers (DIDs) and verifiable credentials (VCs) in conjunction with an OAuth-based authorization framework, as they are the key to protecting IoT healthcare devices. DIDs enable autonomous authentication and trust formation between IoT devices and other entities. To authorize users and enforce access controls based on verified claims, VCs offer a secure and adaptable solution. Through the proposed framework, medical facilities can improve the privacy and security of their IoT devices while streamlining access control administration. An Smart pill dispenser in a hospital setting is used to illustrate the advantages of this method. The findings demonstrate the value of DIDs, VCs, and OAuth-based delegation in protecting the IoT devices. Improved processes for authorizing and controlling access to IoT devices are possible thanks to the research findings, which also help ensure patient confidentiality in the healthcare sector.

CCS CONCEPTS

• **Security and privacy** → Usability in security and privacy.

KEYWORDS

Internet of things, verifiable credentials, Decentralized identifiers, security, authorization, authentication

ACM Reference Format:
Maruf Farhan, Abdulrahman Salih, and Usman Javid Butt. 2023. Enhancing Secure Access and Authorization in Healthcare IoT through an Innovative Framework: Integrating OAuth, DIDs, and VCs. In *2023 The 6th International Conference on Information Science and Systems (ICISS 2023), August 11–13, 2023, Edinburgh, United Kingdom.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3625156.3625193

1 INTRODUCTION

Security, privacy, and interoperability are among the issues arising as IoT devices have been more widely used. When managing authorization and authentication processes securely, restricted IoT devices like intelligent pill dispensers in healthcare environments confront unique hurdles. This work seeks to solve these issues by proposing a method that blends Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) with OAuth-based delegation, providing a privacy-enhancing and scalable strategy for resource-constrained IoT devices. Decentralized identifiers (DIDs) allow people to establish their identities independently of any governing body [34]. To confirm qualities or privileges without providing unneeded personal information [35], VCs provide a flexible and secure framework for granting and verifying credentials.

This study uses the OAuth framework and its ACE extension (Authentication and Authorization for Constrained Environments) [36] to allow DIDs and VCs in resource limited IoT devices. ACE enhances the functionality of the already powerful OAuth authorization mechanism for low-power mobile devices. Together, these technologies allow limited IoT devices like intelligent pill dispensers to use the privacy-enhancing qualities of DIDs and VCs by delegating their processing to an OAuth Authorization Server [37].

This academic journal article helps advance IoT security and privacy research by providing a workable strategy for utilizing DIDs and VCs in resource limited IoT gadgets. In addition to allowing interoperability with current authentication and authorization frameworks, the suggested method can potentially improve user privacy and access control regulations.

The goal of this research is to find solutions to the problems associated with implementing DIDs and VCs on resource limited IoT devices. The authors' goal in proposing an OAuth-based delegation technique is to make it possible for systems with resource-constrained IoT devices to take use of DIDs and VCs while also successfully handling the complications that come with doing so. The study appears to be primarily concerned with developing a solution that strikes a compromise between leveraging cutting-edge privacy-preserving standards (DIDs and VCs) and addressing the constraints of restricted IoT devices. Using an external Authorization Server, the OAuth-based solution described in the study intends to facilitate a wider use of DIDs and VCs in IoT contexts. This strategy could make it possible to integrate DIDs and VCs more effectively and scalable within restricted IoT networks.

[*]Corresponding author

ICISS 2023, August 11–13, 2023, Edinburgh, United Kingdom

ACM ISBN 979-8-4007-0820-6/23/08…$15.00
https://doi.org/10.1145/3625156.3625193

2 AUTHORIZATION AND AUTHENTICATION ALLOCATION WITH IOT

Internet of Things (IoT) devices are employed in various scenarios, encompassing the transportation of perishable goods such as fruits. In this context, these devices are utilised to constantly monitor climate sensor values, which are subsequently used to regulate climate actuators. Additionally, IoT devices are employed to facilitate the effortless configuration of new lighting devices, establish their authorization policies, and grant temporary permissions to guests in smart home environments.

This section provides an overview of the primary authentication and authorization methods now employed in the context of the Internet of Things (IoT). These solutions include OAuth 2.0 and its associated technologies, such as Authentication and Authorization for Constrained Environments (ACE), OpenID Connect, and User-Managed Access (UMA) 2.0. These protocols have the potential to be utilised in conjunction with various authentication techniques. By incorporating them with decentralised identifiers (DIDs) and verifiable credentials (VCs), further flexibility is achieved, as these privacy-enhancing technologies are supported. Table 1 presents the advantages and disadvantages of the various authentication and authorization protocols.

2.1 OAuth 2.0

Individuals, smart-systems, and IoT-connected objects can all benefit from DIMS's improved identification and authentication procedures [10]. Today's DIMS, for instance, heavily incorporates third-party authentication tokens (like OpenID or OAuth 2.0) into diverse online systems and services that rely on user-supplied credentials (like Google and Facebook) [11]. Authentication and authorization are two subjects that are frequently included under the same umbrella. A standard called OAuth 2.0, which is an abbreviation that stands for "Open Authorization," is designed to make it possible for a website or application to access resources that are hosted by other web apps on behalf of a user. In 2012, it took the place of OAuth 1.0 and has since become the de facto industry standard for online authorization. The OAuth 2.0 architecture consists of a four-part structure with four distinct roles: the resource owner, the client, the resource server, and the authorization server. OAuth 2.0 is a widely used authorization system that facilitates the acquisition of limited access by a third-party application or client to a protected resource that is housed on a resource server (RS) [12]. OAuth 2.0 facilitates authorised access and imposes limitations on the operations that the client application can execute on behalf of the user, while ensuring the user's credentials remain undisclosed [13].

Resource Owner: A person or thing that has the authority to open access to a restricted resource. In most cases, this refers to the final consumer [14].

Client: The term "Client" refers to an individual who makes a request to an application for access to a protected resource on behalf of the Resource Owner [14].

Resource Server: Server that hosts confidential information. Access the Application Programming Interface (API) found here [14].

Authorization Server: Server that verifies the identity of the Resource Owner and distributes Access Tokens after confirming that they have the necessary permissions. In this scenario, Auth0 [14].

Because clients are required to make a request to the resource owner before they may access resources, OAuth 2.0 is suitable for use in IoT environments. Before accessing an Internet of Things device, it is vital to obtain the permission of the resource owner to ensure one's personal safety and privacy. Failing to do so will cause the device to use the policies that were previously established.

2.2 ACE-OAuth

(Authentication and Authorization in Resource-Limited Settings) is an OAuth-based framework developed for low-powered Internet of Things gadgets. It's an extension of OAuth 2.0 that adds security and efficiency to authentication and authorization in limited-access settings [15, 16].

2.3 UMA 2.0

As a protocol built on top of OAuth 2.0, UMA (User-Managed Access) 2.0 lets users' control who has access to what data across different services. It's a defined system for determining who has access to a user's information and under what circumstances [17].

2.4 OpenID Connect

Using OAuth 2.0 as its foundation, connect provides a secure identity layer. It allows clients to get basic profile information about a user in an interoperable and REST-like fashion depending on the authentication done by an authorization server [18].

3 SELF-SOVEREIGN IDENTITY WITH IOT

3.1 Self-Sovereign Identity

At now, decentralized identifiers (DIDs) are a popular identity technology. An essential feature of DIDs is their independence from a central identity provider (IdP) that produces and controls the identity. Self-sovereign identity refers to the management of DIDs by the identity owner or their guardian [1]. The concept of "Self-Sovereign Identity" (SSI) is quickly becoming the standard for online ids. With the help of Self-Sovereign Identity (SSI), users may maintain complete control over their PII (personally identifiable information) in relation to all authorities. However, there is disagreement concerning the SSI's precise nature. Allan tries to distinguish SSI by presenting 10 ideas that are exclusive to it [2].

In the past few years, the phrase Self-Sovereign Identity (SSI) has grown significantly [3]. The term "secure self-identity" (SSI) refers to a method of identity management that gives individuals control over their online personas [3]. It might also be considered as an improvement on non-centric identity management solutions, which place less emphasis on a centralized authority and instead place more authority in the hands of the users [4]. This means that service providers cannot sell users' personal information and are limited in their ability to use users' identities [5].

3.2 Decentralized Identifiers:

Storing identities and independently verifiable claims on the blockchain is made possible by the concept of self-sovereign identity using Decentralized Identifiers (DIDs) [7]. To access the online

Table 1: Advantages and disadvantages of protocols

Protocol	Pros	Cons
ACE-OAuth	Lightweight and designed for resource constrained IoT devices	Limited adoption and support in comparison to traditional OAuth and other protocols
	Utilizes OAuth concepts adapted for IoT device constraints	Requires careful consideration of security implications for constrained devices
	Offers various authentication methods suitable for IoT	Complex implementation and configuration
OpenID	Decentralized authentication protocol	Requires integration with existing identity providers
	Single set of credentials for multiple services and applications	Relies on centralized identity providers, introducing potential single point of failure
	OIDC extension provides additional features like identity federation and user information sharing	May introduce additional complexity in implementation and configuration
UMA	User-centric authorization framework	Requires support from IoT platforms and services to implement UMA
	Users control the authorization of their resources	Implementation may involve additional development and configuration efforts
	Suitable for scenarios where users want granular control over IoT device access	Potential complexity in managing and enforcing user-managed access policies
OAuth	Widely adopted and supported protocol for authorization and delegation	Can be challenging to configure and secure properly
	Supports various authentication and authorization flows	May introduce additional overhead due to its comprehensive nature
	Interoperability with existing systems and services	Requires careful management of client credentials and tokens
	Extensive community and resources for implementation and integration	

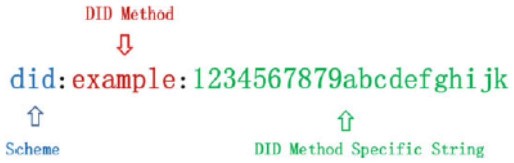

Figure 1: example of DID

services, first user needs to create the account (Identity) and once it's approved then they are allowed to use it for the online services. In this scenario, along with the user, a 3rd party also has access to his identity. DIDs developed due to give users control over their digital identities. DIDs created to give users control over their digital identities [7]. DIDs are essential in online services by providing users with authorization and authentication [8]. Each DID is accompanied by a DID document that details the proper way to communicate with and manage the devices it identifies. The DIDs document contains all the necessary information to describe the entity it represents.

The scheme is represented by the first portion, and the DID technique, which details how DID operates on a given distributed network, is represented by the second part. Operations such as adding, removing, reading, and updating DID documents are defined in the DID method specification for a given target system.

3.3 Verifiable Credentials:

Nevertheless, credentials come with several drawbacks, including the fact that they are simple to fake, that it is simple to mimic the rightful owner, that they can be misplaced, and that they are difficult or impossible to scale. In addition, it is quite challenging to validate the veracity of these credentials through the internet platform. To resolve the issue verifiable credentials are required. verifiable credentials (VCs) is an electronic document that attests to the identity of one person on behalf of another [9]. The issuer makes claims about the prover's qualities in a Verifiable Credential (VC). In the below 2 it shows the flow of verifiable credentials with zero knowledge proof and the selective disclosure. The prover must either show that they have physical possession of the private key, or give further proof, to use a credential as evidence. Because of this, sensitive information can be withheld while still confirming certain assertions or revealing features. DID technology determines the types of credentials that can be issued, and the method used to verify their authenticity.

4 RELATED WORK

In the field of IoT, many researchers are working on security and privacy [19–26]. This article explores the privacy and security risks associated with implementing Internet of Things (IoT) healthcare solutions for people with disabilities in third world countries. However, the authors noticed that there are a few problems, such as:

1) The absence of data protection laws in poor countries 2) Secondly, the implementation of insecure communication protocols

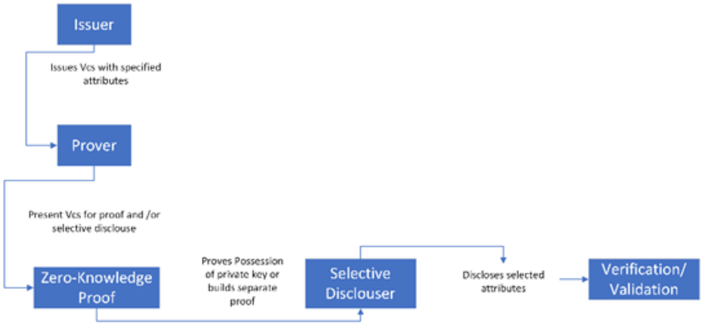
Issuer
Issues Vcs with specified attributes
Prover
Present Vcs for proof and /or selective disclouse
Zero-Knowledge Proof
Proves Possession of private key or builds separate proof
Selective Disclouser
Discloses selected attributes
Verification/ Validation

Figure 2: Flow of Verifiable Credentials, Zero-Knowledge Proofs, and Selective Disclosure

and Concerns about privacy and security among disabled people and healthcare professionals [27]. Apart from that the author also provided solution such as The establishment of safety and privacy standards for healthcare Internet of Things applications, The implementation of encrypted methods of communication, training for healthcare professionals and people with disabilities on the importance of data security and privacy [27].

AI-driven IoT security and privacy challenges in healthcare are discussed in another study [28]. The collecting and storage of enormous volumes of sensitive data, the usage of complicated algorithms that can be difficult to understand and audit, and the possibility for AI-driven IoT devices to be hacked or manipulated are all challenges, according to the authors [28]. Strong encryption and access control are among the measures suggested by the authors. Developing transparent and auditable AI algorithms and educating healthcare professionals and patients about AI-driven IoT security and privacy issues [28]. Another research discusses IoT healthcare system security and privacy issues. The authors observed several problems, including IoT devices' heterogeneity, healthcare personnel' lack of security and privacy knowledge, and the difficulty of safeguarding IoT networks. The authors also suggest creating a security and privacy framework for IoT healthcare systems, educating healthcare professionals about security and privacy risks, and using tailored security and privacy solutions [29]. This study [30] suggests a blockchain-based framework to improve healthcare IoT's privacy and security. Issues of data privacy, security, and confidentiality will be tackled. The study proposes a distributed system that makes use of blockchain technology to keep medical records safe from manipulation. Smart contracts are discussed as a means of implementing access control regulations and protecting patient privacy. The purpose of this second survey paper [31] is to offer a broad perspective on the challenges of privacy and security in IoT-based healthcare infrastructure. Unauthorized access, data breaches, and identity theft are just some of the vulnerabilities and risks that are investigated. Guidelines for improving privacy and security are proposed, and existing security measures such data encryption, secure data exchange, and user authentication procedures are surveyed.

Using decentralized identities (DIDs) and verifiable credentials (VCs), the authors of this work sought to address the difficulty of enabling safe and privacy-preserving access to limited IoT devices, such as smart pill dispensers. Specifically, their goal was to find a solution that would use DIDs. Even though DIDs and VCs have emerged as potentially valuable solutions for decentralized digital identity and attribute verification, deploying these solutions on constrained IoT devices is still challenging due to the limited computing power, memory, and energy resources available.The authors believe that there is a research vacuum in Internet of Things authentication and authorization because there is yet to be a scalable method that protects users' privacy and can support DIDs and VCs for restricted devices. Because of their large computational and communication overheads and dependency on centralized trust authorities, existing solutions such as Public Key Infrastructures (PKIs) and X.509 certificates are not suited for restricted Internet of Things devices.

To enable DIDs and VCs for limited IoT devices, the authors developed an OAuth-based delegation strategy that leverages the OAuth 2.0 framework and its Authentication and Authorization for restricted Environments (ACE) extension. The goal of the suggested solution is to provide a method of authentication and authorization for the Internet of Things (IoT) that is more secure, scalable, and protective of users' privacy, all while upholding users' and devices' respective self-sovereignty and confidentiality.

5 OAUTH BASED PROPOSED FRAMEWORK

An approach is described here for relying on the OAuth Authorization Server to handle verification of credentials and the processing of decentralized identifiers. More privacy and adaptability in the authorization procedure are now available to even the most limited IoT devices.

In the medication management use case, the actors include:

Health professional: who might benefit from using a smart pill dispenser (an Internet of Things device)

Medication Management System (MMS): that owns the dispenser.

Hospital: This grants the Health Care Provider a VC for drug management

Smart Pill dispenser: The IoT device.

Authorization server (AS): authorized to act as the dispenser's official authenticator.

Let's say a visiting doctor must manage the hospital's medications and needs access to the facility's smart pill dispenser. The health care provider's duties include medication management, and

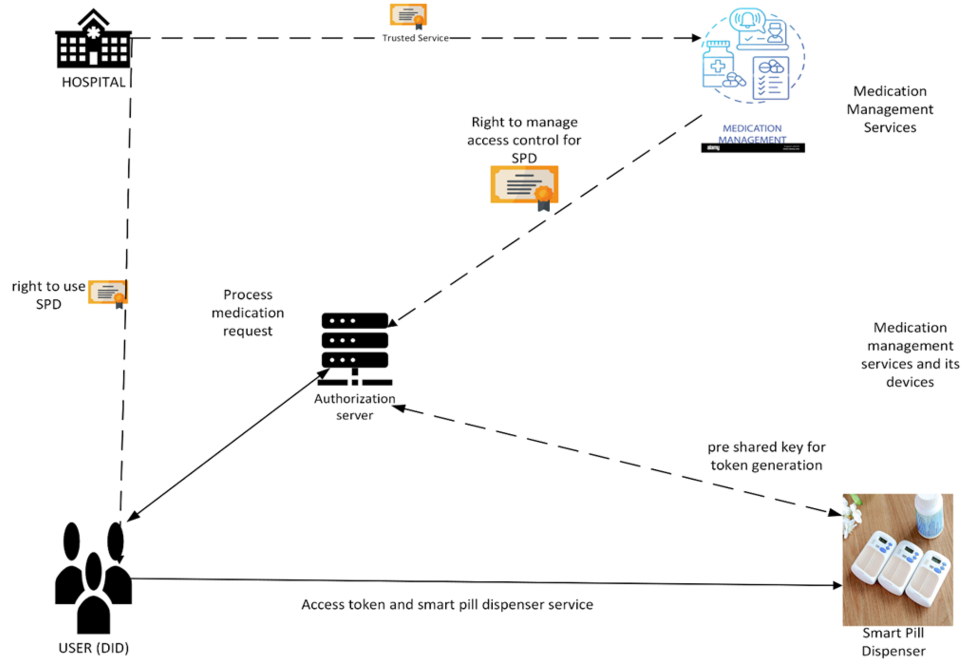
HOSPITAL
Trusted Service
MEDICATION MANAGEMENT
Medication Management Services
Right to manage access control for SPD
right to use SPD
Process medication request
Authorization server
Medication management services and its devices
pre shared key for token generation
USER (DID)
Access token and smart pill dispenser service
Smart Pill Dispenser

Figure 3: Authentication and authorization process between healthcare professional and smart poll dispenser

the hospital has given them permission to do so. The reliable Medication Management Service (MMS) offers a variety of smart pill dispensers that can be used by the medical staff. The MMS and the smart pill dispenser both need to prevent unauthorized individuals from gaining access to or managing drugs without disclosing the identity of the healthcare provider.

The Medication Management Service cannot function if it needs user-issued credentials to do its job, as in the case of the visiting health professional who does not have a hospital identity or user account. To assure the safety of interactions between users and smart pill dispensers, authentication is performed using user-generated Decentralized Identifiers (DIDs). In addition, the Medication Management Service will use the healthcare provider's verified credentials (VCs) granted by the hospital to confirm that the smart pill dispenser is an approved device.The Medication Management Service uses a streamlined verification and authorization approach to facilitate the management of several smart pill dispensers and users, including those with limited processing capabilities. The AS's primary function is to authenticate the smart pill dispenser on behalf of the healthcare provider and to handle authorization requests. Fig. 1 shows the relationships between the various participants in this use case, including the Health Professional, Medication Management Service, Smart Pill Dispenser, Hospital, and Authorization Server. The continuous lines represent the flow of dialogue in the use case, while the dashed lines represent the actors' trust in one another.

For constrained IoT devices like smart pill dispensers in the context of medication management in hospitals, the proposed approach demonstrates how DIDs and VCs, in conjunction with the OAuth-based delegation model, can be used to enable secure and privacy-preserving authorization and authentication.

The authorization server authorizes users based on access control policies defined by the hospital. These policies can take many forms, such as a combination of information previously stored on the authorization server by the hospital (e.g., the health professional is allowed to manage medication) and the health professional's credentials that were issued by the hospital. Together, these form proof that the health professional is allowed to manage medication using the smart pill dispenser.

Additionally, the health professional only wants to manage medication using smart pill dispensers owned by the hospital, so mutual authentication between the health professional and the smart pill dispenser is necessary. Two sets of evidence based on independently substantiated credentials will be presented to the medical professional to demonstrate the smart pill dispenser's reliability. The first proof states that the hospital is authorized to offer medication management services using smart pill dispensers. The second proof states that the authorization server is authorized to validate, control authorization requests, and in the name of that smart pill dispenser, give tokens to users.Credentials that can be checked make the method even safer. The hospital gives the health professional a credential that can be checked for medication management. The authorization server can use this credential to make sure that the health professional is allowed to use the smart pill dispenser to handle medication. Overall, the system is made up of several people and tools that work together to make sure that medications are managed safely. By using credentials that can be checked and access control policies, the system can make sure that only authorized users can use the smart pill dispenser to handle medication and that the smart pill dispenser is reliable and has been given permission by the hospital to offer medication management services.

1. Local service discovery through Wi-Fi or Bluetooth Direct are just two instances of how a medical practitioner (user) could come across a smart pill dispenser and its accompanying authorization server (AS).

2. The healthcare provider expresses interest in utilizing the smart pill dispenser and asks the AS for evidence that (a) the smart pill dispenser has been validated as trustworthy by the hospital and (b) the AS has been granted permission by the smart pill dispenser to manage prescription requests.

3. The AS will make the necessary proof using the provided credentials. The AS also requests that the health professional produce proof of the right to manage medication, which is forwarded together with the documentation to the health professional.

4. The healthcare provider checks the AS's evidence and, if everything checks out (the hospital trusts the smart pill dispenser, and the smart pill dispenser trusts the AS), provides the AS a credential proving the AS's authority to manage medication.

5. AS proof is verified by the health professional. If everything is satisfactory (i.e., the MMS is trusted by the Hospital and the AS is trusted by the MMS), the health professional provides confirmation of the authority to manage pharmaceuticals, established using the Hospital credential, back to the AS.

6. The AS issues a PoP access token after verifying the health professional's proof and user can access the IoT device using this PoP access token.

6 DISCUSSION

The old X.509 certificates and PKIs are designed to be permanent and readable by humans. A certificate is issued once and can be used elsewhere. These certificates often need more user information, including their genuine identity. Certificate users must reveal all properties. Certification expenses are high because confirming a user's identification requires manual verification. Due to certificate information, various parties can easily track a user's activities across many services.

However, IoT authorization and authentication with DIDs and VCs have several benefits. While DIDs and VCs could benefit from standard X.509 certificates and PKIs, their high prices and impracticality make deployment challenging. DIDs and VCs allow users to express vital attributes without revealing unnecessary personal details. This decreases certificate costs and overcomes privacy problems related to tracking user behavior across numerous services.

A decentralized identifier (DID) or verifiable credential (VC) is a type of digital credential designed to be more secure than a traditional password and easily read and understood by machines. As a result of this improvement, the issuing of credentials is more secure and cheaper. A traditional requirement for Health professionals who wish to use the Hospital's smart pill dispenser service has been to obtain a hospital-issued IT account. However, this is usually only available to industry insiders. The proposed solution takes a new tack by having the healthcare provider earn credentials for using the smart pill dispenser. A new DID and verification code (VC) would be used if the Health professional used the dispenser for a different purpose, such as for a different medication management duty. Therefore, neither the Authorization server (AS), the smart pill dispenser service, nor the dispenser itself can monitor the health professional's actions.

Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) are integral to the suggested system. In particular, the security mechanism OAuth is compatible with this approach. The smart pill dispenser scenario in the medical field addresses several issues that OAuth needs to address completely.

OAuth is like a collection of rules followed by various system components to ensure that only authorized users and programs have access to restricted resources. There is a description of the interoperability of these components, but it needs an explanation of how a name check is performed. OAuth now aids in managing the interactions between healthcare providers and the smart pill dispenser. OAuth, however, needs to adequately explain how the supplier verifies the identity of the Health professional and how the Health professional verifies that they are communicating with the genuine smart pill distributor. Where the proposed solution comes in at this point. What was lost is now restored. The smart pill dispenser and the medical professional's identities are verified (through authentication) and kept private (via mutual authentication).

In addition, the anticipated response provides scope for individual choice. The smart pill dispenser's data storage (resource server) and the system that authorizes access (Authorization Server or AS) can function independently in the medical field. This is different from the way OAuth recommends they interact. To avoid overreliance on the authorization system, the smart pill gadget can do some checks independently. This means that the existing OAuth system in the healthcare sector may be expanded to include the additional option based on DIDs and VCs. Adding this new, more secure method of managing identities and access to the smart pill dispenser's already-used OAuth system is simplified this integration.

7 FUTURE WORKS

How Internet of Things (IoT) use cases, such as those stated in a previous source [6]), can benefit from Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) is an area that could use more research. Scalable user authentication and authorization must be achieved by finding a way to make DIDs and VCs compatible with existing industry standards. It's possible that both DIDs' decentralized nature and VCs' emphasis on user agency will prove useful here.

The World Wide Web Consortium (W3C) is also demonstrating how virtual currencies (VCs) can be represented in a format called JSON Web Token (JWT), which is something to keep in mind. This format is used by things like OpenID Connect, which facilitates online identity verification. Updating existing OpenID-based systems to include DIDs and VCs would be simpler if verification codes could be converted into OpenID ID tokens in this format. For the layperson, this means that research is being conducted to ensure that virtual credit cards are compatible with existing online identity verification systems, and that DIDs can be used to improve IoT in the future.Security protocols like OAuth rely on the wide adoption of TLS to ensure that data is exchanged securely.

The OAuth-secured communication process is recommended to be simplified. Presenting evidence (proofs) at designated sites is a standard part of the current procedures for establishing one's identity. Instead of handling these proofs independently, it is proposed that they be incorporated within the TLS handshake itself.

The technique of "Server Name Indication" (SNI) can be utilized for this purpose. When initiating a TLS connection, the user has the option of specifying the target endpoint. The "client hello" message sent by a device always contains its unique identifier. The TLS response from the Authorization Server (AS), which is responsible for granting access, might then include the necessary proof. This proof establishes the user's legitimacy as the owner of the authorized device. To ensure a smooth and secure two-way authentication process, the AS may send the user a "client certificate request" message requesting additional confirmation. With these adjustments, the TLS handshake can function as if it has always been part of the communication process **[38]**. The process of conveying information is simplified as a result.

In terms of technology, TLS already uses a certificate format called X.509, so the proofs may be incorporated into that. Alternatively, certificates-focused TLS extensions could be used to transmit the proofs [34]. This optimization strategy does have one drawback, though. Someone listening in on the network in secret might be able to tell which device the user is trying to access. The only defense is for users to securely acquire the AS's public key for use in encryption. During service discovery or by consulting DNS records are two examples of safe ways to acquire this information. X.509 certificates may support zero knowledge properties **[32] but** DID solutions like Sovrin already support zero knowledge proofs, enhancing privacy by enabling users to prove their own properties without revealing credentials.

TLS 1.3 adds a new security feature called "Encrypted Server Name Indication" (ESNI) to further solve this problem by encrypting the server's identification information. This provides an additional layer of protection during transmission [33].

8 CONCLUSION

This Proposed Framework Recommends A Method For Implementing The ACE-Oauth Framework. This framework allows an access control server (OAuth Authorization Server) to take on a larger role in handling unique identifiers (DIDs) and verification credentials (VCs). Systems with devices that support ACE-OAuth but don't have the processing capability to handle DIDs or VCs on their own can benefit from this approach. For instance, there are limitations imposed by the IoT's devices. DIDs and VCs are beneficial because they simplify the process of regulating who has access to a system and how they can use it. For the sake of the future, this is invaluable. This paper proposes a method through which low-powered devices can make use of DIDs and VCs with the assistance of a dedicated server, thus allowing them to fully realize their potential. Controlling who has access to a system and how can be improved using DIDs and VCs. In terms of future productivity, this is crucial information.

REFERENCES

[1] C. Allen, The path to self-sovereign identity. 2016.

[2] 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, vol. 2, 2020.

[3] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, 'A survey on essential components of a Self-Sovereign Identity', arXiv [cs.CR], 2018.

[4] A. Abraham, C. Schinnerl, and S. More, SSI Strong Authentication using a Mobile-phone based Identity Wallet Reaching a High Level of Assurance: In: Proceedings of the 18th International Conference on Security and Cryptography. 2021.

[5] N. Naik and P. Jenkins, 'Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology', in 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2020.

[6] F. Schardong and R. Custódio, 'Self-Sovereign Identity: A systematic review, mapping and taxonomy', Sensors (Basel), vol. 22, no. 15, 2022.

[7] 'Decentralized Identifiers (DIDs) v1.0', Github.io. [Online]. Available: https://w3c.github.io/did-core/. [Accessed: 30-May-2023].

[8] M. Sharma and J. Lim, 'A survey of methods guaranteeing user privacy based on blockchain in internet-of -things', in Proceedings of the 2019 2nd International Conference on Data Science and Information Technology, 2019.

[9] 'Verifiable credentials data model v2.0', Github.io. [Online]. Available: https://w3c.github.io/vc-data-model/. [Accessed: 30-May-2023].

[10] T. Zhou, X. Li, and H. Zhao, 'EverSSDI: blockchain-based framework for verification, authorisation and recovery of self-sovereign identity using smart contracts', Int. J. Comput. Appl. Technol., vol. 60, no. 3, p. 281, 2019.

[11] L. Bathen *et al.*, 'SelfIs: Self-Sovereign Biometric IDs', in 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2019.

[12] D. Hardt, 'The OAuth 2.0 authorization framework', RFC Editor, 2012.

[13] 'What is OAuth 2.0 and what does it do for you?', Auth0. [Online]. Available: https://auth0.com/intro-to-iam/what-is-oauth-2. [Accessed: 30-May-2023].

[14] Auth, 'Which OAuth 2.0 flow should I use?', Auth0 Docs. [Online]. Available: https://auth0.com/docs/get-started/authentication-and-authorization-flow/which-oauth-2-0-flow-should-i-use. [Accessed: 30-May-2023].

[15] L. Seitz, S. Gerdes, G. Selander, M. Mani, and S. Kumar, 'RFC 7744: Use cases for authentication and authorization in constrained environments', IETF Datatracker, 29-Jan-2016. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7744. [Accessed: 31-May-2023].

[16] M. B. Jones, E. Wahlstroem, S. Erdtman, and H. Tschofenig, 'RFC 8392: CBOR Web Token (CWT)', IETF Datatracker, 08-May-2018. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8392. [Accessed: 31-May-2023].

[17] 'Federated authorization for user-managed access (UMA) 2.0', Kantarainitiative.org. [Online]. Available: https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-federated-authz-2.0.html. [Accessed: 31-May-2023].

[18] 'OpenID Connect Core 1.0 incorporating errata set 1', Openid.net. [Online]. Available: https://openid.net/specs/openid-connect-core-1_0.html. [Accessed: 31-May-2023].

[19] S. C. Tamane, V. K. Solanki, and M. S. Joshi, 'The basics of big data and security concerns', in Privacy and Security Policies in Big Data, IGI Global, 2017, pp. 1–12.

[20] M. Yamin and A. A. A. Sen, 'Improving privacy and security of user data in location Based Services', in Research Anthology on Privatizing and Securing Data, IGI Global, 2021, pp. 1411–1437.

[21] P. Mahalle, S. Babar, N. R. Prasad, and R. Prasad, 'Identity management framework towards internet of things (IoT): Roadmap and key challenges', in Recent Trends in Network Security and Applications, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 430–439.

[22] N. Ambritta P, P. N. Railkar, P. N. Mahalle, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering,University of Pune, Pune, India-411041, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering,University of Pune, Pune, India-411041, and Department of Computer Engineering, Smt. Kashibai Navale College of Engineering,University of Pune, Pune, India-411041, 'Proposed identity and access management in future internet (IAMFI): A behavioral modeling approach', J. ICT Stand., vol. 2, no. 1, pp. 1–36, 2014.

[23] S. Ben Mokhtar, P.-G. Raverdy, A. Urbieta, and R. S. Cardoso, 'Interoperable semantic and syntactic service discovery for ambient computing environments', in Innovative Applications of Ambient Intelligence, IGI Global, 2011, pp. 213–232.

[24] P. A. Shelar, P. N. Mahalle, and G. Shinde, 'Secure data transmission in underwater sensor network: Survey and discussion', in Studies in Systems, Decision and Control, Cham: Springer International Publishing, 2020, pp. 323–360.

[25] 'Vehicular networks security: attacks, requirements, challenges and current contributions', Int. J. Ambient Comput. Intell.

[26] M. B. Salunke, P. N. Mahalle, and P. S. Dhotre, 'Comprehensive threat analysis and activity modelling of physical layer attacks in internet of things', in Handbook on ICT in Developing Countries, 1st Edition., New York: River Publishers, 2022, pp. 237–267.

[27] K. Assa-Agyei, F. Olajide, and A. Lotfi, 'Security and privacy issues in IoT healthcare application for disabled users in developing economies', J. Internet Technol. Secur. Trans., vol. 10, no. 1, pp. 770–779, 2022.

[28] I. Keshta, 'AI-driven IoT for smart health care: Security and privacy issues', Inform. Med. Unlocked, vol. 30, no. 100903, p. 100903, 2022.

[29] I. Sadek, J. Codjo, S. U. Rehman, and B. Abdulrazak, 'Security and privacy in the internet of things healthcare systems: Toward a robust solution in real-life deployment', Comput. Methods Programs Biomed. Update, vol. 2, no. 100071, p. 100071, 2022.

[30] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, 'PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities', Comput. Secur., vol. 88, no. 101653, p. 101653, 2020.

[31] I. Sadek, S. U. Rehman, J. Codjo, and B. Abdulrazak, 'Privacy and security of IoT based healthcare systems: Concerns, solutions, and recommendations', in How AI Impacts Urban Living and Public Health, Cham: Springer International Publishing, 2019, pp. 3–17.

[32] A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, and B. Parno, 'Cinderella: Turning shabby X.509 certificates into elegant anonymous credentials with the magic of verifiable computation', in 2016 IEEE Symposium on Security and Privacy (SP), 2016.

[33] E. Rescorla, K. Oku, N. Sullivan, and C. A. Wood, 'Encrypted Server Name Indication for TLS 1.3', IETF Datatracker. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-02. [Accessed: 31-May-2023].

[34] 'Decentralized identifiers (DIDs) v1.0', Www.w3.org. [Online]. Available: https://www.w3.org/TR/did-core/. [Accessed: 31-May-2023].

[35] 'Verifiable credentials data model v1.1', Www.w3.org. [Online]. Available: https://www.w3.org/TR/vc-data-model/. [Accessed: 31-May-2023].

[36] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig, 'Authentication and authorization for constrained environments using the OAuth 2.0 framework (ACE-OAuth)', RFC Editor, 2022.

[37] 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 Proceedings 2019 Workshop on Decentralized IoT Systems and Security, 2019

[38] P. Wouters, H. Tschofenig, J. Gilmore, S. Weiler, and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)," IETF RFC7250, 2014