Leveraging Self-Sovereign Identity for e-Health Applications

Aristeidis Farao[1], Georgios Paparis[1], Michail-Alexandros Kourtis[2], Margarita Anastassova[3], Christian Bolzmacher[3], Stéphane Bouilland[4], Evangelos Markakis[5], Ilias Politis[6], Christos Xenakis[6], George Xilouris[2]

[1] Department of Digital Systems, University of Piraeus, Greece
[2] National Center of Scientific Research "Demokritos", Athens, Greece
[3] CEA-LIST, 91191 Gif-sur-Yvette, France
[4] Fondation Hopale, 62608 Berck-sur-Mer, France
[5] Department of Electrical and Computer Engineering, Hellenic Mediterranean University, Heraklion, Crete, Greece
[6] InQBit, Romania

Abstract. The rapid convergence of various evolving ICT technologies, namely Artificial Intelligence, Machine Learning and Distributed Ledgers with different medical applications has contributed to the creation of different innovations in the field. However, rapid technology disruption in various cases may generate privacy breaches and security vulnerabilities, which is a critical factor especially when dealing with sensitive data. This paper leverages the paradigm of Self-Sovereign Identity (SSI), a decentralized approach for identity management, and proposes a prototype integration to smart medical sensors for acoustic analysis of voice in Parkinson Disease (PD) with the Hyperledger Aries. The work is also evaluated in terms of performance and scalability regarding the issuance and verification of verifiable credentials for a medical data scenario.

Keywords: Self-Sovereign Identity, Decentralized Identifier, e-Health.

1 Introduction

The proliferation of different technology enablers, such as Artificial Intelligence (AI) and Machine Learning (ML) in the field of healthcare has paved the way for different applications with a wide range of use cases, from gaining insights into patient satisfaction [1] to investigating the association between depression and quality of life [2]. The evolution of AI/ML in different scopes [3], [4] continues to progress rapidly and more use cases are continuously being investigated in the medical field. However, handling of sensitive medical data can always pose a significant threat to the security and privacy protection of an individual's information. Medical data infrastructure continue to be a top priority for cyber-attacks [5], thus the storage and processing of medical data needs to be done in trusted and secure manner. Different works in the sector of cybersecurity and blockchain technologies have investigated the combination of distributed ledger technologies (DLT) in favor of medical data privacy [6] and differential privacy [7]. A

key concept in the convergence of DLT and advance medical applications, towards a privacy preserving and trusted ecosystem, is Self-sovereign identity (SSI), which is a decentralized approach to identity management that empowers individuals to control and manage their own digital identity [8]. Detailed specifications and directives on its definition and different operations have been defined by the Sovrin Foundation [9], which leads the efforts for wider adoption and integration. Unlike traditional forms of identity management [10], which rely on centralized authorities to verify and manage identities, SSI utilizes blockchain technology to enable individuals to own and control their own digital identity. This means that individuals can choose which personal and medical information to share with healthcare providers, and they can do so on a need-to-know basis.

The healthcare industry is an area where SSI has the potential to make a significant impact [11]. In the traditional healthcare system, patients' personal and medical information is often stored and managed by various healthcare providers and institutions, leaving patients with little control over their own data [6]. This can lead to privacy and security concerns, as well as difficulties in accessing and managing one's own health information. SSI presents an opportunity to change this dynamic by enabling patients to take ownership of their own health data and share it with healthcare providers on a need-to-know basis. There are several key benefits to using SSI in the healthcare industry. First, it gives patients more control and autonomy over their own data, which is especially important in an age where data privacy and security are major concerns [12]. Second, it has the potential to improve data interoperability in the healthcare industry, as patients can easily share their health data with multiple providers without having to rely on centralized systems [13]. Third, it can help to reduce the burden on healthcare providers, who no longer have to spend time and resources on managing and verifying patients' identities [14].

However, there are also challenges to implementing SSI in the healthcare industry [12]. One concern is the need for a critical mass of healthcare providers and patients to adopt the system in order for it to be effective [15]. Another challenge is the need for robust security measures to protect individuals' personal and medical information [16]. In addition, there may be regulatory and legal hurdles to overcome in order to implement SSI in the healthcare industry.

In this paper, we present the architectural approach of OASEES, a framework focused on implementing SSI for different IoT use cases in the scope of swarm intelligence. OASEES is based upon the paradigms of SSI and Decentralized Autonomous Organizations (DAOs) for building trusted and secure communication across a swarm of devices, while involving human based decision making, i.e., Human-in-the-loop (HITL). This work will explore the integration of SSI and DAO architecture in a medical use case regarding the acoustic analysis of voice in Parkinson Disease, and how a swarm of sensors can be efficiently coordinated as a DAO, while preserving the privacy of sensitive patient medical data.

The remainder of the paper is organized as follows. Section 2 describes the overall OASEES architecture and focuses on the identity and swarm intelligence layer with focus on a medical use case. Section 3 describes a medical use case focused on acoustic analysis of voice for Parkinson Disorder. Section 4 describes how different SSI

implementations and approaches can benefit medical data privacy, and how they behave performance and scalability-wise. Finally, Section 5 concludes the paper and draws future research lines

2 OASEES Overview

This section, firstly, details the overall OASEES architecture, and then, reviews the definition of the swarm programmability and identity layer in the context of medical use cases.

2.1 OASEES Overall architecture

The OASEES stack is split among in two layers of operation. The first one, Swarm organization and Identity layer mainly focuses on swarm device organization based on the DAO paradigm and decentralized identity management based on SSI. Therefore, it is split in different modules to be detailed in this section. In its second layer, the deployment and execution layer, the proposed stack is focused on the deployment and execution layer, where the intelligence is deployed in the actual testbed. This layer is depicted in more detail in Section III, focusing on medical devices.

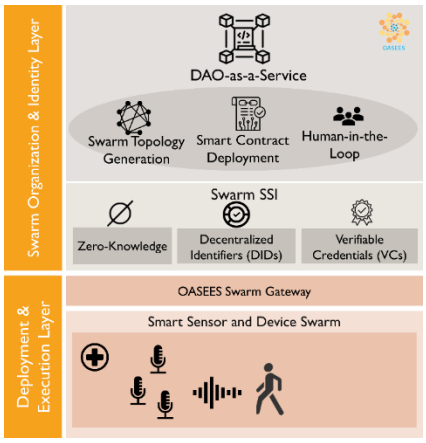

Fig. 1. OASEES SSI architecture stack.

DAO-as-a-Service.

The Decentralized Autonomous Organization (DAO) is an open-source, distributed software that exists "simultaneously nowhere and everywhere," thereby creating a paradigm shift that offers new opportunities to democratize business and enable developers of the future to design their own entirely virtual organizations customized to the optimal needs of their use case. IoT with its underlying machine-to-machine (M2M) communications is useful for enabling the automation of industrial and other machine-centric processes. It is designed to enable communications among machines without relying on any human involvement. Conversely, the Tactile Internet will add a new dimension to human-to-machine interaction involving its inherent human-in-the-loop (HITL) nature, thus allowing for a human-centric design approach toward creating novel immersive experiences and extending the capabilities of the human through the Internet, that is, augmentation rather than automation of the human. Unlike AI based agents that are completely autonomous, a DAO can comprise involvement from humans interacting

according to a protocol defined by the DAO in order to operate, for example a medical practitioner confirming the final decision for an e-health scenario.

SSI

DIDs.

A decentralized identifier (DID) is a globally unique identifier that is the core component of the decentralized digital identity and decentralized public key infrastructure (DPKI) for the Internet layer. Combined with the use of distributed ledger technology (DLTs), DIDs become the central component of a globally resolvable identifier that can cryptographically verify ownership of the identifier. A DID is associated with exactly one DID Document. For Self-Sovereign Identity (SSI), which can be defined as a lifetime portable digital identity that does not depend on any centralized authority, DIDs provide a new class of identifier that fulfills all four requirements: persistence, global resolvability, cryptographic verifiability, and decentralization.

VCs.

A set of one or more claims made by an issuer. A verifiable credential is a tamper-evident credential that has authorship that can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified. The claims in a credential can be about different subjects. Homomorphic Self Sovereign framework will be: (a) Searching in the encrypted domain, (b) Data privacy and data confidentiality & (c) Real-time network alarm processing using the public Cloud.

Hyperledger ARIES.

Hyperledger Aries [17] is an infrastructure for peer-to-peer interactions based on blockchain technology. It consists of a shared encrypted store for blockchain clients and a communication protocol that enables off-ledger interactions between these clients. Aries utilizes the cryptographic support offered by Hyperledger Ursa to provide safe secret management and decentralized key management capability. At the heart of Hyperledger ARIES lie DIDs correlated with a pair of public and secret keys, and VCs [21]. The involved participants in Hyperledger ARIES are the user, an issuer and a verifier.

General speaking the Hyperledger ARIES supports the following:

- *DIDComm* that is a messaging protocol that provides safe and private communication utilizing DIDs and VC between diverse participants in decentralized networks. It permits end-to-end encryption of messages, authentication of messages, and selective disclosure of personal information.
- *Verifiable Credentials Exchange* that offers a structure for establishing and transferring digital credentials that can be cryptographically validated, and that are portable across multiple computers. It allows individuals and businesses to authenticate their identity and qualifications without having to expose unneeded personal details.

Hyperledger ARIES consists of the two basic operations:

- *Credential Issuance* that involves the user acting as a holder, and the issuer. Both have already created their DIDs and stored them within the Blockchain. The user submits its verified data (e.g, personal information) to the issuer. The latter verifies their legitimacy and creates a VC that includes a set of claims about the corresponding user. Next, the issuer signs the VC using its private key; it can be verified with its public key. Then, via the *DIDComm* the issuer sends the VC to the user. The latter stores it within its digital identity wallet [18,19, 20].
- *Presentation Verification* that involves the user acting as a prover, and the verifier. First and foremost, the verifier demands that the prover shows a VC proving specific requirement. The prover picks the pertinent claims from its digital wallet and generates a verifiable presentation, consisting of a set of claims and a proof that can be validated by the verifier. Also, the prover chooses which attributes will be disclosed and which attributes will be partially revealed (selective disclosure). The VC is transferred to the verifier via the DIDComm. The verifier validates the VC's validity by checking the digital signature and the issuer's DID. Also, the verifier determines if the credential has been revoked or is still valid. If the verifier is satisfied that the VC's presentation is correct, the claims can be accepted as true and utilized for their intended purpose.

3 e-Health Application in the OASEES framework

Within OASEES, an innovative smart edge-connected sensor is developed and tested, which will be the basis of an interactive and intelligent wearable for the acoustic analysis of voice in Parkinson Disease (PD). Voice alterations and oral communication disorders, especially in articulation, are present in 75 to 90% of patients with PD [22]. Impaired speech reduces the ability to interact with others and, hence, independence and quality of life [23]. Instrumented voice analysis allows an early identification in order to design supportive interventions. These impairments are due to the lack of coordination of the muscles responsible for speech. Voice, articulation and fluency disorders can be present in the early phases of PD. Voice disorders occur more frequently than articulation ones and appear earlier in patients with PD, followed by articulation and fluency abnormalities [24]. The intelligent edge device developed within OASEES is capable of sensing, recording and analyzing patients' utterances, as well as providing smart, adaptive and personalized guidance on rhythm and intonation. The system is usable both in rehabilitation centers during sessions with therapists and at home. The SSI and DAO approach described in this paper is implemented when collecting, treating and sharing patients' acoustic data in order to maintain a maximum level of privacy.

The neck-worn edge devices built in the OASEES project comprises microphones and loudspeakers connected to AI edge accelerators. The edge devices are operated and monitored over the OASEES DAO, supporting real-time monitoring of the health

information in a trusted and private manner, while allowing the medical practitioner to take the crucial decisions with regard to the adaptation of PD-related treatment. Therefore, the system is co-developed with speech therapists, patients with PD and their carers adopting a real-world data-driven approach. Acoustic and speech data is collected and examined for different intonational and speech profiles among a sample of patients with PD applying a standard research protocol (i.e. data collection in a sound-attenuated room based on the repetition of identical sets of stimuli used in speech therapy for PD). Naturally occurring verbalizations of patients with PD are identified, who have similar speech features and characterized for the effect of different intonational and speech profiles on intelligibility. This is done using objective intonational measures such as: 1) fundamental frequency (F0), which is perceived as pitch, 2) intensity, which is perceived as loudness, 3) timing, which is perceived as speech rate, rhythm, and patterning; 4) jitter and shimmer (cycle-to-cycle variation in frequency and intensity).

As there will be only limited data at the beginning of edge device deployment, data is annotated manually and is related to intelligibility, rated by independent evaluators. The correlation between the intonational features and the intelligibility of speech for a person is analyzed using human expertise combined with supervised learning methods like support vector machines, decision trees, or random forests. Once enough data is acquired, unsupervised learning approaches such as cluster analysis are deployed to extract a specific model linking the intonational features to speech intelligibility in patients with PD to be deployed on the edge devices. The detection and guidance by these algorithms is compared to human expert evaluations.

In order to further increase the amount of data as well as to improve long-term prognostic precision, the devices will operate then in the form of swarm and be able to be updated automatically and also leverage the swarm AI edge accelerators of OASEES for advanced processing and insights. New features extracted by a swarm device are shared in a secured manner through the DAO with the other devices to further improve the PD model.

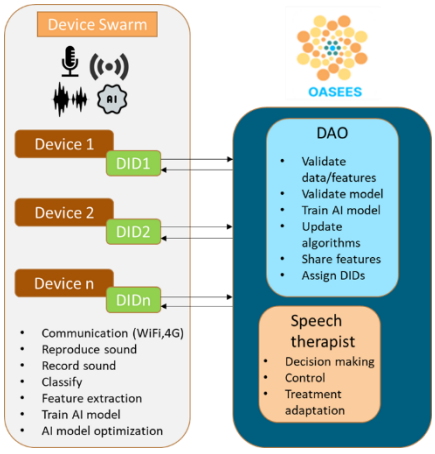

Fig. 3. E-health use case architecture.

In the end, this specific model established for PD can be combined with transfer learning approaches to be able to personalize the diagnostic and treatment for the individual patient. The speech therapist is able to interact with this last layer of the neural network using HITL approaches. Doing so very specific adaptations can be carried out for the individual patient such as focus of the training on individual sounds. Figure 2 shows the system architecture for this e-Health use case including a DAO and the before mentioned SSI.

3.1 Performance evaluation

In this section, we analyze the performance evaluation of the Hyperledger ARIES. We focus on the execution time of issuing and verifying a Hyperledger ARIES presentation. For our proof-of-concept implementation the Hyperledger ARIES 0.51 has been deployed in an Ubuntu 18.04 desktop PC being equipped with an Intel Xeon® Silver 4114 CPU @ 2.20 GHz and 12GB RAM.

For the performance evaluation, we have created a Hyperledger ARIES credential that consist of the following attributes:

Table 1. SSI Attributes.

Personal Patient Identity attributes	***Age***: holder's age (e.g., 28 years), ***Weight***: holder's weight (e.g., 75Kg).
Use case specific attributes	***Fundamental Frequency***: perceived as pitch, ***Intensity***: loudness in dB, ***Timing***: speech rate, rhythm, patterning, ***Jitter***: cycle-to-cycle variation in frequency, ***Shimmer***: cycle-to-cycle variation in intensity.
Overall health condition attributes	***Temperature***: holder's body temperature (e.g., 36 Celsius degree), ***Respiration Level***: holder's number of breaths per minute (e.g., 15), ***Insulin Level***: holder's amount of insulin in the blood (e.g., 230 mIU/L), ***Height***: holder's height (e.g., 185cm). ***Sex***: holder's sex (e.g., male), ***Race***: holder's categorization based on shared physical or social qualities (e.g., Caucasoid), ***Heredity***: transfer of PD from holders' parents (e.g., NO), ***Dopamine***: holders' amount of dopamine in the blood (e.g., 0.8), ***Daily walking steps***: amount of holder's walking steps per day (e.g., 7777), ***Dailysleepminutes***: holder's amount of sleep time per day (e.g., 8hours), ***Timestamp***: the creation timestamp of verifiable credential (e.g., 2022-02-21T21:21:21Z).

We have calculated the average time (*seconds*) needed for issuing a Hyperledger ARIES credential and verifying Hyperledger ARIES presentation. The experiment carried out by sending bulk requests (5, 10, 50, 100, 200, 300, 400, 1000 requests) at the same time with specific number of attributes (6, 12, 18 attributes per credential/presentation). To conduct this experiment, we utilized a script developed in Python. To calculate the average duration of each process we executed it 3 times.

The experiments regarding the average time needed to issue a Hyperledger ARIES credential is depicted in Figure 3 and elaborated below. The average time needed to issue a credential with 6 attributes is 0.406 *secs*, 0.3575 *secs*, 0.31 *secs*, 0.3333 *secs*, 0.3366 *secs*, 0.3433 *secs*, 0.34 *secs* and *0.3566 secs* requesting 5, 10, 50, 100, 200, 300, 400 and 1000 credentials correspondingly. Moreover, the average time needed to issue a credential with 12 attributes is 0.4166 *secs*, 0.37 *secs*, 0.3366 *secs*, 0.3466 *secs,*

0.*3533 secs, 0*.3533 *secs*, 0.*36 secs* and *0*.36 *secs* requesting 5, 10, 50, 100, 200, 300, 400 and 1000 credentials correspondingly. Additionally, the average time needed to issue a credential with 18 attributes is 0.47 *secs*, 0.4066 *secs*, 0.3433 *secs*, 0.3566 *secs*, 0.37 *secs*, 0.3733 *secs*, 0.3866 *secs*, 0.3733 *secs* requesting 5, 10, 50, 100, 200, 300, 400 and 1000 credentials correspondingly. We may observe that the average time needed to issue a credential increase as the number of the credential's requested attributes rises. Also, there is fluctuation in the average time needed to issue a credential regardless the number of requested attributes. It decreases from when the number of requested credentials is from 5 to 50, while it increased when the number of requested credentials is bigger than 50.

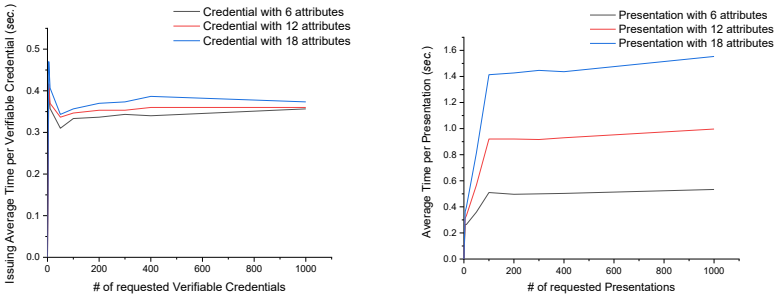

Fig. 3. Average Times of Hyperledger ARIES Presentation (a) and Credential Issuance (b).

The experiments regarding the average time needed to verify Hyperledger ARIES presentation is depicted in Figure 3(b) and elaborated below. The average time needed to verify a Hyperledger ARIES presentation with 6 attributes is 0.264 *secs*, 0.265 *secs*, 0.36 *secs*, 0.51 *secs*, 0.4966 *secs*, 0.5 *secs*, 0.5033 *secs*, 0.5333 *secs* verifying 5, 10, 50, 100, 200, 300, 400 and 1000 presentations correspondingly. Moreover, the average time needed to issue a credential with 12 attributes is 0.3133 *secs*, 0.3333 *secs*, 0.5666 *secs*, 0.92 *secs*, 0.92 *secs*, 0.9166 *secs*, 0.93 *secs*, 0.9966 *secs*, verifying 5, 10, 50, 100, 200, 300, 400 and 1000 presentations correspondingly. We may observe that the average time needed to verify a presentation increase as the number of the presentation's requested attributes rises. In general, the average time increases as the number of the requested presentations rises.

Overall, the average time need to verify a presentation in Hyperledger ARIES is bigger than the average time needed to issue Hyperledger ARIES credential. The presented results show promising potential for a decentralized swarm identity management system, that could be deployed on a real-world scenario, as the increasing number of verifications affects the average time in a stable manner, rendering Hyperledger Aries as a valid candidate for biomedical applications.

4 Conclusions

This paper presented the OASEES framework for decentralized identification and verifiable credential management for biomedical and health applications, along with a preliminary performance analysis of its scalability. The proposed architecture is presented in detail and a sub-set of its modules are analyzed and integrated in a PD-based scenario. The experimental setup is based on the Hyperledger Aries framework extended with the necessary modules to support the use case specific attributes. Based on this extension an evaluation of the framework is presented for different scalability scenarios. The final evaluation results show a promising capability for an OASEES based system to operate for biomedical use cases and provide the swarm identity management of devices. Overall, the paper aims to propose a decentralized architecture for swarm computation and organization with focus on health applications, where identity management and protection is of utmost importance. For future steps, the proposed framework can be extended to support also real-time processing of other types of medical use cases and cover more medical fields.

Acknowledgments. The research leading to these results has been supported by the OASEES project (no. 101092702) and the project TRUSTEE (no. 101070214).

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. N. Liu, S. Kumara and E. Reich, "Gaining Insights Into Patient Satisfaction Through Interpretable Machine Learning," in IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 6, pp. 2215-2226, June 2021, doi: 10.1109/JBHI.2020.3038194.
2. M. Habib, Z. Wang, S. Qiu, H. Zhao and A. S. Murthy, "Machine Learning Based Healthcare System for Investigating the Association Between Depression and Quality of Life," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 2008-2019, May 2022, doi: 10.1109/JBHI.2022.3140433.
3. Z. M. Ibrahim et al., "A Knowledge Distillation Ensemble Framework for Predicting Short- and Long-Term Hospitalization Outcomes From Electronic Health Records Data," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 1, pp. 423-435, Jan. 2022, doi: 10.1109/JBHI.2021.3089287.
4. N. Reamaroon, M. W. Sjoding, K. Lin, T. J. Iwashyna and K. Najarian, "Accounting for Label Uncertainty in Machine Learning for Detection of Acute Respiratory Distress Syndrome," in IEEE Journal of Biomedical and Health Informatics, vol. 23, no. 1, pp. 407-415, Jan. 2019, doi: 10.1109/JBHI.2018.2810820.
5. A/P Sinnathamby Sehgar, S.; Zukarnain, Z.A. Online Identity Theft, Security Issues, and Reputational Damage. Preprints 2021, 2021020082 (doi: 10.20944/preprints202102.0082.v1).
6. J. Tao and L. Ling, ‘‘Practical medical files sharing scheme based on 1201 blockchain and decentralized attribute-based encryption,’’ IEEE Access, 1202 vol. 9, pp. 118771–118781, 2021.

7. O. K. Ngangmo, A. A. A. Ari, A. Mohamadou, O. Thiare, and 1208 D. T. Kolyang, ‘‘Guarantees of differential privacy in cloud of things: 1209 A multilevel data publication scheme,’’ Int. J. Eng. Res. Afr., vol. 56, 1210 pp. 199–212, Oct. 2021.
8. Schardong, F.; Custódio, R. Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. Sensors 2022, 22, 5641. https://doi.org/10.3390/s22155641
9. The Sovrin Foundation. Sovrin. 2016. Available online: https://sovrin.org/
10. Liu, Y.; He, D.; Obaidat, M.S.; Kumar, N.; Khan, M.K.; Raymond Choo, K.K.K. Blockchain-based identity management systems: A review. J. Netw. Comput. Appl. 2020, 166, 102731.
11. L. Chen, Q. Yu, W. Liang, J. Cai, H. Zhu and S. Xie, "Overview of Medical Data Privacy Protection based on Blockchain Technology," 2022 IEEE 7th International Conference on Smart Cloud (SmartCloud), Shanghai, China, 2022, pp. 200-205, doi: 10.1109/SmartCloud55982.2022.00039.
12. G. Kondova and J. Erbguth, ‘‘Self-sovereign identity on public blockchains 1215 and the GDPR,’’ in Proc. 35th Annu. ACM Symp. Appl. Comput., 1216 Mar. 2020, pp. 342–345.
13. S. Y. Lim, O. B. Musa, B. A. S. Al-Rimy, and A. Almasri, ‘‘Trust models 1218 for blockchain-based self-sovereign identity management: A survey and 1219 research directions,’’ in Advances in Blockchain Technology for Cyber 1220 Physical Systems, Internet of Things. Cham, Switzerland: Springer, 2022, 1221 pp. 277–302.
14. M. Lacity and E. Carmel, ‘‘Implementing self-sovereign identity (SSI) for 1223 a digital staff passport at U.K. national health service (NHS),’’ BCoE, 1224 Kanhor, India, White Paper 2022-1, 2022.
15. P. Zhang, D. C. Schmidt, J. White, and G. Lenz, ‘‘Blockchain technology 1236 use cases in healthcare,’’ Adv. Comput., vol. 111, pp. 1–41, Jan. 2018.
16. J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, ‘‘Healthchain: A 1238 blockchain-based privacy preserving scheme for large-scale health data,’’ 1239 IEEE Internet Things J., vol. 6, no. 5, pp. 8770–8781, Oct. 2019.
17. Hyperledger ARIES, https://www.hyperledger.org/use/aries [Online: Last access: 17/2/2023]
18. Farao, A., Veroni, E., Ntantogian, C. and Xenakis, C., 2021. P4G2Go: A Privacy-Preserving Scheme for Roaming Energy Consumers of the Smart Grid-to-Go. Sensors, 21(8), p.2686.
19. Muñoz, A., Farao, A., Correia, J.R.C. and Xenakis, C., 2021. P2ISE: Preserving Project Integrity in CI/CD Based on Secure Elements. Information, 12(9), p.357.
20. Muñoz, A., Farao, A., Correia, J.R.C. and Xenakis, C., 2020. ICITPM: integrity validation of software in iterative continuous integration through the use of Trusted Platform Module (TPM). In Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17–18, 2020, Revised Selected Papers 25 (pp. 147-165). Springer International Publishing.
21. Bolgouras, V., Angelogianni, A., Politis, I. and Xenakis, C., 2022, August. Trusted and Secure Self-Sovereign Identity framework. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-6).
22. Defazio, G., Guerrieri, M., Liuzzi, D., Gigante, A.F., di Nicola, V., 2016, Assessment of voice and speech symptoms in early Parkinson’s disease by the Robertson dysarthria profile. Neurological Sciences, 37(3), pp. 443–9.
23. Ramig, L.O., Fox, C., Sapir, S., 2008, Speech treatment for Parkinson’s disease. Expert Review of Neurotherapeutics, 8 (2), pp. 297–309.
24. Tjaden, K., 2008, Speech and Swallowing in Parkinson's Disease. Top Geriatr Rehabil., 24 (2), pp. 115-126.