DID-IMP

Decentralized public key infrastructure for Defended IoT data Management and Procurement

Authors — Evgenii Zhdarkin (Lead Developer), François Chiron (CTO), Benoît Maïsseu (CEO)

Company — Werenode SAS

Abstract — The DID-IMP project introduces a Decentralized Public Key Infrastructure (DPKI) designed to enable secure, automated, and verifiable data exchange for Internet of Things (IoT) devices. Traditional Certificate Authorities (CA) and Registration Authorities (RA) introduce centralization risks, inefficiencies, and single points of failure. To address these challenges, DID-IMP leverages a feeless Web3.0 protocol that replaces centralized trust entities with decentralized identity (DID) mechanisms secured by blockchain-based smart contracts. A Certificate Store deployed on-chain enables service providers and IoT Fleet Managers to issue and manage revocable verifiable credentials (VCs), ensuring data authenticity, privacy, and compliance with emerging security standards.

To enhance trust and security within the DID-IMP ecosystem, we integrate a DID Risk Assessment Model, an on-chain trust scoring algorithm that proactively detects fraudulent or high-risk DIDs attempting to manipulate verifiable credential issuance. This model continuously monitors issuer behaviors, revocation rates, and transactional anomalies, applying machine learning-driven anomaly detection to identify malicious credential issuers. By integrating smart contract-based risk scoring, DID-IMP strengthens decentralized authentication, ensuring robust security without reliance on central authorities.

This architecture is optimized for IoT Secure Automatic Data Sharing (SADS), supporting trustless, privacy-preserving, and tamper-resistant data exchanges across smart cities, connected vehicles, decentralized energy grids, and industrial IoT ecosystems. By enhancing scalability, interoperability, and trust, DID-IMP establishes decentralized identity as a cornerstone of next-generation IoT networks, reducing administrative overhead and regulatory friction while empowering users with self-sovereign identity management.

Keywords — Blockchain, decentralized identity, verifiable credentials, IoT security, smart contracts, data privacy, Web3.0, risk-based trust assessment, anomaly detection.

I. Introduction

The Internet of Things (IoT) is becoming an integral part of everyday life, spanning applications from smart homes to industrial automation. Currently, nearly half of the 160 zettabytes (ZB) of data generated worldwide comes from IoT devices [1]. As the number of connected devices continues to rise, so does the demand for efficient, secure, and automated data exchange mechanisms.

The Big Data market, valued at $190.1 billion in 2023, is projected to double to $400 billion by 2028, growing at a 12.3% compound annual growth rate (CAGR) [2]. This growth is fueled by the increasing penetration of mobile devices and the rising demand for real-time, privacy-preserving data sharing. Similarly, the IoT automated data exchange sector is experiencing exponential expansion, reinforcing the need for trust-based identity verification.

A study by Allied Market Research [3] estimates that the global IoT payments market, which aligns with secure data-sharing ecosystems, was valued at $7.6 billion in 2018 and is expected to reach $27.8 billion by 2026, with a CAGR of 17.6%. This surge is driven by cashless transaction adoption, enhanced mobile connectivity, and security concerns.

In parallel, the Artificial Intelligence of Things (AIoT) is emerging as a transformative force, integrating machine learning and autonomous decision-making into IoT networks. The AIoT market, valued at $171.40 billion in 2024, is projected to grow at a 31.7% CAGR from 2025 to 2030. [4] AI integration enhances device intelligence, automation capabilities, and data security, fostering the need for Secure Automatic Data Sharing (SADS) mechanisms that ensure privacy-preserving and tamper-resistant communication.

However, as IoT and AIoT ecosystems expand, they introduce new challenges related to trust, security, and identity management. Traditional identity models, which rely on centralized authorities, create scalability bottlenecks and security vulnerabilities, making them unsuitable for decentralized IoT environments. Ensuring trust in automated IoT transactions requires an identity verification system that is secure, scalable, and resistant to tampering.

To address these challenges, the DID-IMP project introduces a Decentralized Public Key Infrastructure (DPKI) that leverages blockchain-based smart contracts for secure, automated, and verifiable identity management. By replacing traditional Certificate Authorities (CAs) and Registration Authorities (RAs) with decentralized identifiers (DIDs) and verifiable credentials (VCs), DID-IMP provides a trustless, scalable, and privacy-enhancing solution for IoT and AIoT data exchange.

The DID-IMP project, developed as part of NGI Trustchain's OC2 initiative, has received European funding (Grant Agreement No. 101093274), underscoring the EU's commitment to driving innovation in secure IoT data management.

II. Project Description

Drawing from existing research on decentralized blockchain techniques for enhancing IoT security and privacy [5], safety and security analysis frameworks tailored for IoT environments [6], and critical evaluations of blockchain's performance and scalability in IoT applications [7], the DID-IMP framework introduces a decentralized public key infrastructure (DPKI) designed to address trust management, data integrity, and access control in IoT ecosystems.

A. Core Components

The DID-IMP infrastructure is built on a set of interdependent components that enable trustless identity management and secure data transactions. At the foundation of this architecture lies the **blockchain layer**, which serves as a decentralized and immutable ledger. This layer functions as a Decentralized Identifier (DID) registry, a Certificate Store, and an execution environment for smart contracts. The DID registry ensures that IoT devices and service providers have unique, verifiable identities, while the Certificate Store enables the issuance, storage, and verification of verifiable credentials (VCs). Smart contracts automate key processes such as credential issuance, revocation, and verification. Though DID-IMP is designed for multiple blockchain solutions, whether layer 1 or 2, the first implementation was made with Alastria, a public-permissioned blockchain. [8]

Another fundamental aspect of DID-IMP is its **Decentralized Identifier (DID) management system**, which provides self-sovereign, cryptographically secure identity records for IoT devices and organizations. Unlike traditional identity solutions that depend on centralized certificate authorities, DIDs in DID-IMP allow entities to establish and control their own identity without reliance on third-party intermediaries. These identifiers comply with W3C standards, ensuring interoperability with other decentralized identity frameworks. Each DID can be associated with verifiable credentials that define attributes such as the authorization to procure or transfer data, but also device ownership, other permissions, and operational status. To enhance decentralized trust and certificate validation in IoT ecosystems, DID-IMP builds upon established research in certificate chain discovery, which provides efficient algorithms for verifying delegation and authorization in distributed public key infrastructures. [24]

To manage the automated identity verification, DID-IMP leverages **smart contracts** deployed on an Ethereum-compatible blockchain or Ethereum Virtual Machine (EVM). These smart contracts govern credential issuance and revocation, providing a transparent, tamper-proof mechanism for operating IoT identities. When a verifiable credential is issued to a device, it is recorded on-chain, making it instantly accessible for verification by authorized parties. If a device is decommissioned, compromised, or requires updated permissions, its credentials can be revoked, ensuring that only trusted entities retain authorization. The system is designed to support automated authentication and access control, enabling real-time interactions between IoT devices and service providers.

The solution also includes an **embedded wallet and a web and mobile user interface**. The embedded wallet allows IoT devices to store, manage, and present their DIDs and verifiable credentials, enabling identity verification without manual intervention. The user interface provides a dashboard for service providers and IoT fleet managers to monitor and manage credential activity in real time. It includes features such as credential issuance, verification logs, automated policy enforcement, and security alerts. By integrating these components, DID-IMP establishes a scalable, decentralized identity solution for IoT ecosystems, enhancing trust, security, and regulatory compliance.

B. System Protocol

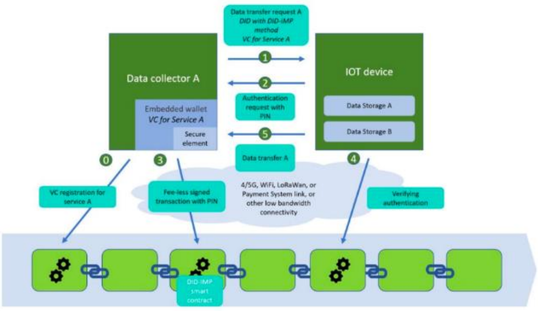

Figure 1: DID-IMP protocol

The DID-IMP SADS system is designed to provide a secure framework for managing decentralized identities and automating data exchange in IoT ecosystems. In a nutshell, devices authenticate each other's credentials before exchanging data, ensuring that only verified entities participate in the network. The authentication process can follow different security models, including **single asymmetric authentication**, where a sender verifies the recipient's identity before transferring data, or **double symmetric authentication**, where both parties mutually authenticate before engaging in a transaction. Additionally, DID-IMP supports **zero-knowledge proof (ZKP) authentication**, which allows devices to prove their identity or attributes without exposing sensitive information. [11]

The operational workflow (Figure 1) begins with the **device registration process**, where an IoT device generates a Decentralized Identifier (DID) and registers it on the blockchain. This registration ensures that the device has a unique, verifiable identity that can be used for authentication and secure communication. Depending on the use cases, this operation can also be handled or overviewed by the IoT Fleet Manager of the relevant IoT device. Once registered, the device receives **verifiable credentials (VCs)** issued by a trusted entity, such as a service provider, an IoT fleet manager, or a regulatory authority. These credentials specify the device's permissions, data-sharing capabilities, and compliance with industry standards.

Following the registration and issuance phase, verifiable credentials are stored securely on the blockchain, making them accessible for verification by authorized entities. When an IoT device interacts with another system, it must prove its identity and authorization status by presenting its VCs. The verification process ensures that only trusted devices participate in the network, reducing the risk of identity spoofing or data tampering. Smart contracts facilitate the verification process by enabling **automated, real-time credential checks** without requiring manual intervention from administrators. The use of blockchain guarantees that once a credential is issued or revoked, the update is immutable and cannot be altered by unauthorized parties. Once authentication is complete, IoT devices engage in the data exchange itself.

Credential revocation is an essential feature of DID-IMP, ensuring that compromised or outdated credentials can be removed from the system in real time. If a device is decommissioned, compromised, or transferred to a new owner, its credentials can be revoked through an on-chain smart contract. This prevents unauthorized access and ensures that only valid credentials remain in circulation. Additionally, the DID Risk Assessment Model (DID-RAM) (see Chapter III) continuously monitors issuer behavior, detecting anomalies or fraudulent activity within the ecosystem. If an issuer is found to be generating suspicious credentials, the system can automatically flag or revoke their privileges, maintaining the integrity of the decentralized identity framework.

By integrating these operational principles, DID-IMP provides a trustless, automated, and privacy-preserving identity verification system tailored for large-scale IoT networks. The combination of blockchain, smart contracts, and cryptographic authentication mechanisms ensures that identity management remains scalable, transparent, and resilient against cyber threats. This approach eliminates the reliance on centralized authorities while maintaining regulatory compliance and enhancing interoperability across various IoT applications.

DID-IMP is fully **compatible with W3C recommendations**, particularly the Decentralized Identifiers (DIDs) v1.0 and Verifiable Credentials (VCs) v2.0 standards. [9] [10] The DID-IMP framework adheres to W3C's specifications by utilizing DIDs to create cryptographically verifiable, self-sovereign identities that can be resolved across decentralized systems. By implementing Verifiable Credentials (VCs), DID-IMP enables trustable and tamper-proof credential issuance, ensuring that data exchanged between IoT devices is authenticated and compliant with global interoperability standards. Additionally, DID-IMP follows W3C's principles of privacy-by-design, providing users and devices with selective disclosure capabilities to enhance security without compromising personal information. [10] [23] This alignment with W3C ensures that DID-IMP remains adaptable to evolving digital identity regulations and integrates into broader decentralized identity ecosystems.

III. DID Risk Assessment Model

Ensuring trust and security within a decentralized identity ecosystem is critical, especially in permissionless Web3.0 environments where verifiable credentials (VCs) can be issued by multiple entities without central oversight. While decentralized identity solutions such as DID-IMP eliminate reliance on traditional Certificate Authorities (CA) and Registration Authorities (RA), they introduce new challenges related to credential fraud, issuer accountability, and trust inference.

To address these challenges, DID-IMP integrates a DID Risk Assessment Model (DID-RAM), a simple real-time, mainly on-chain risk evaluation framework that continuously monitors issuer behavior, credential revocation patterns, and transactional anomalies, incorporating principles analogous to CredTrust or VChain [18] [19]. This model additionally employs machine learning-based anomaly detection and blockchain smart contract enforcement to mitigate risks associated with fraudulent DID issuers.

DID-RAM operates through two core components. The Issuer Reputation Scoring (IRS) module evaluates the credibility of verifiable credential issuers based on their revocation history, credential longevity, and associated trust scores. This is implemented on-chain to manage the risk scoring, enabling real-time risk-aware authentication and authorizations revocation. The Anomaly Detection Engine (ADE) applies behavioral analytics and machine learning algorithms to identify suspicious credential issuance patterns and detect fraudulent activities; this component is partly implemented off-chain.

A. Issuer Reputation Scoring (IRS)

The trust score (T) of a DID issuer is calculated based on several historical factors that assess its reliability. One key parameter is the Credential Revocation Rate (CRR), which represents the proportion of credentials revoked relative to the total issued. A high revocation rate may indicate potential fraud, where the formula is defined as:

$$CRR(Issuer) = \frac{R_{Revoked}}{R_{Total}}$$

$$CRR \in [0,1]_{\mathbb{R}}$$

where $R_{Revoked}$ is the number of revoked credentials, and R_{Total} is the total number of credentials issued by the entity. A high CRR suggests an increased likelihood of issuer misconduct or improper credential issuance.

Another factor in the trust score is the Credential Lifespan Analysis (CLA), which measures the average validity period of issued credentials. If a credential frequently expires or is revoked within a short timeframe, it may indicate malicious behavior or improper credential management.

$$CLA(Issuer) = \frac{1}{N}\sum_{i=1}^{N}(t_{expiry,i} - t_{issued,i})$$

where *N* is the Total number of credentials issued by the relevant Issuer. In the following, we will only use the normalized CLA.

$$CLA_{Normalized} = \frac{1}{T_{Max}} CLA$$

$$CLA_{Normalized} \in [0,1]_{\mathbb{R}}$$

where T_{Max} is the Maximum expected credential lifespan, usually depending on the considered application.

The Transaction Pattern Analysis (TPA) evaluates how frequently an issuer interacts with different DID wallets and smart contracts. Unusual bursts of activity, such as issuing a large number of credentials in a short time, could indicate a fraudulent mass issuance scheme.

$$TPA(Issuer, T) = \frac{\sigma(N_{Issued,T})}{\mu(N_{Issued,T})}$$

where T is the period of time considered, $N_{Issued,T}$ the Number of credentials issued by the relevant issuer over the period of time T, $\sigma(N_{Issued,T})$ the Standard quadratic deviation of credential issuance over time and $\mu(N_{Issued,T})$ the Average issuance rate over the same time period T.

The TPA also needs to be normalized to be used in the overall trust score:

$$TPA(Issuer, T)_{Normalized} = 1 - \min\left(\frac{TPA(Issuer, T)}{TPA_{Max}}, 1\right)$$

where TPA_{Max} is the expected TPA for normal variance in issuance behavior (which is also highly depending on the application).

Additionally, the Cross-Issuer Association (CIA) metric identifies clusters of issuers that repeatedly verify each other's credentials, potentially forming a collusive trust circle that undermines decentralized identity verification.

$$CIA(Issuer) = \frac{C_{Mutual}}{C_{Total}}$$

where C_{Mutual} is the Number of credentials issued to or verified by issuers that also issued credentials to the considered Issuer and C_{Total} C is the Total number of credentials issued by the considered Issuer.

$$CIA(Issuer)_{Normalized} = 1 - \min\left(\frac{CIA(Issuer, T)}{CIA_{Max}}, 1\right)$$

The overall trust score of a DID/VC issuer is computed as:

$$T(Issuer) = \alpha(1 - CRR) + \beta.CLA + \gamma(1 - TPA) + \delta(1 - CIA)$$

where α, β, γ and δ are adjustable weighting factors that prioritize the different normalized risk parameters.

To ensure transparency and automation, this scoring mechanism is deployed on each DID-IMP smart contract version for a compatible set of use cases and application (since the parameters are application specific). This implementation enables to dynamically update trust scores, to enforce risk-based credential revocations, and allows credential verifiers to query issuer reputation before validating a credential. The smart contract ensures that risk-prone issuers are flagged and prevents malicious entities from continuing to issue credentials unchecked. Indeed, high-risk issuers are automatically restricted from issuing or verifying credentials. If an issuer's trust score falls below a predefined threshold, the smart contract triggers automated revocations, preventing the continued misuse of fraudulent credentials. Services that rely on DID-IMP for authentication can query the smart contract to determine whether an issuer remains trustworthy before accepting a verifiable credential. If an entity is flagged as high risk, access to IoT services may be temporarily restricted until further validation is conducted. Of course, the optimization of the trigger threshold value highly depends on the application considered. Alternatively, this mechanism can be implemented in a separate smart contract.

B. Anomaly Detection Engine (ADE)

The Anomaly Detection Engine (ADE) is responsible for identifying fraudulent behavior within the DID-IMP ecosystem by continuously analyzing DID and VC transaction patterns. To detect unusual activity, the ADE employs a set of machine learning-based fraud detection techniques. Autoencoder models are used to identify outlier transaction behaviors, detecting anomalies in credential issuance frequency and revocation rates. Graph-based fraud detection methods are applied to uncover collusive networks, where issuers attempt to verify each other's credentials in a structured manner to manipulate trust scores. Additionally, supervised learning models are trained on historical fraudulent DID activity to improve predictive accuracy in identifying new cases of fraudulent credential issuance.

A separate DID-RAM-ADE smart contract within the DID-IMP ecosystem facilitates the collection and analysis of on-chain credential issuance data. This process includes monitoring the frequency of verifiable credential issuance per issuer, analyzing patterns of revocation events, and assessing the distribution of credential usage across IoT devices and services. When a suspicious issuer is detected, the ADE flags its credentials for further manual verification or automatic revocation, preventing the proliferation of untrustworthy credentials within the decentralized network.

The ADE in DID-RAM operates using a hybrid model, incorporating both on-chain and off-chain components to balance security, efficiency, and scalability. On-chain functions of the ADE leverage a dedicated smart contract to ensure that fraud detection remains verifiable, immutable, and tamper-resistant. These functions include storing credential issuance and revocation events, allowing for transparent tracking of credential behaviors. Additionally, basic anomaly detection rules, such as monitoring for high-frequency issuances or sudden bursts of activity, are implemented through on-chain smart contract logic. When an issuer surpasses a predefined risk threshold, such as issuing an abnormally high number of credentials in a short period, the smart contract flags the issuer for further analysis or restricts further credential issuance until additional verification is completed.

More complex fraud detection and machine learning-based analytics are handled off-chain due to the computational and storage limitations of blockchain networks. Off-chain components include machine learning-based anomaly detection, where AI models analyze historical DID/VC transactions, revocation rates, and issuer behavior trends. These models detect sophisticated fraud patterns, such as collusive issuers or Sybil attacks. Additionally, off-chain graph-based analysis maps issuer interactions and identifies clusters of malicious DIDs that verify each other in structured fraud networks. Risk scoring and trust propagation algorithms are also executed off-chain, where an analytics engine computes trust scores based on behavioral patterns, periodically updating the issuer reputation score. This approach can be compared to the strategy described in other solutions like Reputable. [20] [21] [22]

The ADE functions in conjunction with the blockchain, analyzing data off-chain while enforcing actions on-chain. When an anomaly is detected in off-chain analysis, the system transmits the risk evaluation results to the DID-RAM-ADE smart contract that updates the issuer's trust score on-chain. If the trust score falls below a certain threshold, the smart contract revokes the issuer's permission to issue further credentials to prevent fraudulent activity. In cases where false positives are detected, an override mechanism allows manual verification before permanent revocation.

Although blockchain smart contracts handle basic rule-based anomaly detection and credential enforcement, computationally intensive fraud detection mechanisms, such as machine learning, behavioral analytics, and graph-based fraud detection, operate off-chain. This hybrid approach ensures that fraud detection remains scalable, efficient, and secure, while still leveraging blockchain's immutability and transparency to maintain trust in the system.

IV. DID-IMP/DID-RAM efficiency evaluation

To validate the effectiveness of DID-RAM within DID-IMP, a prototype implementation has been deployed on an Ethereum-compatible testnet (in this case Sepolia), integrating key risk assessment components. The system consists of Solidity smart contracts that govern trust scoring and automated enforcement, an off-chain analytics engine (Python-based) that runs machine learning-driven fraud detection, and decentralized storage mechanisms for maintaining historical risk assessments.

Performance evaluation is conducted through a series of benchmark tests that measure the accuracy of fraud detection, the stability of trust scores, and the efficiency of on-chain execution costs. Fraud detection accuracy is a key metric, indicating the percentage of correctly flagged fraudulent issuers. Trust score stability is measured by analyzing how quickly and accurately scores reflect changes in issuer behavior. The cost of executing smart contracts is also assessed, ensuring that risk evaluations remain efficient and scalable.

The dataset used for this assessment comprises a mix of real-world and simulated data. Real-world data was sourced from the Electric Vehicle Supply Equipment (EVSE) and anonymized charging station user credentials within Werenode's operational Web3.0 ecosystem. This was complemented by simulated data from home energy management systems participating in a decentralized energy community. To evaluate fraud detection capabilities, synthetic fraudulent DID and VC issuers were introduced into the dataset, allowing for the measurement of fraud detection accuracy and false positive rates. The rate of fraudulent credential issuers was set to 5% with a mix of behaviours:

Fraud Type	**% of Frauds**	**Description**
Mass Issuers (High-Volume Fraud)	40%	Issues excessive credentials in a short time (e.g., 1000 VCs per hour).
Collusion Rings (Credential Laundering)	25%	Multiple issuers falsely validating each other's fraudulent credentials.
Credential Cycling (Repeated Revocations/Re-Issuance)	15%	Issuers rapidly revoke and reissue credentials to evade detection.
Selective Fraud (Targeted Attacks)	20%	Issuers appear normal but selectively create fraudulent credentials.

Figure 2: Simulated Frauds Panel

Metric	**Value (Testnet)**
Fraud Detection Rate	94.5%
False Positives	2.3%
Trust Score Update Latency	< 2 seconds
Gas Cost per Query	150,000 gas

Figure 3: DID-RAM efficiency evaluation

The DID Risk Assessment Model (DID-RAM) enhances security and trust within the DID-IMP ecosystem by providing real-time risk scoring for credential issuers. Through issuer reputation tracking, anomaly detection, and smart contract-based enforcement, DID-RAM significantly reduces the risk of fraudulent credential issuance without compromising decentralization.

Future improvements to DID-IMP/DID-RAM will focus on cross-chain risk scoring mechanisms to enable multi-blockchain identity verification. Further enhancements will include the integration of Zero-Knowledge Proofs (ZKPs) to preserve user privacy while ensuring accountability, as well as Federated Learning Models to enhance collaborative fraud detection across multiple IoT networks. Several other interesting algorithms have been investigated in the literature [18] [19] and could be complementing or replacing DID-RAM. By embedding DID-RAM into the DID-IMP protocol, trust, security, and resilience are strengthened, paving the way for next-generation identity frameworks across IoT, smart cities, and decentralized applications.

V. Benefits of DID-IMP

The DID-IMP solution is designed to operate in a decentralized manner, adhering to the principles of Decentralized Identifiers (DIDs). By eliminating reliance on a central authority, it ensures that no single entity holds predominant control over the system, thereby avoiding single points of failure and maintaining the integrity of the network. The scalability of the solution is a key advantage, as it is capable of handling the rapid expansion of IoT ecosystems, supporting a large and continuously growing number of identifiers while efficiently managing massive volumes of data transfers.

Another fundamental characteristic of the DID-IMP framework is its feeless transaction model, which ensures that IoT devices do not incur directly high gas fees typically associated with blockchain transactions, which would complexify the IoT device management. This approach enhances accessibility and usability, making the system more resilient for a broad range of applications. Moreover, delegating costs through a feeless protocol allows a lot of cost optimization. The maturity of the solution is also a priority, as it has been developed with direct input from potential clients, ensuring that it effectively addresses real-world needs and challenges in identity management for IoT ecosystems.

User experience is another essential consideration in the development of DID-IMP. The application is designed to be intuitive and user-friendly, minimizing the complexity for end users, who do not need extensive technical knowledge to manage their digital identities and credentials. Lastly, the system ensures reliable identification of IoT devices, leveraging unique DIDs and verifiable credentials (VCs) stored on the blockchain. This mechanism provides a high level of security and trust, making it a robust and tamper-proof identity verification solution that is critical for secure IoT and AIoT ecosystems.

VI. Application examples

A. Connected cars

With DID-IMP, vehicles would be able to automatically transmit data about parking, charging and other transport processes, making the services more comfortable for drivers. They will be able to send maintenance data using IoT data transfer between devices in their respective organizations' fleets.

In the simplest case, the station system communicates with the vehicle, authenticating it and its owner using DID-IMP for secure data exchange. The refueling hose with IoT sensors automatically connects to the vehicle's fuel tank, initiating the refueling process and monitoring pressure and temperature to optimize safety. Once the refueling is complete, a digital receipt is sent to the driver's smartphone, where transaction history and fuel efficiency metrics can also be viewed. [11]

B. Remote healthcare

DID-IMP would be able to improves access to telemedicine and remote patient monitoring while ensuring data security and personalization. For example, a user has different IoT health monitoring devices like fitness trackers, smart scales, tonometers etc. And user's phone collect data from then via the DIDIMP app and synchronize it with an electronic medical record. Using this data the medical app can provide personalized recommendations and notifications of potential health issues or even notifies emergency services and the user's contacts in emergency situations. [12]

C. Cognitive cities

DID-IMP would be able to enables secure data exchange between IoT devices, helping to create smart/cognitive cities. Users register their devices through the DID-IMP app, linking them to decentralized identifiers (DIDs) and verification certificates (VCs).

Once registered, users could customize program settings according to personal preferences by selecting devices to communicate with, configuring data sharing settings, and receiving real-time notifications. With DID-IMP, users can easily connect to city IoT devices to monitor traffic, control water usage, manage waste and receive safety notifications. Devices exchange data through smart contracts, ensuring that information is verified and protected.

DID-IMP protects personal data, contributes to the city's sustainable development goals and provides users with access to a variety of innovative services, making their lives more convenient and safer. [13] [14]

D. Energy Management

DID-IMP enables secure management of IoT devices in the energy industry, such as smart meters and grid sensors. Users register devices through the DID-IMP app, enabling accurate and secure data exchange.

The app provides real-time data on energy consumption and distribution, allowing users to monitor trends and receive alerts when problems occur. Users can participate in local energy communities, sharing data to optimize energy use and deploy renewable sources.

DID-IMP makes it easy to register and manage IoT devices, monitor energy and participate in energy communities through secure data sharing. [15]

E. Smart Homes

DID-IMP would be able to enable secure control of smart home IoT devices such as thermostats, cameras etc. Users download the DID-IMP app and go through a simple setup process, registering each device and associating it with the DID.

The DID-IMP app would allow for real-time monitoring, sending notifications about events such as movement in front of the camera or temperature changes. This makes it possible to monitor the safety, energy consumption and condition of the house.

Of course, data privacy and security come first in such private side of life as houses. DID-IMP would use authentication mechanisms to protect against unauthorized access. [16]

F. Supply Chain

DID-IMP provides an opportunity to leverage IoT technologies for logistics and supply chain management, enabling secure data exchange to monitor the location, condition and status of shipments during transportation to help prevent theft, damage or tampering.

For example, a logistics company specializing in the transportation of perishable goods can use DID-IMP to integrate IoT devices such as temperature sensors and GPS trackers. Once successfully integrated, the company has access to a dashboard that displays real time location and temperature information for each device. Automatic notifications of any deviations or unexpected events help to take instant action to prevent spoilage of goods. In addition, the application allows you to analyze historical data, identify trends and optimize delivery processes. Effective integration with other company systems improves visibility and transparency in the supply chain, facilitating better collaboration between process participants. [17]

VII. Compliance with Relevant Standards

DID-IMP is designed to align with key global regulatory frameworks, ensuring compliance with data protection, digital identity, and trust services standards. Specifically, the system is built to conform to the General Data Protection Regulation (GDPR), Electronic Identification Authentication and Trust Services (eIDAS) Regulation, and other emerging global identity standards.

Even though DID-IMP focuses on IoT devices rather than human users, its features proactively uphold the privacy-by-design principles outlined in GDPR (Regulation (EU) 2016/679) by ensuring that personal data is not stored on-chain and that individuals retain full control over their identity credentials. Users will be able to selectively disclose attributes using Zero-Knowledge Proofs (ZKPs), allowing them to verify credentials without revealing unnecessary personal information. Additionally, the decentralized architecture minimizes the risk of data breaches, as personal identifiers are not centrally stored or exposed to unauthorized access. The right to erasure (Article 17, GDPR) is respected through revocable credentials, enabling users to remove access to their verifiable credentials when necessary. Under the eIDAS Regulation (EU) 910/2014), DID-IMP supports qualified electronic signatures (QES) and qualified electronic seals through the use of blockchain-based verifiable credentials. The framework enables secure, cross-border authentication by allowing trust service providers (TSPs) to issue digitally signed credentials that meet eIDAS certification standards. The DID-IMP system ensures strong authentication mechanisms, enhancing the security and validity of electronic data transfers within the European Union.

Thanks to its alignment with the fundamental principles of GDPR and eIDAS, DID-IMP ensures a legally compliant and privacy-centric identity verification system, fostering secure and trustworthy interactions within IoT networks and ecosystems.

VIII. Conclusion

The DID-IMP project represents a significant advancement in decentralized identity management for IoT and AIoT ecosystems, offering a scalable, secure, and trustless framework for automated identity verification and data exchange. By leveraging blockchain-based Decentralized Public Key Infrastructure (DPKI), verifiable credentials (VCs), and smart contract automation, DID-IMP eliminates reliance on centralized identity authorities, ensuring greater transparency, security, and resilience against fraudulent credential issuance. The integration of Secure Automatic Data Sharing (SADS) further enhances the efficiency and interoperability of IoT devices, allowing them to authenticate, communicate, and share data in a privacy-preserving and tamper-resistant manner.

A core innovation of DID-IMP is the DID Risk Assessment Model (DID-RAM), which strengthens trust and fraud detection through issuer reputation scoring, machine learning-based anomaly detection, and smart contract enforcement. DID-RAM enables real-time risk evaluation of credential issuers, ensuring that malicious actors are quickly identified and restricted. Performance evaluations on a testnet deployment demonstrate high fraud detection accuracy (94.5%), fast trust score updates (<2 seconds latency), and efficient smart contract execution (150,000 gas per query).

Future Directions

To further enhance the capabilities of DID-IMP, several key improvements are planned. The integration of Zero-Knowledge Proofs (ZKPs) will enable privacy-preserving identity verification, allowing devices to prove credentials without revealing sensitive information. Additionally, cross-chain compatibility will be explored to enable multi-blockchain identity verification, ensuring seamless interoperability between different decentralized networks. Another important development is the implementation of Federated Learning Models, which will allow collaborative fraud detection across multiple IoT environments, improving the accuracy of anomaly detection mechanisms.

Next Steps

Moving forward, the next phase of DID-IMP will focus on expanding pilot implementations across various industries, including smart cities, connected vehicles, healthcare, and decentralized energy management. Further benchmark testing and optimization will be conducted to assess scalability under real-world conditions, ensuring the framework can support large-scale IoT networks. Engagement with regulatory bodies and industry partners will also be prioritized to align DID-IMP with the next versions of global data protection and identity management standards such as GDPR, HIPAA, and eIDAS.

By integrating cutting-edge blockchain security, cryptographic identity verification, and AI-driven risk assessment, DID-IMP lays the foundation for a decentralized, trust-based IoT identity framework that is secure, efficient, and future-proof. As the project advances, it has the potential to become a standardized solution for next-generation identity management, empowering individuals and organizations with self-sovereign identity control while ensuring trusted and verifiable interactions in IoT ecosystems.

References

1. "IoT devices ‘to generate nearly 80 zettabytes of data’ by 2025," 2023. [Online]. Available: https://aro.tech/iot-devices-to-generatenearly-80-zettabytes-of-data-by-2025/
2. "Big Data Market Worth $229.4 Billion by 2025," MarketsandMarkets™, 2020. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/big-data-market-1068.html
3. "Internet of Things (IoT) Market," Allied Market Research™, 2023. [Online]. Available: https://www.alliedmarketresearch.com/internet-of-things-IoT-market/
4. "Artificial Intelligence of Things (AIoT) Market Report," Grand View Research, 2023. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-of-things-aiot-market-report
5. V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A review of IoT security and privacy using decentralized blockchain techniques," *Comput. Sci. Rev.*, vol. 50, p. 100585, 2023. DOI: 10.1016/j.cosrev.2023.100585
6. A. Abdulhamid, S. Kabir, I. Ghafir, and C. Lei, "An Overview of Safety and Security Analysis Frameworks for the Internet of Things," *Electronics*, vol. 12, no. 14, p. 3086, 2023. DOI: 10.3390/electronics12143086
7. Z. Rahman, X. Yi, I. Khalil, and A. Kelarev, "Blockchain for IoT: A Critical Analysis Concerning Performance and Scalability," *arXiv*, 2023. [Online]. Available: https://arxiv.org/abs/2111.11158
8. "Alastria Blockchain Network," Alastria, 2023. [Online]. Available: https://alastria.io
9. "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, 2022. [Online]. Available: https://www.w3.org/TR/did-core/
10. "Verifiable Credentials Data Model v2.0," W3C Working Draft, 2024. [Online]. Available: https://www.w3.org/TR/vc-data-model/
11. A. Mykola and A. Anastasiia, "Internet of Things in the Automotive Industry: Solutions for Vehicles, Smart, and Connected Cars," 2023. [Online]. Available: https://www.aimprosoft.com/blog/automotive-iot-usecases-for-cars-vehicles/
12. P. S. Akram, M. Ramesha, S. A. S. Valiveti, S. Sohail, and K. T. S. S. Rao, "IoT-based Remote Patient Health Monitoring System," in *Proc. 7th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Coimbatore, India, 2021, pp. 1519-1524. DOI: 10.1109/ICACCS51430.2021.9441874
13. J. Park, M. Salim, J. Jo, J. Sicato, S. Rathore, and J. Park, "CIoT-Net: A Scalable Cognitive IoT-Based Smart City Network Architecture," *Hum.-Cent. Comput. Inf. Sci.*, 2019. DOI: 10.1186/s13673-019-0190-9
14. M. Mahmoud, "Smart City vs. Cognitive City," 2023. [Online]. Available: https://mostafame.medium.com/smart-city-vs-cognitivecity-94271c2222d7
15. K. Oliynyk, "How IoT Can Help With Energy Management Systems?," 2024. [Online]. Available: https://webbylab.com/blog/how-iot-can-help-with-energymanagement/
16. "Internet of Things In Smart Home," 2023. [Online]. Available: https://scand.com/company/blog/internet-of-things-in-smart-home/
17. M. Baig, D. Sunny, A. Alqahtani, S. Alsubai, A. Binbusayyis, and M. Muzammal, "A Study on the Adoption of Blockchain for IoT Devices in Supply Chain," *Comput. Intell. Neurosci.*, vol. 2022, Art. ID 9228982, 25 pages, 2022. DOI: 10.1155/2022/9228982
18. T. G. Papaioannou and V. Ritas, "VChain: Establishing Trust Based on Verifiable Credential Chains," in *Proc. ICIN 2025 Conf.*, 2025.

19. R. Mukta, H.-Y. Paik, Q. Lu, and S. S. Kanhere, "CredTrust: Credential-Based Issuer Management for Trust in Self-Sovereign Identity," in *Proc. IEEE Blockchain Conf.*, 2022, pp. 334–339.

20. O. Dogan and H. Karacan, "A Blockchain-Based E-Commerce Reputation System Built with Verifiable Credentials," *IEEE Access*, vol. 11, pp. 47080–47097, 2023.

21. J. Arshad, M. A. Azad, A. Prince, J. Ali, and T. G. Papaioannou, "Reputable: A Decentralized Reputation System for Blockchain-Based Ecosystems," *IEEE Access*, vol. 10, pp. 79948–79961, 2022.

22. M. Mehdi, N. Bouguila, and J. Bentahar, "Trust and Reputation of Web Services through QoS Correlation Lens," *IEEE Trans. Serv. Comput.*, vol. 9, no. 6, pp. 968–981, 2016.

23. R. Mukta, J. Martens, H.-Y. Paik, Q. Lu, and S. S. Kanhere, "Blockchain-Based Verifiable Credential Sharing with Selective Disclosure," in *Proc. IEEE TrustCom*, 2020.

24. D. Clarke, J.-E. Elien, C. Ellison, M. Fredette, A. Morcos, and R. L. Rivest, "Certificate Chain Discovery in SPKI/SDSI," *J. Comput. Secur.*, vol. 9, no. 4, pp. 285–322, Feb. 2002.