RESEARCH ARTICLE OPEN ACCESS

Decentralized Identity (DID)-Based Authentication Algorithms For Data Access Using Block chain: A Comparative Study.

Ms. Priyanka S. Yengantwar (Chandawar)[#1], Dr Ujwal A. Lanjewar[#2],

[#1]*Research Scholar, Department of Electronics & Computer Science Rashtrasant Tukadoji Maharaj Nagpur University, Research Centre, Nagpur, MS. (India)*

[#2]*Professor, & Principal, Department of Computer Science, Binzani Mahila Mahavidyalaya, Nagpur, MS. (India)*

ABSTRACT

Fog-IoT networks are expanding at an accelerated rate, hence it has made necessary to develop scalable and secure authentication methodologies to secure data access and facilitate communication between IoT devices and Fog servers. The implementation of blockchain technology allows for Decentralized Identity (DID)-based authentication, which establishes a tamper-resistant and self-governing identity management framework. On the other hand, the security, efficiency, and scalability of DID authentication are significantly influenced by the cryptographic techniques employed. This paper explores and compares different DID-based authentication algorithms for data access, emphasizing their suitability for various applications.

Keywords: Decentralized Identity (DID), Authentication, Internet of Things and Blockchain.

I. INTRODUCTION

The accelerated expansion of Internet of Things (IoT) devices has resulted in an exponential increase in data transmission, thereby requiring the implementation of secure and efficient authentication protocols. Traditional authentication system mainly depends on centralized identity management, which introduces substantial security risks, such as single points of failure, identity theft and unauthorized data retrieval.

To address these challenges, Decentralized Identity (DID)-based authentication standardized by W3C [1] has emerged as a promising solution, leveraging blockchain technology to enhance security, privacy, and trust in IoT ecosystems.

Decentralized identity (DID) [2] is an identity system in which identity information is owned by the entity that creates it.

II. ARCHITECTURE OF DID

Architecture of DID shown in Fig 1. which consist of following terminologies:

1. **Decentralised Identifiers**: DIDs are unique identifiers created using cryptographic key-pairs. The public key is published on the blockchain, while the private key remains securely with the user. Documents that contain service endpoints and public keys vital for interactions are systematically linked with Decentralized Identifiers (DIDs) [3,4].

2. **Blockchain and Distributed Ledger Technology**: The system employs Distributed Ledger Technology (DLT) to guarantee security, immutability, and transparency. In order to uphold confidentiality, only essential information such as Decentralized Identifier (DID) documents or attestations is recorded on the blockchain. Personal data is preserved off-

chain, with the blockchain maintaining references to this data and proofs of transactions [4,5].

3. **Credential Issuance and Verification**: Verifiable credentials are issued by trusted issuers, cryptographically signed, and kept in the user's digital wallet. Users provide these credentials for identity verification when required [6].

4. **Role of SSI**: Users control and manage their identities using digital wallets that contain their DIDs, private keys, and verifiable credentials according to the SSI principles. This guarantees transparency, empowers users, and reduces identity theft, which is common in centralized systems [6].

5. **Agent-Driven Interoperability and Privacy Protection:** Identity agents enable complex interactions for users, ensuring that transactions remain secure and private. Advanced cryptographic techniques such as zero-knowledge proofs and selective disclosure enable users to authenticate and reveal specific features while keeping the underlying data confidential [6].

6. **Revocation and Persistence**: The issuers can revoke credentials before they expire using the system's built-in procedures. Verifiers can use the blockchain to rapidly check revocations. Backup techniques ensure persistence, allowing users to recover their credentials and identities even if keys are lost[4].

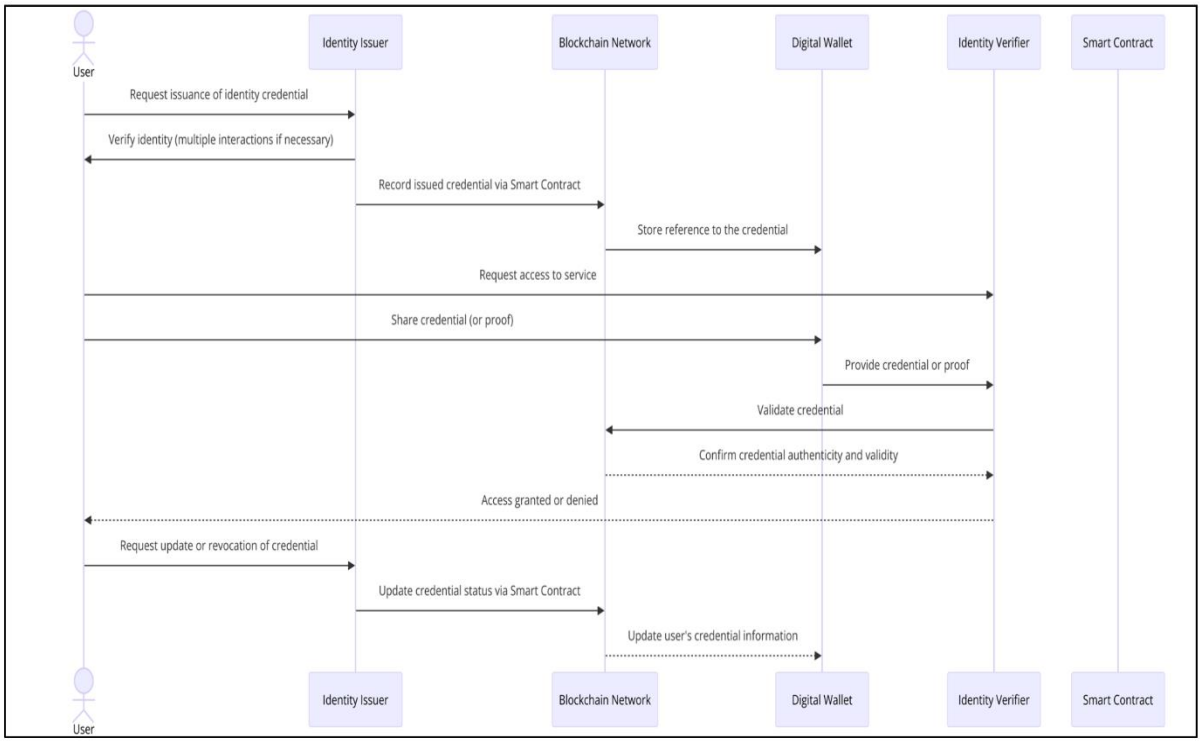

Fig. 1: Architecture of DID

III. LITERATURE REVIEW

The survey is about thorough analysis of DIDs and VCs in terms of implementations, application domains, and regulations. While the analysis of the application DIDs and VCs demonstrates that their utility goes far beyond SSI systems. [8]
Author stated that Identity is a central pillar of trust and identity and access management is a vibrant, multidisciplinary, and growing field that requires attention, research, experimentation, and collaboration.[9]
The paper comprehensively discusses how the use of blockchain in SSI. The concept of DIDs and VCs are only presented as the foundational technologies of SSI, without delving into an examination of relevant research papers.[10]
Here author discussed how DIDs and VCs can be deployed in SSI systems. However, the review does not extend to exploring other application domains, nor does it encompass a discussion on emerging regulations and initiatives.[11]
The work covers all the key aspects related to DIDs and VCs technologies, ranging from the primary implementations and their applications across different domains, to the exploration of emerging regulations and initiatives proposed by governments and organizations[12].
When comparing authentication algorithms within a Decentralized Identifier (DID) system, key factors to consider include security level, privacy considerations, scalability, ease of implementation, and compatibility with existing standards; with prominent algorithms like ECDSA (Elliptic Curve Digital Signature Algorithm), RSA (Rivest-Shamir-Adleman), and Schnorr Signatures often being compared based on these aspects:

IV. VARIOUS AUTHENTICATION ALGORITHMS IN DID[13][14][15][16][17]

- **ECDSA:**
  Strengths: Considered highly secure, computationally efficient, and widely adopted in blockchain applications, making it a popular choice for DID authentication due to its balance between security and performance.
  Weaknesses: May require more complex key management compared to simpler algorithms.
- **RSA:**
  Strengths: Well-established, widely understood, and provides strong security for asymmetric cryptography, making it a familiar option for developers.
  Weaknesses: Can be computationally intensive for large key sizes, potentially impacting performance in scenarios requiring high transaction volumes.
- **Schnorr Signatures:**
  Strengths: Offers good security with potential for improved efficiency compared to ECDSA, particularly in certain scenarios involving signature aggregation.
  Weaknesses: May be less widely adopted than ECDSA, requiring additional consideration for compatibility with existing systems.

V. COMPARISON OF ECDSA, RSA AND SCHNORR SIGNATURE

ECDSA, RSA and Schnorr Signature are used for secure authentication using blockchain and in this paper we compare them on the basis of following levels

1. **Security Level:**

- ECDSA: Generally considered the most secure option due to its strong cryptographic properties and resistance to known attacks.
- RSA: Offers strong security when properly implemented with sufficient key length, but may become less secure with smaller key sizes.
- Schnorr Signatures: Provides a high level of security, often considered comparable to ECDSA, with potential efficiency advantages in certain situations.

2. Privacy Considerations:

- ECDSA: Provides good privacy as only the public key is publicly visible, protecting the private key.
- RSA: Similar privacy benefits as ECDSA when used correctly.
- Schnorr Signatures: Generally maintains privacy by only exposing the public key.

3. Scalability:

- ECDSA: Considered highly scalable due to its efficient cryptographic operations, making it suitable for large-scale DID systems.
- RSA: Can be scalable depending on key size and implementation, potentially becoming less efficient with very large key sizes.
- Schnorr Signatures: May offer improved scalability in certain scenarios due to potential for signature aggregation.

4. Ease of Implementation:

- ECDSA: Widely supported by libraries and frameworks, making implementation relatively straightforward.
- RSA: Well-documented and widely available, facilitating implementation across different platforms.
- Schnorr Signatures: May require additional development effort due to potentially less widespread adoption.

VI. CONCLUSION

The comparative study of Decentralized Identity (DID)-based authentication algorithms for data access using blockchain highlights the strengths and limitations of various approaches. DID systems leverage blockchain's decentralized, tamper-resistant nature to provide secure and transparent identity management. Among the algorithms evaluated, **Schnorr Signatures** are generally the best choice for secure authentication in blockchain systems due to their efficiency in multi-signature, smaller key size and lower computational overhead and enhanced privacy and scalability features.

Where as **ECDSA** is a close second and is still widely used in many blockchain systems and widespread support. However, it lacks the advanced features of Schnorr signatures.

And **RSA** is less suitable for blockchain due to its inefficiency and larger key sizes, though it remains a strong choice for traditional systems.

REFERENCES

[1]. DID Specification. 2020. Available online: https://www.w3.org/TR/did-core/
[2]. Decentralized Identity Foundation. 2018. Available online: https://identity.foundation/
[3]. Paik, H.; Liu, Y.; Lu, Q.; Kanhere, S.S. Decentralised identity management and blockchains: Design patterns and architectures. In Blockchains; Ruj, S., Kanhere, S.S., Conti, M., Eds.; Springer: Cham, Switzerland, 2024; pp. 105–128. [Google Scholar] [CrossRef]

[4]. Mazzocca, C.; Acar, A.; Uluagac, S.; Montanari, R.; Bellavista, P.; Conti, M. A survey on decentralised identifiers and verifiable credentials. arXiv 2024, arXiv:2402.02455. [Google Scholar]
[5]. Satybaldy, A.; Nowostawski, M.; Ellingsen, J. Self-sovereign identity systems: Evaluation framework. In Privacy and Identity Management: Data for Better Living: AI and Privacy; IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2; Springer: Cham, Switzerland, 2020; pp. 447–461. [Google Scholar]
[6]. Baars, D.S. Towards Self-Sovereign Identity Using Blockchain Technology. Master's Thesis, University of Twente, Enschede, The Netherlands, 2016. [Google Scholar]
[7]. https://tinyurl.com/y89tahad DIDAuth. 2018
[8]. M. A. Olivero, A. Bertolino, F. J. Domínguez-Mayo, M. J. Escalona, and I. Matteucci, "Digital persona portrayal: Identifying pluridentity vulnerabilities in digital life," Journal of Information Security and Applications, vol. 52, p. 102492, 2020.
[9]. N. Romandini, A. Mora, C. Mazzocca, R. Montanari, and P. Bellavista, "Federated Unlearning: A Survey on Methods, Design Guidelines, and Evaluation Metrics," arXiv preprint arXiv:2401.05146, 2024.
[10]. W3 Recommendation, "Decentralized Identifiers (DIDs) v1.0," 2022. [Online]. Available: https://www.w3.org/TR/did-core/
[11]. W. Recommendation, "Verifiable Credentials Data Model v1.1," 2022. [Online]. Available: https://www.w3.org/TR/vc-data-model/
[12]. S. Cucko and M. Turkanović, "Decentralized and Self-Sovereign Identity: Systematic Mapping Study," *IEEE Access*, vol. 9, pp. 139 009–139 027, 2021.
[13]. Buchanan, Bill. "What Is The Fastest Signing and Verification Method for Digital Signatures." *Medium*, 16 Oct. 2023. https://billatnapier.medium.com/what-is-the-fastest-signing-and-verification-method-for-digital-signatures-0b2df0d61529.
[14]. "Elliptic Curve Digital Signature Algorithm." *Wikipedia*, 20 Jan. 2025. https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm.
[15]. "Schnorr Signature." *Wikipedia*, 20 Jan. 2025. https://en.wikipedia.org/wiki/Schnorr_signature.
[16]. "Digital Signature Scheme for Information Non-Repudiation in Blockchain: A State of the Art Review." *EURASIP Journal on Wireless Communications and Networking*, 2020. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-020-01665-w.
[17]. "What Are the Differences in Cryptographic Algorithms for PKI?" *Keytos Documentation*, https://www.keytos.io/docs/azure-pki/creating-your-first-ca/difference-between-rsa-and-ecdsa/.