Blockchain-Based Device Identity Management and Authentication in Cyber-Physical Systems

Uttam Ghosh *, Debashis Das[†], Sourav Banerjee[‡], and Saraju Mohanty[§]
*[†]Department of CS and DS, Meharry Medical College, Nashville, TN, USA
[‡]Department of CSE, Kalyani Government Engineering College, Kalyani, WB, India
[§]Computer Science and Engineering, University of North Texas, Denton, Texas, USA
ghosh.uttam@ieee.org*, debashis.das@ieee.org[†], mr.sourav.banerjee@ieee.org[‡], saraju.mohanty@unt.edu[§]

***Abstract*—The proliferation of interconnected devices in the era of the Internet of Things (IoT) has given rise to the need for robust device identity management and authentication mechanisms in cyber-physical systems (CPSs). Traditional centralized approaches to identity management face challenges of security, scalability, and privacy. Therefore, the paper provides an innovative approach by fusing Self-Sovereign Identity (SSI) with blockchain technology to revolutionize device identity management within CPS environments. In this paper, devices autonomously initiate their identity-creation processes. Each device generates a cryptographic key pair comprising a public key for openly identifying the device and a closely guarded private key used for authentication and decryption purposes. The research also introduces an innovative authentication algorithm within CPS environments that employs secure tokens to validate the authenticity of devices. The proposed framework reduces the risk of unauthorized access and data breaches while empowering devices with control over their identities. Overall, the proposed approach not only enhances security, privacy, and resilience within CPSs but also provides a transformative solution for identity management in dynamic and autonomous device environments.**

***Index Terms*—Cyber-Physical Systems, Internet of Things, Blockchain, Cryptography, Self-Sovereign Identity, Data Security.**

I. Introduction

The technological landscape has undergone a revolutionary transformation with the advent of the Internet of Things (IoT). The seamless integration of smart devices into our lives has facilitated novel applications in various domains, propelling us into the era of Cyber-Physical Systems (CPSs) [1]. The integration of IoT devices into critical infrastructure systems introduces security concerns due to the heterogeneity and large-scale nature of interconnected devices. Traditional centralized identity management methods are ill-suited for managing the complexities and security demands of these systems [2].

The rapid integration of IoT devices into CPSs has ushered in an era of unprecedented connectivity and functionality. However, this interconnected landscape brings with it a host of security challenges [3]. The large volume of devices and the dynamic nature of their interactions make it difficult for centralized systems to effectively manage and authenticate identities in a timely and secure manner, which demands innovative solutions for identity management and authentication [4]. Moreover, the criticality of CPSs introduces additional security demands. For instance, consider a smart city's infrastructure, where IoT devices control traffic signals, power distribution, and emergency response systems (see Fig. 1). If these devices are not identified and authenticated, malicious actors could manipulate them to cause traffic chaos, disrupt power supplies, or even compromise public safety.

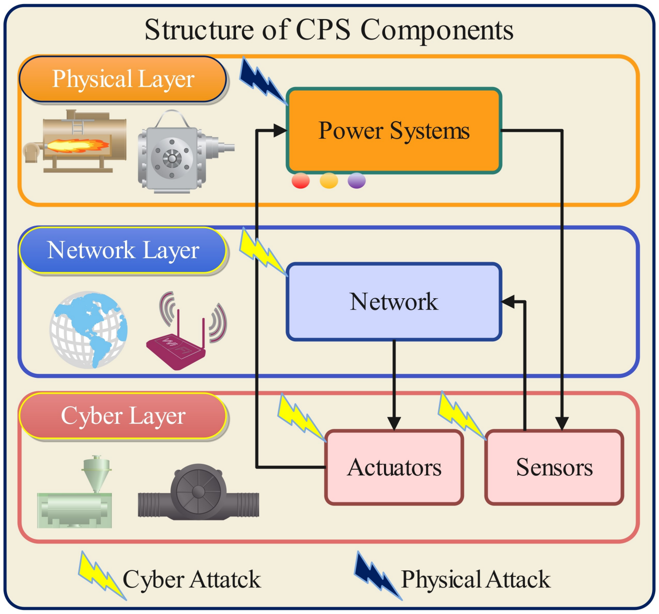

Fig. 1: Basic components of CPSs

These challenges underscore the need for a paradigm shift in identity management and authentication. Blockchain technology [5] emerges as a promising candidate to address these concerns. By using the decentralized and tamper-resistant nature of blockchain [6], it becomes possible to establish a trusted framework that operates without the need for a single centralized authority. This enables secure and efficient identity management and authentication by allowing each device to have a verifiable and immutable identity on the blockchain [1]. Furthermore, effective device identity management is pivotal for the security, trustworthiness, and efficient operation of CPSs [7]. Blockchain technology presents a powerful solution to address the challenges posed by identity management within CPSs. By leveraging its decentralization, immutability, and secure token exchange capabilities, blockchain enhances security and trust among CPSs devices [8].

Therefore, we propose an approach for device identity management and authentication within CPSs by combining self-sovereign identity (SSI) [9] principles with blockchain technology [10]. In this framework, devices autonomously create and manage their identities, enhancing security, privacy, and resilience in CPS environments. Each device generates a unique cryptographic key pair comprising a public key (PK) for identification and a closely guarded private key (SK) for authentication and decryption. These keys are recorded on a blockchain, ensuring immutability and trustworthiness. Secure authentication tokens are used to verify the authenticity of devices, reducing the risk of unauthorized access and data breaches [8].

A. Contribution of the Paper

The objectives of the paper aim to provide an assessment of the potential benefits of using SSI in combination with blockchain technology for device identity management and authentication in CPSs.

- Integrate SSI with blockchain technology for device identity management and authentication in CPSs.
- Examine the privacy implications of the SSI approach and determine how it protects the privacy of device owners and users in CPSs.

B. Oraganization of the Paper

The paper layout is structured into several sections to systematically address the research objectives. In Section II, we provide background information and motivation for the study, highlighting the challenges in digital identity management within Cyber-Physical Systems (CPSs). Section III presents an overview of related works, emphasizing the existing research landscape in this domain. Section IV outlines the proposed methodology, introducing the fusion of Self-Sovereign Identity (SSI) principles with blockchain technology to enhance device identity management and authentication in CPSs. Section V conducts a performance analysis, assessing the benefits and implications of the proposed approach. Finally, in Section VI, the paper concludes its findings and sets the stage for future work.

II. Background and Motivation

CPSs represent the convergence of physical processes with digital technologies, creating interconnected systems that impact various aspects of our lives, from transportation and healthcare to industrial automation and smart cities. Ensuring the security of these systems and managing identities within them is paramount. Identity management in CPSs is the framework of processes, policies, and technologies that provide only authorized individuals and devices access to technology resources, information, or services within these complex applications for safeguarding the interconnected systems to make Trusted communication in smart cities.

A. Problems With Current Digital Identity Management

In the context of CPSs, digital identity is a crucial element that encompasses all the information about individuals or entities that exist online and is connected to the CPSs. This digital identity includes a wide range of data, such as usernames, purchasing history, identification numbers, and search history. However, managing digital identities within CPSs presents unique challenges and privacy risks. Table I gives the motivation for using decentralized digital identity and authentication management in CPSs [11].

B. Key Considerations for Identity of CPSs Security

1) Data Encryption: Implementing robust data encryption within CPSs is essential to protect sensitive information. Encryption ensures that data transmitted or stored within these systems is unintelligible to unauthorized parties.

2) User Authentication: Implement robust user authentication mechanisms, such as multi-factor authentication (MFA), to verify the identity of individuals using CPSs. This mitigates the risk of unauthorized access.

3) Identity Verification: Employ reliable identity verification processes, particularly for access to critical services within CPSs. These processes should include checks to confirm the user's identity before granting access to sensitive data or functionalities.

4) Security Updates and Patch Management: Regularly update and patch CPSs components to address security vulnerabilities. Outdated systems are more susceptible to identity theft-related attacks.

5) Monitoring and Incident Response: Implement monitoring systems to detect suspicious activities within CPSs. Develop robust incident response plans to address security breaches promptly.

C. Decentralized Identity

In traditional computer systems, device identities are often handled by centralized authorities, which leaves these systems open to the possibility of being attacked or having their security compromised. In the context of decentralized identity management, each device that is part of the CPSs ecosystem is given a distinct and unchangeable identity, which is often stored on the blockchain. This identification takes the form of a cryptographic hash [4]. This identification acts as the device's digital fingerprint and identifies it uniquely. Once an identity has been formed and stored on a blockchain, the immutability of the blockchain assures that it cannot be changed without the agreement of all of the members of the network. Because the identification of each device is recorded in a distributed ledger that is then shared throughout the network, it is feasible for all participants to independently determine whether or not an identity recorded by a device is legitimate.

D. Self-Sovereign Identity

Traditional identity management systems involve a central authority, like a certificate authority or a database, that

TABLE I: A comparison analysis of conventional methods with SSI Blockchain

Aspect	Conventional Methods	SSI with Blockchain
Centralization	Typically centralized, relying on a central authority or server for identity verification and access control.	Decentralized, eliminating the need for a single central authority and reducing the risk of single points of failure.
Security	Vulnerable to single points of failure and breaches. Identity data stored on centralized servers can be attractive targets for attackers.	Highly secure due to the cryptographic protection of identity data on the blockchain. Immutable record-keeping ensures data integrity.
Privacy	May involve the sharing of sensitive personal data with central authorities, raising privacy concerns.	Enables users to have greater control over their data, sharing only the necessary information required for verification, enhancing privacy.
Trust	Relies on trust in central authorities or intermediaries.	Built on trust in cryptographic mechanisms and transparency of blockchain transactions.
Scalability	May face scalability challenges as the number of devices and transactions increase.	Potential for scalability improvements through blockchain enhancements and optimizations.
Regulatory Compliance	Compliance with data protection regulations may be complex due to centralized data storage and sharing.	Enhanced potential for regulatory compliance through user-centric data control and consent mechanisms.
Ease of Use	User experiences may vary, and identity management may be complex.	Offers the potential for user-friendly, self-managed identity control and consent through mobile apps and interfaces.
Resilience to Attacks	Vulnerable to various attacks, such as data breaches and identity theft.	Resilient to many common attacks due to cryptographic security and immutability of data.
Interoperability	Integration with other systems and platforms can be challenging due to a lack of standardization.	Can facilitate interoperability through standardized blockchain protocols and open standards.
Ownership of Identity	Users often have limited control over their identities, which are managed by centralized entities.	Promotes the concept of self-sovereign identity, giving users control and ownership over their identities.

validates and manages identities. However, such systems can introduce risks, including the potential compromise of the central authority. SSI [12] empowers devices to manage their own identity and authentication without relying on a central authority. This decentralized approach enhances security, minimizes vulnerabilities, and eliminates the risk of single points of failure. In SSI, devices are granted the autonomy to create and manage their identities. Each device possesses its unique cryptographic keys [13], which are used to authenticate and sign transactions. These keys form the basis of the device's identity, and only the device itself holds the private key.

For example, In the traditional model of identity management, there is a central authority (CA) responsible for creating and managing identities. CA creates a lock: (L), which represents the digital identity of a device. This L is used to secure access and interactions. The CA holds the key: (K) that corresponds to the L. This key is required to unlock the identity and access the associated resources or services. In this model, CA has complete control over both the creation of locks (e.g., L) and the possession of keys (e.g., K). This centralization introduces risks, as a compromise of the CA's control could lead to unauthorized access or breaches.

In the SSI Model, devices have autonomy over their own identity management [14]. Each device(D) takes on the role of creating and managing its own digital identity. This identity is unique to the device and is crucial for secure interactions within a network. The device creates its lock: (L_D), which represents its own digital identity. This (L_D) is generated using the device's cryptographic keys, which are unique to that device. The device also holds the key: (K_D) corresponding to its own (L_D). This (K_D) is used to unlock the device's identity and gain access to the services or resources it is authorized to use [15]. The Traditional Model involves a central authority creating locks and holding keys, while the SSI Model empowers each device to create its own lock and hold its own key. This paradigm shift in identity management enhances security, privacy, and resilience in interconnected systems, such as the IoT and CPSs.

E. Authentication Tokens

The technology behind blockchain allows devices to produce and trade authentication tokens through blockchain transactions [16]. These tokens serve as cryptographic evidence that the device in question is who it claims to be. When a piece of hardware has to prove its identity to another part of the hardware or system, it does so by generating an authentication token with the use of its private key. Following that, the receiving entity is given access to this token. The public key of the device, which is connected with the immutable identity of the device stored on the blockchain, can be used by the entity that is receiving the token to validate the legitimacy of the token. Verification of identification is made safe and confidential by the use of this technique. It gives devices the ability to demonstrate their identification without divulging any vital information, which simultaneously strengthens both security and privacy [17].

III. Related Works

The authors [18] explored the role of medical CPSs (MCPSs) in enhancing patient-medical system interaction in smart healthcare. It underscores the need for secure device identity authentication to meet MCPS requirements. The review introduces a blockchain-based lightweight authentication scheme for devices and users within MCPSs, highlighting its efficacy in resisting attacks and its potential for medical field applications. However, it's important to note that the study does not extensively address potential scalability challenges associated with implementing the proposed blockchain-based authentication scheme in larger-scale MCPSs. Thus, there is a need for identity management.

The authors [19] focused on the potential of blockchain technology in enhancing trust and security in CPSs. The proposed solution involves a blockchain-based signature storage system to ensure trust among participants, addressing device identification, authentication, integrity, and non-repudiation. Implemented on Ethereum using Docker Tools, this approach not only enhances security but also reduces storage space and costs compared to traditional blockchain usage in CPSs, offering a promising solution for a wide range of blockchain-based CPS applications.

This article [20] introduced a novel approach to address the limitations of blockchain in IoT applications. It presents a multi-chain structure based on a directed acyclic graph (DAG) to enhance scalability and storage. A new consensus algorithm called ”Multi-Chain Proof of Rapid Authentication” (McPoRA) significantly improves latency, making it approximately 4000 times faster than proof-of-work (PoW) and 55 times faster than Proof-of-Authentication (PoAh). This innovative combination offers a promising solution for secure and efficient IoT systems.

In [1], the authors explored the potential of blockchain technology to address security, trust, and privacy challenges in CPSs. It discusses the benefits of blockchain applications in improving the performance of CPSs, particularly in domains like smart grids and connected vehicles. The paper proposes blockchain-enabled solutions and outlines the integration process of blockchain into various CPSs components, ultimately enhancing security, privacy, and trust management within CPSs. They discussed the limitation of implementing blockchain in CPSs, which is the potential increase in computational overhead and resource requirements, which can be a challenge for resource-constrained CPSs devices and may affect real-time responsiveness in certain applications.

This study [21] introduced a reputation-based blockchain framework to enhance patient data security and privacy in medical CPSs. It addresses issues like data leakage and manipulation. The framework is analyzed for security and performance, demonstrating lower latency and higher throughput with increased user numbers. However, a potential limitation could be the computational resources required for maintaining the blockchain, which might pose challenges in resource-constrained healthcare environments.

IV. Proposed Methods

In the dynamic landscape of CPSs, where real-time and autonomous device interactions are the norm, the secure management of device identities and authentication is paramount. SSI presents a decentralized paradigm for identity management, uniquely suited to the intricacies of CPS environments. The envisioned framework, as illustrated in Fig. 2, signifies a revolutionary stride in CPS identity management by fortifying security measures, preserving user privacy, and endowing devices with autonomy. This decentralized approach not only addresses the specific challenges of CPSs but also provides a more resilient, interoperable, and user-centric identity ecosystem within CPSs environments.

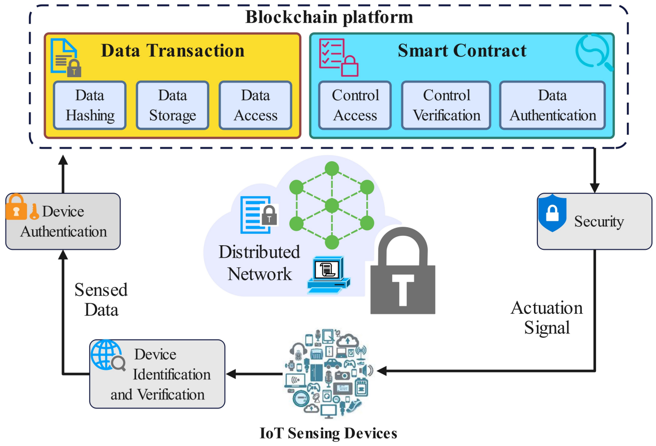

Fig. 2: Proposed System Model.

A. Identity Generation

1) Unique Device Identity Creation: In CPSs, each device, whether it’s a sensor, controller, or any other component, initiates the identity creation process autonomously. As shown in Fig. 3, the device generates a cryptographic key pair. This key pair consists of: Public Key (PK_D): This key is intended to be shared openly and serves as the device’s unique identifier within the CPSs. Other devices or entities can use this public key to encrypt messages or data meant for the device. Private Key (SK_D): The private key is a closely guarded secret that should never be shared. It’s used for decrypting messages or data encrypted with the corresponding public key and for digitally signing transactions or messages to prove the device’s authenticity. Beyond the key pair, the device’s identity is enriched with associated metadata. This metadata can include: **Device Name:** A human-readable name or label for the device. **Device Type:** The device’s category or functionality within the CPSs. **Manufacturer Information:** Details about the device’s manufacturer, model, and version. **Geolocation:** The device’s physical location coordinates. **Lifecycle Information:** The device’s operational status, such as creation date and current state.

2) Cryptography Key Pair: The heart of the device’s identity is its cryptographic key pair: a public key (PK_D) and a private key (SK_D). The public key is shared openly and serves as the device’s identifier. It can be used by other devices or entities to encrypt data meant for the device. The private key, on the other hand, is kept securely within the device and should never be shared. It is used for decrypting data encrypted with the corresponding public key and for signing transactions to prove the device’s authenticity.

3) Registration on the Blockchain: To establish trust and immutability, the device registers its public key and associated metadata on a blockchain platform such as Ethereum. This registration becomes a permanent and tamper-resistant record that can be verified by other devices and entities in the CPSs. The registration on the Blockchain serves as a form of attestation, confirming the authenticity and validity of the device’s identity.

```
Algorithm 1: Authentication in CPSs with SSI
Input: $PK_{Auth}$, $SK_{Auth}$;
Output: accept/reject;
The initiating device (Device A) wishes to authenticate itself to the
  target device (Device B);
Device B generates a random challenge (Challenge_B) and sends it
  to Device A;
Device A receives Challenge_B from Device B;
Device A combines the received challenge (Challenge_B) with its
  own identity (Public Key: $PK_{Auth}$) and other relevant
  information to create a token generation request.;
This token generation request is hashed to create a unique token
  generation hash using equation 1;
Device A signs the token generation hash $TG_{Hash}$ with its
  private key $SK_{Auth}$ to create the secure authentication token
  using equation 2;
Device A sends $Auth_{Token}$ to Device B;
Device B verifies the received $Auth_{Token}$ using Device A's
  public key $PK_{Auth}$ using equation 3;
if $Valid_{Token}$ is true then
    Device B accepts Device A as an authentic entity and
      proceeds with the requested interaction.;
else
    Device B rejects the authentication attempt, indicating that
      Device A's identity couldn't be verified.;
end
```

B. Authentication in CPSs with SSI

SSI introduces a robust and secure method for identity generation and authentication within CPSs. Devices autonomously create and manage their unique identities, enhancing security, privacy, and resilience in CPS environments. Algorithm 1 illustrates the generation of secure authentication tokens in CPSs, enhancing the security and trustworthiness of interactions between devices. It ensures that only authentic devices can successfully complete the authentication process.

$$TG_{Hash} = Hash(Challenge_B || PK_{Auth} || T || Metadata) \tag{1}$$

$$Auth_{Token} = Sign(TG_{Hash}, SK_{Auth}) \tag{2}$$

$$Valid_{Token} = Verify(Auth_{Token}, TG_{Hash}, PK_{Auth}) \tag{3}$$

1) Secure Authentication Tokens: To establish trust and immutability, the device registers its public key and associated metadata on a blockchain platform such as Ethereum. This registration becomes a permanent and tamper-resistant record that can be verified by other devices and entities in the CPSs. The registration on the Blockchain serves as a form of attestation, confirming the authenticity and validity of the device's identity.

2) Request and Verification: Device A sends the authentication token, along with its identity (public key), to the target device. The target device receives the token and uses the public key of the initiating device (PK_Auth) to verify the signature on the token. If the signature is valid, the target device can be confident that the token came from the legitimate device.

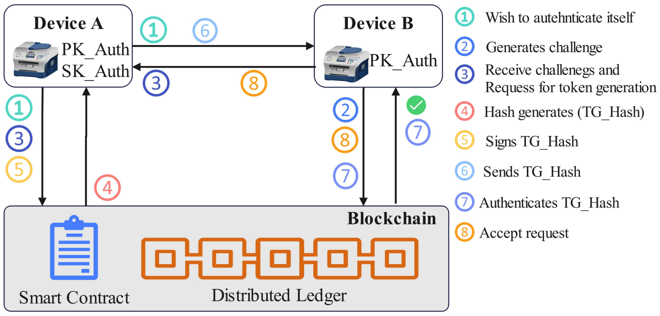

Fig. 3: Device authentication using SSI

3) Access Granted: Once the target device validates the authentication token, it grants the initiating device access to the requested resource or service. This access can be temporary and specific to the task at hand, enhancing security and reducing potential risks.

V. Performance Analysis

The proposed method ensures that Device A's ability to generate a valid authentication token is based on its possession of the private key (SK_Auth). The unique token generation hash prevents replay attacks, as the same token cannot be reused for subsequent authentication attempts. The proposed framework involves evaluating its efficiency in terms of data processing, authentication speed, and scalability. This decentralized framework mitigates the vulnerabilities associated with centralized identity systems and establishes resilient and adaptable identity management in CPSs.

A. Privacy Preservation

CPSs often involve the collection and sharing of sensitive data. SIS allows devices to selectively share only the necessary information required for authentication preserving their privacy. This device-centric approach to identity management empowers individual devices to control their digital identities.

B. Trustworthiness and Authenticity

The proposed framework enhances trustworthiness and authenticity in CPSs. Each device's identity is cryptographically linked to its private key. This linkage ensures that any interaction or transaction involving the device can be authenticated with a high degree of confidence. It's challenging for malicious actors to impersonate devices or manipulate their identities without possessing the corresponding private keys.

C. Device-Centric Control and Immutability

The proposed framework empowers devices to have greater control over their identities and personal information. Devices can selectively disclose identity attributes, sharing only the necessary information for a particular interaction. This device-centric approach enhances privacy and empowers individuals to manage their digital presence. When device identities and transactions are recorded on a blockchain, they become immutable and auditable. This means that the history of identity-related interactions is tamper-resistant and can be audited for compliance and security purposes.

D. Scalability

The proposed framework is highly scalable. As new devices are added to CPSs, they can autonomously create their identities without causing bottlenecks or overloading a centralized identity management system. This scalability is crucial in dynamic CPS environments with a growing number of interconnected devices.

E. Cross-Domain Applications

The flexibility of the proposed framework extends beyond singular CPS domains, showcasing its applicability across diverse sectors such as healthcare, transportation, smart cities, and industrial automation. This adaptability underscores the broad utility of SSI, positioning it as a valuable and versatile solution for identity management within the complex and interconnected ecosystems of different CPS domains. Whether in healthcare for patient data security or in smart cities for efficient resource allocation, the principles of SSI offer a unified and effective approach to identity management.

VI. Conclusion

The proposed framework uses SSI principles combined with blockchain technology to provide device identity management and authentication within CPSs. This innovative approach empowers devices to autonomously create and manage their identities to enhance security, privacy, and resilience within CPS environments. By eliminating the need for centralized authorities, it reduces the risk of single points of failure and enhances trustworthiness. The use of secure authentication tokens ensures that only authentic devices can access CPS resources or services. Furthermore, device-centric control over identity attributes increases user privacy and data protection. The immutability of identity-related transactions recorded on the blockchain provides auditability and compliance capabilities that ensure the integrity of interactions within CPSs. In future work, this research can delve into optimizing the efficiency of identity creation and management processes within large-scale CPSs. Furthermore, the energy efficiency of blockchain-based SSI in resource-constrained CPS devices and exploring methods for reducing computational overhead are potential focuses.

References

[1] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, U. Biswas, and W. Mansoor, "Security, trust, and privacy management framework in cyber-physical systems using blockchain," in *2023 IEEE 20th Consumer Communications Networking Conference (CCNC)*, 2023, pp. 1–6.

[2] X. Zhu and Y. Badr, "Identity management systems for the internet of things: a survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, p. 4215, 2018.

[3] A. Mishra, A. V. Jha, B. Appasani, A. K. Ray, D. K. Gupta, and A. N. Ghazali, "Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective," *International Journal of System Assurance Engineering and Management*, vol. 14, no. Suppl 3, pp. 699–721, 2023.

[4] D. Das, K. Dasgupta, and U. Biswas, "A secure blockchain-enabled vehicle identity management framework for intelligent transportation systems," *Computers and Electrical Engineering*, vol. 105, p. 108535, 2023.

[5] D. Das, S. Banerjee, K. Dasgupta, P. Chatterjee, U. Ghosh, and U. Biswas, "Blockchain enabled sdn framework for security management in 5g applications," in *Proceedings of the 24th International Conference on Distributed Computing and Networking*, 2023, pp. 414–419.

[6] K. Gupta, K. D. Gupta, D. Kumar, G. Srivastava, and D. K. Sharma, "Bids: Blockchain and intrusion detection system coalition for securing internet of medical things networks," *IEEE Journal of Biomedical and Health Informatics*, pp. 1–9, 2023.

[7] A. Riyal, G. Kumar, D. K. Sharma, K. D. Gupta, and G. Srivastava, "Blockchain tree powered green communication for efficient and sustainable connected autonomous vehicles," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 3, pp. 1428–1437, 2022.

[8] P. K. Lahiri, D. Das, W. Mansoor, S. Banerjee, and P. Chatterjee, "A trustworthy blockchain based framework for impregnable iov in edge computing," in *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, 2020, pp. 26–31.

[9] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," *Blockchain: Research and Applications*, vol. 2, no. 2, p. 100014, 2021.

[10] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, W. Mansoor, and U. Biswas, "Design of a blockchain enabled secure vehicle-to-vehicle communication system," in *2021 4th International Conference on Signal Processing and Information Security (ICSPIS)*. IEEE, 2021, pp. 29–32.

[11] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey," *IEEE Access*, vol. 10, pp. 113 436–113 481, 2022.

[12] 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)*. IEEE, 2020, pp. 90–95.

[13] N. M. Mukhammadovich and A. R. Djuraevich, "Working with cryptographic key information," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 1, p. 911, 2023.

[14] M. Dieye, P. Valiorgue, J.-P. Gelas, E.-H. Diallo, P. Ghodous, F. Biennier, and É. Peyrol, "A self-sovereign identity based on zero-knowledge proof and blockchain," *IEEE Access*, 2023.

[15] P. M. Yawalkar, D. N. Paithankar, A. R. Pabale, R. V. Kolhe, and P. William, "Integrated identity and auditing management using blockchain mechanism," *Measurement: Sensors*, vol. 27, p. 100732, 2023.

[16] G. Manogaran, B. S. Rawal, V. Saravanan, P. MK, Q. Xin, and P. Shakeel, "Token-based authorization and authentication for secure internet of vehicles communication," *ACM Transactions on Internet Technology*, vol. 22, no. 4, pp. 1–20, 2023.

[17] M. O. Ahmad, G. Tripathi, F. Siddiqui, M. A. Alam, M. A. Ahad, M. M. Akhtar, and G. Casalino, "Bauth-zkp—a blockchain-based multi-factor authentication mechanism for securing smart cities," *Sensors*, vol. 23, no. 5, p. 2757, 2023.

[18] F. Chen, Y. Tang, X. Cheng, D. Xie, T. Wang, and C. Zhao, "Blockchain-based efficient device authentication protocol for medical cyber-physical systems," *Security and Communication Networks*, vol. 2021, pp. 1–13, 2021.

[19] B. K. Mohanta, U. Satapathy, M. R. Dey, S. S. Panda, and D. Jena, "Trust management in cyber physical system using blockchain," in *2020 11th international conference on computing, communication and networking technologies (ICCCNT)*. IEEE, 2020, pp. 1–5.

[20] A. Alkhodair, S. Mohanty, E. Kougianos, and D. Puthal, "Mcpora: A multi-chain proof of rapid authentication for post-blockchain based security in large scale complex cyber-physical systems," in *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446–451.

[21] A. Kumar and K. Chatterjee, "A lightweight blockchain-based framework for medical cyber-physical system," *The Journal of Supercomputing*, pp. 1–29, 2023.