Empowering Secure Data-Driven Services for CPS: An Attribute-Based Access Control Model with Experimental Validation

Htet Htet Hlaing, Yuuichi Teranishi, and Hitoshi Asaeda
National Institute of Information and Communications Technology (NICT), Japan
Email: htethtethlaing@nict.go.jp

***Abstract*—The convergence of physical and computational components in cyber-physical systems (CPS) is driving innovations that revolutionize diverse sectors, from self-driving cars and smart industry to healthcare. However, this interconnection expands the risk of cyberattacks and data breaches as the constant exchange of large amounts of sensitive data creates more opportunities for data exploitation. Addressing this problem through effective data access control in dynamic and complex CPS remains challenging due to the trade-off between security and efficiency. Moreover, the lack of large-scale real-world implementations of access control mechanisms in CPS restricts the evaluation of existing solutions, highlighting the need for further research and development. To fulfill these requirements, we propose a secure data sharing framework that leverages ciphertext-policy attribute-based proxy re-encryption for fine-grained access control with flexible policy updates and secure delegation of decryption rights within CPS, named "SDS-CPS." We further enhance our proposal by employing an information-centric networking approach, which decouples data from its source and enables in-network caching for efficient data delivery in heterogeneous CPS environments. For validation, we implemented and evaluated SDS-CPS on an actual testbed. The experimental results demonstrate significant improvements in data access efficiency while securely handling dynamic access policies with minimal computational overhead.**

***Index Terms*—CPS, secure data sharing, access control, information-centric networking, testbed validation**

I. Introduction

Intelligent cyber-physical systems (CPS) integrate the digital and physical worlds, where networks of computational and communication elements seamlessly intertwine with sensors and actuators embedded in real-world physical environments. This allows users to create digital representations or "digital twins," that capture the key attributes and behaviors of the physical system to monitor and control physical processes in real-time [1]. In addition, the explosion of inter-connected devices through the IoT revolution has expanded the scale and complexity of CPS. Consequently, data exchange has become a critical and prominent aspect of CPS operations driven by the need to manage and share high volumes of data that are continuously generated and processed in the system [2].

Given the sensitive nature of data handled by CPS and the critical data-driven services they support, such as smart manufacturing, intelligent transportation, and healthcare, secure data sharing has emerged as a pressing concern. Unauthorized access to sensitive information may compromise the system functionality and tamper with critical data, possibly leading to system-wide operational failures or physical damage [3]. For example, in autonomous vehicles, a security breach can exploit malicious actors to manipulate critical navigation systems, which may in turn lead to accidents or hazardous situations. Thus, robust data protection and access control mechanisms are critical to ensure that data is protected and access is restricted based on services and security requirements [4].

Previous studies [5]–[11] have investigated establishing secure CPS services by addressing its main security goals through various access control solutions, including role-based and attribute-based encryption. However, a key limitation of static access control approaches is the requirement for re-encryption by the data owner whenever access policies change, especially as CPS dynamic policy changes are frequent and unpredictable. The lack of flexible access control prevents existing solutions from enforcing fine-grained and dynamic policies based on specific roles, locations, and diverse attributes in a heterogeneous CPS ecosystem [12].

Furthermore, this re-encryption process introduces additional overhead in network latency and data access time. It becomes problematic in time-sensitive CPS applications, in which low latency is essential for maintaining optimal performance and responsiveness. These limitations underscore the need for more adaptive access control and efficient data-sharing mechanisms capable of handling dynamic policies without compromising the real-time requirements of CPS. Moreover, existing systems are limited by a lack of infrastructure and actual implementation for large-scale deployment, which restricts their effectiveness in real-world CPS applications that demand high scalability and adaptability [13].

To address existing challenges, we introduce a secure data sharing framework for CPS (SDS-CPS) that leverages ciphertext-policy attribute-based proxy re-encryption (CP-ABPRE) [14] to enable fine-grained, flexible, and efficient data access control for data-driven services that demands sensitive data to be securely shared among multiple entities. SDS-CPS allows data owners to enforce strict access control policies, and a proxy can transform ciphertexts encrypted under one access policy into that under another policy without learning plaintext data. It ensures that only authorized entities can access data or control devices and provides dynamic adaptation of access policies while maintaining data confidentiality.

979-8-3315-2096-0/25/$31.00 ©2025 IEEE

A potential limitation of this approach is the increased network overhead and computational delay associated with higher security levels; however, we mitigate this by using information-centric networking (ICN) [15]. ICN reduces the latency and computational costs by efficiently delivering data and caching it closer to users, thereby mitigating redundant transmissions and re-encryption. Unlike existing solutions, we present a first-of-its-kind actual implementation of SDS-CPS and evaluation in a testbed to facilitate a foundation for future research and enable practical CPS applications. The evaluation results prove that SDS-CPS enables efficient and secure data sharing with high scalability and reduced data retrieval time.

Organization. In Section II, we present the system architecture and outline the corresponding adversary models. Section III elaborates on the detailed implementation of SDS-CPS, and Section IV presents an in-depth security analysis and performance assessment conducted on an experimental testbed. Section V provides an extensive review of related work. Finally, the paper is concluded in Section VI.

II. Preliminaries and System Architecture

A. Ciphertext Policy Attribute-based Proxy Re-encryption

Ciphertext policy attribute-based proxy re-encryption (CP-ABPRE) [14] utilizes proxy re-encryption within an attribute-based encryption framework. It adds a layer of flexibility and on-demand data access in sharing encrypted data by enabling a proxy to re-encrypt ciphertext without revealing the underlying plaintext, allowing new recipients with matching attributes to decrypt it. CP-ABPRE consists of the following algorithms to facilitate secure and flexible data access.

1) $(param, msk) \leftarrow \mathsf{Setup}(1^k, \mathcal{U})$: Given a security parameter k and an attribute universe $\mathcal{U}$, the algorithm outputs a public parameter $param$ and a master secret key msk.
2) $sk_S \leftarrow \mathsf{KeyGen}(param, msk, S)$: This algorithm takes $param, msk$ and the attribute set S to generate a private key sk_S, where sk_S is related to S.
3) $rk_{S\rightarrow(M',\rho')} \leftarrow \mathsf{ReKeyGen}(param, sk_S, S, (M', \rho'))$: It inputs $param, sk_S, S$, and an access structure (M', ρ') over $\mathcal{U}$ and outputs a re-encryption key $rk_{S\rightarrow(M',\rho')}$.
4) $C_{(M,\rho)} \leftarrow \mathsf{Enc}(param, (M, \rho), m)$: With inputs $param$ and $(M, \rho) \in \mathcal{U}$, along with a plaintext m, the original ciphertext $C_{(M,\rho)}$ is produced.
5) $C^R_{(M',\rho')} \leftarrow \mathsf{ReEnc}(param, rk_{S\rightarrow(M',\rho')}, C_{(M,\rho)})$: It re-encrypts the original ciphertext $C_{(M,\rho)}$ to a new ciphertext $C^R_{(M',\rho')}$ using inputs $param$ and $rk_{S\rightarrow(M',\rho')}$.
6) $m \leftarrow \mathsf{Dec}(param, S, sk_S, C_{(M,\rho)})$: The algorithm outputs a plaintext m by decrypting an original ciphertext $C_{(M,\rho)}$ with $param, S$, and the private key sk_S.
7) $m \leftarrow \mathsf{Dec_R}(param, S', sk_{S'}, C^R_{(M',\rho')})$: The original plaintext m to be recovered from $C^R_{(M',\rho')}$ by using $param$, an attribute set S', and the private key $sk_{S'}$.

B. Information-centric Networking (ICN)

ICN follows a receiver-driven data-centric model, in contrast to the sender-driven end-to-end delivery model used in traditional networks [15]–[18]. ICN enables data users or applications to initiate a request for data ("Interest" packet) specifying the name of the required information, such as "temperature_sensor/log_1" or "traffic_update/route_1." Then, the corresponding ("Data" packet) is generated by CPS devices or components (e.g., a sensor, actuator, or controller) containing the requested information with the matching name from the Interest packet.

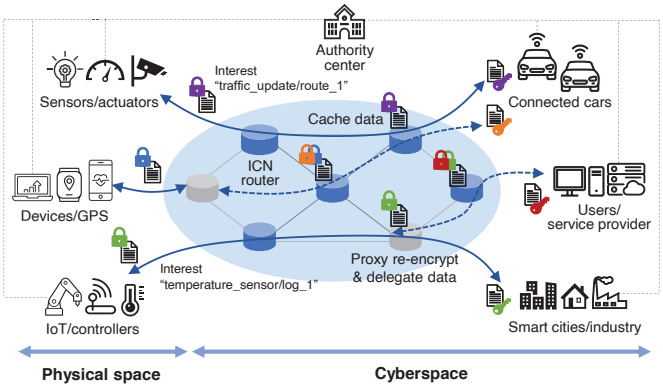

Fig. 1. System model of our proposed SDS-CPS.

Intermediate network nodes (i.e., ICN routers) then use a name-based forwarding mechanism to route packets efficiently within the CPS network, enabling seamless communication and data exchange between various CPS components. Additionally, ICN supports in-network caching to temporarily store data passing through network nodes, which enables faster data retrieval for subsequent identical requests, as data can be served directly from the nearest router's cache rather than the distant source. This results in lower latency and enhanced efficiency in CPS, where real-time data access is critical for the seamless coordination of both physical and cyber components.

C. System Model

Fig. 1 illustrates the system model underlying our proposed SDS-CPS, where each entity has distinct roles and possesses different privileges to execute the algorithms across each phase of the framework, as outlined below.

- *The authority center* initializes the system by generating system parameters and distributing keys to entities.
- CPS devices (*data owners*), such as smart sensors, IoT devices, or mobile nodes, embedded within the physical environment protect their sensitive data in accordance with their predefined access policies.
- *ICN routers* facilitate the forwarding and caching of data as it traverses the network for efficient data distribution within the CPS environment.
- Edge nodes (*proxy servers*) re-encrypt data to align with different users' access rights, enabling secure data delegation based on new policies defined by the data owner.
- *Data users*, such as operators, autonomous systems, or external service providers, with the appropriate access privileges can access and consume data.

D. Security Assumption and Relaxations

We assume that the authority center is trusted to generate system parameters and private keys and manage key distributions without any compromise to guarantee system security. The proxy servers are considered semi-trusted; while they are expected to adhere to the protocol correctly, they may attempt to extract or infer additional information from the data they process. However, they are assumed not to collude with adversaries. Data users are assumed to define and enforce access policies accurately and act within their authorized privileges unless explicitly identified as malicious insiders. To strengthen this assumption, the system allows data owners to update and modify access policies and user privileges dynamically, accommodating real-world CPS scenarios such as changing user attributes. ICN routers follow the protocol for efficient forwarding and caching but may be compromised by adversaries attempting to tamper with cached data.

E. Adversarial Modeling

The system considers a range of adversarial behaviors that may compromise its confidentiality and integrity. External adversaries are modeled as capable of passively eavesdropping on network communications and attempting to compromise ICN routers to tamper with cached data or gain unauthorized access to breach data confidentiality. In addition, malicious insiders (e.g., authorized users or compromised CPS devices) may exploit their access privileges to gain unauthorized access to sensitive data or collude with others to bypass access policies and other control mechanisms.

III. Proposed SDS-CPS Framework

We present SDS-CPS for data-driven services in CPS, where various entities with diverse attributes (e.g., access permissions or operational roles) retrieve sensitive data to enable a secure data sharing scenario where data confidentiality and controlled access are critical. As depicted in Fig. 2, SDS-CPS incorporates the key phases detailed below:

A. Fine-Grained Access Control in Secure Data Sharing

In this phase, the authority center initiates the system by establishing a secure communication network, which executes the algorithm $(p, g, G, G_T, e) \leftarrow \mathsf{Setup}(1^k, \mathcal{U})$ and chooses two random numbers $a, \alpha \in \mathbb{Z}_p^*$, a random generator $g_1 \in G$, to generate system-wide public parameters $param = (p, g, G, G_T, e, g_1, g^a, e(g,g)^\alpha, H_1, H_2, H_3, H_4, H_5, H_6)$, and a master secret key $msk = g^\alpha$. These parameters are subsequently used to issue private keys sk_S for the attribute set S, defined by the data owner, after choosing $t \in_R \mathbb{Z}_p^*$ as follows:

$$K = g^{a \cdot t} \cdot g^\alpha, \quad L = g^t, \quad \forall x \in S \; K_x = H_3(x)^t \tag{1}$$

Considering industrial IoT and smart manufacturing scenarios, sensitive sensor data must be securely shared but not universally accessible because access should be restricted based on user privileges. For instance, detailed temperature logs may be crucial for system administrators and on-site operators to troubleshoot equipment issues, while summarized log extracts could be shared with external analysts for maintenance. To control access to sensitive data and ensure confidentiality, the data owner initially encrypts its data m, such as temperature logs with CP-ABPRE that uses a linear secret sharing scheme access structure (M, ρ). It generates encrypted data $C_{(M,\rho)}$, which can be securely shared with CPS users who satisfy the access policy (e.g., Admin $\vee$ Engineer) (Fig. 2).

Additionally, the data owner attaches its signature to the encrypted ICN Data packet by computing $\sigma = \mathsf{Sign}[sk_{Owner}, name || H(C_{(M,\rho)})]$ to ensure the integrity and authenticity of the original data before sharing. Then, all data users in CPS can initiate a data request by issuing an ICN Interest packet specifying the desired data name (e.g., "temperature_sensor/log_1") to retrieve the relevant information. Upon receiving the Interest packet, the ICN network forwards and retrieves the corresponding encrypted data, and the returned ICN Data packet (e.g., "temperature_sensor/log_1/$< signature : \sigma >/< metadata : pk_{Owner} >/< C_{(M,\rho)} >$") is then strategically placed in the intermediate ICN routers within the CPS to cache and make the data readily accessible for the future requests.

B. Flexible Access Delegation

If the data owner wants to grant access to an operator who needs to review the sensor log while performing on-site repairs, the data owner generates a re-encryption key rk that embeds a new access policy (M', ρ') to delegate data access to (Operator $\wedge$ On-site). It chooses $\theta \in_R \mathbb{Z}_p^*$, $\delta \in_R \{0,1\}^k$, and defines $rk_1 = K^{H_5(\delta)} {g_1}^\theta, rk_2 = g^\theta, rk_3 = L^{H_5(\delta)}, \forall x \in S \; R_x = K_x^{H_5(\delta)}, rk_4 = C_{(M',\rho')}$. By using its private key $sk_{Owner} = (K, L, \forall x \in S \; K_x)$ and the data owner issues rk as follows:

$$rk_{S \to (M',\rho')} = (S, rk_1, rk_2, rk_3, rk_4, R_x) \tag{2}$$

The data owner delegates data re-encryption to the proxy server by sending $rk_{S \to (M',\rho')}$, which is then used to re-encrypt the original ciphertext, generating a new ciphertext that can only be decrypted by users who possess the "Operator" attribute and are physically located "On-site." Through this mechanism, our proposed SDS-CPS ensures dynamic and flexible access control based on specific user attributes.

C. Efficient Data Dissemination

Upon receiving $C_{(M,\rho)}$ and $rk_{S \to (M',\rho')}$ from the data owner, the proxy executes the $\mathsf{ReEnc}()$ algorithm using public parameters and the re-encryption key to transform the original ciphertext $C_{(M,\rho)}$ into a new ciphertext $C^R_{(M',\rho')}$ without decrypting or revealing the plaintext. This transformation allows to delegate access from the original policy to multiple CPS users whose attributes satisfy the newly defined access policy, (M', ρ'), which enables the data owner to efficiently update access policies without re-encrypting the original data. The re-encrypted ciphertext, $C^R_{(M',\rho')}$, is signed with the proxy private key to provide assurance that re-encryption is performed correctly by the authorized proxy as $\sigma' = \mathsf{Sign}[sk_{Proxy}, name || H(C^R_{(M',\rho')})]$.

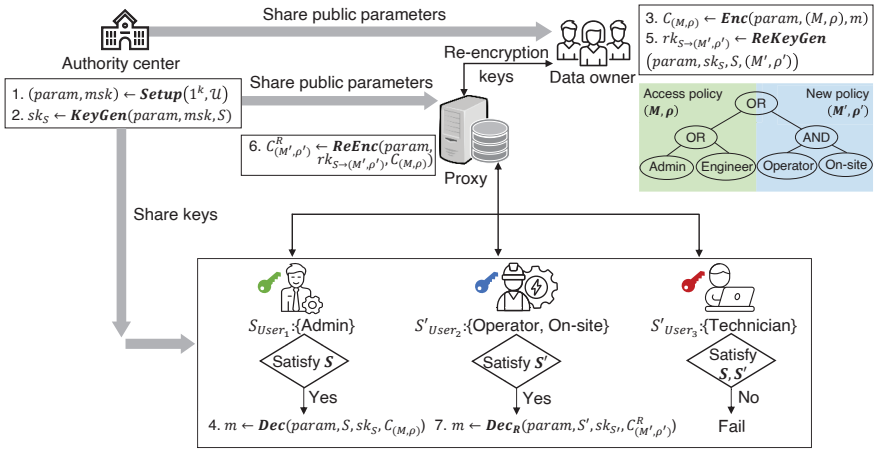

Fig. 2. Detailed access control procedures of SDS-CPS.

Subsequently, the new ciphertext is securely forwarded as an ICN Data packet (e.g., "temperature_sensor/log_1/< $signature : \sigma' >$/< $metadata : pk_{Proxy} >$/< $C^R_{(M',\rho')} >$") and cached at the ICN routers along the path back to the requesting users. It allows efficient data retrieval by authorized CPS components or users, significantly reducing latency and optimizing the network performance, as data can be accessed directly from the nearest cache without requiring repeated re-encryption at the proxy or querying distant data owners.

D. Access-Controlled Data Retrieval and Authentication

Upon receiving the corresponding encrypted data, either the original ciphertext, $C_{(M,\rho)}$, or re-encrypted ciphertext, $C^R_{(M',\rho')}$, from the ICN network, the data user attempts decryption to retrieve the plaintext information. If the user possesses the necessary attribute private key that satisfy the access control policy embedded in the received ciphertext, it can successfully decrypt and access the original sensor data log m. The user employs either the $\mathsf{Dec}()$ algorithm for the original ciphertext with its private key $sk_S = (K, L, \forall x \in S\ K_x)$ or the $\mathsf{Dec_R}()$ algorithm for the re-encrypted ciphertext with the privacy key $sk_{S'} = (K', L', \forall x \in S'\ K'_x)$ to perform the decryption process. Furthermore, users can ensure the integrity of re-encrypted data by verifying the signatures embedded in ICN packets. For the original ciphertext, users can verify as:

$$\mathsf{Verify}\left(pk_{\mathrm{Owner}}, \sigma, \mathrm{name} \,||\, H(C_{(M,\rho)})\right) \stackrel{?}{=} \mathrm{True} \qquad (3)$$

and the re-encrypted ciphertext is verified as:

$$\mathsf{Verify}\left(pk_{\mathrm{Proxy}}, \sigma', \mathrm{name} \,||\, H(C^R_{(M',\rho')})\right) \stackrel{?}{=} \mathrm{True} \qquad (4)$$

In case of an invalid signature, users can generate proofs of unauthorized data alterations or invalid re-encryptions to ensure the trustworthiness and reliability of information shared in the connected CPS. Therefore, the proposed SDS-CPS ensures secure and flexible data sharing among diverse CPS users by allowing the original data to be encrypted only once and enabling dynamic access to the encrypted data without re-encrypting by the data owner or individual key management.

IV. Security and Performance Evaluation

In this section, we demonstrate the effectiveness of SDS-CPS through a comprehensive security and access control analysis, followed by extensive experimental evaluations on an actual distributed testbed environment to assess its efficiency and scalability compared to state-of-the-art solutions.

A. Security and Access Control Analysis

Data Confidentiality: Consider an adversary $\mathcal{A}$ that can eavesdrop on ICN communications or compromise ICN routers or the proxy; it only has access to encrypted data $C_{(M,\rho)}$ or $C^R_{(M',\rho')}$. In SDS-CPS, all data transmitted through the network is encrypted, and CP-ABPRE ensures that only users possessing the necessary attributes defined by the data owner can decrypt the data. The security of SDS-CPS relies on the decisional q-parallel bilinear Diffie-Hellman assumption, which asserts that $\mathcal{A}$ cannot distinguish between $e(g,g)^{a^{q+1}\cdot s}$, where $a, s \in_R \mathbb{Z}_p$ and a random group element. Even if $\mathcal{A}$ gains access to cached data, it cannot recover the original data m without the correct attributes and private keys sk, which prevents unauthorized access and potential misuse.

Access Control Enforcement and Authenticity: SDS-CPS allows the proxy to adapt to changing contexts in CPS and re-encrypt data whenever access requirements change without decrypting the original ciphertext or manipulating the re-encrypted ciphertext. This limits the capacity to learn the original data m by adhering to the principle of least privilege. If a malicious insider attempts to collude with others to bypass the access policies, or if a malicious proxy tries to generate a re-encryption key rk, SDS-CPS ensures that rk are bound to the original encryption parameters and new access policy specified by the data owner, making the adversary impossible to alter the access policy. In the event of a detected breach, the data owner can immediately update the encryption policy and revoke access by invalidating the affected rk, ensuring that the system remains secure and protected from future attempts to exploit access policies. Moreover, by integrating a robust signature within ICN Data packets, SDS-CPS ensures the integrity of both data m and the re-encryption process,

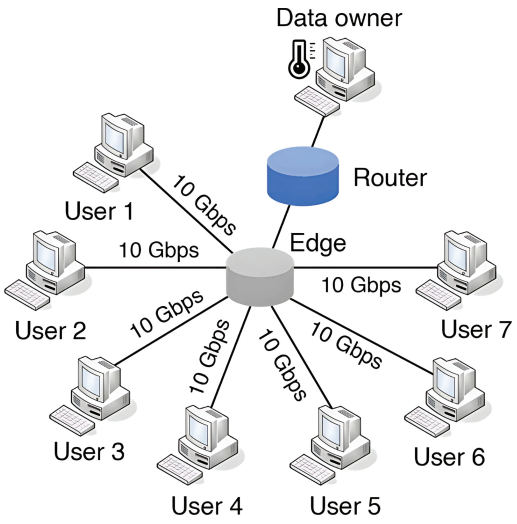

Fig. 3. Experimental scenario on testbed [19].

even if data is delivered through multiple intermediate nodes or retrieved from a cache. Hence, SDS-CPS offers secure and flexible data sharing in CPS by mitigating the adversaries defined in Section II-E.

B. Comprehensive Performance Evaluation and Analysis

1) Implementation and Experimental Testbed: We implemented SDS-CPS and conducted a performance evaluation in a large-scale experiment using a distributed testbed [19] to assess its realistic efficacy. To implement the cryptographic operations of CP-ABPRE, we utilized the Java Pairing-Based Cryptography (jPBC) library [20] with Type A parameters. For ICN functionalities, we employed Cefore [21], [22], an open-source software platform, to forward and receive Interest and Data packets in the network.

Our CPS scenario featured the node group N of testbed with 7 data users with different attributes, each connected to a network of one router and one edge server. The users interacted with a data owner, generating diverse types of sensor log files, each of 10KB. The communication delay on each link was 1.5 ms, with a bandwidth of 10 Gbps. The experimental setup is illustrated in Fig. 3, in which all the nodes were deployed on different virtual machines with the host machine running Ubuntu 20.04.5 LTS on a computer equipped with an Intel Xeon Processor (Cascade Lake) and 16 GB of memory.

2) Computational Efficiency Analysis: We evaluated the processing time of cryptographic operations to compare the efficiency of our security mechanism with that of existing approaches [5], [6]. In all schemes, initial encryption took 5.9 s, while decryption of the original ciphertext required 3.7 s. When access policies change, SDS-CPS reduces re-encryption time to 4.8 s and decryption to 3.2 s by delegating the re-encryption process to the proxy instead of burdening the data owner with re-encrypting the entire data under the new policy.

As depicted in Fig. 4, existing schemes experienced high computational costs, as each attribute change necessitated the

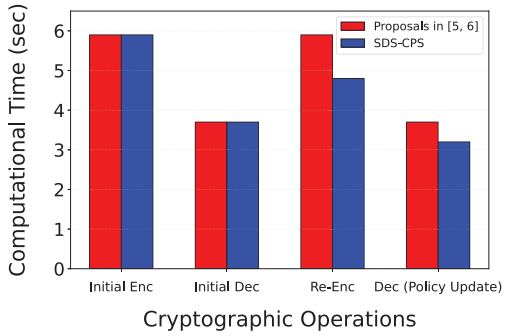

Fig. 4. Performance comparison of cryptographic operations.

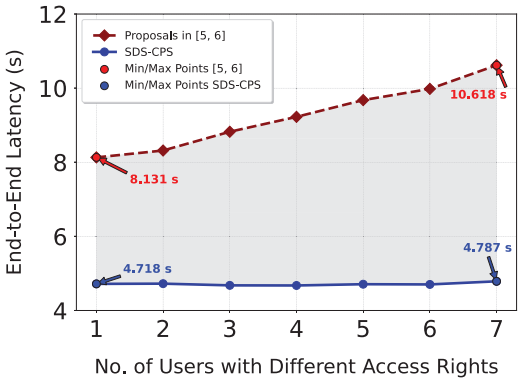

Fig. 5. Average end-to-end latency vs. number of users.

data owner to encrypt data repeatedly, resulting in significant overhead and key management complexity. In contrast, SDS-CPS efficiently managed access policy updates by eliminating the need for full re-encryption by the data owner, which reduced computational costs by balancing the security overhead across the encryption, re-encryption, and decryption processes.

3) Data Retrieval Time: Fig. 5 illustrates the average end-to-end latency per user as the number of users with different access rights increases, measured as the time taken from requesting to receiving the data. The results indicate that SDS-CPS achieved a 40% reduction in latency compared to existing work [5], [6]. This significant improvement is driven by the application of ICN and proxy re-encryption, which minimize communication time for distant data owners, demonstrating its efficiency for data sharing in CPS. On the other hand, state-of-the-art schemes exhibited higher latency due to direct user-to-owner communication and repetitive encryption processes.

V. Related Work

Recent studies have seen considerable progress in investigating the importance of access control needed to ensure the security of CPS [4]. He et al. [5] investigated a lightweight access mechanism for mobile cloud CPS using ciphertext-policy attribute-based encryption and proxy service model. However, its static access policy limits flexibility, as any changes to user permissions require re-encryption of the entire

dataset, making it less adaptable in dynamic CPS scenarios. A flexible attribute-based access control framework for cloud-based CPS is proposed in [6] using decentralized multiauthority ciphertext-policy attribute-based encryption for online authentication and authorization of legitimate entities. The evaluation proves that the system is resilient to attacks with acceptable communication latency.

Tan et al. [7] introduced a blockchain-based access control framework that considers big data in CPS through lightweight symmetric encryption for identity and redefines access control permissions stored on the blockchain to enable secure and private network access. In parallel, a blockchain-based medical data access framework with role-based access control was proposed in [8]. Despite their benefits, the complex certificate management, on-chain/off-chain data synchronization, and role handling processes in large organizations within these systems can compromise data integrity.

In [9], a selective encryption method was designed to protect medical data where end-users controlled access to medical CPS, ensuring security and privacy in untrusted cloud servers. This method outperformed traditional AES in terms of speed when implemented and tested on a smartphone. In [10], a self-healing mechanism based on a practical policy, role-based, and attribute-based access control was presented to guarantee secure interconnection between multiple CPS entities. It introduces a new context parameter for managing perturbation severity and presents the dynamic separation of duties model across different attacks.

Moreover, the work in [11] presented an ICN-based edge-assisted authentication scheme for edge data processing and securing CPS with a delegation model and session handshake through edge routers. Despite the progress from prior studies, notable limitations remain in terms of computational overhead and network delay, particularly in handling the complex access control and dynamic data sharing requirements of heterogeneous CPS environments. Furthermore, there is a significant lack of advancement in translating these innovations into practical implementations, highlighting the gap between theoretical and real-world deployment in large-scale CPS. A more holistic approach to CPS security, incorporating real-world evaluation, is crucial for addressing these limitations and ensuring effective protection for these complex systems.

VI. Conclusion

We propose SDS-CPS, a secure data sharing framework to enable scalable and efficient data-driven services in CPS by combining the advantages of CP-ABPRE with the ICN approach. Our proposal offers fine-grained access control and efficient delegation of decryption rights to multiple entities at the proxy level while ensuring confidentiality in dynamic CPS. The integration of ICN further enhances SDS-CPS's performance by enabling efficient data sharing, thereby reducing latency and improving overall scalability. We implemented SDS-CPS and conducted real-world testbed experiments. Our findings clearly demonstrate that SDS-CPS enables faster data access with minimal computational overhead compared to state-of-the-art solutions. In future work, we will explore enhanced data management strategies to optimize secure data sharing and dynamic resource allocation in complex and heterogeneous CPS ecosystems.

Acknowledgment

This work was partly supported by the JSPS KAKENHI under Grant Numbers 24K20769 and 20H04187.

References

[1] R. Baheti and H. Gill, "Cyber-physical systems," *The impact of control technology*, vol. 12, no. 1, pp. 161–166, 2011.
[2] E. A. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, 2008, pp. 363–369.
[3] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—a survey," *IEEE Internet of Things Journal*, no. 6, 2017.
[4] M. Gupta *et al.*, *Access control models and architectures for IoT and cyber physical systems*. Springer, 2022.
[5] Q. He, N. Zhang, Y. Wei, and Y. Zhang, "Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems," *Computer Networks*, vol. 140, pp. 163–173, 2018.
[6] S. Sciancalepore, G. Piro, D. Caldarola, G. Boggia, and G. Bianchi, "On the design of a decentralized and multiauthority access control scheme in federated and cloud-assisted cyber-physical systems," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5190–5204, 2018.
[7] L. Tan, Shi *et al.*, "A blockchain-based access control framework for cyber-physical-social system big data," *IEEE Access*, vol. 8, 2020.
[8] F. Chen *et al.*, "Data access control based on blockchain in medical cyber physical systems," *Security and Communication Networks*, 2021.
[9] H. Qiu, M. Qiu, M. Liu, and G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 9, pp. 2499–2505, 2020.
[10] C. Alcaraz, J. Lopez, and K.-K. R. Choo, "Resilient interconnection in cyber-physical control systems," *Computers & Security*, vol. 71, 2017.
[11] Y. Lu, D. Wang, M. S. Obaidat, and P. Vijayakumar, "Edge-assisted intelligent device authentication in cyber–physical systems," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3057–3070, 2022.
[12] W. Damm *et al.*, "A reference architecture of human cyber-physical systems – part i: Fundamental concepts," *ACM Trans. Cyber-Phys. Syst.*, vol. 8, no. 1, 2024.
[13] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: analysis, challenges and solutions," *Computers & Security*, vol. 68, 2017.
[14] K. Liang, L. Fang, W. Susilo, and D. S. Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," in *2013 5th international conference on intelligent networking and collaborative systems*. IEEE, 2013, pp. 552–559.
[15] H. Asaeda, K. Matsuzono, Y. Hayamizu, H. H. Hlaing, and A. Ooka, "A survey of information-centric networking: The quest for innovation," *IEICE Trans. on Comm.*, vol. E107.B, no. 1, pp. 139–153, 2024.
[16] M. Mosko, I. Solis, and C. A. Wood, "Content-Centric Networking (CCNx) Messages in TLV Format," RFC 8609, Jul. 2019.
[17] V. Jacobson, Smetters *et al.*, "Networking named content," in *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies*, ser. CoNEXT '09, 2009.
[18] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, p. 66–73, 2014.
[19] "Beyond 5g reliable virtualization infrastructure integrated testbed," https://testbed.nict.go.jp/english/b5gv/, (Hokuriku/Ishikawa), accessed on: Sept 10, 2024.
[20] A. De Caro and V. Iovino, "jpbc: Java pairing based cryptography," in *IEEE Symposium on Computers and Communications (ISCC)*, 2011.
[21] H. Asaeda, A. Ooka, K. Matsuzono, and R. Li, "Cefore: Software platform enabling content-centric networking and beyond," *IEICE Transactions on Communications*, vol. E102.B, no. 9, pp. 1792–1803, 2019.
[22] "Cefore," https://github.com/cefore, accessed on: Sept 10, 2024.