International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A CONSENT-BASED PRIVACY-COMPLAINT PERSONAL DATA SHARING SYSTEM

Varshit Arigela[1], G Uday Kumar[1], Nakka Kranthi[1] , T Rama Krishna[2]

[1]Department of IT, Guru Nanak Institutions Technical Campus, Hyderabad.
[2]Assistant Professor, Department of IT, Guru Nanak Institutions Technical Campus, Hyderabad.

Abstract - In the evolving landscape where personal data holds increasing value, businesses seek insights through data processing, but this poses potential risks to individuals' privacy. While many companies collect consent for direct handling of personal data, a need for transparency and accountability arises to align data processing with obtained consent. This paper presents a novel Consent-Based Privacy-Compliant Personal Data-Sharing System, designed to enhance data quality while adhering to privacy regulations. The system addresses personal data-sharing flows and enterprise requirements, ensuring alignment with privacy frameworks. Through a comprehensive analysis of data-sharing processes and roles within enterprise environments based on established privacy frameworks, this paper outlines system requirements, architecture, and a detailed procedure for a consent-based privacy-compliant processing method, encompassing both compliance and consent checks. To validate the system's feasibility, a prototype is demonstrated, and performance analysis is conducted in both laboratory and real-world environments. This proposal aims to establish a robust framework for privacy-aware personal data sharing, fostering ethical and responsible practices in the evolving data-driven landscape.

Key Words: Data processing, Privacy regulations, Personal data, Ethical data sharing.

1.INTRODUCTION

Advancements in artificial intelligence and data processing technology [1] have enabled data-driven insights, uncovering business potentials and opportunities. Companies are now actively willing to utilize data to operate and expand their businesses. By combining and synthesizing large amounts of high-quality data, companies can gain deeper insights and improve their predictive capabilities. In this aspect, among all types of data, personal data plays a key role in maximizing the value of data in business by giving a basis for understanding and predicting customers' behavior as well as market trends. Thus, companies are making efforts to gather more personal data for their business through various channels. A company's proactive sharing and utilization of personal data can benefit its own business growth. Since it is challenging to have data-driven innovation while protecting privacy [4], the necessity of guidance that can mitigate negative impacts and risks, safeguard data subjects' rights, and enable corporate data utilization has increased. In response to these issues, many governments have implemented legal and regulatory frameworks, including the General Data Protection Regulation (GDPR) in the European Union [5], California Consumer Privacy Act (CCPA) in the United States [6], etc. These laws and regulations aim to protect individuals' personal data by setting rules and guidelines for companies and organizations to collect, process, store, and share personal data. Companies are now obliged to have systems and procedures in place for the legitimate use of personal data. Under the advent of new or more stringent regulatory frameworks, one approach to securely use and share (personal) data is applying privacy-preserving techniques. Applying privacy-preserving technologies (e.g., data anonymization, differential privacy, secure multi-party computation, homomorphic encryption, etc.) [7], [8], [9] can make the sharing parties unable to recognize any personal data By making personal data unidentifiable among the data processing parties, privacy-preserving technology ensures the protection of sensitive or personal data from unauthorized access, disclosure, or misuse. However, such technologies require extra data processing resources and can diminish the value of the data due to the loss of information in quantity and quality. Therefore, it is necessary to handle personal data without privacy-preserving techniques (i.e., handling personal data as it is for obtaining better quality information) in a privacy-compliant manner that supports and protects individuals' rights. To use and share personal data without compromising its quality and quantity while adhering to privacy regulations, it is necessary to consider various privacy-related compliance requirements for companies. Therefore, it is important to build a personal data-sharing system for supporting the data utilization stakeholders, which considers individuals' consent and other privacy compliance requirements. There are several ways to follow privacy compliance requirements (e.g., consent-based, privacy-preserving based, legal-based, etc.); particularly, considering consent-based personal data handling mechanisms draws attention from both academia and industry since new data-related regulations and governance has emphasized individuals' rights and consent management.

personal data-sharing system needs to be implemented to cover the data utilization processes among the data subjects (or data providers), the data controller, the data processor, and the third party (or data requester) according to standards and regulations [5], [10]. Note that, in this paper, the terms ‘‘data subject’’ and ‘‘data provider’’ are used interchangeably, which means that an individual provides

personal data to the data controller and the data processor. Figure 1 (inspired by [10], [11]) shows a general sequence of consent-based privacy-compliant personal data utilization among the actors. The company, which is responsible for providing a service to data

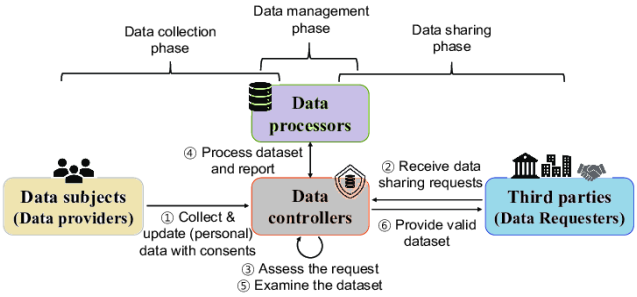

FIGURE 1: A general sequence of a consent-based privacy-compliant personal data utilization.

subjects, acts as a data controller (usually acts as a data processor, too) and obtains personal data with necessary consent from the data subjects (or data providers). While the data controller manages the collected personal data and consent from data providers, it receives many data-sharing requests from data requesters who want to utilize personal data for their own purposes (e.g., internal departments, contracted third parties, or regulatory authorities, etc.). Upon receiving data-sharing requests from data requesters, the data controller assesses the requests. If a data request is acceptable, the data controller instructs the data processor to process the requested dataset in accordance with the obtained consent, applicable requirements, and compliance. After the data processor reports the processing result, the data controller reviews and examines the processed dataset to make a decision. When the data controller decides to share, then the data requester receives a valid dataset.

While the data controller manages the collected personal data and consent from data providers, it receives many data-sharing requests from data requesters who want to utilize personal data for their own purposes (e.g., internal departments, contracted third parties, or regulatory authorities, etc.). Upon receiving data-sharing requests from data requesters, the data controller assesses the requests. If a data request is acceptable, the data controller instructs the data processor to process the requested dataset in accordance with the obtained consent, applicable requirements, and compliance. After the data processor reports the processing result, the data controller reviews and examines the processed dataset to make a decision. When the data controller decides to share, then the data requester receives a valid database.

2. LITERATURE REVIEWS

To support data providers' rights and comply with privacy regulations for sharing personal data with stakeholders, two primary approaches are considered: privacy-preserving-based sharing and consent-based sharing. The main distinction lies in their ability to share raw data. Privacy-preserving-based sharing involves filtering or processing sensitive data, resulting in lower-quality datasets, which simplifies compliance with privacy regulations. Alternatively, consent-based sharing allows for the sharing of raw personal data, albeit with increased complexity in compliance.

Privacy-Preserving-Based Sharing:

This approach involves techniques such as anonymization or pseudonymization to delete or mask sensitive data, resulting in shared datasets containing only non-sensitive information. While this approach simplifies privacy concerns for data providers, it may limit the usefulness of the datasets for data consumers due to reduced information quality. Several studies have explored privacy-preserving big data management models, including schemes for privacy-preserving data aggregation and deep learning-based privacy-preserving data distillation.

Consent-Based Sharing:

With the rise of blockchain technology, many studies have investigated utilizing blockchain characteristics to manage data access consent effectively. However, blockchain-based solutions face performance challenges in real-world implementations. Alternatively, some studies focus on integrating consent management into existing systems, enabling data consumers to access only consented datasets. These approaches include semantic web-based consent management, informed consent management engines, and technical architectures for enforcing consent policies.

The studies discussed highlight the importance of consent-based access management for datasets, including attribute-level access control, which allows for more precise consent management. These approaches demonstrate feasibility in existing database systems but require further validation in real-world environments. This paper proposes a consent-based privacy-compliant personal data-sharing system that considers both the data export process and consent mapping methods for enterprise-level systems, aiming to address privacy concerns effectively in practice.

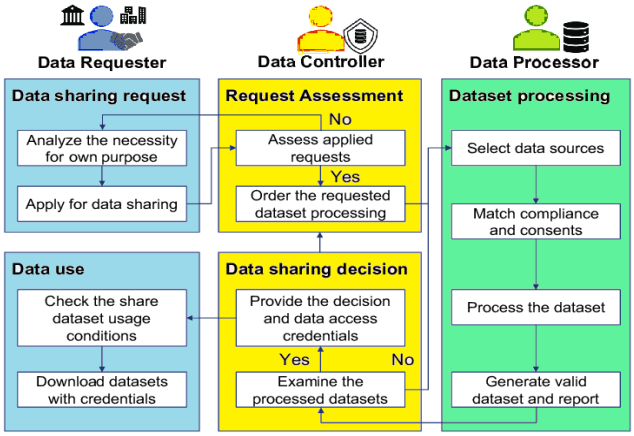

FIGURE 2: A general flow of privacy-complaint enterprise data-sharing.

3. PROPOSED SYSTEM

Since consent management and consent-based personal data processing techniques become important parts of the data utilization process, a consent-based privacy-compliant. A general sequence of a consent-based privacy-compliant personal data utilization. personal data-sharing system needs to be implemented to cover the data utilization processes among the data subjects (or data providers), the data controller, the data processor, and the third party (or data requester) according to standards and regulations. Note that, in this paper, the terms ‘‘data subject’’ and ‘‘data provider’’ are used interchangeably, which means that an individual provides personal data to the data controller and the data processor.

PROPOSED SYSTEM ADVANTAGE

- Enhances individuals' privacy rights and control over their personal data.
- Promotes transparency and accountability in data processing practices.
- Fosters trust between individuals and organizations handling their data.
- Reduces the risk of data breaches and unauthorized access to personal information.

4. PROPOSED TECHNIQUE USED

➢ General Data Protection Regulation (GDPR)

GDPR sets out rules for how organizations must handle personal data, which includes any information that can directly or indirectly identify a person, such as names, addresses, email addresses, and GDPR include requirements for obtaining explicit consent before processing personal data, providing clear and transparent information about data processing activities, implementing appropriate security measures to protect personal data, and granting individual’s rights such as the right to access, rectify, and delete their data.

- This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
- The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system

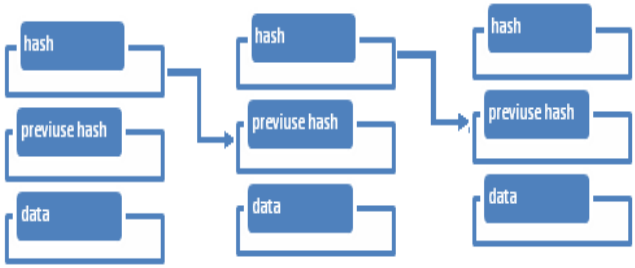

FIGURE 3: Blockchain Generation

4. RESULTS AND DISCUSSION

While the data controller manages the collected personal data and consent from data providers, it receives many data-sharing requests from data requesters who want to utilize personal data for their own purposes (e.g., internal departments, contracted third parties, or regulatory authorities, etc.). Upon receiving data-sharing requests from data requesters, the data controller assesses the requests. If a data request is acceptable, the data controller instructs the data processor to process the requested dataset in accordance with the obtained consent, applicable requirements, and compliance. After the data processor reports the processing result, the data controller reviews and examines the processed dataset to make a decision. When the data controller decides to share, then the data requester receives a valid database.

User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page

Data Requestors

This is the first module. Data Requestors can a register and login with a user id and password. Data requestor has a search

a data with a file name. And send a request to the data processor has a view a data and send a secret key to the requestor then the with a secret key we can view a data.

Data Controller

This is the Second module of this project. In this module has data controller has a register with a user id and password. Data controller has a login with a user id and password. Data controller has a upload a data. Data controller has a upload a view data. Data controller has also a delete a data.

Data Processor

This is the third module of this project. In this module the data processor has a login with a user id and password. Data processor has a generate a keys. The data processor has a check the file and send a keys to the data requestors.

Cloud

This is the fourth module of this project. In this module the cloud has a login with a user id and password. Data processor has a generate a keys. The cloud has a view a data controller's Details and delete the controllers. The Cloud has a view a data requestors details and delete from the database.

4. CONCLUSIONS

Since the issues of utilizing personal data while protecting privacy and data providers' right have focused, many companies now require tools for safely handling personal data. Especially, since identifying whether data is personal data or not becomes more difficult, a data provider's explicit consent on data utilization becomes more important to companies that want to utilize personal data. Therefore, this paper has proposed a consent-based privacy-compliant data sharing system. By analyzing a general process and the roles of actors for data-sharing in an enterprise environment, this paper has proposed system requirements that can support a consent-based privacy-compliant personal data-sharing system.

REFERENCES

1] K. D. C. Adje, A. B. Letaifa, M. Haddad, and O. Habachi, ''Smart city based on open data: A survey,'' IEEE Access, vol. 11, pp. 56726–56748, 2023.

[2] Fortune Business Insights. (Jun. 2023). Big Data Analytics Market Size, Share & COVID-19 Impact Analysis, By Component (Software, Hardware, and Services), By Enterprise Type (Large Enterprises, Small & Medium Enterprises (SMEs)), By Application (Data Discovery and Visualization, Advanced Analytics, and Others), By Vertical (BFSI, Automotive, Telecom/Media, Healthcare, Life Sciences, Retail, Energy & Utility, Government, and Others), and Regional Forecast, 2023–2030. Accessed: Jul. 21, 2023. [Online]. Available: https://www.fortunebusinessinsights.com/big-data-analytics-market106179

[3] G. Malgieri and B. Custers, ''Pricing privacy—The right to know the value of your personal data,'' Comput. Law Secur. Rev., vol. 34, no. 2, pp. 289–303, Apr. 2018.

[4] F. Schäfer, H. Gebauer, C. Gröger, O. Gassmann, and F. Wortmann, ''Datadriven business and data privacy: Challenges and measures for productbased companies,'' Bus. Horizons, vol. 66, no. 4, pp. 493–504, Jul. 2023.

[5] (2018). General Data Protection Regulation (GDPR). Accessed: Jun. 13, 2023. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/ oj

[6] (2023). California Consumer Privacy Act (CCPA). Accessed: Jun. 13, 2023. [Online]. Available:

[7] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, ''Ensuring security and privacy preservation for cloud data services,'' ACM Comput. Surv., vol. 49, no. 1, pp. 1–39, Mar. 2017.

[8] F. N. Wirth, T. Meurers, M. Johns, and F. Prasser, ''Privacy-preserving data sharing infrastructures for medical research: Systematization and comparison,'' BMC Med. Informat. Decis. Making, vol. 21, no. 1, p. 242, Aug. 2021.

[9] R. Podschwadt, D. Takabi, P. Hu, M. H. Rafiei, and Z. Cai, ''A survey of deep learning architectures for privacy-preserving machine learning with fully homomorphic encryption,'' IEEE Access, vol. 10, pp. 117477–117500, 2022.

[10] Information Technology—Security techniques—Privacy Framework, International Organization for Standardization, ISO Central Secretary, Geneva, Switzerland, Standard ISO/IEC 29100:2011, 2017. [Online]. Available:

[11] N. Kim, H. Oh, and J. K. Choi, ''A privacy scoring framework: Automation of privacy compliance and risk evaluation with standard indicators,'' J. King Saud Univ., Comput. Inf. Sci., vol. 35, no. 1, pp. 514–525, Jan. 2023.

[12] J. Zhang and C. Dong, ''Privacy-preserving data aggregation scheme against deletion and tampering attacks from aggregators,'' J. King Saud Univ., Comput. Inf. Sci., vol. 35, no. 4, pp. 100–111, Apr. 2023.

[13] P. Shojaee, Y. Zeng, M. Wahed, A. Seth, R. Jin, and I. Lourentzou, ''Task-driven privacy-preserving data-sharing framework for the industrial internet,'' in Proc. IEEE Int. Conf. Big Data (Big Data), Dec. 2022, pp. 1505–1514.

[14] Z. Xiao, X. Fu, and R. S. M. Goh, ''Data privacy-preserving automation architecture for industrial data exchange in smart cities,'' IEEE Trans. Ind. Informat., vol. 14, no. 6, pp. 2780–2791, Jun. 2018.

[15] G. Wu, S. Wang, Z. Ning, and B. Zhu, ''Privacy-preserved electronic medical record exchanging and sharing: A blockchain-based smart healthcare system,'' IEEE J. Biomed. Health Informat., vol. 26, no. 5, pp. 1917–1927, May 2022.

[16] B. Li and K. He, ''Local generalization and bucketization technique for personalized privacy preservation,'' J. King Saud Univ., Comput. Inf. Sci., vol. 35, no. 1, pp. 393–404, Jan. 2023.

[17] Z. Xu, T. Jiao, Z. Wang, S. Wen, S. Chen, and Y. Xiang, ''AC2M: An automated consent management model for blockchain financial services platform,'' in Proc. IEEE Int. Conf. Smart Data Services (SMDS), Sep. 2021, pp. 33–41.

[18] I. Román-Martínez, J. Calvillo-Arbizu, V. J. Mayor-Gallego, G. Madinabeitia-Luque, A. J. Estepa-Alonso, and R. M. Estepa-Alonso, ''Blockchain-based service-oriented architecture for consent

management, access control, and auditing,'' IEEE Access, vol. 11, pp. 12727–12741, 2023.

[19] E. Olca and O. Can, ''DICON: A domain-independent consent management for personal data protection,'' IEEE Access, vol. 10, pp. 95479–95497, 2022.

[20] C. Pathmabandu, J. Grundy, M. B. Chhetri, and Z. Baig, ''ICME: An informed consent management engine for conformance in smart building environments,'' in Proc. ESEC/FSE. New York, NY, USA: Association for Computing Machinery, Aug. 2021, pp. 1545–1549.

[21] L. Debackere, P. Colpaert, R. Taelman, and R. Verborgh, ''A policyoriented architecture for enforcing consent in solid,'' in Proc. Companion Web Conf. New York, NY, USA: Association for Computing Machinery, Apr. 2022, pp. 516–524.

[22] O. Drien, A. Amarilli, and Y. Amsterdamer, ''Managing consent for data access in shared databases,'' in Proc. IEEE 37th Int. Conf. Data Eng. (ICDE), Apr. 2021, pp. 1949–1954.

[23] G. Konstantinidis, J. Holt, and A. Chapman, ''Enabling personal consent in databases,'' Proc. VLDB Endowment, vol. 15, no. 2, pp. 375–387, Oct. 2021.

[24] C. Matte, N. Bielova, and C. Santos, ''Do cookie banners respect my choice? Measuring legal compliance of banners from IAB Europe's transparency and consent framework,'' in Proc. IEEE Symp. Secur. Privacy (SP), May 2020, pp. 791–809.

[25] T. T. Nguyen, M. Backes, N. Marnau, and B. Stock, ''Share first, ask later (or never?) Studying violations of GDPR's explicit consent in Android apps,'' in Proc. 30th USENIX Secur. Symp. (USENIX Security). Berkeley, CA, USA: USENIX Association, Aug. 2021, pp. 3667–3684.

[26] D. Bollinger, K. Kubicek, C. Cotrini, and D. Basin, ''Automating cookie consent and GDPR violation detection,'' in Proc. 31st USENIX Secur. Symp. (USENIX Security). Boston, MA, USA: USENIX Association, Aug. 2022, pp. 2893–2910.

[27] Information Security Management Systems—Requirements, International Organization for Standardization, ISO Central Secretary, Geneva, Switzerland, Standard ISO/IEC 27001:2022, 2022. [Online]. Available: https://www.iso.org/standard/27001