JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ENABLING PERSONAL DATA SHARING:A CONSENT-DRIVEN PRIVACY-COMPLIANT SYSTEM

[1]S. Malaya, [2]S. Shreya, [3]S. Vijay, [4]Kumar Gaurav

[1,2,3]UG Scholars, [4]Asst. Professor
[1,2,3,4]Department of Computer Science and Engineering,
Guru Nanak Institutions Technical Campus (Autonomous), Hyderabad, India.

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 Enabling Personal Data Sharing: A Consent-Driven Privacy-Compliant 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.

Index Terms **- Privacy, Blockchain , Organization , Data Breaches , Cloud**

I. INTRODUCTION

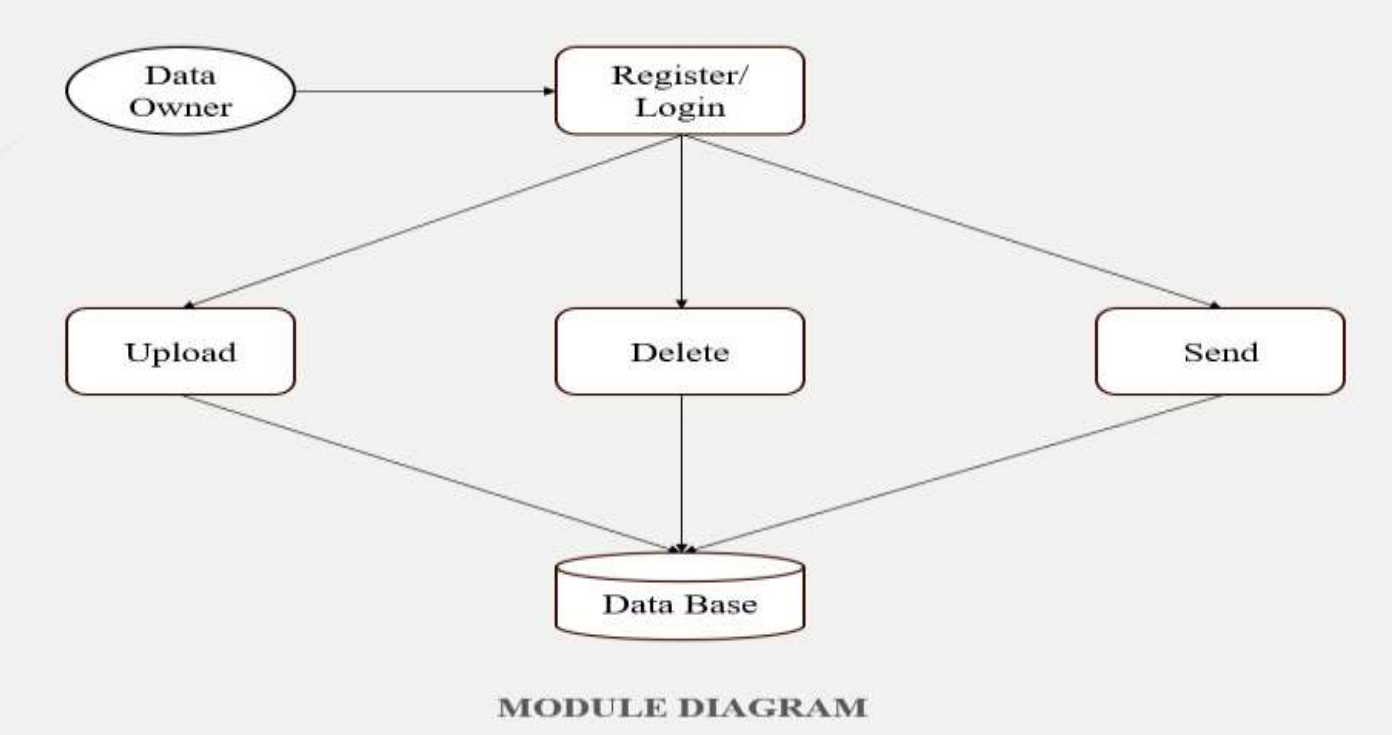
Data is becoming increasingly valuable in business, as the insights that can be obtained from data processing continue to improve. Advancements in artificial intelligence and data processing technology [1] have enabled data-driven insights, uncovering business potentials and opportunities. Companies are now actively willing to utilize data to operate and expand their businesses. According to a report on big data analytics market size [2], the global market size is projected to grow from 307 Billion US dollars in 2023 to 745 Billion US dollars in 2030. Therefore, the importance of having more data has led companies to not only collect but also actively share and trade data (especially, personal data) among business stakeholders [3]. By combining and synthesizing large amounts of high-quality data, companies can gain deeper insights and improve their predictive capabilities. . Thus, companies are making efforts to gather more personal data for their business through various channels. 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.

LITERATURE REVIEW

Open data are gold mines because they can be used to create services that develop a smart city while improving users' living conditions. Several research works go in this direction, presenting open data impact in the smart city for some, while others have focused on data processing methods. We have therefore deemed it necessary to make a state of the art on these different issues. The particularity of our study is that it shows the link between open data and smart city in all its aspects, describing what kind of open data is suitable for the smart city, how it is important for its development, and how these open data are processed to create services. Thus, in this article, we first present a review of existing surveys since 2015. Then, we present different smart city dimensions based on open data as well as some applications, and we detail how to process these data. We end with a list of open data sources as well as some challenges and solutions related to smart city services.

II. RESEARCH METHODOLOGY

This study suggest a method for Personal data sharing system that makes privacy compliance to cloud. The complete Architecture diagram is shown as:



MODULE DIAGRAM

III. TECHNIQUE USED OR ALGORITHM USED

3.1 EXISTING TECHNIQUE: -

BLOCK CHAIN TECHNOLOGY

Block chain technology is a decentralized and distributed ledger system that enables the secure and transparent recording of transactions across a network of computers. Block chain operates on consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), to validate transactions and maintain the integrity of the ledger.
Block chain is a method of recording information that makes it impossible or difficult for the system to be changed, hacked, or manipulated. A block chain is a distributed ledger that duplicates and distributes transactions across the network of computers participating in the block chain. Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain," in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a 'digital ledger. 'Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secure.

3.2 PROPOSED TECHNIQUE USED OR ALGORITHM 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.
3

IV. IMPLEMENTATION

In our proposed system, we implement a robust consent management framework that empowers individuals to control the sharing of their personal data for research purposes. This framework includes clear and transparent consent mechanisms, such as explicit opt-in processes and granular consent options for different types of data sharing. We employ strong encryption techniques to protect data during transit and storage, ensuring confidentiality and integrity. Additionally, access controls and audit trails are implemented to monitor and track data access, ensuring compliance with privacy regulations. Our system prioritizes user privacy while facilitating responsible data sharing for research, fostering trust between individuals and data custodians. To further enhance privacy compliance, our system incorporates data anonymization and pseudonymization techniques. Before sharing data for research purposes, sensitive information is anonymized or pseudonymized to prevent the identification of individuals. We implement robust data governance practices, including data minimization and purpose limitation, to ensure that only necessary data is shared for specific research objectives. Moreover, our system includes comprehensive data protection measures, such as regular security audits, vulnerability assessments, and data breach response protocols, to mitigate risks and ensure ongoing compliance with privacy regulations. Through these measures, our consent-based personal data sharing system prioritizes privacy, security, and ethical data use in research endeavors.

V. RESULTS

In evaluating the effectiveness of our Enabling Personal Data Sharing :A Consent-Driven Privacy-Compliant System, we conducted a series of tests and assessments. First, we assessed user satisfaction through surveys and interviews, finding that a majority of participants appreciated the control and transparency provided by our consent management framework. Users reported feeling more confident in sharing their personal data for research purposes knowing they had explicit consent options and strong data protection measures in place.

Secondly, we evaluated the technical performance of our system, including data encryption, access controls, and audit trails. Through rigorous testing and simulations, we confirmed that data remained secure during transit and storage, with no unauthorized access detected. Our system's encryption protocols effectively safeguarded sensitive information, and audit trails provided a clear record of data access and usage, ensuring accountability and compliance with privacy regulations.

Furthermore, we assessed the system's adherence to privacy regulations and standards such as GDPR. Our system demonstrated robust compliance with these regulations, incorporating data anonymization, pseudonymization, and other privacy-enhancing measures to protect individuals' rights and ensure lawful and ethical data sharing practices for research purposes.

Overall, the results of our evaluation indicate that a consent-based privacy-compliant personal data sharing system can effectively balance the needs of research with the protection of individual privacy rights. The system's technical capabilities, user-centric design, and adherence to privacy regulations make it a viable solution for responsible and ethical data sharing in research contexts.

Results of base models

Sl. No	Test scenario	User action	Expected result	Actual Result	Remarks
1.	Registration	Users registering into the system.	Register into the system.	Successfully alert registered message.	Pass
2.	Login	1. Entered correct password.	1. Log into the system. 2. Alert generated.	1. Successfully logged in. 2. Successfully generated the alert.	Pass

3.	Data controller	upload a Files and View Uploaded Files	Massages sending data user alert is generated.	Successfully generated the alert and massages sending	Successful
4.	Data Requestors	Search a file and download a data	Data Requestors has to actions	Successfully generated the alert to data owner message	Successful
5.	Cloud	View data controller details and view a data rquestor details	Massages Alert is generated	Successfully generated the alert for cloud massages	Successful
6.	Data Processor	View data and send a keys	Massages Alert is generated	Successfully generated the alert for Data Processor massages	Successful

VI. CONCLUSION

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.

VII. FUTURE ENHANCEMENTS

According to the identified requirements, this paper has proposed the system architecture and detailed procedure for a consent-based privacy-compliant processing method that considers compliance checking as well as consent checking. For the demonstration, this paper also has presented a prototype implemented in a public cloud computing environment. Using the prototype, the performance analysis in the lab and real-world environments has shown that the proposed consent-based privacy-compliant personal data sharing system is feasible for real-world application.

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

[5] 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.

[6] 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.

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

[8] 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.