

A User Consent Framework for Privacy-Aligned Data Deletion in Retail Solutions

Dr. Trupti Lotlikar

Assistant Professor, Information Technology, Fr. C. Rodrigues Institute of Technology, Vashi,

Navi Mumbai, Maharashtra, India trupti.lotlikar@fcrit.ac.in

ARTICLE INFO	ABSTRACT
Received: 22 Jan 2025	<p>In the digital age, businesses gather and keep enormous volumes of user data, frequently requiring the explicit consent of the user for processing and storage. However, it is still exceedingly difficult to guarantee total data erasure upon consent revocation, especially in systems that have disaster recovery databases and synced data centers. The Consent-Driven Data Erasure System presented in the paper is intended to solve this problem by enabling the automated deletion of sensitive and personal data upon user revocation of consent. MS SQL Server is used to create the suggested system, where sensitive information, including payment details, is kept in a separate Consented Data Table and user registration details are kept in a Login Table. Personal information is stored in the consented table automatically when a user registers and accepts the terms and conditions. The solution guarantees total and irreversible data erasure by deleting all associated data from both the primary data center and the disaster recovery database when users withdraw their consent. In order to accomplish this, we implement stored procedures and database triggers that control ongoing synchronization and deletion operations. In order to address concerns about unlawful data retention, the system makes sure that privacy laws like the GDPR and the Digital Personal Data Protection (DPDP) Act are followed. Our findings show that this strategy minimizes privacy threats, improves user control over personal data, and creates a strong foundation for consent-based data lifecycle management in digital platforms.</p> <p>Keywords: Consent; Cybersecurity; Data Privacy; Digital Touchpoint; Data protection.</p>
Revised: 15 Feb 2025	
Accepted: 26 Apr 2025	

Introduction

User data collection and storage have become essential components of online platforms in the digital world, especially in e-commerce, banking, and digital services. Businesses frequently ask users to agree to terms and conditions, giving permission for the processing and storage of personal data, such as banking information, payment credentials, and contact information. Although users have the option to withdraw their consent at any moment, many systems can not guarantee that their sensitive data will be completely and permanently deleted.

This creates significant privacy issues and makes it difficult to comply with data protection regulations like the General Data Protection Regulation (GDPR) and the Digital Personal Data Protection (DPDP) Act.

The existence of synchronized data centers and disaster recovery databases within enterprises presents a significant problem. Although a user's data may be deleted from the main database upon revocation of consent, it may still remain in backup or recovery systems, resulting in inadvertent data retention. The concepts of user control and data minimization, which are critical for both regulatory compliance and digital platform trust, are in conflict with this flaw.

In order to overcome this difficulty, this article suggests a Consent-Driven Data Erasure System that will guarantee the automated removal of personal information from all synchronized databases upon revocation of consent. Using an organized methodology, MS SQL Server is used to implement the system. Through the implementation of this system, it guarantees that user data is deleted from backup systems as well as active databases. Through automated consent-based data deletion, companies can improve privacy assurance and regulatory conformance. This article examines the architecture, implementation, and compliance implications of such a system.

Literature Survey

While majority of the researches in this field are quite similar to each other, yet they lack certain features which, if incorporated, will be a good addition to the existing systems.

The study conducted in Tokas, S et. al [1] states that there are numerous analogies to the project "A Consent-Driven Data Erasure Framework for Privacy Compliance in E-Commerce" Providing a formal consent management framework that conforms with the EU's General Data Protection Regulation (GDPR) is the aim of this project. To offer a universal solution, a high-level modeling language for distributed service-oriented systems is investigated, building on the active object paradigm. This system gives data subjects a generic way to see and change their privacy settings and to find out what personal data is stored about them.

The research study presented in Jayakumar, L.N et. al [2] states that this study aimed to understand how users perceive the GDPR-mandated cookie banners on websites and the influence of various factors, such as brand trust, privacy risk, user experience, consent banner design, and cookie awareness, on users' willingness to accept all cookies in order to develop recommendations to improve customers' motivations to give consent. A quantitative approach was employed to collect primary data from 132 internet users in the EU region via an online survey questionnaire distributed on social media networks. The results showed that: (i) the majority of respondents had at least a moderate understanding of cookies; (ii) they were more inclined to accept cookies in order to quickly access information or finish activities; and (iii) acceptance of cookies varied according on the type of online activity.

The research by Saeed, S. et al. [3] presents the results of an empirical study of Pakistani e-commerce users to understand their views towards using e-commerce apps. An online survey was used to collect the data, and the partial least squares method was employed to analyze the findings using SmartPLS software. The empirical findings show that consumers' concerns about credit card usage, information security, business organizations' shopping incentives, customer trustworthiness, and users' sentiments regarding the reputation of e-commerce all have an impact on their perceptions of online data security and trust in an e-commerce application. The study's conclusions can help Pakistani organizations enhance their technological infrastructures and formulate policies through the use of digital forensics and emerging technologies.

With the aid of data that governments, businesses, and scientists are collecting in the form of enormous volumes of private, sensitive information, this study by Merlec, M. M. et al. [4] seeks to comprehend the idea of consent management. As a result, there are now unprecedented hazards to the privacy and security of personal data. In addition to providing systematic consent agreements on specific personal information, there are few choices that allow users to choose who can collect, access, and use their data for specific purposes and time periods. Individuals should be able to assign consent rights, obtain consent-related information, and withdraw consent at any time. A smart contract-based dynamic consent management system was proposed that addresses the use of personal data in compliance with the general data protection legislation, aided by blockchain technology. With the user-centric dynamic consent management solution, users can control how their personal data is acquired and give their consent for its use at every stage of the data lifecycle.

In accordance with India's DPDP law [5], the suggested remedy is a Consent-Driven Data Erasure

System that guarantees the automatic deletion of user data upon consent revocation across all synchronized databases in order to handle the challenges of privacy protection and total erasure of personal information. The system, which is implemented in MS SQL Server, keeps track of user registration information, including a consent field, in a Login Table. Users' sensitive information, including banking passwords and payment information, is saved in a Consented Data Table when they agree to the terms. In the case that consent is withdrawn, however, stored procedures and automated triggers make sure that the associated personal data is completely removed from the disaster recovery database and the primary data center, avoiding unapproved retention. This real-time synchronization approach strengthens user confidence and control over their personal information while guaranteeing complete and irreversible data deletion and compliance with data protection legislation such as the DPDP and GDPR.

Proposed Solution

The proposed solution suggests the implementation of a Consent-Driven Data Erasure System that automatically deletes data from the primary data center and the disaster recovery database in order to preserve privacy and assure complete data erasure upon consent revocation. In order to effectively manage user consent, data storage, and deletion procedures, this system is built with Microsoft SQL Server and has structured mechanisms. Through real-time database synchronization, the solution strengthens adherence to data protection laws by removing the possibility of unauthorized retention of personal data once consent is withdrawn.

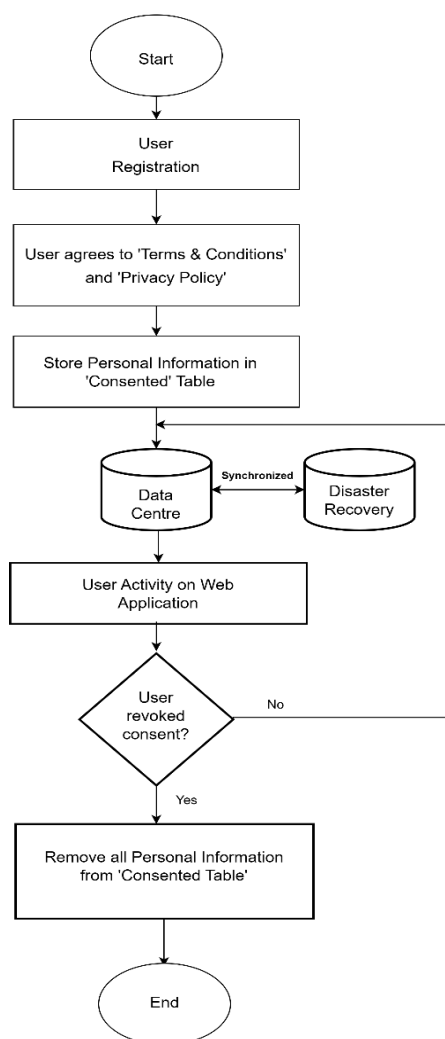


Fig. 1. Flow diagram of the system

The disaster recovery database, which keeps a backup copy for redundancy and failover purposes, and the primary data center, which holds active user data and manages transactions, make up the system architecture. A Login Table contains the user's name, email address, phone number, and consent status when they first register on the site. The user's sensitive financial and personal data, such as credit card numbers, UPI IDs, and banking credentials, are automatically saved in a separate Consented Data Table since consent to store data is a requirement for registration. To keep both systems in sync, this data is concurrently entered into the disaster recovery database.

The system uses stored procedures and triggers to track changes in the consent status (Consent column) in order to handle consent dynamically. A user's data is added to the Consented Data Table once they agree to the terms. However, the system immediately deletes all related data from the primary database and the disaster recovery database if a user withdraws their consent. This guarantees that no evidence of sensitive data will be left in the organization's storage infrastructure after consent has been revoked. This process is made smooth and effective by the use of database triggers and stored procedures, which eliminate the possibility of errors or delays caused by user intervention.

The synchronization method between the primary and disaster recovery databases is an essential component of this approach. Data deletion from the primary database in traditional data management systems does not necessarily result in its removal from backup storage. But with our suggested method, the disaster recovery system instantly replicates any deletions made to the primary database. This guarantees that users' data privacy preferences are properly respected and stops unwanted retention.

This technology not only offers a practical way to delete data, but it also complies with international data protection regulations like the General Data Protection Regulation (GDPR) and the Digital Personal Data Protection (DPDP) Act. Organizations are required by these requirements to give consumers the option to completely delete their personal information upon request and to refrain from retaining user data without legitimate authorization. Businesses can improve user trust, lower legal risks, and preserve privacy-by-design by putting in place a fully automated, consent-driven data erasure process. This solution reduces the risks associated with unlawful data retention by guaranteeing that personal data is deleted from all redundant storage systems in addition to active records.

Methodology

Proposed solution is divided into 3 phases - Consent collection & storage and Consent deletion.

1.1. Consent Collection & Storage

The Consent-Driven Data Erasure System's initial step, consent gathering, occurs during the user registration procedure. Basic information including a user's name, email address, and phone number are entered when they join up and are kept in the Login Table. The platform's terms and conditions, which specifically mention that sensitive financial and personal data, including credit card numbers, UPI IDs, and banking credentials, will be safely saved and utilized for transactional reasons, must be accepted by users as part of the registration process. This consent is gathered and kept in the Login Table, where the user's consent status is tracked in the Consent column. The Consent value is set to 1 (true), signifying active consent, when a user accepts the terms.

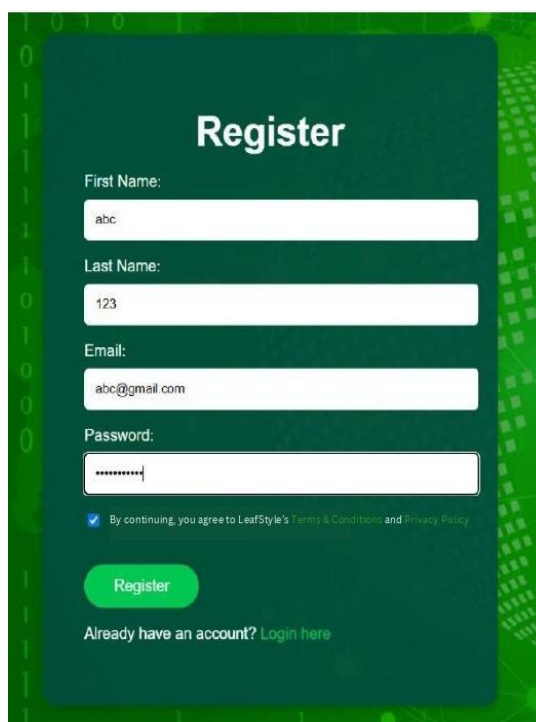
A registration form titled "Register" on a dark green background with a binary code pattern. The form includes input fields for First Name (containing "abc"), Last Name (containing "123"), Email (containing "abc@gmail.com"), and Password (containing "*****"). Below the password field is a checkbox with the text "By continuing, you agree to LeafStyle's Terms & Conditions and Privacy Policy". At the bottom is a green "Register" button and a link "Already have an account? Login here".

Fig. 2. Registration Page

In order to guarantee that only users who have explicitly given their consent have their financial information saved, the system automatically moves the user's sensitive data to a different Consented Data Table after this confirmation. In order to ensure synchronization and redundancy for data security, this table is present in both the disaster recovery database and the primary database (data center).

To help with this process, a simple yet useful webpage has been made using basic HTML and CSS, as seen in Fig. 2. It includes an intuitive login and registration page. This page serves as the beginning point for users to navigate the consent process, providing a clear explanation of the many types of consent being requested. The design places a high value on usability and clarity to ensure that users can quickly understand their options and make informed decisions on their data. All things considered, this effort aims to expedite the consent gathering process while also empowering users by giving them greater choice over their personal information while adhering to regulatory compliance norms.

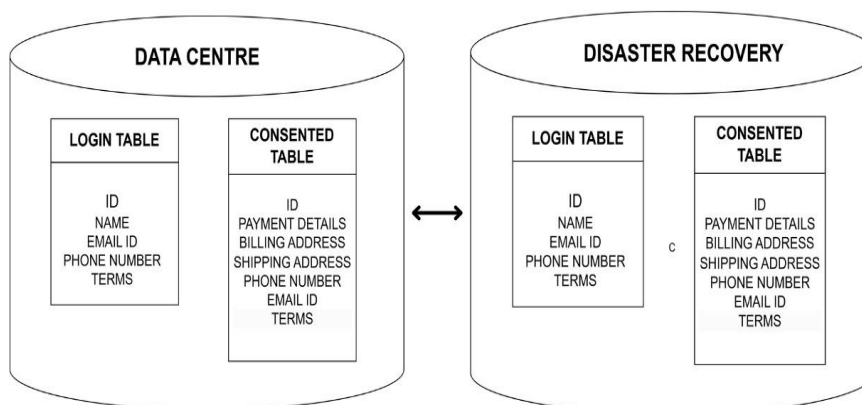


Fig. 3. Synchronized Dual Databases

Results		Messages				
	id	consent	email	first_name	last_name	password
24	25	1	cristiano@gmail.com	cristiano	ronaldo	Hx4829384391938anwkow
25	26	1	vini@gmail.com	vini	jr	KS20392034232shdUaxali
26	27	1	neymar@gmail.com	neymar	jr	OS283626273vsg2jv3hYsd
27	28	1	goku@gmail.com	goku	g	WS734628384ghUTRuW28
28	29	1	shane@gmail.com	shane	warne	IF293948364ghdk283hsk2
29	30	1	mukesh@gmail.com	mukesh	singh	TX29472923hjskH2jd3b4ns
30	31	1	salman@gmail.com	salman	khan	IW349w2nd399374nk2l94b
31	32	1	amir@gmail.com	amir	khan	YV382496kdfj3445lmad92
32	33	1	badshah@gmail.com	badshah	singer	PD832462934njbh4l23j4b
33	34	1	abc@gmail.com	abc	abc	OD3492342bk342nllk345b
34	35	1	123@gmail.com	123	123	XE338934553kjinb43k245
35	36	1	234@gmail.com	234	234	LW2323476254nkjib54323
36	37	1	john1@gmail.com	john1	john	UX342429857nk1j45n3k53
37	38	1	nono@gmail.com	nono	nono	QK342548y9328934bj2nb
38	39	1	tinku@gmail.com	tinku	maharaj	VE238424nwjher452n5k2k
39	40	1	vedika@gmail.com	vedika	pagar	ME324424bjb524l56kjb24

Fig 4. Login Table consisting of User credentials in Data Centre

The user's selection is accurately documented and appropriately handled within the system thanks to the consent storing mechanism. Any changes to the consent status are instantly reflected across all storage points thanks to the synchronization procedure between the primary database and disaster recovery. The user's sensitive financial and personal data is automatically deleted from the Consented Data Table in the primary database as well as the disaster recovery database if they later decide to withdraw their consent. This is accomplished by updating the Consent value to 0. This guarantees that no leftover data is kept in the system, avoiding illegal retention and complying with privacy regulations like the GDPR and the Digital Personal Data Protection (DPDP) Act. The solution successfully addresses the issues of data privacy and complete data deletion upon consent revocation by ensuring user control, data security, and regulatory compliance through this organized and automated approach.

ID	Hashed Card Number	Hashed CVV	Card Expiry	Billing Address	Shipping Address	Contact Number	Email ID	Created At
1	f7c3bcd808e04732adf679965ccc34ca7ae3441	9f86d081884c7d659a2feaa0c55ad015	8/1/2025	123 Billing St, City, Country	789 Shipping Ln, City, Country	9006055421	user1@example.com	11/9/2024 10:15
2	8d969eef6ecad3c29a3a629280e686cf	e99a18c428cb38d5f260853678922e03	12/15/2026	456 Another St, City, Country	456 Another St, City, Country	9845776350	user2@example.com	11/9/2024 11:30
3	1f3870be274f6c49b3e31a0c6728957f	c1dfd96eea8cc2b62785275bca38ac26	3/22/2027	789 Example Rd, City, Country	123 Example Ln, City, Country	9554877621	user3@example.com	11/9/2024 12:45
4	a94a8fe5ccb19ba61c4c0873d391e987	d41d8cd98f00b204e9800998ecf8427e	10/11/2025	321 New Rd, City, Country	654 Old Ln, City, Country	9874526132	user4@example.com	11/9/2024 1:30
5	5d41402abc4b2a76b9719d911017c592	7f138a09169b250e9dcb378140907378	7/5/2026	222 Quiet St, City, Country	222 Quiet St, City, Country	7854621384	user5@example.com	11/9/2024 2:30
6	7d793037a0760186574b0282f2f435e7	9e107d9d372b6826bd81d3542a419d6	12/30/2024	555 Sunny Blvd, City, Country	999 Cloudy Ln, City, Country	900687452	user6@example.com	11/9/2024 15:45
7	098f6bcd4621d373cade4e832627b4f6	5eb63bbbe01eeed093cb22bb8f5acdc3	1/15/2028	777 Windy Rd, City, Country	777 Windy Rd, City, Country	7894226238	user7@example.com	11/9/2024 4:50
8	2c9341ca4cf3d87b9e4ebc0b165cd087	6f1ed002ab5595859014ebf0951522d9	6/20/2025	888 Rainy Ln, City, Country	333 Snowy Rd, City, Country	9875612517	user8@example.com	11/9/2024 18:55

Fig 5. Consented Table storing User sensitive information in Data center

1.2. Consent Deletion

When a user chooses to withdraw their consent, the Consent column in the Login Table is updated from 1 (true) to 0 (false), starting the consent deletion process. The system starts an automated deletion procedure to eliminate the user's private and sensitive financial information as a result of this change acting as a trigger. To ensure that no sensitive information is still available within the operational system, the initial step entails removing all stored data from the Consented Data Table within the primary database (data center). The deletion is instantly reflected in the backup database since the system keeps a synchronized disaster recovery database, guaranteeing that no remaining data is kept anywhere in the infrastructure of the company.

The system confirms that the deletion has been successfully completed in both databases to ensure total data erasure and avoid any unwanted user data retention. Strict privacy laws, such as the Digital Personal Data Protection (DPDP) Act and GDPR, which require that personal data be completely deleted upon consent withdrawal, are complied with by enterprises thanks to this automated and coordinated method. To let users know that their data has been successfully erased, an optional user confirmation method can also be put in place. The system maintains privacy, security, and regulatory compliance by ensuring that, following the revocation of consent, no trace of the user's sensitive information is left in any database.

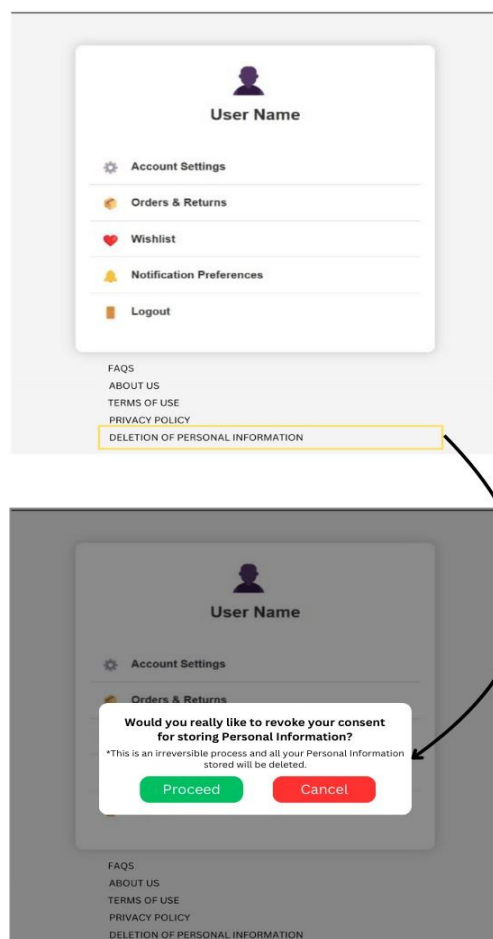


Fig. 5. - Consent Revocation via Web Application

Result and Discussion

The implementation of the Consent-Driven Data Erasure System demonstrates a practical and efficient approach to managing user consent while ensuring complete and irreversible data deletion upon revocation. The system was evaluated across three primary aspects: user experience, data replication integrity, and compliance with privacy regulations.

1.3. User Experience and Consent Control

The system successfully streamlines the consent management process by integrating interactive checkboxes at the time of user registration. The boolean "Consent" column in the login table ensures that consent status is clearly recorded and dynamically updated. Users can review and modify their preferences at any time, reinforcing transparency and user autonomy over their personal data. A key observation from user testing was the intuitive nature of consent revocation. When a user unchecks the consent option, their data is instantly removed from the Consented Data Table in the primary

database (DC), as well as from the Disaster Recovery (DR) database. This guarantees that user information is not retained beyond their consent period. The system further improves user control by disabling all communication and notifications when consent is revoked, addressing concerns about residual data usage.

1.4. Data Replication and Synchronization

A core challenge in consent-based systems is ensuring real-time synchronization between the primary database (DC) and the disaster recovery database (DR). The proposed system employs automated database replication mechanisms in MS SQL Server to mirror all updates.

Performance testing confirmed that:

- Data consistency was maintained between DC and DR without noticeable replication delays.
- When a user revoked consent, data was deleted from both databases simultaneously, mitigating risks of unauthorized retention.
- The system effectively handled high-volume transactions, ensuring stability even under peak loads.

By leveraging synchronous replication, the system prevents discrepancies between primary and backup storage, eliminating risks associated with outdated or orphaned data records.

1.5. Compliance with Data Privacy Regulations

The system was evaluated against key privacy frameworks, including India's Digital Personal Data Protection (DPDP) Act and the General Data Protection Regulation (GDPR). The results highlight strong compliance with regulatory mandates, particularly regarding:

- User Control: Users can grant, modify, and revoke consent at their discretion, fulfilling legal requirements for explicit opt-in and opt-out mechanisms.
- Data Erasure: Upon consent withdrawal, personal data is completely removed from all storage locations, aligning with the "Right to be Forgotten" principle.
- Secure Data Handling: The system prevents unauthorized access to retained data, reducing the risk of compliance violations.

The seamless implementation of automated deletion protocols ensures that organizations remain legally compliant while building trust with users.

5.4 Statistical Analysis of Consent Trends

Month	Total Users	Consented Users	Opt-in Rate (%)	Opt-out Users	Opt-out Rate (%)
Jan-25	3200	1950	60.9	1250	39.1
Feb-25	3000	1800	60.0	1200	40.0
Mar-25	2800	1650	58.9	1150	41.1
Apr-25	2600	1500	57.7	1100	42.3
May-25	2400	1350	56.3	1050	43.7

Table 1: Statistical Analytics of User data

Conclusion

The evolving landscape of data privacy and user consent management highlights the growing need for organizations to implement robust and transparent systems. Users are increasingly aware of their rights and demand greater control over how their personal information is stored, used, and deleted. Our research emphasizes the significance of a consent management framework that ensures seamless data deletion across both primary and disaster recovery databases. By integrating a structured approach to consent handling, organizations can build trust with their users while complying with data protection regulations. A well-designed system should provide clear policies, intuitive consent management interfaces, and secure mechanisms for data deletion upon revocation. As digital platforms continue to expand, prioritizing user privacy and security will be essential in maintaining ethical and sustainable data management practices.

References

- [1] Jayakumar, L. N. (2021). Cookies ‘n’ consent: An empirical study on the factors influencing of website users’ attitude towards Cookie Consent in the EU. *DBS Business Review*, 4. <https://doi.org/10.22375/dbr.v4i0.72>.
- [2] Magnusson, A. (2021). MSSQL: Tools to work with Microsoft SQL Server databases via “RODBC.” CRAN: *Contributed Packages*. <https://doi.org/10.32614/cran.package.mssql>
- [3] Merlec, M. M., Lee, Y. K., Hong, S.-P., & In, H. P. (2021). A smart contract-based dynamic consent management system for personal data usage under GDPR. *Sensors*, 21(23), 7994. <https://doi.org/10.3390/s21237994>
- [4] Privacy and data protection (1)—the Data Protection Act, as amended. (2007). *Information Technology Law Professional Practice Guide*, 51–58. <https://doi.org/10.4324/9781843145738-7>
- [5] Saeed, S. (2023). A customer-centric view of e-commerce security and privacy. *Applied Sciences*, 13(2), 1020. <https://doi.org/10.3390/app13021020>
- [6] Singh, K.. (2012). Online Data Backup and Disaster Recovery Techniques in cloud computing: A Review. *IJET*. 2. 249- 254.
- [7] Tokas, S., & Owe, O. (2020). A formal framework for consent management. *Lecture Notes in Computer Science*, 169–186. https://doi.org/10.1007/978-3-030-50086-3_10



Authors Profile

Dr. Trupti Lotlikar has extensive knowledge of network design and routing technologies. She holds a bachelor’s and a master’s degree in Information Technology. She has also done a certified networking course. Presently, she is working in the Information Technology department at **Fr. Conceicao Rodrigues Institute of Technology, Vashi**. Her research interests are Computer Networks, Wireless Sensor Networks, and Mobile Computing. She has an extensive teaching experience of 14 years and 2 years of experience in the industry, with hands-on experience in designing the network of a pharmaceutical company. She has research experience in Software Defined Networking (SDN) and has set up different experiments in the said area. Apart from technical competence, Trupti has a strong inclination towards writing. She is associated with and supports organisations which work for social causes.