International Journal of Engineering and Techniques - Volume 12 Issue 2, March-April - 2026

RESEARCH ARTICLE OPEN ACCESS

Consent Management System DPDPA 2023

J.Premalatha[1], R.S. Saran[2], Raama Arun Prakash[3], P. Prathiusha[4], K.Reshma[5]

[1] *Professor, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu – 613006, India*
Email: spdhpremasasi1977@gmail.com

[2]*UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu – 613006, India*
Email: saaisaran1212@gmail.com

[3] *UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu 613006, India*
Email: raamaarunprakash2005@gmail.com

[4]*UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu – 613006, India*
Email: prathiusha004@gmail.com

[5]*UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu – 613006, India*
Email: reshmakaliyaperumal02@gmail.com

Abstract:

The rapid growth of digital systems has led organizations to store large volumes of sensitive information, including Personally Identifiable Information. Improper handling of such data can result in privacy breaches and significant security risks. This paper presents a Data Privacy Enforcement Tool that focuses on protecting sensitive data using data masking techniques. The proposed system identifies PII fields within datasets and applies masking methods such as partial masking, character replacement and format-preserving masking to conceal confidential information while retaining its usability.

The system is implemented using a Django-based backend and a React-based web interface, allowing users to upload datasets, configure masking rules and export the protected data in formats such as CSV, JSON and Excel. By restricting the solution to data masking, the tool ensures simplicity, efficiency and ease of integration into existing data workflows.

Experimental results demonstrate that the proposed approach effectively protects sensitive information while maintaining the structural integrity and usability of the data for analysis and testing purposes.

***Keywords*— Data Privacy, Data Masking, Personally Identifiable Information, Data Security**

I. INTRODUCTION:

The digital technologies and internet-based services has significantly increased the collection, storage, and processing of personal data across various sectors. Organizations rely heavily on this data for providing personalized services, analytics, and decision-making. However, this extensive data usage has raised serious concerns regarding privacy, security, and unauthorized access. Data breaches and misuse of sensitive information have become common, highlighting the need for strong data protection mechanisms and regulatory frameworks. To address these challenges, the Digital Personal Data Protection Act (DPDPA) 2023 was introduced in India to ensure the lawful, fair, and transparent processing of personal data while safeguarding individual rights .A key principle of the DPDPA is consent-based data processing, where individuals, known as Data Principals, must provide explicit permission before their data is collected or used. This project presents a Consent Management System (CMS)

designed to handle the complete lifecycle of user consent in a secure and efficient manner. The system enables users to grant, view, modify, and withdraw consent, while Data Fiduciaries can request and process data based on clearly defined purposes. It incorporates essential security features such as authentication, role-based access control (RBAC), encryption, and audit logging to ensure data protection and accountability. Additionally, the system supports real-time consent tracking, automated validation, and grievance redressal mechanisms, improving transparency and compliance. By aligning with DPDPA principles, the CMS reduces legal risks, enhances trust, and promotes a privacy-centric digital ecosystem.

II. RELATED WORK:

Emre Olca and Özgü Can [1] proposed DICON, a domain-independent consent management framework that ensures structured and compliant handling of user consent. The system separates consent management from application logic, making it reusable across domains such as healthcare, finance, and e-commerce. It emphasizes transparency and user control over personal data. Users can easily grant, review, and withdraw consent. The framework supports auditability and traceability of consent records. This helps organizations demonstrate regulatory compliance. It also improves accountability in data processing. Overall, the model is scalable and standardized. It strengthens privacy-preserving system design.

Prof. (Dr.) Vani Bhushan [2] analyzed the Digital Personal Data Protection Act (DPDP) 2023, focusing on key principles such as lawful processing, consent-based data collection, purpose limitation, and data minimization. The paper highlights how the Act empowers individuals by providing rights to access, correct, and erase personal data. It also includes grievance redressal mechanisms for users. The study discusses the responsibilities of data fiduciaries in ensuring data security and transparency. Regulatory authorities and penalties for non-compliance are explained. The Act enforces accountability in data processing. It strengthens user trust in digital systems. Overall, it promotes a privacy-centric ecosystem.

Nikos Kyriakoulis and Charis Dimopoulos [3] proposed CONSENTIS, an identity and consent management framework aligned with EU digital strategies. The system addresses challenges in identity verification, consent collection, and secure data sharing. It enables users to manage digital identities while controlling their personal data. The framework emphasizes transparency and user autonomy. Users can grant, monitor, and withdraw consent easily. It supports secure authentication mechanisms. Standardized consent records improve accountability. It ensures compliance with privacy regulations. Overall, it enhances trust in cross-border digital ecosystems.

Yucheng Wang and Yong Yu [4] proposed a consent-based personal data-sharing system that ensures data is shared only with explicit user permission. The paper highlights growing privacy concerns due to digital data exchange. The system focuses on consent management and access control. It allows users to define how their data is used and who can access it. Secure data handling prevents unauthorized sharing. The system maintains records of consent and transactions. This improves transparency and accountability. It supports regulatory compliance. Overall, it enables secure and privacy-aware data sharing.

Multiple authors [5] examined challenges in implementing informed consent in digital environments. The paper identifies issues such as complex privacy policies, lack of user understanding, consent fatigue, and dark patterns. It highlights that users often give consent without full awareness. Technical limitations in consent management are also discussed. The study emphasizes regulatory requirements like transparency and user control. It proposes solutions such as simplified interfaces and layered notices. User dashboards and dynamic consent models are suggested. Automated systems improve consent handling. Overall, it enhances usability and privacy protection.

Watcharinthorn Neamhom and Chetneti Srisaan [6] proposed a smart contract-based consent management system using blockchain technology. The approach automates consent recording, verification, and enforcement. Smart contracts ensure data is accessed only under agreed conditions. Blockchain provides immutability and decentralization. This improves trust, security, and accountability. Consent records cannot be altered without authorization. The system supports transparency and auditability. Users can securely manage their consent. Organizations can demonstrate compliance effectively. Overall, it offers a tamper-resistant consent framework.

Aditya Sushant Jain [7] analyzed Consent Managers under the DPDP Act 2023, focusing on architecture, business models, and incentive alignment. The paper explains their role as intermediaries between Data Principals and Data Fiduciaries. It ensures lawful, transparent, and accountable consent management. Users can give, review, and withdraw consent easily. The study discusses platform architecture and design. It also explores revenue models and sustainability. Regulatory compliance requirements are addressed. Incentive alignment ensures trust and neutrality. Overall, it strengthens governance and user autonomy.

Mohamed Moussa Madine and Al-Hammadi [8] proposed a fully decentralized multi-party consent management system for healthcare data sharing. The framework addresses secure sharing of patient records among multiple entities. It uses blockchain to eliminate

central control and improve transparency. The system enhances security and trust. Patients can grant, monitor, and revoke consent dynamically. It ensures controlled and auditable access to sensitive data. The model improves data integrity and prevents unauthorized access. It supports compliance with healthcare regulations. Overall, it provides a scalable and patient-centric solution.

III. PROPOSED METHODOLOGY

The proposed system is a secure, centralized web-based application designed to manage the complete consent lifecycle in compliance with the DPDPA 2023.It enables Data Principals to give, view, update, or withdraw consent at any time, while Data Fiduciaries can collect time-stamped consent and generate audit logs. The system implements role-based access control (RBAC) for Data Principals, Data Fiduciaries, and Data Protection Officers, ensuring transparency, accountability, and secure storage of consent records. Additionally, the system provides real-time consent tracking and automated consent validation to ensure that data processing activities strictly follow user permissions. It includes grievance redressal mechanisms with SLA monitoring, allowing users to raise and track complaints efficiently. Advanced security features such as data encryption, secure authentication, and activity logging protect against unauthorized access and data breaches. The system also supports consent history management and data access audit logs, enabling organizations to demonstrate compliance during audits. Overall, the system improves user trust, regulatory compliance, and operational efficiency by centralizing and securing all consent-related process

a. System Overview

The architecture consists of key modules including Data Principal Management, Consent Request Handling, Consent Lifecycle Management, Grievance Redressal and Compliance Monitoring. Each module performs a specific function, contributing to the overall effectiveness of the system. The Consent Management module enables Data Principals to provide, review and withdraw consent using user-friendly interfaces, while the Data Fiduciary module creates and manages purpose-based consent requests and processes data accordingly. The system incorporates security mechanisms such as Role-Based Access Control and Row-Level Security to protect sensitive information and prevent unauthorized access. The system ensures that all consent records are securely maintained with audit logs and can be effectively used for compliance monitoring, reporting and regulatory purposes.

b. Authentication (RBAC)

The Authentication module is responsible for ensuring secure access to the system by validating user identity and controlling permissions based on predefined roles. The system implements Role-Based Access Control (RBAC), where users are assigned specific roles such as Data Principal, Data Fiduciary, Data Processor and Data Protection Officer, each with different levels of access. This ensures that only authorized users can manage consent, process data or access sensitive information within the system. The module manages login credentials and enforces secure authentication mechanisms to prevent unauthorized access. It also restricts sensitive operations based on user privileges, enhancing overall system security. By controlling access to critical functionalities, this module ensures that consent management processes are performed only by authorized personnel. The Authentication module plays a vital role in maintaining data security and system integrity.

c. Project Creation

The Project Creation module allows users to organize and manage consent-related activities by creating separate projects within the system. Each project acts as an independent workspace where users can manage Data Principals, define purposes, and handle consent requests. This modular approach helps in handling multiple projects efficiently without mixing configurations or records. Users can define project-specific settings, including project name, purpose definitions, data categories, and consent duration. The module ensures that all operations such as consent collection, approval and withdrawal are performed within the selected project context. It also helps in maintaining proper organization and traceability of consent records. By providing a structured environment, this module improves usability and workflow management. Overall, the Project Creation module enhances the flexibility and scalability of the system.

d. Database Connection

The system focuses on establishing a secure connection with the backend database and managing consent-related data for further processing. The system enables users to configure database connection parameters through the application interface. Once the connection is successfully established, the system retrieves required data such as user records, consent details, and audit logs for processing and monitoring. During this stage, several important operations are performed, including:

- Database Configuration: The system is configured with database details such as database type, host address, port number, database name

and authentication credentials through the application setup.

- Connection Validation: The backend verifies the provided credentials and establishes a secure connection with the database server to ensure accessibility and reliability.
- Schema Retrieval: After a successful connection, the system fetches metadata information such as available tables, fields and data structures related to users, consent records and system logs.
- Data Retrieval: The system retrieves relevant data such as consent records, user details and transaction logs required for system operations and monitoring.
- Data Preparation: The collected data is organized and structured for further processing such as consent lifecycle management, audit logging and compliance tracking.

e. Consent Capture

The system focuses on capturing and managing user consent securely for further processing and compliance. The system enables Data Fiduciaries to create consent requests and allows Data Principals to review, approve, or reject them through the application interface. Once the consent is provided, the system records and processes it for monitoring, audit, and regulatory purposes. During this stage, several important operations are performed, including:

- Consent Request Creation: The Data Fiduciary defines consent details such as purpose, data categories, and duration through the system interface. The system presents the consent request clearly to the Data Principal, ensuring transparency and understanding.
- Consent Decision: The Data Principal reviews the request and provides consent by approving or rejecting it.
- Schema Validation: The system validates the consent data against predefined formats and rules to ensure correctness and completeness.
- Non-Repudiation: The system ensures that consent actions cannot be denied by maintaining secure and verifiable records.
- Data Storage (ORM/SQL): The consent data is processed using ORM and stored in the database using SQL queries.
- Audit Logging: All consent-related activities are recorded in secure logs for traceability, monitoring, and compliance.

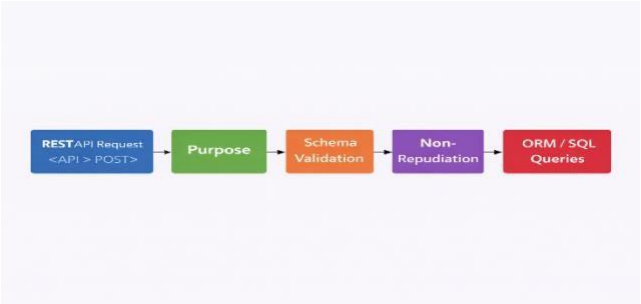

Fig 1. Consent Capture

Purpose:

- Marketing Communication
- Contract Performance
- Legal Obligation
- Legitimate Interest

a. Marketing communication
Processing personal data to send promotional messages, offers, and updates to users. It requires explicit consent and allows users to opt-in or withdraw at any time.

b. Contract performance
Processing personal data necessary to full fill a contract or provide agreed services. It ensures data is used only for service execution and not beyond the contract scope.

c. Legal Obligation
Processing personal data required to comply with legal and regulatory requirements. It includes activities like KYC, tax reporting, and maintaining records for audits.

d. Legitimate Interest
Processing personal data for business needs such as fraud detection, security, and analytics. It requires balancing organizational interests with user privacy and rights.

f. Consent Validation & Lifecycle Module

The system focuses on validating user consent and managing its complete lifecycle to ensure that personal data is accessed only when valid consent exists. Before any data processing, the system verifies whether consent has been granted for the specific purpose and data category. The module manages different consent states such as requested, approved, active, withdrawn, and expired. Data processing is allowed only when consent is active, while access is blocked if consent is withdrawn or expired, ensuring compliance with DPDP Act 2023.During this stage, several important operations are performed, including:

- Consent Validation: The system verifies whether

valid consent exists before allowing any data access or processing.

- Consent State Management: The system manages lifecycle states such as Requested, Approved, Active, Withdrawn, and Expired.
- Consent Record Creation: When consent is approved, the system creates a record storing details such as User ID, purpose, duration, and status using ORM and SQL queries.
- Access Control Enforcement: The backend checks consent status before processing data and allows access only when consent is active.
- Consent Revocation Handling: Users can withdraw consent through secure APIs, and the system updates the status to withdrawn, stopping further processing.
- Expiration Monitoring: The system tracks consent validity periods and automatically updates expired consents, preventing unauthorized data usage.

Fig 2.Consent Validation

g. Audit Log & Compliance Reporting

The system focuses on recording system activities such as authentication, consent actions, and data access for monitoring and compliance. It ensures that all events are securely logged and can be used for auditing, tracking, and regulatory reporting purposes. During this stage, several important operations are performed, including:

- Event Monitoring**:** The system tracks critical ev ents such as login, consent approval, data access, and grievance handling.
- Metadata Capture**:** Each log stores details like user ID, action type, timestamp, and IP address.
- Log Storage**:** Event records are stored securely in structured audit log tables.
- Audit Retrieval**:** Administrators can access logs using APIs with filtering and pagination.
- Compliance Reporting**:** Audit logs are used to generate reports for regulatory compliance and audits.

IV. SYSTEM ARCHITECTURE

The system architecture is designed as a modular framework consisting of Data Principal, Data Fiduciary, Consent Management System, Database, and Data Protection Officer (DPO). The Data Fiduciary initiates consent requests, which are validated and stored by the system and forwarded to the Data Principal for review. The Data Principal can approve or reject the request, and the system updates the consent status accordingly. If approved, data is shared; otherwise, processing is restricted. All activities are recorded in the database and audit logs to ensure security, transparency, and compliance.

a. Data Principal

The Data Principal is the individual whose personal data is collected and processed by the system. They have full control over their personal data and how it is used. The Data Principal can provide, review, modify, or withdraw consent at any time. They also have rights such as data access, correction, erasure, and portability. This ensures transparency and protects user privacy under data protection laws.

b. Data Fiduciary

The Data Fiduciary is the organization or entity that collects and processes personal data. It determines the purpose and means of data processing. The fiduciary is responsible for obtaining valid consent from users before processing data. It must ensure data security, privacy, and compliance with regulations like DPDP Act 2023. It is also accountable for any misuse or breach of personal data.

c. Consent Management System (CMS)

The Consent Management System is a platform used to manage user consent throughout its lifecycle. It allows users to give, review, update, or withdraw consent easily. The system ensures secure storage and tracking of consent records. It supports compliance by maintaining audit logs and monitoring activities. It enhances transparency and trust between users and organizations.

d. Data Protection Officer

The Data Protection Officer is responsible for ensuring compliance with data protection laws. They monitor how personal data is collected, processed, and stored within the organization. The DPO conducts audits, manages risks, and handles data protection issues. They also act as a point of contact between the organization and regulatory authorities.

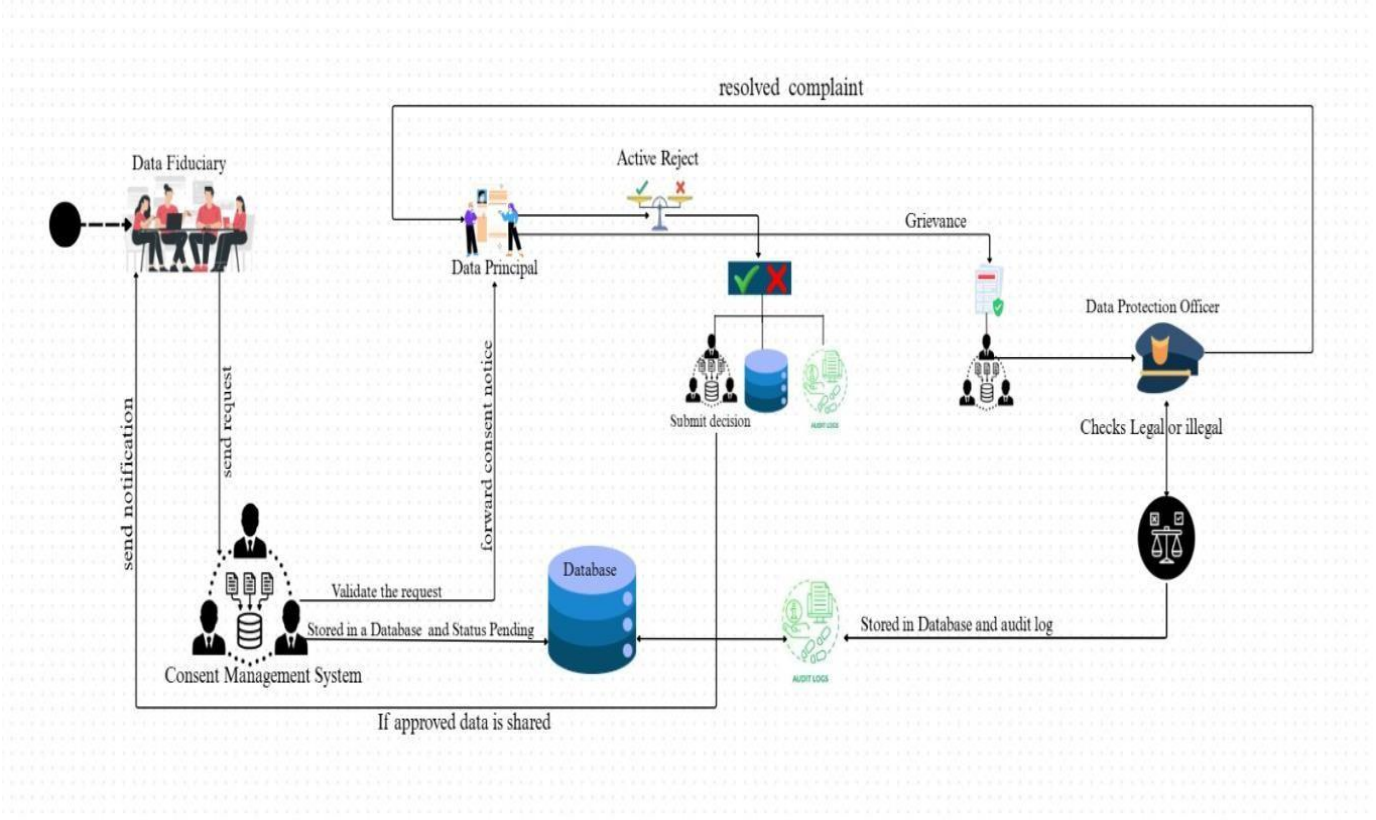

Fig 3. Architecture Diagram

V. CONCLUSION

The Consent Management System developed in this project provides a secure and structured platform for managing personal data in compliance with the Digital Personal Data Protection Act (DPDP) 2023. The system ensures that personal data is processed only after obtaining proper consent, with a clear workflow for consent requests, approvals, and withdrawals. It enhances transparency, accountability, and user control over personal data. The platform also supports grievance handling, audit logging, and compliance monitoring to ensure regulatory adherence. By integrating role-based access control and complete consent lifecycle management, the system strengthens data security and prevents unauthorized access. Overall, the project demonstrates an effective approach to building a privacy-focused and compliant data management system.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to their project guide and faculty members of the Department of Computer Science and Engineering for their continuous support, valuable guidance, and encouragement throughout this research work.

The authors also extend their thanks to their external guide, Mr. T. Siva, from Cybersecurity Nerds Lab, for providing valuable insights, technical guidance and necessary resources that contributed to the successful completion of this work.

Additionally, the authors acknowledge the use of publicly available datasets and tools that supported the development and evaluation of the proposed system.

REFERENCES

[1] E. Olca and O. Can, "DICON: A Domain-Independent Consent Management Framework for Personal Data Protection," *IEEE International Conference on Data Security and Privacy*, 2022.
[2] V. Bhushan, "Empowering Individuals: A Deep Dive into the Digital Personal Data Protection Act, 2023," *Journal of Data Protection and Privacy*, 2024.
[3] N. Kyriakoulis, "CONSENTIS – An Innovative Framework for Identity and Consent Management for EU Digital and Data Strategies," *International Journal of Information Security*, 2025.
[4] Y. Wang and Y. Yu, "A Consent-Based Privacy-Compliant Personal Data-Sharing System," *IEEE Access*, 2019.
[5] W. Neamhom, "Smart Contract-Based Consent Management System for Data Privacy Protection," *Proceedings of Blockchain Technology Conference*, 2024.
[6] A. S. Jain, "Decoding Consent Managers under the

Digital Personal Data Protection Act, 2023: Empowerment Architecture, Business Models and Incentive Alignment," *Data Governance Review*, 2025.
[7] M. M. Madine *et al*., "Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records," *IEEE Journal of Biomedical and Health Informatics*, 2020.
[8] Multiple Authors, "Challenges and Solutions in Implementing Informed Consent in Digital Environments: A Scoping Review," *Journal of Digital Ethics and Privacy*, 2025.
[9] European Union Agency for Cybersecurity (ENISA), "Privacy by Design in Consent Management Systems," *ENISA Technical Report*, 2023.
[10] National e-Governance Division (NGD), "Business Requirement Document for Consent Management System under the DPDP Act, 2023," *Government of India*, 2023.