IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15190

ConsentGuard: Digital Consent Tracker

Prof. Smita K. Thakare [1], Ms. Monali Arjun Kokate[2], Ms. Sanjeevani Pradeep Khairnar[3], Ms. Snehal Satish Kedar[4], Ms. Pinal Dineshbhai Lagdhir[5]

Information Technology, Pune Vidyarthi Griha's College of Engineering and Shrikrushna S. Dhamankar Institute of Management, Nashik, India[1-5]

Abstract: In the digital era, users often provide consent on online platforms without fully understanding the implications of privacy policies and data-sharing terms. The Digital Consent Tracker aims to solve this issue using Artificial Intelligence (AI) and Natural Language Processing (NLP). The system extracts key points from lengthy privacy agreements, generates userfriendly summaries, and categorizes them into areas such as data collection, thirdparty sharing, data retention, and user rights. It offers a web dashboard and browser extension to help users instantly review simplified versions of consent documents. This approach promotes transparency, improves user awareness, and encourages ethical data-handling practices. Overall, this project demonstrates how AI-driven solutions can support informed decision-making, build user trust, and align with global privacy regulations such as GDPR and CCPA.

Keywords: AI, NLP, Privacy Policy, Digital Consent, Data Protection, GDPR, CCPA, Summarization, Browser Extension, User Awareness.

I. INTRODUCTION

In today's digital age, individuals continuously interact with online platforms such as websites, mobile applications, and social media networks. During these interactions, users are required to accept various Terms Conditions, Privacy Policies, and Cookie Consent Notices. Such consents are legally mandated under global data protection regulations including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). However, most users accept these agreements without reading or understanding them. The documents typically contain lengthy legal and technical language, making them difficult for non-technical users to comprehend. Consequently, users remain unaware of what personal data is being collected, how it is processed, and whether it is shared with third parties. This results in privacy risks, a lack of transparency, and reduced control over user data. Additionally, users often provide multiple consents across different platforms without a centralized mechanism to monitor or manage them. Revoking permissions or deleting accounts usually requires navigating through each platform individually, making the process inefficient and confusing. To overcome these challenges, the Digital Consent Tracker introduces an AIpowered and user-friendly approach for managing online consents. The system acts as a personal privacy manager that automatically detects, extracts, summarizes, and organizes user consents in real time.

The proposed solution utilizes a browser extension integrated with a secure backend and an AI/NLP-based summarization engine. When a user clicks "Accept" on a cookie banner or terms page, the extension captures the relevant content, which is then processed by an intelligent summarization module to generate a simplified plainlanguage summary of the agreement. Both the raw and summarized consent data are securely stored in a MySQL database. Users can access this information through a React-based web dashboard with Google Sign-In authentication. The dashboard provides search and filtering functionalities, along with options to revoke consents and export consent records as PDF or CSV files. By integrating automation, artificial intelligence, and secure web technologies, the Digital Consent Tracker empowers users to make informed decisions and regain control over their digital privacy. In addition to the challenges of understanding lengthy consent documents, users also lack visibility into the permissions they have granted across different websites. Modern web platforms often request multiple permissions such as cookies, notifications, location access, and third-party data sharing, yet users are rarely provided with a unified view of these permissions after consent is granted. This absence of centralized tracking further limits user awareness and control over personal data.

To address this limitation, the Digital Consent Tracker extends beyond summarization by maintaining a website-wise record of user consents and permissions. Each visited website is logged along with the specific actions performed by the

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15190

user, enabling transparent monitoring of consent decisions. Furthermore, the system allows users to revoke or deny previously granted permissions directly through a centralized dashboard, eliminating the need to navigate individual platforms. By integrating real-time consent tracking, secure Google based authentication, and AI-driven policy analysis, the proposed system provides a comprehensive and user-centric solution for digital consent management. This approach not only enhances transparency and user control but also aligns with privacy regulations such as GDPR, CCPA, and India's Digital Personal Data Protection (DPDP) Act. Additionally, the system enables centralized monitoring of user permissions across multiple platforms, allowing users to review, manage, and revoke consents in real time. The simplified visualization of consent information reduces complexity and improves usability for nontechnical users. Overall, the proposed solution promotes ethical data handling practices and strengthens trust between users and digital platforms.

II. PROBLEM STATEMENT

In the current digital environment, users frequently interact with various websites, mobile applications, and online services that collect personal data for purposes such as analytics, advertising, and personalization. However, users are often unaware of when and how their data is being collected, processed, stored, or shared with third parties. Existing consent mechanisms are typically lengthy, inconsistent, and difficult to understand, resulting in poor user awareness and data privacy concerns. Traditional systems rely on static pop-up messages or long privacy policy documents that users tend to ignore due to repetitive content and complex terminology. Additionally, organizations often face challenges in maintaining compliance with data protection laws such as GDPR, CCPA, and India's Digital Personal Data Protection (DPDP) Act, which mandate explicit user consent along with clear provisions for withdrawal and audit tracking. Therefore, there is a need for a smart and automated consent management solution. The proposed Digital Consent Tracker aims to provide a centralized platform along with a browser extension that enables users to view, track, modify, and revoke consents easily across multiple platforms. This system ensures enhanced transparency, user control over personal data.

III. RESEARCH OBJECTIVES

I. To develop a real-time AI- and NLP-based detection mechanism capable of identifying and extracting digital consent content such as cookie notices, privacy policies, and terms & conditions from websites with high accuracy.

II. To design an intelligent consent analysis system that automatically classifies consent information related to data collection, third-party sharing, data retention, and user rights.

III. To implement AI-driven summarization techniques that convert complex legal consent text into concise, userfriendly, and understandable summaries for informed decision-making.

IV. To create a secure, centralized, and scalable consent management platform that stores consent records with metadata including timestamps, website URLs, and consent status, ensuring compliance with data protection regulations.

V. To provide an intuitive dashboard interface that delivers real-time alerts, consent history, and actionable insights, enabling users to review, modify, or withdraw their digital consents efficiently.

IV. RESEARCH BACKGROUND

The research background of the Consent Guard – Digital Consent Tracker is rooted in the growing concerns surrounding digital privacy, data misuse, and lack of transparency in online consent mechanisms. In the modern digital ecosystem, users are frequently exposed to lengthy and complex privacy policies, cookie notices, and consent forms that are difficult to understand, leading to uninformed or forced consent. Traditional consent systems rely heavily on static text and manual user interaction, offering limited transparency, control, and accountability over personal data usage. With the rapid expansion of data-driven technologies, targeted advertising, and cross-platform tracking, organizations increasingly collect, share, and process user data across multiple third-party services. This has made it challenging for users to track where, when, and how their consent has been given. Regulatory frameworks such as GDPR, CCPA, and the DPDP Act emphasize informed consent, data minimization, and user rights; however, existing systems often fail to provide effective tools for monitoring and managing consent histories.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15190

Recent advancements in Artificial Intelligence (AI) and Natural Language Processing (NLP) offer promising solutions to these challenges by enabling automated detection, analysis, and summarization of legal text. AI-powered consent tracking systems can enhance user awareness by simplifying complex policies, ensuring transparency, and enabling centralized consent management. The development of intelligent and automated consent management frameworks like Consent Guard is therefore essential to empower users, improve regulatory compliance, and foster trust in digital platforms while addressing the evolving challenges of data privacy in the digital age.

V. LITERATURE REVIEW

- 2021 | Browser-Based Tools for Web Consent and Text Handling
  Mehta and Gupta (2021) proposed a Google Chrome web extension framework for secure text authentication, demonstrating the effectiveness of browser extensions in intercepting and processing web-based content in real time. Their work highlighted the feasibility of using lightweight extensions for monitoring and interacting with online textual data, which forms the foundation for automated consent detection systems.
- 2021 | NLP Techniques for Simplifying Legal and Policy Texts
  Brown and Chen (2021) explored Natural Language Processing techniques to simplify complex legal documents. Their study showed that tokenization, semantic analysis, and extractive summarization significantly improve user comprehension of legal content, emphasizing the role of NLP in making privacy policies and consent forms more understandable.
- 2022 | AI-Based Privacy Policy Summarization for Transparency
  Wilson and Kumar (2022) introduced an AI-powered framework for summarizing privacy policies to enhance user transparency. Their research demonstrated that automated summarization reduces cognitive overload and improves informed consent, highlighting the importance of AI-driven summarization in digital consent management systems.
- 2022 | Integrating Consent Management into Intelligent Systems
  Sharma and Deshmukh (2022) presented a formal model for integrating consent management within AI-driven operational pipelines. Their work emphasized structured consent handling, traceability, and compliance, underlining the necessity of auditable and well-governed consent records in intelligent systems.
- 2022 | AI-Driven Transparency in Data Collection Practices
  Smith and Li (2022) proposed AI-based policy summarization techniques to improve transparency in data collection processes. Their findings showed that automated interpretation of policies empowers users to better understand how their data is collected and used, reinforcing the need for user-centric consent tools.
- 2023 | Cookie-Less and Secure Consent-Oriented Session Management
  Shah and Jain (2023) introduced a key-based cookie-less session management framework aimed at enhancing application-layer security. Their work is relevant in the context of evolving privacy requirements, supporting consent-aware system designs that minimize unnecessary tracking while maintaining secure user sessions.

VI. PROPOSED SYSTEM

The proposed Digital Consent Tracker aims to provide a centralized, automated, and intelligent solution for managing user consents across multiple digital platforms. The system is designed to enhance user awareness, simplify decision making, and improve transparency in digital data handling practices by addressing the limitations of traditional consent mechanisms. It integrates Artificial Intelligence (AI), Natural Language Processing (NLP), and secure web technologies to automatically extract, analyze, and summarize consent data in real time. The system operates through a browser extension connected to a secure backend server, along with a web-based dashboard that enables users to review and manage their consents efficiently. When a user interacts with a website displaying a privacy policy or consent form, such as a cookie notice or terms and conditions page, the browser extension automatically detects and captures the displayed consent text along with relevant metadata including website URL and timestamp.

The captured content is then processed using AI/NLP based summarization techniques to transform complex and lengthy legal text into simple, easy-to-understand sentences. This allows users to quickly comprehend key aspects of the agreement, such as data collection practices, third-party data sharing, data retention policies, and user rights. Both the original consent text and the AI-generated summarized version are securely stored in a MySQL database to ensure reliability and future reference. Users can access their stored consent history through a React-based web dashboard integrated with Google Sign-In authentication, ensuring secure and personalized access. The dashboard provides features such as viewing summarized consents, searching and filtering records, and managing previously granted permissions.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15190

Additionally, users are provided with options to revoke consents and export consent records in PDF or CSV format, thereby promoting transparency, accountability, and enhanced control over personal data.

The proposed system maintains a website-wise record of user consent and permission details. Each website visited by the user is logged along with the permissions granted or denied, such as cookies, notifications, location access, and third party data sharing. This structured tracking enables users to clearly identify which platforms have access to their data and the specific permissions associated with each website, thereby enhancing transparency and informed consent management.

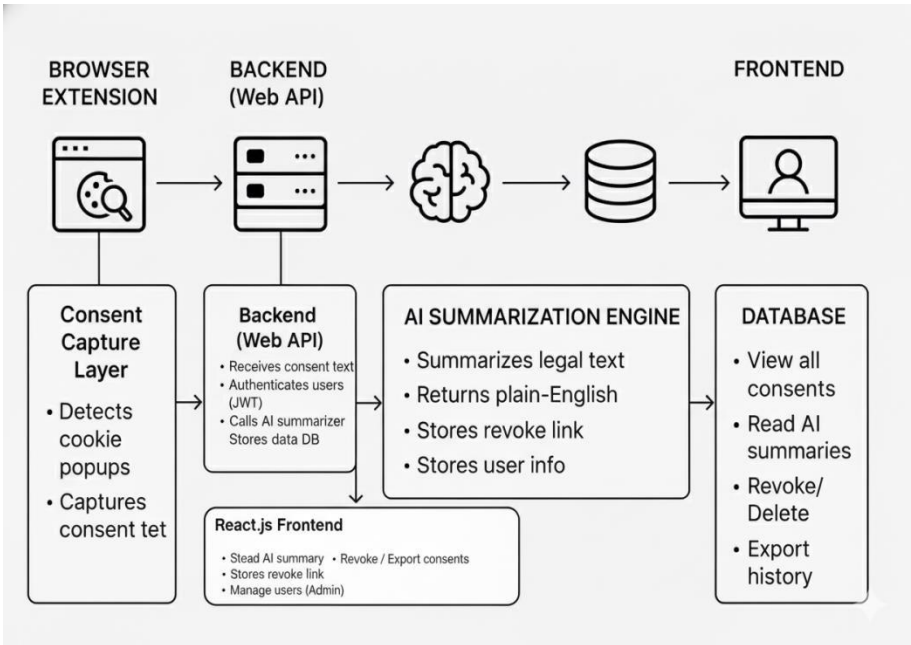

Fig. 1 System architecture.

The architecture diagram for the Digital Consent Tracker (Consent Guard) represents **a** modular, AI-driven, multi-layered system designed to capture, analyze, store, and manage user consents securely and transparently. The system ensures real-time consent tracking, intelligent summarization, and centralized user control.

- Browser Extension (Consent Capture Layer):
  This layer acts as the first point of interaction with the user's browsing activity. The browser extension continuously monitors visited websites to detect consent-related interfaces such as cookie pop-ups, privacy policies, and terms & conditions. Upon detection, it automatically captures the displayed consent text along with relevant metadata such as website URL and timestamp. This real-time extraction enables seamless and automated consent tracking without manual user intervention.

- Backend Web API (Processing and Authentication Layer)):
  The backend Web API serves as the core processing unit of the system. It receives consent text from the browser extension and authenticates users using secure mechanisms such as JWT and Google Sign-In. The backend handles business logic, manages API requests, and forwards consent data to the AI/NLP engine for intelligent processing. It also ensures secure communication between the frontend dashboard, AI engine, and database.

- AI/NLP Summarization Engine (Intelligence Layer):

  This layer functions as the analytical brain of the system. Using Artificial Intelligence and Natural Language Processing techniques, the engine analyzes lengthy and complex legal consent text and generates concise, plain-English summaries. It identifies key clauses related to data collection, third-party sharing, retention policies, and user rights. The summarized output significantly enhances user understanding and supports informed consent decisions.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15190

- Database (Secure Storage Layer):
  The database layer provides structured and secure storage of all consent-related data. It stores original consent text, AI-generated summaries, permission status, revoke links, timestamps, and user-specific information. A relational database such as MySQL is used to ensure data integrity, auditability, and regulatory compliance. This layer enables long-term consent history tracking and retrieval.
- Frontend Dashboard (Visualization and Control Layer):
  The frontend dashboard, developed using React.js, provides users with an intuitive interface to view and manage their consent data. It displays website-wise permission details, summarized consent information, and timestamps in a structured format. Users can revoke or modify permissions in real time, export consent records in PDF or CSV formats, and manage their data efficiently from a centralized platform.

- Consent Revocation and Permission Control (User Control Layer):
  This layer empowers users with full control over their previously granted consents. Through the dashboard, users can withdraw or modify permissions without revisiting individual websites. This feature directly supports the "Right to Withdraw Consent" mandated by data protection regulations such as GDPR, CCPA, and India's DPDP Act, enhancing user autonomy and privacy protection.

- Feedback and Update Mechanism (Learning and Adaptation Layer):
  Consent updates, revocation actions, and user interactions are continuously logged and fed back into the system. This feedback loop helps refine consent classification, improve summarization accuracy, and maintain up-to-date consent records. It ensures the system adapts to evolving website consent practices and regulatory requirements.

Process Flow:

1. The browser extension detects and captures consent text from websites.
2. The captured data is securely transmitted to the backend Web API.
3. The backend authenticates the user and forwards data to the AI/NLP engine.
4. The AI engine generates simplified consent summaries.
5. Consent data and summaries are stored securely in the database.
6. The frontend dashboard visualizes consent history and enables user actions such as revocation and export.

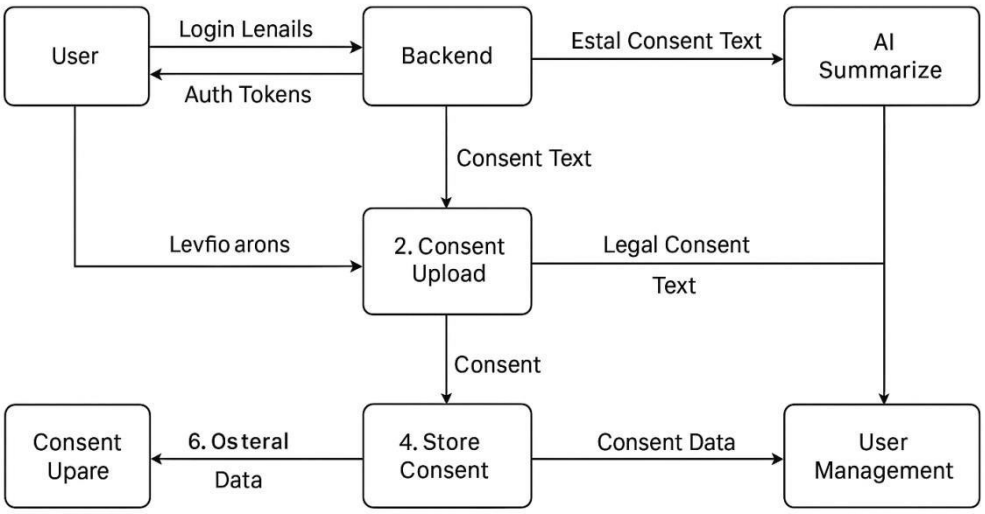

Fig. 2 Overall methodology of Digital Consent Tracker.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15190

The methodology of the Digital Consent Tracker follows a phased, modular, and AI-driven approach to ensure accuracy, scalability, and user-centric privacy management. The process begins with automated data extraction using a browser extension that continuously monitors user interactions with consent banners, cookie pop-ups, and privacy policy pages across various websites. Upon user interaction, the extension captures the relevant consent text along with associated metadata such as website URL, consent type, and timestamp. In the next phase, the captured data is transmitted securely to the backend server, where AI and Natural Language Processing (NLP) techniques are applied for text analysis and summarization. The summarization module processes lengthy and complex legal documents and converts them into concise, plain-language summaries that highlight key aspects such as data collection practices, thirdparty data sharing, retention policies, and user rights. This step significantly enhances user understanding and decisionmaking The backend system ensures secure data handling through authenticated APIs and structured storage mechanisms. Both the original consent text and the AI-generated summaries are stored in a relational database, enabling efficient retrieval and long-term record maintenance. Security measures such as authentication and access control are implemented to protect user data and ensure privacy compliance. Finally, the processed consent information is presented to users through an intuitive, React-based web dashboard. The dashboard enables users to view, search, and filter their consent history, manage granted permissions, and revoke or withdraw consent when required. This centralized visualization and control mechanism ensures real-time consent management, transparency, and alignment with data protection regulations such as GDPR, CCPA, and India's DPDP Act.

Following AI-based summarization, the system performs categorization and semantic classification of the summarized consent text. This step ensures that each policy or clause is not only simplified but also structured into meaningful and predefined categories to enhance clarity and compliance monitoring. Categories may include data collection, data usage purpose, third-party sharing, retention period, and user rights. The core objective of this phase is to identify what type of user information is being processed, how it is handled, and what rights the user holds under applicable data protection laws. Categorization enables better organization of digital consents and supports filtered searches, risk detection, and automated consent management within the dashboard. This structured representation allows users to easily analyze their consent history and take informed actions such as modifying or revoking permissions when necessary.

VII. ALGORITHM USED

The proposed Digital Consent Tracker (Consent Guard) utilizes a combination of Natural Language Processing (NLP), Machine Learning (ML), and rule-based algorithms to automatically detect, analyse, classify, and summarize digital consent information in real time. Unlike traditional consent systems that rely on static text and manual user interaction, the proposed system intelligently processes consent data to enhance transparency and user control.

For consent detection, rule-based DOM analysis and pattern-matching algorithms are employed within the browser extension. These algorithms scan webpage structures to identify consent-related components such as cookie banners, privacy policy dialogs, and terms & conditions pop-ups. Keyword matching and regular expressions are used to extract relevant legal text efficiently during user interaction with websites. Once extracted, the consent text undergoes NLP preprocessing, including tokenization, stop-word removal, lemmatization, and sentence segmentation. These steps normalize the legal text and improve the performance of downstream classification and summarization models.

To classify consent clauses, the system applies machine learning algorithms such as Logistic Regression (LR), Support Vector Machines (SVM), Naïve Bayes (NB), and Random Forest (RF)**.** These classifiers categorize consent content into predefined classes such as data collection, third-party data sharing, data retention, and user rights. Experimental studies reported in the literature indicate that Random Forest and SVM classifiers achieve higher accuracy due to their ability to model complex semantic relationships present in legal documents.

For simplifying lengthy legal content, the system integrates AI-based text summarization algorithms**.** Both extractive summarization techniques (using TF-IDF and sentence ranking) and transformer-based models are employed to generate concise, plain-language summaries of privacy policies. This enables users to quickly understand consent implications without reading extensive legal text. The system further implements rule-based decision logic to manage consent permissions, enabling real-time grant, deny, and revoke operations. Secure authentication mechanisms such **as** OAuth 2.0 (Google Sign-In) and JWT-based authorization ensure that consent data remains protected and accessible only to authorized users.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15190

The effectiveness of the proposed system lies in its multi-layered algorithmic approach, where consent detection, classification, and summarization work together. Rule-based detection ensures real-time extraction, machine learning enables accurate categorization, and AI summarization enhances user understanding. This combination reduces information overload, minimizes uninformed consent, and strengthens compliance with privacy regulations such as GDPR, CCPA, and the DPDP Act.

Overall, the hybrid integration of rule-based detection, NLP preprocessing, machine learning classification, and AIdriven summarization forms a robust and scalable approach for automated consent tracking and management.

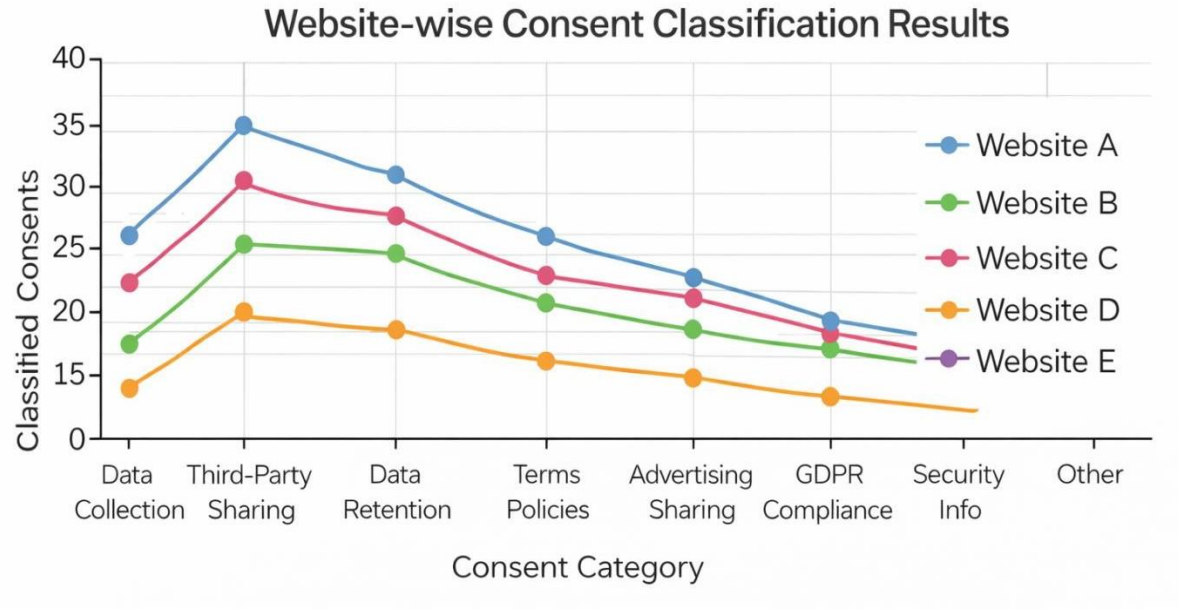

Fig. 3 Website-wise Consent Classification Results.

Fig. 3 illustrates the classification results of consent clauses extracted from multiple websites. The graph demonstrates how different consent categories—such as data collection, third-party sharing, and retention policies—are identified and classified using machine learning models. The results show consistent classification patterns across websites, highlighting the effectiveness of ML-based consent categorization.

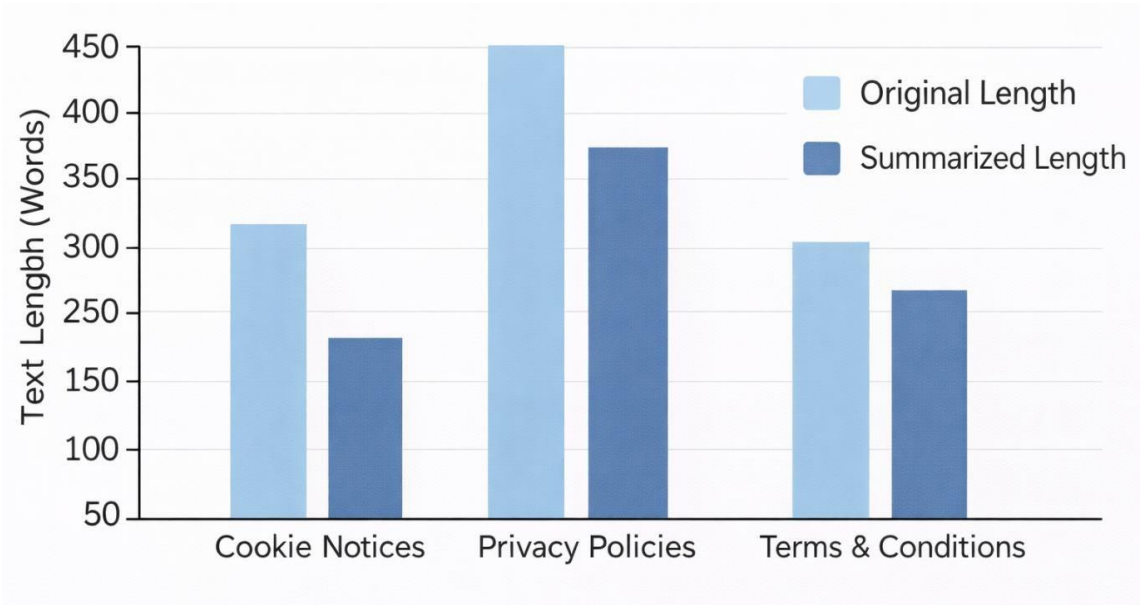

Fig.4 Consent Text Summarization Output by Category.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411138

Sentence In the proposed system, sentence importance for text summarization is computed using the Term Frequency–Inverse Document Frequency (TF-IDF) weighting scheme. Each sentence is assigned a relevance score based on the cumulative importance of the words it contains. The scoring formula is defined as:

$$\text{Score (sentence)} = \sum \text{TF (word)} \times \text{IDF (word)}$$

Where TF (word) represents the frequency of a word within the sentence, indicating its local importance and IDF (word) denotes the inverse document frequency, which measures the global significance of the word across the entire document corpus. Words that appear frequently in a sentence but are rare across documents receive higher TF-IDF weights.

This scoring mechanism prioritizes sentences containing legally and semantically significant terms such as data collection, third-party sharing, user consent, and retention policy. Sentences with higher scores are selected as part of the extractive summary, ensuring that the generated summary preserves critical consent-related information while reducing redundancy. By applying TF-IDF-based sentence scoring, the system effectively balances relevance and conciseness, producing clear and informative summaries that enhance user understanding of complex consent documents.

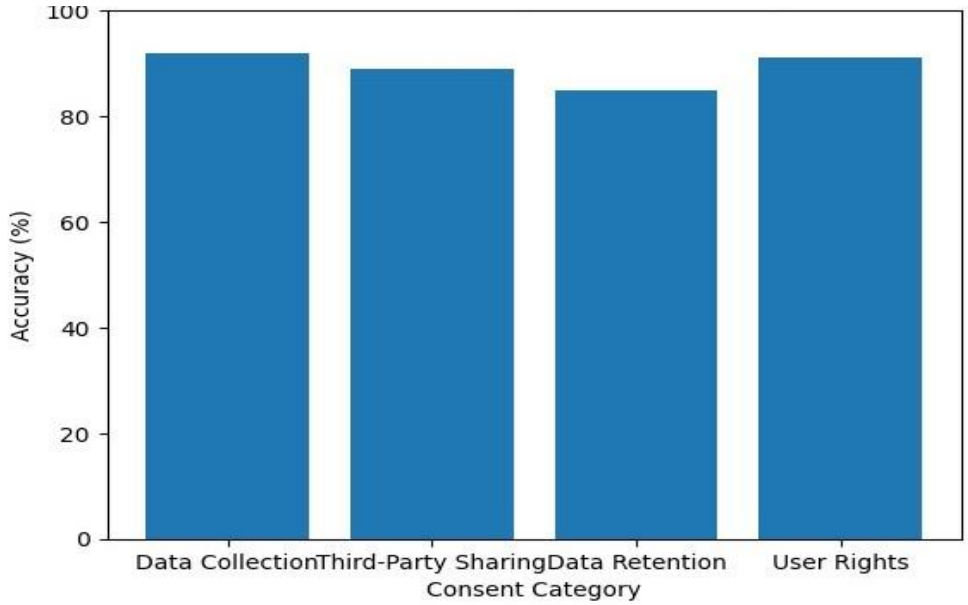

Fig.5 Classification Accuracy of Consent Categories

The proposed system applies machine learning–based classification techniques to automatically analyze and categorize extracted consent clauses into predefined and meaningful categories, including Data Collection, Third-Party Data Sharing, Data Retention, and User Rights. This classification process enables the system to structure unorganized legal consent text into clearly defined segments, making it easier for users to understand the specific implications of their consent.

Experimental observations demonstrate that the classification module performs consistently and reliably across multiple websites, regardless of variations in consent formats, policy structures, or legal language. The machine learning models effectively capture semantic patterns within consent documents, allowing accurate identification of consent categories even when policies differ in wording and layout. This consistency highlights the robustness and adaptability of the proposed approach in real-world web environments.

Furthermore, accurate classification of consent clauses forms the foundation for advanced features such as AI-based summarization, risk awareness, and consent revocation. By systematically organizing consent information, the system enhances transparency, reduces cognitive overload, and supports informed user decision-making. The results confirm that machine learning–driven consent classification is a practical and scalable solution for automated digital consent management while supporting compliance with data protection regulations such as GDPR, CCPA, and India's DPDP Act.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15190

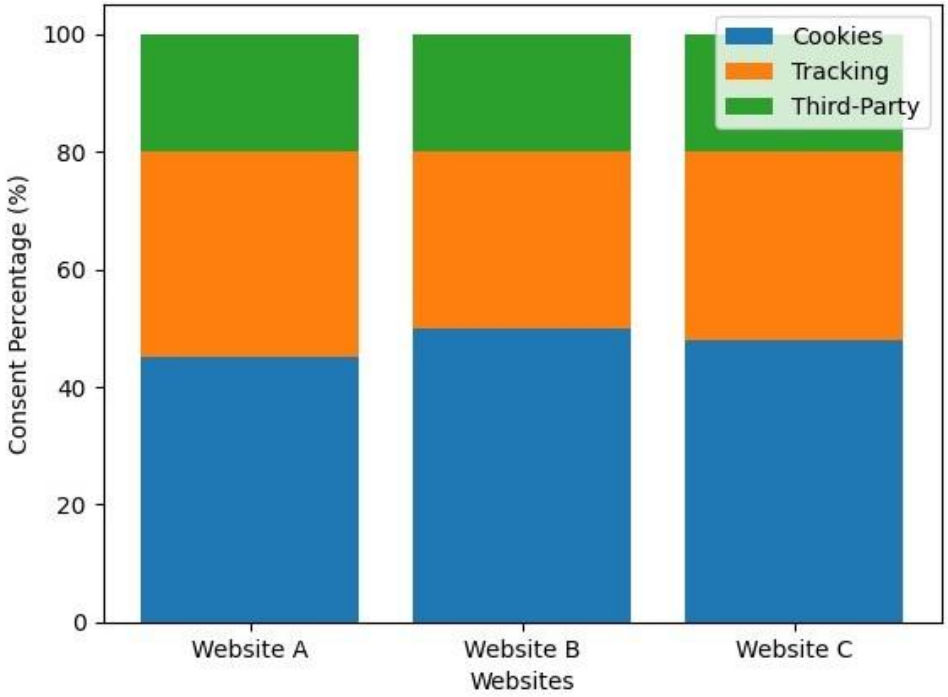

Fig.6 Website-wise Distribution of Consent Types

The proposed system maintains a structured, website-wise repository of user consent records, which enables transparent and systematic monitoring of permissions granted across multiple digital platforms. For each visited website, the system captures and stores detailed information regarding the type of consent requested, including cookies, user tracking, and third-party data sharing, along with relevant metadata such as website URL and timestamp. This structured approach allows users to clearly identify which websites have access to their data and the nature of permissions granted.

The analysis of collected consent data indicates that cookie-based consent requests are the most prevalent across websites, reflecting their widespread use for session management, personalization, and analytics. Tracking-related permissions are observed as the second most commonly requested category, followed by third-party data sharing consents, which are often associated with advertising and external analytics services. These findings demonstrate that users are frequently exposed to multiple consent requests during routine browsing activities.

This outcome highlights the critical need for a centralized consent monitoring mechanism, as users typically grant multiple permissions across different platforms without having a unified view of their consent history. In the absence of such visibility, users may unknowingly allow extensive data collection and sharing. By organizing consent information in a website-wise and category-wise manner, the proposed system enhances transparency, improves user awareness, and supports informed decision-making. Additionally, this centralized monitoring capability empowers users to review, manage, and revoke previously granted consents efficiently, thereby strengthening user control over personal data and aligning with global data protection regulations.

VIII. IMPLEMENTATION

The implementation of the proposed Digital Consent Tracker (Consent Guard) leverages real-time browser-based monitoring, Natural Language Processing (NLP), machine learning–assisted text analysis, and secure web technologies to ensure transparent, user-centric, and regulation-compliant consent management. The system is designed as a distributed yet coordinated architecture, where data capture; processing, analysis, and visualization are handled through well-defined modular components. The browser extension acts as the client-side component and continuously monitors user interactions with websites. It detects consent-related elements such as cookie pop-ups, privacy policies, and terms & conditions dialogs in real time. Upon detection, the extension extracts consent text along with contextual metadata (website URL, timestamp, permission type) and securely transmits this data to the backend for further processing. The backend server processes incoming consent data, manages authentication and authorization, and coordinates communication between the frontend dashboard, database, and AI/NLP engine. Machine learning–assisted NLP models

DOI: 10.17148/IJARCCE.2026.15190

analyse the extracted text to classify consent clauses and generate concise summaries. The processed results are stored securely and made available to users through a centralized dashboard to ensure secure and personalized access, the system integrates Google Sign-In authentication. This ensures that consent data is accessible only to authorized users and remains protected against unauthorized access. Secure APIs, access control mechanisms, and encrypted data storage are employed to safeguard sensitive consent information and maintain compliance with privacy and security standards.

I. **Client Deployment (Browser Extension Layer)**

Each user installs a lightweight browser extension that operates locally within the browser environment. The extension monitors:

- Website DOM elements
- Cookie banners and modal dialogs.

II. **Client Deployment (Browser Extension Layer)**

Each user installs a lightweight browser extension that operates locally within the browser environment. The extension monitors:

- Website DOM elements
- Cookie banners and modal dialogs
- Privacy policy and terms & conditions pages

This enables real-time detection and extraction of consent-related text during normal browsing activity without disrupting the user experience.

III. **Text Capture and Feature Extraction**

The extension extracts:

- Raw consent text
- Website URL and domain
- Consent type (cookies, tracking, third-party sharing, notifications, etc.)
- Timestamp and user interaction context

IV. **NLP and ML-Based Analysis**

The backend integrates an AI/NLP engine that performs:

- Text preprocessing (tokenization, stop-word removal, lemmatization)
- Clause classification using ML algorithms (Logistic Regression, SVM, Random Forest)
- Extractive and transformer-based summarization

These models are trained on consent and legal-policy datasets to accurately identify key clauses related to:

- Data collection
- Data usage
- Third-party sharing

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15190

- Retention policies
- User rights

V. Secure Authentication and Access Control

The system implements Google Sign-In (OAuth 2.0) for secure user authentication. JWT-based session handling ensures that consent data is:

- User-specific
- Securely accessed
- Protected from unauthorized usage
- Role-based access control supports both end-user and admin-level operations.

VI. Consent Management and Revocation

Processed consent data is stored in a centralized database and made accessible through a web-based dashboard. Users can:

- View website-wise consent history
- Read AI-generated summaries
- Revoke or modify permissions in real time
- Export consent records for compliance and auditing

This mechanism directly supports the Right to Withdraw Consent as mandated by GDPR, CCPA, and India's DPDP Act.

Tools Used

● Programming Languages

- Java (Spring Boot backend)
- JavaScript (Browser Extension)
- JavaScript / TypeScript (React Frontend)

● Frontend

- React.js
- HTML, CSS
- Axios for API communication

● Backend

- Spring Boot
- RESTful APIs
- JWT Authentication

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15190

- **AI / NLP**
  - NLP libraries (tokenization, summarization models)
  - TF-IDF–based scoring
- **Database**
  - MySQL (structured storage of consent records)
- **Authentication & Security**
  - Google OAuth 2.0
  - JWT
  - HTTPS-secured APIs
- **Deployment & Testing**
  - Docker (optional containerization)
  - Postman (API testing)
  - Chrome Developer Tools (extension testing)

Hardware / Software Setup

- **Client (User Side)**
  - OS: Windows / Linux / macOS
  - Browser: Google Chrome (or Chromium-based browsers)
  - Hardware: Standard PC or laptop, 2–4 GB RAM minimum
- **Server (Backend)**
  - OS: Linux (Ubuntu) or Windows Server
  - Hardware: 8–16 GB RAM, multi-core processor
  - Storage: SSD for faster database access

Experimental Environment

- **Training and Validation Phase**
  - Use consent and privacy policy datasets
  - Evaluate summarization accuracy and classification consistency
- **Testing Phase**
  - Deploy browser extension in controlled environments
  - Test with real-world websites using different consent formats
  - Measure system latency, accuracy, and usability

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15190

- **Monitoring and Evaluation**
  - Track consent capture success rate
  - Validate revocation effectiveness
  - Assess improvement in user comprehension through summaries

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15190

IX. RESULTS & ANALYSIS

The proposed Digital Consent Tracker system is expected to significantly enhance user awareness, control, and transparency in digital privacy management. By automatically analyzing and summarizing lengthy and complex legal consent documents using Artificial Intelligence and Natural Language Processing techniques, the system helps users easily understand critical aspects of privacy policies such as data collection practices, usage purposes, third-party data sharing, retention duration, and user rights. This improved clarity enables individuals to make informed decisions before granting consent, thereby reducing the risk of unintended or uninformed data sharing. The centralized web-based dashboard provides users with a unified platform to view, track, search, and manage all previously accepted consents across multiple digital platforms. By presenting consent history in an organized and user-friendly manner, the system simplifies consent monitoring and enhances transparency

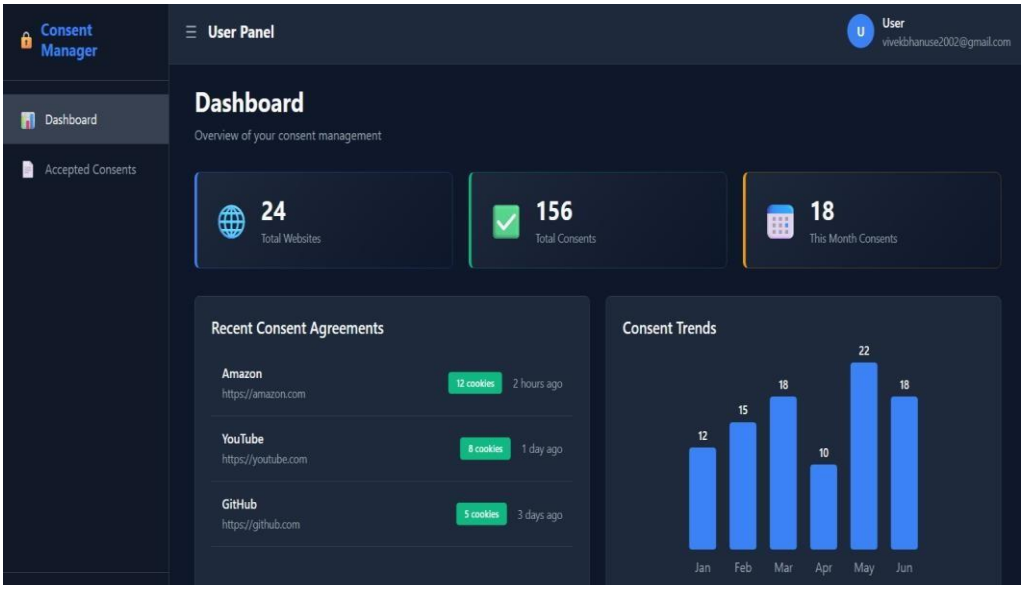

Fig. 5. Real Time View Dashboard.

Users are empowered to revoke or modify permissions at any time, ensuring continuous control over their personal data without the need to revisit individual websites. In addition to improving user experience, the system is expected to indirectly support organizations in aligning with global and national data protection regulations such as GDPR, CCPA, and India's Digital Personal Data Protection Act. The ability to export consent records in PDF or CSV format allows users to maintain verifiable documentation for personal reference, compliance verification, or legal audits. Overall, the Digital Consent Tracker promotes ethical data handling practices, strengthens accountability in digital environments, and builds greater user trust by providing simplified, accurate, and actionable consent information within a secure and transparent framework.

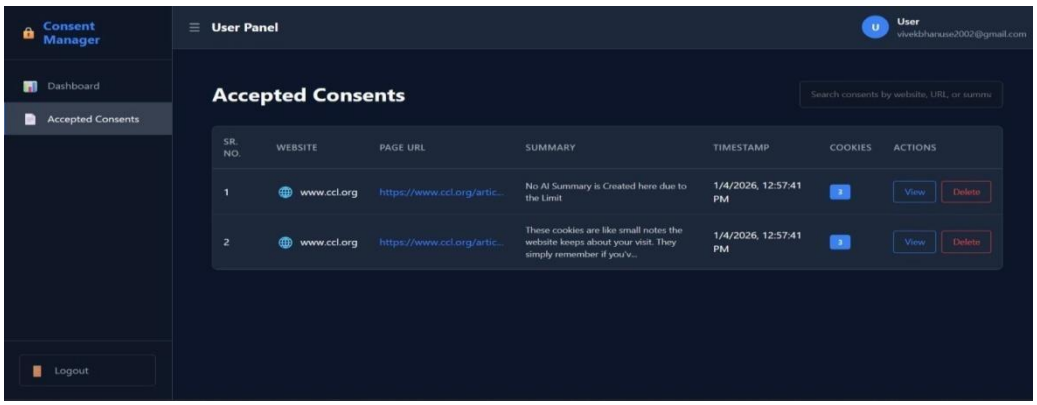

Fig. 6 Real time Accepted Consents

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15190

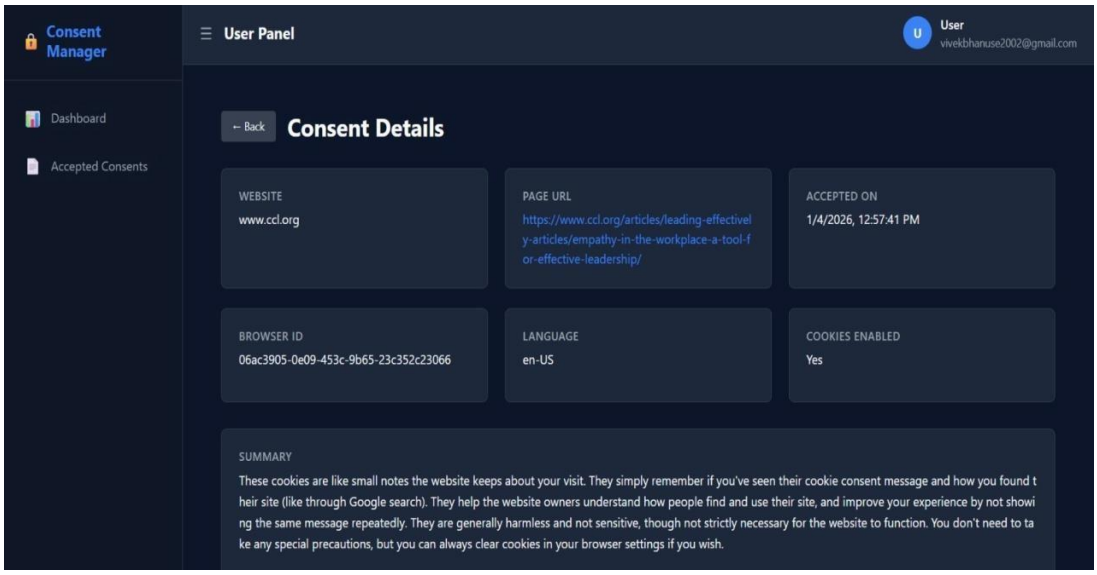

Fig. 7 Consent Details.

This consent record indicates that the user accepted the consent **on** www.ccl.org while visiting a specific webpage related to leadership and workplace empathy. The consent was accepted on January 4, 2026, at 12:57:41 PM using a browser identified by the unique browser ID 06ac3905-0e09-453c-9b65-23c352c23066**.** The content was displayed in the English (en-US) language, and cookies were enabled at the time of acceptance. The cookies associated with this consent are primarily used to remember whether the user has acknowledged the cookie notice and to understand how users discover and interact with the website, such as through search engines. These cookies do not contain sensitive personal information and are intended to enhance user experience by preventing repeated consent prompts and improving website usability.

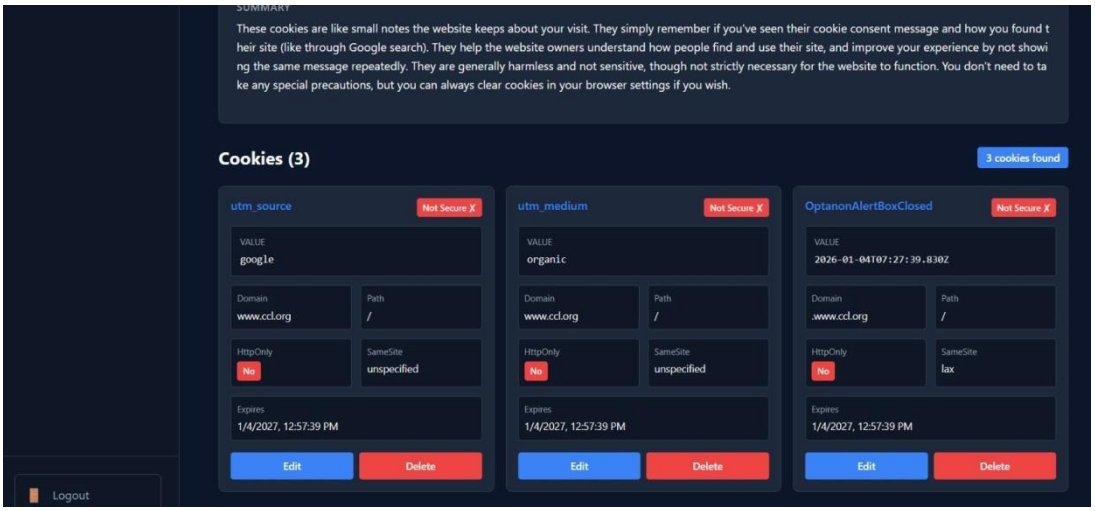

Fig. 8 Cookies Update.

In the cookie management section, users are provided only with the option to delete cookies. This design decision is based on the fact that cookies are system-generated entities and do not require manual modification by users. Instead, presenting cookie information in a read-only format improves clarity, reduces user error, and aligns with standard privacy and usability practices. The delete option empowers users to maintain control over their data by removing unwanted cookies without unnecessary complexity.

X. CONCLUSION

The Digital Consent Tracker presents an effective and innovative solution to address the growing challenges associated with online privacy management and uninformed consent acceptance in modern digital environments. By leveraging Artificial Intelligence (AI) and Natural Language Processing (NLP), the system simplifies complex and lengthy legal documents into concise, comprehensible summaries, enabling users to clearly understand the key implications of their

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15190

digital consent. This enhanced clarity empowers users to make better-informed decisions and significantly reduces the risk of unintended or accidental data exposure. Furthermore, the centralized web-based dashboard enables users to view, track, manage, and revoke previously accepted consents from a single unified platform. This centralized approach improves transparency and provides continuous control over personal data, eliminating the need for users to navigate individual websites to manage permissions. The ability to filter, export, and review consent records further strengthens accountability and allows users to maintain reliable documentation of their consent history. The proposed system also contributes to responsible and ethical data governance by supporting compliance with international and national data protection regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and India's Digital Personal Data Protection (DPDP) Act. By aligning technological innovation with legal and ethical standards, the Digital Consent Tracker promotes privacy-by-design principles and encourages responsible data handling practices across digital platforms. Overall, the implementation of this system demonstrates the potential of AIdriven technologies in transforming digital privacy awareness and consent management. By enhancing transparency, strengthening user trust, and enabling informed decision-making, the Digital Consent Tracker contributes to the development of a more secure, ethical, and user-centric digital ecosystem..

ACKNOWLEDGMENT

We deeply appreciate **Dr. Vijay R. Sonawane** for his expert guidance, constant encouragement, and valuable support throughout the project, as well as for his inspiring leadership as the Head of the Department of Information Technology. We are also sincerely grateful to **Prof.S.K.Thakare**, Project Coordinator, for her continuous support, valuable suggestions, and encouragement that greatly contributed to the successful completion of our project.

We would like to express our deepest appreciation to **Dr. M.V. Bhalerao**, Principal of Pune Vidyarthi Griha's College of Engineering, Nashik, whose invaluable guidance supported us in completing this project.

Finally, we extend our heartfelt gratitude to all the staff members of the Information Technology Department who helped us directly or indirectly during the course of this work.

REFERENCES

[1]. A. Sharma and K. Deshmukh, "A Formal Model for Integrating Consent Management Into MLOps," in Proceedings of the International Conference on Artificial Intelligence and Privacy Engineering, pp. 45–52, 2022.

[2]. L. Mehta and R. S. Gupta, "On the Development of a Web Extension for Text Authentication on Google Chrome," IEEE International Workshop on Web Security Technologies, pp. 34–40, 2021.

[3] P. Shah and V. Jain, "Key-based cookie-less session management framework for application layer security," *International Journal of Network Security Engineering*, vol. 18, no. 3, pp. 105–113, 2023.

[4] M. H. Wilson and A. Kumar, "AI-powered summarization of privacy policies for user transparency," *IEEE Access*, vol. 10, pp. 45123–45135, 2022.

[5] J. Brown and L. Chen, "Natural language processing techniques for simplifying legal texts," *Journal of Artificial Intelligence Research*, vol. 74, pp. 115–130, 2021.

[6] T. Nguyen and R. Patel, "Automated consent management system using machine learning and NLP," in *Proceedings of the IEEE International Conference on Data Privacy and Ethics*, pp. 101–110, 2023.

[7]. A. Smith and P. Li, "Improving transparency in data collection through AI-based policy summarization," *ACM Journal on Responsible Computing*, vol. 4, no. 2, pp. 65–78, 2022.

[8]. R. Kaur and N. Sharma, "Legal document simplification using transformer-based language models," *International Journal of Computer Applications*, vol. 185, no. 17, pp. 22–29, 2023.

[9]. S. Johnson and Y. Zhang, "Hugging Face transformers for context-aware privacy policy analysis," *IEEE Transactions on Computational Linguistics*, vol. 9, pp. 211–223, 2023.

[10]. A. Banerjee and M. Singh, "AI-driven framework for GDPR and CCPA compliance monitoring," *Journal of Data Protection and Privacy*, vol. 5, no. 1, pp. 33–47, 2022.4

[11] C. Wang and E. Rober, "Advanced AI-enabled consent governance for secure data handling," in *Proceedings of the International Symposium on Digital Trust and Cybersecurity*, pp. 88–96, 2023.

[12] J. Verma and S. Thomas, "Machine learning approaches for consent compliance and data rights management," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1321–1335, 2023.

[13] D. I. Rivera and K. Yadav, "Automated legal consent extraction using transformer-based architectures," in *Proceedings of the IEEE International Conference on AI and Law (ICAIL)*, pp. 76–84, 2022.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15190

[14] S. Patel, M. Dutta, and J. Lee, "A user-centric framework for managing digital consent using browser extensions," *International Journal of Web Privacy Engineering*, vol. 12, no. 3, pp. 44–53, 2023.
[15] H. Nakamura and E. Diaz, "AI-enabled privacy rights enforcement under GDPR via consent automation," *Springer Journal of Cybersecurity Innovations*, vol. 6, no. 1, pp. 21–38, 2024.
[16] S. Zimmeck and S. Bellovin, "Practical privacy policy analysis using machine learning," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 1–15, 2014. [17] A. M. McDonald and L. F. Cranor, "The cost of reading privacy policies," *I/S: A Journal of Law and Policy for the Information Society*, vol. 4, no. 3, pp. 543–568, 2008.
[18] G. Contissa, R. Lagioia, and G. Sartor, "Automated processing of privacy policies under GDPR," *Artificial Intelligence and Law*, vol. 26, no. 2, pp. 163–200, 2018.
[19] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *Proceedings of the IEEE Symposium on Usable Privacy and Security (SOUPS)*, pp. 1–17, 2015.
[20] K. Ganesan and S. Meenakshi, "Text summarization techniques for legal documents using NLP," *International Journal of Computer Science and Engineering*, vol. 11, no. 4, pp. 210–218, 2022.
[21] N. Kshetri, "The economics of privacy, big data and artificial intelligence," *IEEE IT Professional*, vol. 22, no. 2, pp. 5–8, 2020.
[22] A. Gerl, E. Bennani, M. Kosch, and M. Ziekow, "Privacy and data protection by design – from policy to engineering," *IEEE Security & Privacy*, vol. 16, no. 3, pp. 25–34, 2018.
[23] T. Hoang, J. X. Yu, and Y. Zhou, "Efficient privacy policy classification using deep learning," *IEEE Access*, vol. 9, pp. 98721–98733, 2021.
[24] P. L. Koopman and J. D. Hoven, "Ethical issues in AI-based decision systems," *AI and Society*, vol. 35, no. 2, pp. 425–437, 2020.
[25] M. Veale, R. Binns, and L. Edwards, "Algorithms that remember: Model inversion attacks and data protection law," *Philosophical Transactions of the Royal Society A*, vol. 376, no. 2133, pp. 1–15, 2018.
[26] A. Cavoukian, "Privacy by design: The seven foundational principles," *IEEE Consumer Electronics Magazine*, vol. 4, no. 1, pp. 13–18, 2015.
[27] R. G. Nair and S. Pillai, "User-centric consent management framework for web applications," *International Journal of Web Engineering and Technology*, vol. 18, no. 1, pp. 55–72, 2023.
[28] A. T. Smith and H. Jin, "Automated analysis of online privacy policies using deep learning," *IEEE Access*, vol. 8, pp. 141184–141195, 2020.
[29] J. Polonetsky, O. Tene, and J. Jerome, "Privacy by design: Principles and implementation," *IEEE Security & Privacy*, vol. 12, no. 6, pp. 38–45, 2014.
[30] R. Binns, "Human judgements in algorithmic decision-making," in *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (FAccT)*, pp. 1–12, 2018.
[31] S. Zuboff, "Big other: Surveillance capitalism and the prospects of an information civilization," *Journal of Information Technology*, vol. 30, no. 1, pp. 75–89, 2015. [32] M. Lippi, P. Torroni, and A. Squicciarini, "Legal text classification using machine learning," *Artificial Intelligence and Law*, vol. 27, no. 3, pp. 321–347, 2019.
[33] A. Kapoor and S. R. Rao, "Consent management platforms for GDPR compliance: A comparative study," *International Journal of Information Security Science*, vol. 11, no. 2, pp. 89–102, 2022.
[34] L. Sweeney, "Privacy risks in data sharing and consent mechanisms," *IEEE Computer*, vol. 53, no. 1, pp. 45–52, 2020.
[35] E. Bertino and N. Islam, "Botnets and internet privacy: Challenges and solutions," *IEEE Computer*, vol. 50, no. 2, pp. 76–80, 2017.
[36] S. Wachter, B. Mittelstadt, and L. Floridi, "Why a right to explanation of automated decision-making does not exist in the GDPR," *International Data Privacy Law*, vol. 7, no. 2, pp. 76–99, 2017.
[37] P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017.
[38] F. B. Abdessalem, D. Garijo, and O. Corcho, "Consent management and transparency in data-driven systems," *IEEE Internet Computing*, vol. 23, no. 6, pp. 72–79, 2019.
[39] A. Degeling, M. Utz, C. Lentzsch, and T. Holz, "We value your privacy… now take some cookies: Measuring the GDPR's impact on web privacy," in *Proceedings of the Network and Distributed System Security (NDSS) Symposium*, pp. 1–15, 2019.
[40] S. K. Sahay, P. Mittal, and A. Datta, "Automated privacy policy analysis and compliance verification," in *Proceedings of the ACM CCS Workshop on Privacy Engineering*, pp. 1–10, 2020.
[41] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pp. 1310–1321, 2015.

DOI: 10.17148/IJARCCE.2026.15190

[42] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

[43] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," *IEEE Cloud Computing*, vol. 3, no. 2, pp. 14–23, 2016. [44] J. R. Reidenberg, L. F. Cranor, and N. Sadeh, "Privacy interfaces: User-centric privacy design," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 68–71, 2015.

[45] P. Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," *UCLA Law Review*, vol. 57, no. 6, pp. 1701–1777, 2010.

[46] M. Hildebrandt, "Law as computation in the era of artificial legal intelligence," *University of Toronto Law Journal*, vol. 68, no. 1, pp. 12–35, 2018.

[47] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015.

BIOGRAPHY

Prof. Smita K. Thakare is an academician who specializes in big data analytics, data science, and machine learning. She has taught undergraduate and graduate courses in fundamental computing areas like machine learning, social media analysis, computer graphics, digital electronics, and discrete mathematics for more than 8.8 years. Her active participation in academic research is demonstrated by the 11 international research papers she has published and the research she has presented at national and international conferences. She is currently employed at Pune Vidyarthi Griha's College of Engineering in Nashik as an Assistant Professor in the Department of Information Technology, where she teaches, mentors academics, and supports technology-focused education.

Ms. Monali A. Kokate is currently pursuing a B.E. in Information Technology from Savitribai Phule Pune University. She is interested in cloud computing, AI/ML, full stack development, and system architecture. Working on system-level architecture, data-driven decision models, and contemporary security techniques that enable scalable and dependable solutions, she works on creating intelligent and secure software systems.

Ms. Sanjeevani P. Khairnar is currently pursuing a B.E. in Information Technology from Savitribai Phule Pune University and is an alumna of NDMVPS's RSM polytechnic, Nashik. Her areas of interest include data analytics, database management, front-end development, AL/ML, and cloud computing, with a focus on developing efficient and user-centric software solutions. She is enthusiastic about learning emerging technologies and contributing to the development of secure and scalable systems.

Ms. Snehal S. Kedar is currently pursuing a B.E. in Information Technology from Savitribai Phule Pune University. She is particularly interested in full-stack development, cloud computing, AI/ML, and data-driven systems. She has practical expertise with database systems, web technologies, and Internet of Things-based projects. In an effort to support scalable and significant software systems, she actively focuses on system-level thinking, practical problem-solving, and responsible technology design.

Ms. Pinal D. Lagdhir is currently pursuing a B.E. in Information Technology from Savitribai Phule Pune University. She is interested in full-stack web technologies, Java-based apps, and software development. With a strong background in database management systems, object-oriented programming, and data structures, she concentrates on creating dependable and user-friendly software. In order to create reliable and maintainable software systems, she is especially drawn to logical problem-solving, system implementation, and ongoing skill development.

