Encryption using IDPR (International Data Privacy Regulation): An Overview of project IDPR

Prof. Swapnil Wani, Assistant Professor, SIES GST Nerul, Navi Mumbai, India, swapnilw@sies.edu.in

Ms. Srushti Anil Kulkarni, Student, SIES GST Nerul, Navi Mumbai, India, srushtiakiot121@gst.sies.edu.in

Ms. Sushmita R. Yadav, Student, SIES GST Nerul, Navi Mumbai, India, sushmitayiot@gst.sies.edu.in

Mr. Ayush K. Tiwari, Student, SIES GST Nerul, Navi Mumbai, India, ayushktiot121@gst.sies.edu.in

Mr. Omkar B. Gorde, Student, SIES GST Nerul, Navi Mumbai, India, omkarbgiot121@gst.sies.edu.in

***Abstract*— In the era of digital transformation, data privacy and security have become paramount concerns. This research introduces an innovative International Data Privacy Regulation (IDPR) framework leveraging advanced encryption to protect user data during upload, storage, and retrieval. The project utilizes a multi layered approach with React.js for frontend, Spring Boot with Java for backend, and MySQL for secure database management. By implementing symmetric 256-bit encryption, our system ensures end-to-end data protection, enabling secure user authentication, data upload, and controlled access. The proposed IDPR framework demonstrates a scalable and adaptable approach to addressing global data privacy challenges, providing organizations with a secure and robust mechanism to protect sensitive user information while maintaining transparency and user control over the data. The system integrates advanced security technologies to create a comprehensive solution for digital data protection. By implementing cutting edge encryption techniques and user centric design, the research aims to establish a new standard in secure data management that can be applied across various industries and organizational contexts.**

Keywords – Data Protection, Decryption, Encryption, Privacy Laws, User data, Security.

I. INTRODUCTION

In today's interconnected world, data has emerged as a critical and crucial asset, fueling advancements in technology, healthcare, finance, and other sectors. With the faster proliferation of digital platforms, vast amounts of sensitive personal information are collected, processed, and exchanged daily. While this data drives innovation and enables personalized services, it also presents substantial risks to user privacy and security. The increasing frequency of data and security breaches and unauthorized access incidents has exposed the vulnerabilities in existing systems, underlining the need for advanced methods to safeguard sensitive user information [1].

In response, governments and organizations worldwide have introduced regulations like the European Union's General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) [1], [2]. These regulatory frameworks aim to establish strict guidelines for data handling, emphasizing user consent, transparency, and accountability. However, the fragmented and diverse global regulatory landscape complicates compliance for businesses operating across multiple jurisdictions, geographically apart [4]. This calls for not only adherence to these regulations but also the development of innovative solutions to ensure data privacy and security.

This research explores a system designed to address these challenges by implementing robust encryption techniques for securing user data, [6]. The system leverages encryption algorithm to encrypt user information during upload, ensuring it is stored securely in the database. Users can access their encrypted data through an authentication system, which includes functionalities such as login, signup, and data retrieval. Upon a user request, the system decrypts the information, enabling secure access while maintaining confidentiality. The project employs a modern technology stack for its implementation. The frontend is developed using HTML, CSS, JavaScript, and ReactJS to deliver an intuitive user interface. Java Spring Boot and Maven form the core of the backend architecture, enabling seamless communication between the client and the server. The database is managed

 DOI : 10.35291/2454-9150.2025.0037

using SQL, which ensures secure and efficient data storage. This paper aims to provide a comprehensive analysis of the proposed system, detailing its design, architecture, and implementation. It also discusses the role of encryption in enhancing data privacy, the challenges of ensuring compliance with global data protection laws, and the potential impact of secure systems on user trust and organizational accountability.

II. LITERATURE REVIEW

[1] S.Wairimu, L.H.Iwaya, L.Fritsch and S.Lindskog, "On the Evaluation of Privacy Impact Assessment and Privacy Risk Assessment Methodologies: A Systematic Literature Review," in *IEEE Access*, vol. 12, pp. 19625-19650, 2024

Extract- Assessing privacy risks and incorporating privacy measures from the onset requires a comprehensive understanding of potential impacts on data subjects. Privacy Impact Assessments (PIAs) offer a systematic methodology for such purposes, which are closely related to Data Protection Impact Assessments (DPIAs), particularly outlined in Article 35 of the General Data Protection Regulation (GDPR). The core of a PIA is a Privacy Risk Assessment (PRA). PRAs can be integrated as part of full-fledged PIAs or independently developed to support PIA processes.

[2] L.H.Iwaya, M.A.Babar and A.Rashid, "Privacy Engineering in the Wild: Understanding the Practitioners' Mindset, Organizational Aspects, and Current Practices," in *IEEE Transactions on Software Engineering*, vol. 49, no. 9, pp. 4324-4348, Sept. 2023

Extract- Privacy engineering, as an emerging field of research and practice, comprises the technical capabilities and management processes needed to implement, deploy, and operate privacy features and controls in working systems. For that, software practitioners and other stakeholders in software companies need to work cooperatively toward building privacy-preserving businesses and engineering solutions. Significant research has been done to understand the software practitioners' perceptions of information privacy, but more emphasis should be given to the uptake of concrete privacy engineering components. This research delves into the software practitioners' perspectives and mindset, organizational aspects, and current practices on privacy and its engineering processes.

[3] A.Zigomitros, F.Casino, A.Solanas and C.Patsakis,"A Survey on Privacy Properties for Data Publishing of Relational Data," in *IEEE Access*, vol. 8, pp. 51071-51099, 2020

Extract- The scope of this work is to provide an in-depth overview of the current state of the art in Privacy-Preserving Data Publishing (PPDP) for relational data. To counter information leakage, a number of data anonymization methods have been proposed during the past few years, including k -anonymity, ℓ -diversity, t -closeness, to name a few. In this study we analyze these methods providing concrete examples not only to explain how each of them works, but also to facilitate the reader to understand the different usage scenarios in which each of them can be applied. Furthermore, we detail several attacks along with their possible countermeasures, and we discuss open questions and future research directions.

[4] L. Seiling, R. Gsenger, F. Mulugeta, M. Henningsen, L. Mischau and M. Schirmbeck, "Beware: Processing of Personal Data—Informed Consent Through Risk Communication,"in *IEEE Transactions on Professional Communication*, vol. 67, no. 1, pp. 4-25, March 2024

Extract- The results provide controllers, regulatory bodies, data subjects, and experts in the field of professional communication with information on risk formation in personal data processing. Based on our analysis, we propose information categories for risk communication, which expand the current regulatory information requirements.

[5] H. Chen and Z. Hu, "Exploring Data Traceability Methods in Information Management Within Universities: An Action Research and Case Study Approach," in IEEE Access, vol. 12, pp. 175196-175217, 2024

Extract- As university information management grows increasingly complex, the demand for seamless data sharing and interaction across various departments and faculties has surged. However, many universities lack a unified platform for data traceability and sensitive information protection, heightening security risks during frequent data exchanges. Furthermore, the uneven allocation of network resources and the absence of effective traffic analysis tools hinder universities from efficiently managing these resources, exacerbating the challenges of network management. Tight budgets further complicate cybersecurity infrastructure development, particularly as universities expand and diversify their disciplines, leading to even more imbalanced funding and constrained investment in network security. To address these challenges, this paper presents a data traceability system integrating Deep Packet Inspection (DPI) and Deep Flow Inspection (DFI) technologies.

[6] P. Yang, N. Xiong and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," in IEEE Access, vol. 8, pp. 131723-131740, 2020

Extract- The new development trends including Internet of Things (IoT), smart city, enterprises digital transformation and world's digital economy are at the top of the tide. The continuous growth of data storage pressure drives the rapid development of the entire storage market on account of massive data generated. By providing data storage and management, cloud storage system becomes an indispensable part of the new era.

Currently, the governments, enterprises and individual users are actively migrating their data to the cloud. Such a huge amount of data can create magnanimous wealth. However, this increases the possible risk, for instance, unauthorized access, data leakage, sensitive information disclosure and privacy disclosure. Although there are some studies on data security and privacy protection, there is still a lack of

 DOI : 10.35291/2454-9150.2025.0037

systematic surveys on the subject in cloud storage system. In this paper, we make a comprehensive review of the literature on data security and privacy issues, data encryption technology, and applicable countermeasures in cloud storage system. [2] [3] [4] [5] [6] [7] [8] [9]

[7] G. B. Herwanto, F. J. Ekaputra, G. Quirchmayr and A. M. Tjoa, "Toward a Holistic Privacy Requirements Engineering Process: Insights From a Systematic Literature Review," in IEEE Access, vol. 12, pp. 47518-47542, 2024

Extract- Privacy requirements engineering is a crucial aspect of privacy engineering. It aims to integrate privacy principles into organizational and technical processes throughout the software development lifecycle. This specialized field involves various strategies, including compliance with regulatory frameworks, asset analysis, and system diagram development for threat modeling. The wide range of approaches, while beneficial in providing different perspectives, presents a significant challenge to the novice privacy engineer or developer in identifying the most effective methodologies. The lack of a single methodology highlights the need for a systematic literature review (SLR) to establish a standardized process for privacy requirements engineering that promotes consistency across different methodologies. To address this issue, we conducted a comprehensive SLR to synthesize existing privacy requirements in engineering methodologies. Our analysis involved dissecting each method's processes, tasks, techniques, work products, and resources.

[8] A. Majeed and S. O. Hwang, "Quantifying the Vulnerability of Attributes for Effective Privacy Preservation Using Machine Learning," in IEEE Access, vol. 11, pp. 4400-4411, 2023

Extract- Personal data have been increasingly used in data-driven applications to improve quality of life. However, privacy preservation of personal data while sharing it with analysts/ researchers has become an essential requirement to be met by data owners (hospitals, banks, insurance companies, etc.). The existing literature on privacy preservation does not precisely quantify the vulnerability of each item among user attributes, thereby leading to explicit privacy disclosures and poor data utility during published data analytics.

In this work, we propose and implement an automated way of quantifying the vulnerability of each item among the attributes by using a machine learning (ML) technique to significantly preserve the privacy of users without degrading data utility. Our work can solve four technical problems in the privacy preservation field: optimization of the privacy-utility trade-off, privacy guarantees (i.e., safeguard against identity and sensitive information disclosures) in imbalanced data (or clusters), over-anonymization issues, and rectifying or enabling the applicability of prior privacy models when data have skewed distributions.

III. KEY INTERNATIONAL DATA PROTECTION LAWS

A. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) was implemented in 2018 and stands as one of the most comprehensive and stringent data protection laws in the world [1], [4]. Its primary objective is to safeguard the personal data of European Union (EU) residents, extending its reach to any organization that processes the data of EU citizens, irrespective of the organization's location. The regulation covers the entire lifecycle of personal data, including its collection, storage, processing, transfer, and deletion. One of the most important aspects of the GDPR is its extraterritorial scope, meaning that any entity, even outside the EU, that processes the personal data of EU residents must comply with the law.

GDPR introduces several key principles that organizations must adhere to ensure the protection of personal data [1]. Among the most significant is the principle of *Data Protection by Design and by Default*, which mandates that data protection measures be integrated into business processes from the very beginning and that the default settings of any system or service should favor data protection. The *Data Minimization* principle emphasizes that only the minimum amount of data necessary for a specific purpose should be collected, and data should not be kept longer than necessary for that purpose. Furthermore, GDPR mandates that organizations demonstrate *Accountability and Transparency*, meaning that they must not only comply with the regulation but also be able to prove compliance. This includes providing clear and detailed information to individuals about how their data is being used and obtaining explicit consent where necessary before data collection begins.

The GDPR also grants individuals enhanced rights over their personal data, such as the *Right to Access*, *Right to Rectification*, *Right to Erasure* (commonly known as the 'Right to be Forgotten'), and *Right to Data Portability* [1], [2]. Moreover, the regulation includes strict provisions for data breach notification, requiring organizations to notify affected individuals and the relevant authorities within 72 hours of a data breach. Non-compliance with the GDPR can result in hefty fines, up to 4% of an organization's global annual revenue or €20 million, whichever is higher.

B. California Consumer Privacy Act (CCPA) – United States

The California Consumer Privacy Act (CCPA) was enacted in 2018 to provide California residents with enhanced privacy rights and consumer protection [2]. The CCPA applies to businesses that collect, process, or sell the personal data of California residents and meets certain thresholds, such as having gross annual revenues over $25 million or dealing with the personal data of 50,000 or more consumers. The law focuses primarily on transparency and consumer control over personal data. It was one of the first significant state-level privacy laws in the United States and has inspired other states

 DOI : 10.35291/2454-9150.2025.0037

to propose or enact similar legislation. The CCPA grants California residents, rights regarding their personal data. The *Right to Know* allows consumers to request information about the categories and specific pieces of personal data a business collects about them, as well as how it is used and shared.

The *Right to Delete* permits consumers to request the deletion of their personal data from a business's records, subject to certain exceptions, such as when the data is necessary for legal or contractual purposes [2], [4]. The *Right to Opt-Out* gives consumers the ability to prevent businesses from selling their personal data to third parties. Additionally, the *Right to Non-Discrimination* ensures that consumers cannot be discriminated against by businesses for exercising their privacy rights, meaning they cannot be charged higher prices or provided with inferior services if they choose to opt-out of data sales or request deletion. To ensure compliance, businesses must implement measures to verify consumer requests and maintain records of the actions they have taken to respect consumer rights. Businesses must also update their privacy policies to clearly disclose their data practices and inform consumers of their rights under the CCPA. The law also imposes penalties for non-compliance, including fines for violations of the law, which can escalate if a business fails to address issues following a notice of non-compliance.

C. Digital Personal Data Protection (DPDP) Bill – India

The Digital Personal Data Protection (DPDP) Bill is India's first comprehensive legislation aimed at safeguarding the personal data of Indian citizens [4]. The bill was introduced in 2022 and is a significant step toward bringing India's data protection regime in line with global standards, particularly those established by the European Union's GDPR. The DPDP Bill is designed to address the growing concerns regarding data privacy and the increasing volume of personal data being collected, processed, and stored by both Indian and international organizations. The bill seeks to balance the protection of privacy with the need to foster innovation and economic growth, particularly in the technology and data-driven sectors.

The DPDP Bill provides Indian citizens with several important rights over their personal data [4]. The *Right to Access* allows individuals to obtain a copy of the personal data held about them and to seek corrections to any inaccuracies. The *Right to Data Portability* allows individuals to transfer their personal data from one service provider to another, empowering consumers to switch services more easily while retaining control over their data.

The bill also provides a *Right to Erasure* or *Right to be Forgotten*, allowing individuals to request the deletion of their data in certain circumstances, such as when it is no longer needed or if it was processed unlawfully [2], [4].

The DPDP Bill imposes significant obligations on organizations that process personal data, including the requirement for obtaining clear and informed consent from individuals before collecting their data [1], [4]. It states that personal data should be processed in a transparent manner and that individuals are notified about how their data is being used. In addition, the bill introduces the concept of *Data Localization*, requiring certain types of sensitive personal data to be stored and processed within India. This provision is designed to ensure that the government has greater control over how personal data is handled and to mitigate potential security risks arising from the cross-border flow of data.

IV. THE IDPR PROJECT: A COMPRIHENSIVE SOLUTION

A. Project Purpose and Scope

The primary purpose of this project is to enhance data privacy and security through the implementation of a robust encryption framework. Users can securely upload their sensitive data, such as personal information, which is encrypted using the encryption algorithm before storage. When users wish to access their data, it is decrypted securely upon request, ensuring end-to-end data protection.

The scope includes:

Implementing a secure user authentication system with login and signup functionalities [2].

Ensuring encrypted storage and retrieval of sensitive user data [6].

Complying with global data privacy regulations like GDPR and CCPA to build trust and ensure legal compliance [1], [2], [4].

Using modern web development technologies for scalability and user-friendly design [2].

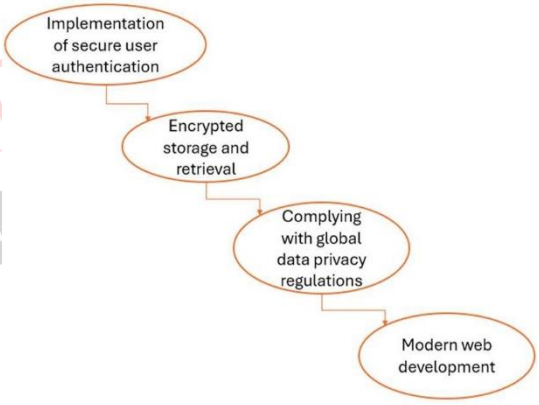

Figure 1. Project overview

To safeguard user data, the IDPR project focuses on putting in place a secure authentication system with signup and login features [2], [6]. The system will allow users to register and log in, and passwords will be encrypted before being stored. Session cookies or JWT tokens will be utilized for secure authentication after a successful login. Sensitive API routes will be protected by middleware, and session management will maintain security by regularly expiring tokens. For further security, multi-factor authentication (MFA) can be used. To prevent unwanted access, the authentication procedure will be made to be effective, safe, and easy to use.

For encrypted storage and retrieval of sensitive data,

 DOI : 10.35291/2454-9150.2025.0037

passwords and personal user information will be stored securely using strong encryption algorithms (e.g., bcrypt, AES-256) [6], [8]. When retrieving data, only authorized users will have access, ensuring privacy and security. Secure file uploads and end-to-end encryption for sensitive files will also be implemented to protect user information.

The system will incorporate data access restrictions, user consent management, and the right to data deletion to adhere to international data privacy laws such as the CCPA and GDPR [1], [2], [4]. Users will oversee their data, and privacy regulations will conform to global norms. Security and compliance will be guaranteed by encryption, role-based access control (RBAC), and logging systems.

To ensure scalability, performance, and an intuitive design, the project will utilize React for the frontend, Spring Boot for the backend, and MySQL for the database [2]. The system will be quick, safe, and easy to use thanks to responsive UI/UX, effective API connectivity, and enhanced security.

B. Key Features of the Project

The project is designed with several essential features that align with current data protection needs:

AES-256 (Advanced Encryption Standard with a 256-bit key) is a symmetric encryption algorithm used to secure data [6]. It uses a 256-bit key for encryption and decryption, making it highly secure and resistant to brute-force attacks

User Authentication and Authorization: Implements a secure mechanism for login and signup to validate user identity and restrict unauthorized access [2], [8].

Data Access Control: Allows users to view or retrieve only their encrypted data, ensuring confidentiality and integrity [3], [6].

Regulatory Compliance: Aligns with international data protection laws to safeguard user rights [1], [2], [4].

Scalable Architecture: Utilizes a robust backend (Java Spring Boot) and modern frontend frameworks (React JS) to accommodate growing user demands [2].

Secure Database Integration: Uses MySQL with encryption at rest to store user data securely [6].

Objectives

The objectives of this project are as follows:

- **Data Security:** Ensure sensitive data is protected from breaches through encryption [3], [6].
- **User Empowerment:** Provide users with control over their data, including uploading, accessing, and deleting it [1], [2], [4].
- **Ease of Use:** Develop an intuitive user interface with a seamless experience for data upload and retrieval [2].
- **Adaptability:** Build a system that can integrate additional data protection features or adapt to new regulations [4].
- **Operational Efficiency:** Leverage technologies like JDBC SQL for efficient data handling and Maven for dependency management.

C. Challenges Addressed

- **Data Breaches:** Prevent unauthorized access by implementing a secure encryption and decryption mechanism [5], [6].
- **Encryption Overhead:** Optimize implementation to ensure encryption does not hinder system performance [6], [8].
- **User Privacy Rights:** Comply with strict legal frameworks to protect user rights over their data [1], [2], [4].
- **Key Management:** Securely generate, store, and manage encryption keys [6], [8].

D. Technology Stack Overview

The project leverages a combination of modern technologies to ensure security, scalability, and efficiency [2]. Each component plays a crucial role in achieving the overall goals of secure authentication, data protection, and compliance with global privacy laws**.** For the frontend**,** the project utilizes HTML, CSS, and JavaScript to create a responsive and interactive user interface**.** These technologies ensure that the website is visually appealing and works well across different devices. React JS is used as the primary frontend framework, offering **dynamic** and efficient UI with a component-based structure, state management, and fast rendering. This enhances the overall user experience and enables smooth interactions with the backend.

The backend is powered by Java Spring Boot, which handles business logic, authentication, and API communication [2]**.** Spring Boot simplifies development by providing a robust framework for building secure and scalable applications. Maven is used for dependency management and efficient project builds, ensuring that the backend remains well-structured and easy to maintain. The backend processes user authentication, encrypts sensitive data, and enforces security policies.

For database management, MySQL is used to store encrypted user data securely [6]. It provides strong indexing and query optimization for fast data retrieval while ensuring data integrity**.** JDBC SQL is implemented to facilitate **seamless** database connectivity and execute SQL queries efficiently, allowing the backend to interact with the database securely.

To ensure secure data handling**,** the project integrates AES-256 encryption, a 256-bit symmetric encryption algorithm that protects sensitive user information [6], [8]. This encryption standard ensures that stored data remains **highly secure**, preventing unauthorized access. When users interact with the system, their data is encrypted before being stored in the database and decrypted only for authorized retrieval. This guarantees compliance with GDPR, DPDP and CCPA while maintaining high security standards.

E. Workflow and System Architecture

User Registration and Authentication:

 DOI : 10.35291/2454-9150.2025.0037

Users register or log in using the frontend interface, where authentication data is securely transmitted to the backend API [2].

Data Upload:

When users upload data, the system encrypts it using algorithm before storing it in the MySQL database [6].

Data Access:

When requested, the backend decrypts the user's data securely and sends it back to the front end for display [3], [6].

V. System Architecture and Design

A. *Presentation Layer*

The presentation layer forms the front-facing component of the system, ensuring a user-friendly interface for administrators and end users [2].

Purpose:

Directly interacts with users to provide intuitive navigation and responsive design for secure access.

Components:

Login and Signup Interfaces:

Allows users to register and log into the system securely [2].

Employs secure authentication mechanisms to validate user credentials.

Administrative Dashboard:

Enables administrators to manage user privacy rights, view logs, monitor requests, and configure system settings.

User Portal:

Facilitates end users in uploading data, viewing encrypted data, and managing their privacy preferences [2], [3].

Design Principles:

Focuses on responsive design using HTML, CSS, and

React.js for cross-platform compatibility [2].

Integrates user role-based access controls to distinguish between admin and end-user functionalities.

Ensures authentication and authorization are seamless and secure.

Technologies Used:

Frontend stack: **HTML, CSS, JavaScript, React.js**. Responsive design frameworks like Bootstrap (optional).

B. *Application Layer*

The application layer is the backbone of the system, handling business logic, encryption processes, and regulatory compliance [3], [6].

Purpose:

Executes core functionalities, such as data encryption, decryption, and compliance checks.

Responsibilities:

Encryption and Decryption using AES 256:

Implements the AES 256 algorithm for securing user-uploaded data. Encrypts data at the point of upload and decrypts upon user request securely.

Authentication and Authorization:

Verifies user credentials and roles through secure protocols [2], [8].

Data Request Processing:

Executes encryption/decryption logic and manages data upload/download workflows [6].

Regulatory Compliance Verification:

Ensures system functionalities align with global standards like GDPR, DPDP and CCPA [1], [2], [4].

Technologies Used:

Backend stack: Java Spring Boot, Maven.

Middleware for monitoring, error handling, and logging to ensure smooth operations.

C. *Data Layer*

The **Data Layer** focuses on securely storing encrypted user data and managing encryption key lifecycles, ensuring compliance and privacy [6], [8].

Purpose

To provide secure and scalable storage while maintaining compliance with data retention policies.

Key Features

AES-256 based Encrypted Data Storage

User-uploaded data is encrypted using the AES-256 algorithm before storage.

Encrypted data is stored in JDBC SQL databases, ensuring robust data security.

Data Retention Policies:

Automatically deletes data based on predefined retention timelines or user-initiated deletion requests [1], [2], [4].

Complies with legal and regulatory requirements for data management.

Technologies Used

Database: MySQL integrated with JDBC for seamless backend connectivity.

Encryption Library: Custom AES-256 encryption module, securely integrated with backend services [6], [8].

D. *Infrastructure Layer*

The Infrastructure Layer ensures system reliability, performance, and scalability to effectively manage user demands.

Purpose

To provide a robust foundation for high availability and optimal system performance.

Key Features

Scalability and Load Balancing

Load balancers distribute user requests efficiently across multiple servers.

 DOI : 10.35291/2454-9150.2025.0037

Supports horizontal scaling by dynamically adjusting server resources based on traffic demands.

Disaster Recovery and Redundancy

Automated backups and geographic replication prevent data loss during system outages [5].

Failover systems ensure minimal downtime and uninterrupted service.

E. Data Flow Process

The overall system design ensures a secure and efficient flow of data from user interaction to secure storage and retrieval.

User Authentication

Users log in or register through the frontend, providing credentials that are securely validated by the backend [2]. Passwords are hashed, and user roles are assigned to enforce access control. Multi-factor authentication (MFA) may be implemented for added security.

Data Upload and Encryption

Users upload data through a secure web portal [3], [6]. The backend encrypts the data using AES-256 before storing it in the database. Encryption keys are managed securely to prevent unauthorized access.

Data Retrieval and Decryption

When users request their data, the backend retrieves the encrypted data, decrypts it using secure keys, and transmits it safely [6], [8]. Only authorized users can access decrypted information.

Monitoring and Logging

All activities, including authentication, data uploads, and access requests, are logged [5]. Logs are stored securely and analysed to detect irregularities, ensuring compliance and security.

Compliance Assurance

The system follows regulations like GDPR, DPDP and CCPA, enforcing strict data handling policies [1], [2], [4]. Users have control over their data, and compliance measures help prevent legal risks.

VI.RESULTS AND DISCUSSIONS

A. Key Generation

AES-256 (Advanced Encryption Standard with a 256-bit key) is a symmetric encryption algorithm used to secure data [6]. It uses a **256-bit key** for encryption and decryption, making it highly secure and resistant to brute-force attacks. AES operates on data in blocks of 128 bits and uses substitution, permutation, and multiple rounds (14 rounds for AES-256) to transform plaintext into ciphertext. It's widely used in applications like secure file storage, HTTPS, and VPNs due to its strong encryption capabilities.

B. Data Encryption Methodology

AES-256 encrypts data by dividing it into fixed 128-bit blocks and transforming each block through 14 rounds of encryption [6], [8]. Each round includes four key steps:

AES-256 encryption follows a structured process to ensure the confidentiality of data [6] .It begins with the **AddRoundKey** step, where the plaintext block undergoes an XOR operation with a round-specific key derived from the original 256-bit encryption key. This step integrates the key into the data, strengthening its security. Next, the **SubBytes** transformation is applied, replacing each byte of the data block with a corresponding value from a predefined S-box, introducing non-linearity to resist cryptanalysis. The **ShiftRows** operation then shifts the rows of the data block, ensuring diffusion by rearranging byte positions. Following this, the **MixColumns** step enhances diffusion further by transforming each column of the block using a mathematical operation, except in the final encryption round where it is omitted to maintain reversibility. Since AES is a symmetric encryption algorithm, decryption follows the same steps in reverse order, using the same secret key. After encryption, the ciphertext is securely stored in a MySQL database, which is protected with strict access controls to prevent unauthorized access [6]. Special attention is given to securing the metadata associated with the encrypted data, ensuring that even if the database is compromised, the stored data remains unreadable without the correct decryption key. This approach adds an essential layer of security, safeguarding sensitive user information from potential breaches and unauthorized disclosures.

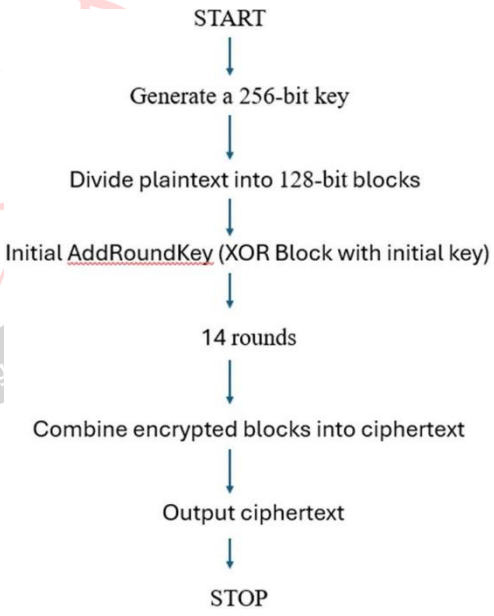

Figure 2. Data Encryption Methodology

Both the decryption and data retrieval procedures are similarly exacting [6], [8]. The system fetches the encrypted data from the database and verifies the user's credentials before granting access to the user's information. The system meticulously decrypts the ciphertext and returns it to its original plaintext form using the private key. To guarantee that only authorized users can access the original material, this procedure entails a precise mathematical calculation that can only be completed with the private key.

Throughout the entire process, additional security measures are implemented for data transmission, periodic security

 DOI : 10.35291/2454-9150.2025.0037

audits, and continuous vulnerability assessments. The system leverages of cutting-edge technologies including React.js for the frontend, Java Spring Boot for the backend, and MySQL for database management, are all underpinned by a robust encryption standard [2], [6].

C. Key generation methodology

The key generation methodology of AES-256 involves creating a 256-bit (32 bytes) cryptographic key, which is used for encryption and decryption [6], [8]. Here's a brief explanation:

Key Size

AES-256 requires a 256-bit key (32 bytes) [6].

This ensures a high level of security against brute-force attacks.

Key Expansion (Key Scheduling)

AES uses a Key Expansion algorithm to derive multiple round keys from the original 256-bit key [6]. These round keys are used in each encryption round. The process involves: Input Key: Start with the 256-bit key provided by the user. Rounds: AES-256 requires 14 rounds, meaning 14 round keys are generated.

Rijndael Key Schedule: The original key is expanded using the following:

SubBytes: A substitute step using an S-box for non-linearity.

RotWord: A byte rotation to create diffusion.

Rcon (Round Constant): A constant XORed into the key to ensure uniqueness of each round key.

Key Storage and Security

The generated key must be securely stored to prevent unauthorized access [6], [8].

Common methods include secure key vaults or encrypting the key with another master key.

By securely generating and managing the key, AES-256 ensures robust encryption for sensitive data [6], [8].

VII. CONCLUSION

In conclusion, this research highlights the evolving landscape of data privacy and protection, emphasizing the indispensable role of encryption in securing sensitive information [3], [6]. The study explored encryption methodologies such as AES-256 and RSA, demonstrating how these cryptographic techniques provide robust security against unauthorized access and cyber threats. AES-256 was identified as a highly secure encryption algorithm widely adopted in industries such as finance, healthcare, and government due to its resistance to brute-force attacks and its efficiency in securing data at rest and in transit [6].

Additionally, the paper examined the impact of modern data privacy regulations, particularly the GDPR, CCPA and DPDP which establish strict guidelines on data collection, storage, and processing [1], [2], [4]. These regulations not only enhance individual control over personal data but also impose significant obligations on organizations to maintain compliance, reducing the risks of data breaches and legal penalties. The integration of encryption with regulatory requirements is crucial for businesses striving to build trust and ensure data security in an increasingly digital world.

The research also underscored the importance of strong encryption key management practices [6], [8]. Proper key management enhances data security by preventing unauthorized access to encrypted information, further strengthening an organization's defence against cyber threats. Moreover, the study emphasized the growing convergence between encryption advancements and regulatory frameworks, highlighting how businesses must adopt a holistic approach that combines technical security measures with legal adherence.

As cyber threats continue to evolve, future advancements in encryption algorithms, key management systems, and privacy-preserving technologies will play a pivotal role in enhancing data security. The integration of cutting-edge cryptographic methods with a comprehensive understanding of legal frameworks will be essential in ensuring secure and private data interactions. This research underscores that data protection is not merely a technical challenge but a multidimensional issue that requires continuous innovation, regulatory adaptation, and a proactive approach to safeguarding sensitive information in an interconnected digital era.

REFERENCES

[1]S.Wairimu,L.H.Iwaya,L.FritschandS.Lindskog," On the Evaluation of Privacy Impact Assessment and Privacy Risk Assessment Methodologies: A Systematic Literature Review," in *IEEE Access*, vol. 12, pp. 19625-19650, 2024

[2] L.H.Iwaya, M.A.Babar and A.Rashid," Privacy Engineering in the Wild: Understanding the Practitioners' Mindset, Organizational Aspects, and Current Practices," in*IEEE Transactions on Software Engineering*, vol. 49, no. 9, pp. 4324-4348, Sept. 2023

[3] A.Zigomitros,F.Casino,A.SolanasandC.Patsakis,"A Survey on Privacy Properties for Data Publishing of Relational Data," in *IEEE Access*, vol. 8, pp. 51071-51099, 2020

[4] H. Chen and Z. Hu, "Exploring Data Traceability Methods in Information Management Within Universities: An Action Research and Case Study Approach," in IEEE Access, vol. 12, pp. 175196-175217, 2024, doi: 10.1109/ACCESS.2024

[5] L. Seiling, R. Gsenger, F. Mulugeta, M. Henningsen, L. Mischau and M. Schirmbeck, "Beware: Processing of Personal Data—Informed Consent Through Risk Communication,"in *IEEE Transactions on Professional Communication*, vol. 67, no. 1, pp. 4-25, March 2024

[6] P. Yang, N. Xiong and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," in IEEE Access, vol. 8, pp. 131723-131740, 2020

[7] G. B. Herwanto, F. J. Ekaputra, G. Quirchmayr and A. M. Tjoa, "Toward a Holistic Privacy Requirements Engineering Process: Insights From a Systematic Literature Review," in IEEE Access, vol. 12, pp. 47518-47542, 2024

[8] A. Majeed and S. O. Hwang, "Quantifying the Vulnerability of Attributes for Effective Privacy Preservation Using Machine Learning," in IEEE Access, vol. 11, pp. 4400-4411, 2023.

 DOI : 10.35291/2454-9150.2025.0037