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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14408

# IDPR –International Data Privacy and Regulation

**Sanika Chawhan[1], Deepali Patil[2], Shreya Shimpi[3], Vaishnavi Gajare[4], Mrs. Deepti Janjani[5]**

Students, Department of AI & DS, Datta Meghe College of Engineering, Navi Mumbai, India[1-4]

Assistant Professor, Department of AI & DS, Datta Meghe College of Engineering, Navi Mumbai, India[5]

**Abstract:** Our project ultimately aims to offer a scalable and flexible solution that can be customized to meet the specific needs of various industries, from finance to healthcare. By ensuring compliance with data privacy regulations and implementing a robust security framework, our project not only protects sensitive data but also helps organizations build trust with customers and regulatory authorities. Its comprehensive approach ensures that data management practices align with both current and future data protection requirements.

With digital connectivity at an all-time high, protecting personal information has become a matter of utmost concern for individuals, organizations, and governments around the world. This paper delves into the complex world of International Data Privacy Regulation (IDPR) and offers a comprehensive solution to tackle global data protection issues. An Electronic Health Record (EHR) is an electronic copy of a patient's paper chart, intended to hold a complete, up-to-date, and patient-focused set of health data. It is utilized by clinics, hospitals, and healthcare providers to coordinate care efficiently.

**Keywords:** Data Privacy, React.Js, Node.Js, MongoDB, Axios, Express.js, Tailwind CSS, Bcrypt

## I. INTRODUCTION

### I. Introduction

In today’s digital landscape, data serves as the driving force behind the global economy. Personal information is transferred across borders at an unparalleled rate, fueling advancements in technology, healthcare, finance, and countless other sectors. However, this vast exchange of information presents significant challenges in safeguarding individual privacy and ensuring responsible data use. As data breaches and privacy scandals continue to make headlines, governments worldwide have responded by implementing increasingly stringent data protection regulations.
The global data privacy regulatory framework is fragmented and complex, with individual countries and regions establishing their own rules and requirements. This disjointed regulatory environment poses substantial challenges for international businesses, as they must navigate a web of diverse and sometimes conflicting compliance mandates. Regulations such as the European Union’s General Data Protection Regulation (GDPR) and California’s Consumer Privacy Act (CCPA) are examples of leading data protection laws, but they represent only part of the global legal landscape.

### I.2. Motivation

The motivation behind the International Data Privacy Regulation project stems from the critical need to address the following challenges:

Importance of Data Privacy, Personal data is today a valuable asset in the international digital economy. Keeping such information safe is not merely a legal requirement but a moral duty to secure people's privacy and safety. Global Data Privacy Challenges, Global laws vary in scope, definition, and enforcement mechanisms, presenting an issue for organizations attempting to guarantee compliance. Given the intricacies, a concerted framework such as IDPR is essential to facilitating compliance efforts while promoting international data privacy.

### I.3. Problem Statement

To create a platform ensuring data privacy and security for electronic health records (EHR) by developing a secure and compliant system. It will encrypt patient data, prevent unauthorized access, and adhere to healthcare regulations like the Health Insurance Portability and Accountability Act (HIPAA). The solution is designed for the IDPR, data privacy, and healthcare domains to enhance system security and regulatory compliance.

**Objectives:**

Our project objective is to encrypt patient data using robust encryption techniques. Store encrypted data securely using MongoDB. Ensure seamless and secure data communication. Develop a scalable and user-friendly system.

### 1.4 Organization of report:

This paper presents the literature survey in Chapter 2, investigating various available methods and their limitations. Chapter 3 focuses on the system design and implementation of the whole research. showcasing various steps to create the project. The results are displayed in Chapter 4, and this paper is concluded in the last chapter

## II. LITERATURE SURVEY

**1) On the Evaluation of Privacy Impact Assessment and Privacy Risk Assessment Methodologies: A Systematic Literature Review**

https://ieeexplore.ieee.org/document/10 418587

The paper "On the Evaluation of Privacy Impact Assessment and Privacy Risk Assessment Methodologies: A Systematic Literature Review" by Wairimu et al. presents a comprehensive evaluation of existing methodologies for Privacy Impact Assessments (PIAs) and Privacy Risk Assessments (PRAs). The study highlights the significance of such methods in implementing privacy-by-design principles, especially in highly regulated environments like the EU General Data Protection Regulation (GDPR). Using a systematic literature review, the authors identified 39 relevant studies, concluding that despite numerous PIA and PRA methods having been proposed, very few have undergone rigorous testing or evaluation. Notably, PIAs have been evaluated more often than PRAs, often through case studies. However, the term "case study" is applied inconsistently, at times to outstanding examples instead of empirical research, casting uncertainty on the applicability of these methods to practice. The paper recognizes a lack of standardization in the development of PIAs, leading to differences in scope and focus among methodologies. There are industry-specific PIAs, such as artificial intelligence or data provenance, and general PIAs. The authors further note that most methodologies do not adequately assess privacy harms, an important aspect of privacy risk assessments overall. When considering PRAs, the study identified that while the majority of approaches assess levels of risk in relation to likelihood and impact, differing methods are applied, using qualitative judgments for some and semi-quantitative or quantitative methods in others. Privacy harms are more prevalent in PRAs compared to PIAs, but are yet to be incorporated in practical use to a greater degree. The authors suggest more rigorous validation and testing of PIA and PRA methods so that they can be shown to be of use in real-world applications. They advocate methods that are theoretically sound but also realistically implementable, with adequate guidance and illustration of effective application. This study offers a rich source for both practitioners and researchers seeking to identify the state of the art in privacy evaluation methods, and also highlights where new innovation and standardization are needed Privacy Engineering in the Wild: Understanding the Practitioners' Mindset, Organizational Aspects, and Current Practices

https://ieeexplore.ieee.org/document/10 167784

The paper "Privacy Engineering in the Wild: Understanding the Practitioners' Mindset, Organizational Aspects, and Current Practices" by Iwaya, Babar, and Rashid presents an in-depth examination of how privacy is conceived and achieved by software practitioners in the wild. Based on 30 interviews with nine countries, the study uncovers the complexities and challenges of incorporating privacy into software development practices. One of the central themes of the research is practitioners' individual privacy mentality, encompassing their attitudes, awareness, and practices towards privacy. While all participants recognize the importance of privacy, excessive overreliance on traditional security methods, for instance, data anonymization and encryption, dominates at the expense of more abstract privacy principles like data minimization and transparency to users. This captures a common perception of privacy primarily in data protection terms, potentially to the neglect of other privacy engineering fundamentals. The study also identifies the significant influence of organizational culture on privacy practice. A positive privacy climate, characterized by active leadership, open communication, and congruence between individual and organizational values, supports more effective privacy outcomes. Conversely, cultures in which privacy is not valued or is perceived as a compliance exercise can hinder effective privacy integration. Some practitioners even felt frustrated or disengaged when their own privacy values were at odds with organizational priorities. From a pragmatic usage point of view, the research indicates minimal standardized procedures in handling issues of privacy and few training or incentives provided on privacy and security. Practitioners do sometimes take initiative on their part to open privacy issues for discussion, but without no arrangements, such issues may not get the proper attention they deserve. The study advises that organizations have to make an investment in educating themselves on privacy, as well as implement well-defined protocols to help practitioners in deploying measures for privacy successfully.

DOI: 10.17148/IJARCCE.2025.14408

As a whole, the paper emphasizes how harmonizing the mindsets of individuals, the culture of the organization, and the hands-on tools is the key to taking privacy engineering further. By providing settings where privacy is valued, proper training is provided, and standardized practices are developed, organizations can prepare practitioners better to navigate the complexities of privacy in software development. The holistic approach is needed in an effort to engrave privacy in the very DNA of technological innovation.

**2) A Survey on Privacy Properties for Data Publishing of Relational Data**

https://ieeexplore.ieee.org/document/90 32138

The Paper "A Survey on Privacy Properties for Data Publishing of Relational Data" by Zigomitros, Casino, Solanas, and Patsakis provides a comprehensive survey of the challenges and solutions pertaining to Privacy-Preserving Data Publishing (PPDP) in relational databases. With the increasing practice of data sharing and mining, privacy risks of individuals in re-identification attacks increase proportionally. The writers point out that deleting explicit identifiers like names or social security numbers is not sufficient, as attackers can employ quasi-identifiers like gender, birthday, and zip code to re-identify victims and obtain sensitive data. Against such challenges, the paper discusses various anonymization techniques developed to minimize the risk of privacy without undermining the data utility. Some of the most important methods discussed are k-anonymity, which provides a guarantee that each record cannot be distinguished from at least k−1 records with respect to some identifying values; ℓ-diversity, an extension of k-anonymity but with the further guarantee of having diversity in the sensitive values in groups; and t-closeness, with further privacy gains by maintaining the distribution of the sensitive values within groups close to the global one. The authors provide real-world examples to illustrate how each method operates and the specific circumstances under which they are most effective. Also, the paper considers some attack models threatening data privacy, such as linkage attacks in which attackers join anonymized information with external knowledge to re-identify individuals, and attribute disclosure attacks aiming at inferring sensitive information without explicitly re-identifying individuals. The authors include potential countermeasures to the attacks, underscoring proper anonymization approach selection based on data type and target use cases. In addition to examining existing methodologies, the authors point out open problems and directions for future research in PPDP. They stress the need to develop stronger privacy models that are robust enough to adapt to the evolving data sharing and analytics environment. The paper is a valuable addition to researchers and practitioners seeking to understand the current state of privacy-preserving techniques for relational data and the current work seeking to balance data utility and personal privacy.

**3) Integrating Technical and Legal Concepts of Privacy**

https://ieeexplore.ieee.org/document/83 58762

The paper "A Survey on Privacy Properties for Data Publishing of Relational Data" by Zigomitros, Casino, Solanas, and Patsakis provides a comprehensive survey of the challenges and solutionsconcerning Privacy-Preserving Data Publishing (PPDP) in relational databases. With the growth of data sharing and mining activities, individual privacy threats in re-identification attacks are also increasing proportionally. The authors point out that de-identification by removing obvious identifiers like names or social security numbers is insufficient, as attackers can utilize quasi-identifiers like gender, date of birth, and zip code to re-identify victims and obtain sensitive information. The paper "Integrating Technical and Legal Concepts of Privacy" by Sokolovska and Kocarev is an overall analysis of the two dynamics between the technical methods and the legal solutions for data privacy. The authors discuss the European Union's General Data Protection Regulation (GDPR), its foundational principles such as the right to erasure (also popularly referred to as the 'right to be forgotten'), data protection by design and by default, and the necessity of data protection impact assessments. The legal concepts are contrasted with technical solutions involving differential privacy, which offers quantifiable protection to individual data in statistical computations. Most of the paper is occupied with discussing the challenges of reconciling legal specifications with technical applications. The authors point out the ambiguities due to different meanings of privacy between jurisdictions, particularly contrasting and comparing the EU's comprehensive data protection system with the United States' sectoral and typically fragmented regime.

This deviation emphasizes the necessity for an interdisciplinary approach that balances legal needs and technological solutions to establish robust data protection. Further, the paper talks about personalized privacy, with an appeal for systems that provide users with control over their personal data. Although personalization can enhance user autonomy, the authors also know of traps, like the 'privacy paradox,' where users are concerned about privacy but act in ways that compromise it. They appeal for greater privacy awareness and the development of tools that facilitate informed user decision-making. In effect, Sokolovska and Kocarev's paper is a groundbreaking study that depicts the multifaceted character of data privacy. By bridging the gap between legal theories and technical practices, the article offers valuable information on the way forward to come up with holistic approaches in countering the complexity of privacy during this modern era. To combat such challenges, the paper discusses various anonymization approaches developed to diminish the risk of privacy without impeding the value of the information. Some of the major methodologies discussed

DOI: 10.17148/IJARCCE.2025.14408

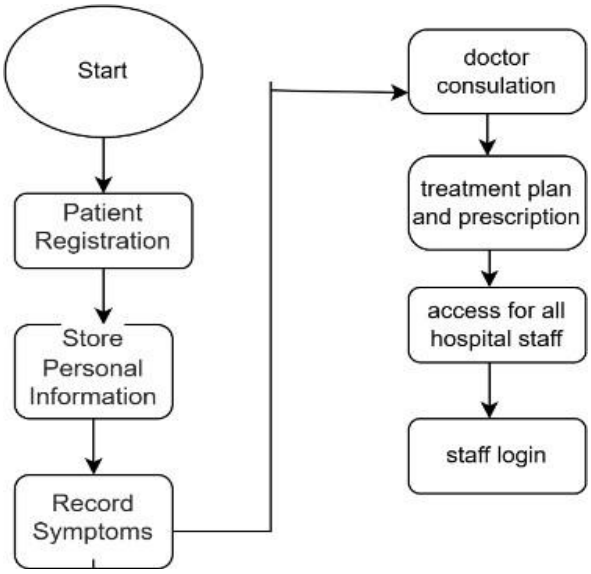
are k-anonymity, which ensures that each record is indistinguishable from a minimum of k−1 other records on some identifying attributes; ℓ-diversity, which is an improvement of k-anonymity with the extra promise of diversity on sensitive attributes across groups; and t-closeness, which has an extra layer of privacy assurance by maintaining the distribution of sensitive attributes within groups near to the global distribution. The authors provide practical examples to illustrate how each method operates and the specific circumstances under which they are most effectively applied. Besides, the article discusses a number of attack models threatening data privacy, such as linkage attacks in which the attackers combine anonymized data with external data to re-identify individuals and attribute disclosure attacks intended to infer sensitive information without necessarily re-identifying individuals. The authors present potential countermeasures to the attacks, highlighting the importance of using the right anonymization techniques based on the data type as well as the intended use cases. In addition to exploring existing methodologies, the authors stress open problems and directions for future research in PPDP. The authors stress that it is paramount to develop privacy models that are robust enough yet flexible enough to deal with shifting data sharing and analytics. The paper provides a valuable contribution to researchers and practitioners wishing to understand the current state of privacy-preserving techniques for relational data and the current work that strives to balance data utility with individual privacy.

## III. SYSTEM DESIGN AND IMPLEMENTATION

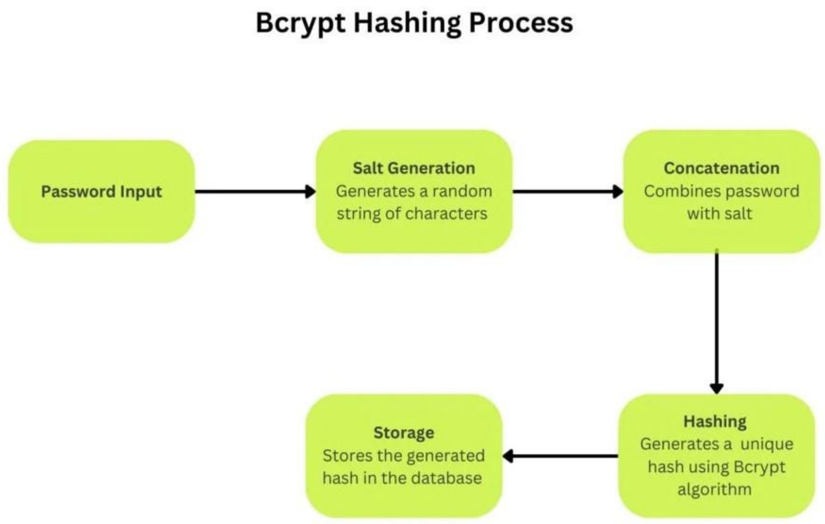
### 3.1. Framework

The International Data Privacy and Regulation (IDPR) platform, which is part of an Electronic Health Record (EHR) system, provides secure, scalable, and compliant patient data management. It adheres to international standards such as HIPAA, GDPR, and CCPA while streamlining healthcare operations with a multi-tiered architecture that includes presentation, application, data, and infrastructure layers. The presentation layer offers role-based interfaces to patients, healthcare practitioners, and administrators. Patients view their records and consent, while physicians and staff view medical history and prescriptions under strict access control.

Administrators configure system roles, logs, and compliance via a secure dashboard with multi-factor authentication and clear navigation. API frameworks like Spring Boot and Flask facilitate ease of system integration, with log and monitor tools providing system reliability. The infrastructure layer maintains scalability and performance through load balancing and caching methods such as Redis and Memcached, shortening response times and supporting high transaction volume. High availability is guaranteed through failover mechanisms, automatic backups, andgeo redundant replication. Compliance is strengthened through Zero Trust Architecture, fine-grained access controls, AI-driven compliance monitoring, and real-time threat detection. Through the integration of encryption, automated compliance, AI-based processing, and secure infrastructure, IDPR facilitates the safe, efficient, and legal management of healthcare data while improving patient ownership of their records.


Start
Patient Registration
Store Personal Information
Record Symptoms
doctor consulation
treatment plan and prescription
access for all hospital staff
staff login

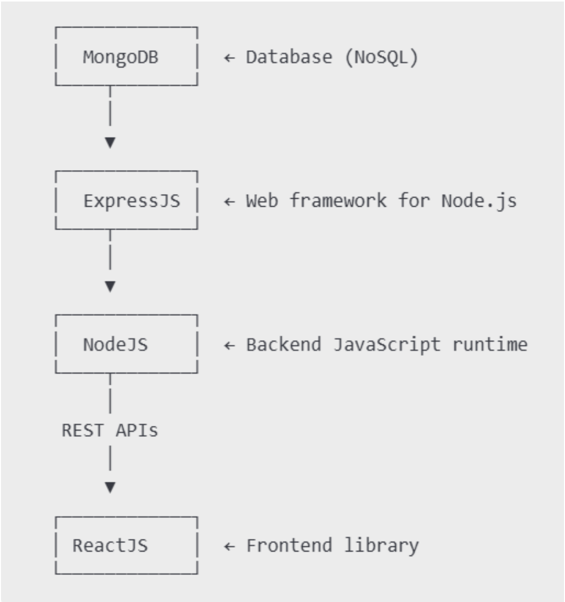
(Fig. 3.1 workflow of the project)


Bcrypt Hashing Process
Password Input
Salt Generation
Generates a random string of characters
Concatenation
Combines password with salt
Hashing
Generates a unique hash using Bcrypt algorithm
Storage
Stores the generated hash in the database

(Fig. 3.2 Bcrypt Algorithm)

The bcrypt method has a multi-step process of operation to keep passwords safe from storage and verification. When registering a user, a user gives a plaintext password, which is then made secure through a process of salting, where the plaintext password has a randomly selected salt added before hashing. This makes identical passwords not create the same hash, thus offering protection against rainbow table attacks. The bcrypt hash algorithm then performs several rounds (10 by default, but tunable) of the Blowfish cipher to cause the transformation to be extremely secure. The final hashed password, including the salt and cost factor, is then stored in the database for subsequent authentication.

At the time of user authentication, when the user logs in, the password is hashed again with the same salt and rounds as initially used. The newly created hash is then compared with the hash stored. If both are the same, authentication is successful; else, access will be denied. Bcrypt provides improved security through its computational cost feature, wherein the iterations (cost factor) can be raised with time to offset increasing computational power. This makes it computationally costly for attackers to break passwords. Therefore, bcrypt is still one of the best and most popular hashing algorithms for safe password storage.



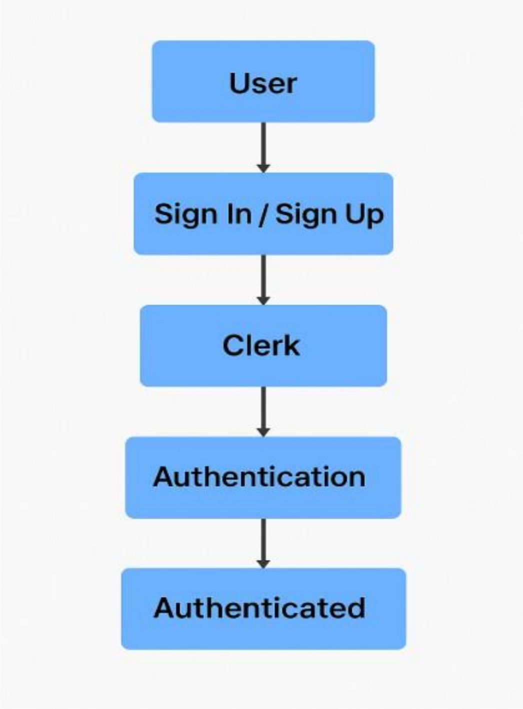
```
┌──────────┐
│ MongoDB  │  ← Database (NoSQL)
└──────────┘
     │
     ▼
┌──────────┐
│ ExpressJS│  ← Web framework for Node.js
└──────────┘
     │
     ▼
┌──────────┐
│ NodeJS   │  ← Backend JavaScript runtime
└──────────┘
     │
  REST APIs
     │
     ▼
┌──────────┐
│ ReactJS  │  ← Frontend library
└──────────┘
```

(Fig. 3.3 MERN Stack)

DOI: 10.17148/IJARCCE.2025.14408

The MERN stack consists of four primary technologies: MongoDB, Express.js, React.js, and Node.js, each having a distinct function in full-stack application development. Beginning with MongoDB, it is a NoSQL database that keeps application data in a flexible JSON-like structure referred to as BSON. One of its most prominent features is that it is schema-less, with documents being able to have varied fields, so it is very flexible and scalable. To communicate with MongoDB effectively in a Node.js environment, developers typically employ Mongoose, an Object Data Modeling (ODM) library that makes data handling and validation easier.

Second, Express.js is a light-weight web framework created on top of Node.js. It makes server-side logic easier to create by offering strong features to route, handle HTTP requests and responses, and attach middleware for operations like logging, data validation, and security. Express facilitates setting up API endpoints such as GET, POST, PUT, and DELETE, making backend development efficient and easy. Node.js itself is a robust JavaScript runtime environment based on Chrome's V8 engine. It supports running JavaScript on the server side and is famous for its non-blocking, asynchronous I/O model, which is perfect for developing high-performance, real-time applications like chat apps or live streaming platforms. Its greatest strength is letting developers use JavaScript both on the frontend and backend and ensuring code reusability and consistency throughout the stack. On the client-side, React.js, created by Facebook, is a JavaScript library to create interactive user interfaces. It has a component-based architecture and includes features such as the virtual DOM, which provides efficient updating and rendering. The use of state and props in React allows for seamless data flow and control of the UI, making the creation of dynamic and responsive web interfaces much simpler. All these technologies integrate smoothly into the MERN stack. The user engages with the frontend developed with React.js. When an action is performed, React makes HTTP requests, most commonly using fetch or AJAX, to the backend APIs developed with Express and Node.js. The APIs handle the request and communicate with MongoDB to retrieve or modify data. After the data operation has been executed, the response is returned along the same route to the frontend, and React updates the user interface accordingly. In a common MERN development cycle, the developers start by creating views, forms, and components using React. On the server side, they establish servers and routes with Express and Node.js. Data models like "User" or "Post" are designed and stored using MongoDB, and Mongoose serves as a middleman to enable the backend and the database to talk to each other. This stack architecture enables us to build new, efficient, and scalable web applications completely using JavaScript.

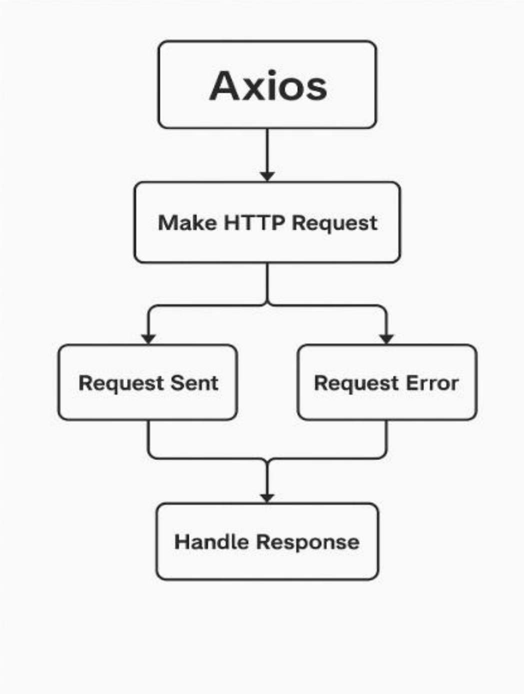


(Fig. 3.4 Clerk Algorithm)

Clerk is a user authentication and management platform that works perfectly with contemporary web applications. It supports a complete set of features such as user registration, login, session management, multi-factor authentication (MFA), and handling user profiles. Clerk provides pre-built UI components that can easily be embedded in frontend frameworks such as React, making it easy to add secure authentication.

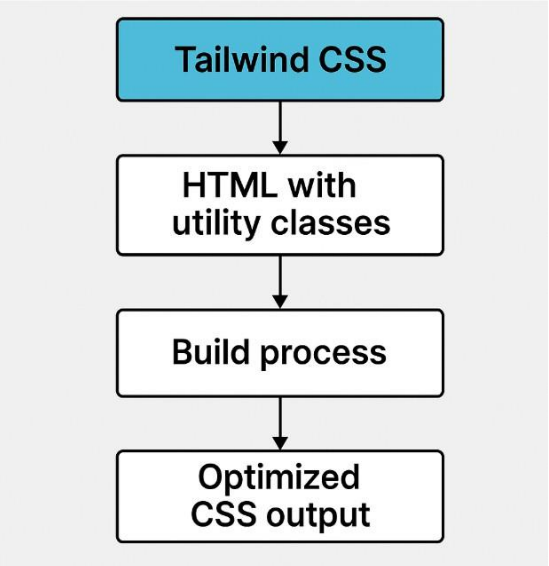
DOI: 10.17148/IJARCCE.2025.14408

It also allows for multiple authentication schemes like email/password, as well as OAuth suppliers like Google or GitHub. Within the patient data management system, Clerk will only allow authenticated users to view or manipulate sensitive health data. After a successful login, Clerk will create a secure session token to be used for authorizing backend API requests.



(Fig. 3.5 Axios Algorithm)

Axios, however, is a widely used promise-based HTTP client in JavaScript applications that interacts with backend servers. It has all the standard HTTP methods like GET, POST, PUT, and DELETE, which makes it highly suitable for CRUD operations. Axios makes it easier to send and receive JSON data and enables developers to set headers, handle errors, and implement request/response interceptors. Within this application, Axios is utilized by the React frontend to communicate with the backend services, e.g., by sending patient form data or retrieving existing records. Following Clerk authentication, Axios adds the user's session token to the headers of every API request so the backend can validate and authorize the request. Together, Axios and Clerk offer a safe and effective way of controlling user sessions and processing data transactions in the web application.



(Fig. 3.6 Tailwind Algorithm)

DOI: 10.17148/IJARCCE.2025.14408

Tailwind CSS is a utility-first, modern CSS framework that enables developers to quickly create unique user interfaces in HTML/JSX with small, flexible classes. Traditional CSS frameworks like Bootstrap offer pre-defined components, but Tailwind provides you with low-level utility classes so you can build components your way.

## IV. RESULTS AND ANALYSIS

**I.** The following information is derived from the output interface of MongoDB Compass, the graphical user interface (GUI) for database management. The interface displays an established connection to a local MongoDB server at localhost:27017, and the user is browsing through the "crud" database. The database has two collections, "Patient" and "patients." The "Patient" collection has one document of storage size 20.48 KB, whereas the "patients" collection is empty with no documents. The interface also gives information such as the average document size, number of indexes, and total index size for both collections. The options available in the interface indicate that the user can create new collections, refresh the database view, or open the MongoDB shell for command-line commands. The analysis suggests that the user is probably viewing database contents, managing collections, or about to perform CRUD (Create, Read, Update, Delete) operations in MongoDB Compass.

**II.** The following analysis is based on the observed output and interface of an application that is an online platform meant to handle user medical data. From the images shown, the frontend of the application is built utilizing React.js, providing a flexible and dynamic user interface. The application also supports Clerk Authentication, which can be inferred from the login page, providing secure user authentication and access control. The procedure followed in the application has several steps. A user logs in to the system via Clerk authentication. On successful authentication, the user is shown a patient data form wherein they can provide vital details like name, age, blood group, medical history, allergies, and ESR (Erythrocyte Sedimentation Rate). After the form submission, the data gets saved and reflected in the well-organized card format, and hence becomes an easy read for the users. Having a "Fetch My Data" option itself indicates that it is possible to retrieve and check old stored records of patients and suggests that the system operates within a CRUD (Create, Read, Update, Delete) operation process. The UI design of MediLock is modern and minimalistic in style, with a gradient background and card-based layout to make it user-friendly. The project is in development, as indicated by the apparent authentication debugging elements. In summary, MediLock integrates a secure authentication mechanism, organized data management, and an easy-to-use user interface to make patient medical record management easy.

**III.** The following description is derived from the visual output and interface elements of an app that seems to be a web-based patient record management system that has been possibly built with React.js for the frontend and Firebase or an SQL-based backend as the data store. The auth system visible on the screenshots hints at the employment of a Clerk to securely authenticate the users. The UI is tidy and trendy, with a gradient blue theme, card-style layout, and minimalist typography, so that it is user-friendly and easy for the eyes. The methodology adopted in this application starts with user verification, where only authentic users get access to the system. After logging in, the user is shown a patient entry form, where the user can fill in information like patientMname, age, blood group, medical history, allergies, and ESR (Erythrocyte Sedimentation Rate). Once the form is filled, the information is posted and saved securely within a database.

**IV.**The following analysis is based on the visual output and interface elements of a web-based patient data management system, which is designed for secure storage and retrieval of patient information. According to the user interface and authentication mechanism observed in the images, this system is most probably developed using React.js as the frontend technology combined with Tailwind CSS as the styling technology, offering a fresh and minimalist look. The backend seems to be serviced by Firebase or any other cloud-based database for effective management of data. Also, user authentication is managed by Clerk, as shown in the top-right user profile block, providing secure login and access control. The sequence of activities undertaken in this application begins with user authentication, wherein users log in with their credentials. Upon authentication, users are redirected to a patient data form in which they can enter information like patient name, age, blood group, medical history, allergies, and ESR (Erythrocyte Sedimentation Rate). Once submitted, the information is safely stored in the backend. It indicates the data retrieval feature, where users can retrieve and view stored patient records in a card-based, structured format. The system would probably be a CRUD (Create, Read, Update, Delete) type, allowing users to manage patient details efficiently.

## V. CONCLUSION AND FUTURE SCOPE

Our project is a visionary solution to the complex issues of global data protection. Through the incorporation of state-of-the-art encryption methods like RSA-based asymmetric encryption, our project provides secure management of sensitive information during storage and transmission. This strong data security approach protects against unauthorized access while building trust among users and stakeholders. Its focus on cutting-edge technologies makes our project a pioneer in data privacy solutions. With efficient data management, the system provides organizations with an effective method of processing personal data, from collection to erasure, in a transparent and user-centric manner. Its alignment with emerging data privacy regulations like GDPR and CCPA guarantees that organizations keep pace with global regulatory standards. The multi-layer architecture of the presentation, application, data, and infrastructure layers supports flexibility, scalability, and ease of integration, making it responsive to varied organizational requirements and transnational operations. As data privacy laws and global regulations continue to evolve, IDPR is built to be adaptable and maintains the highest standards of security and privacy. Its robust framework enables organizations to handle personal data in a responsible manner, reduce risks, and preserve user trust. Through the equilibrium of innovation, security, and compliance, our project provides a benchmark for navigating the challenges of contemporary data protection in a globalized world.

## REFERENCES

[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

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

[4]. A. Sokolovska and L. Kocarev, "Integrating Technical and Legal Concepts of Privacy," in *IEEE Access*, vol. 6, pp. 26543-26557

[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]. L. Xu, C. Jiang, J. Wang, J. Yuan and Y. Ren, "Information Security in Big Data: Privacy and Data Mining," in *IEEE Access*, vol. 2, pp. 1149-1176