International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Citizenship

Karthikayen S[1], Sarika M[2]

[1]Assistant Professor, Department of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur
[2]II MCA, Department of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur

ABSTRACT:
How we handle our personal information becomes very important in the digital age. The aim of this project is to help people keep control of their personal data when using technology. The MERN stack (MongoDB, Express.js, React, Node.js) is used for the system, while Nodemailer is used to keep all communication safe. Users are able to register, verify their accounts and manage their data safely and transparently.These features consist of user authentication, access to account data, the ability to modify those data and tools to erase the account or export information, all for the sake of privacy and data control. The platform includes a secure form for users to submit their questions or requests for deletion to the administrators by email. With an admin account, you have access to more tools made for keeping user accounts in order and handling data requests.The purpose of this app is to let users know their digital rights, support transparency and encourage ethical use of their data, in line with current regulations including the GDPR. As a result of this project, users gain knowledge and tools to protect their data, as well as how to behave responsibly on the internet

INTRODUCTION

Since we live in a digital world, caring for our personal data is now fundamental to being a good digital citizen. Since people share more details online, there's increased demand for platforms that protect users' privacy, show what data is collected and let users manage their details. Part of being a digital citizen is being safe, responsible and ethical with technology and supporting users in controlling how their personal data is used. The application provides users with ways to manage and protect their own information on the web. The platform uses React up front, Express and Node at the backend and MongoDB to securely handle all user information. Consumers may sign up, log in, look at, change or delete their details and export their data abiding by GDPR and similar laws.The system further includes Nodemailer to help ensure that email messages between users and administrators are received securely. This way, users can easily ask about their data or give feedback and are given transparent updates with automatic emails.With this initiative, we seek to inform users about the value of digital rights, motivate them to manage their data wisely and ensure the solution we create meets the key principles of good digital practice**.**

KEY FEATURES

User Authentication:

All users must sign up with an encrypted password (bcrypt).
To ensure security, this user sessions are maintained with JWT (JSON Web Token).
A tool designed to show and manage how businesses handle personal data

Look at, update and manage your personal information in a clean and easy-to-use interface.
The changes you make are instantly seen on the screen because of React's dynamic rendering.

Update or Edit Your Profile

Users are able to modify their account's name, email address, contact information and more.
Forms that check for errors to stop attacks or mistakes from entering your system.

Data Export

Users can export their information in either JSON or PDF format.
Encourages people to share and look after their information.
The Right to Erase Your Personal Data
Take all data corresponding to the user account out of the database.
It makes sure your business follows regulations such as GDPR.

Contact information & Feedback items

The contact form connects directly with Nodemailer to send the admin the information.
User queries are met with an automatic response confirming the email.

How Your Data is Protected

The information from the user needs to be checked and sanitized on both sides of the code.
Prevention for threats that are typical, including XSS, CSRF and SQL Injection.
Designing Web Sites to Be Resizeable
With React, we created a user interface designed for phones, tablets and desktops.
User navigation should be clear and easy to work with.

Teaching Digital Citizenship

Info on what users are allowed to do with their data, right ways to use technology and how to protect themselves online.
Helps individuals behave responsibly and know Digital's risks.

A Premodular & Scalable Architecture

The app was built using the MERN stack for simple future upgrades and maintenance.
Everyone on the team can work well together because the codebase is structured and divided into modules.

EXISTING SYSTEM

At present, central platforms such as Google, Facebook (Meta), Amazon and portals for financial and government services control the bulk of user information in the digital ecosystem. They may promise users they can decide how their data is handled**,** though in fact, the real control is difficult to use. Problems with the current system cause important issues in digital citizenship, data ethics and protecting user privacy.

1. Gaining access to data is disjointed.

All the personal data about a person is not easy to find in one place for users.
Users generally have to look on multiple settings pages or navigate through complex dashboards to get to the information they need.
Since there is no established way to handle data access, users become confused.

2. Different ways to opt out and ensure personally identifiable information is truly deleted

Although users can delete their accounts on many services such services frequently save anonymized or backup data.
Some platforms keep information about users even after they leave, often without telling them, to help with analytics or ads.

Privacy settings for avoiding data tracking are usually not easy to find.

3. Policies That Are Unnecessarily Difficult to Read

Most privacy policies and terms of service are very long, contain complex legal language and are difficult to grasp.

Users are not motivated to consider how their information is being managed by tech companies.

If information is not easy to understand, it goes against informed consent.

4. Little to No Standardization

Privacy settings on every platform are worded and operated differently from one another.

Personal data management expectations differ greatly between applications.

5. Issues of data breaches and inadequate accountability are causes of concern.

Examples of large data breaches (such as Facebook and Cambridge Analytica or Equifax and Yahoo) underline the dangers of storing user information in a central place. Security problems are not usually brought to users' attention quickly and the compensation for privacy loss is often unfair.

6. Not having clear channels for privacy issues.

Trying to close your account or correct GDPR information usually takes a long time and can be difficult to do.

Because users do not get prompt information, they are often confused and mistrustful.

Not enough integration of digital citizenship education

Companies prioritize profit and user interaction, but do not spend much time teaching users about:

- Digital rights
- Needing to behave safely online
- Ethical use of technology.

Many are uninformed about how to safely manage their data because there is not enough help in digital literacy**.**

PROPOSED WORK

It is an application constructed to give individuals more control over their own information online. It targets issues of transparency, ethical use of data and user rights in the internet world by giving tools that fit with internet citizenship and data protection laws.To deliver a modern and scalable solution, the application was made using MongoDB, Express.js, React and Node.js. People who register can securely log into the app, view what data is kept about them, modify it, request the account to be removed and receive a copy of their information. Thanks to Nodemailer, users can use the contact form to get in touch with the system administrators for help.The system is built to be / functional as well as to help people learn about good data habits and responsible online behavior.

Highly Important Parts of the System

Frontend (React.js)

An interface that reacts and changes with the user Ability to edit, delete or export your data from a dashboard

Items needed are secure forms and user notifications.

Developed with Node.js and Express.js on the back-end User operations are managed by RESTful APIs.

Data checking, logging in and administrating sessions Sending and receiving secure email with Nodemailer

Database (MongoDB)

Encryption is used to secure the sensitive information that stores keep about users. Allows users to read, add, update and delete their user profiles

Nodemailer – An Email System

Users get an email to confirm their actions and when something needs their attention.

Treehouse helps users and administrators have discussions about items on the tree.

Security Features

Password encryption done with bcrypt

In future, the option to use 2FA (Two-Factor Authentication) will be available.

Grading Tests Automatically

Computers and new algorithms will be used to grade student work. As a result, teachers don't need to grade tests by hand and students are given faster feedback. Fill in the blanks, multiple choice and essay-

ADVANATGES OF THE SYSTEM WE HAVE PROPOSED

Better protection of your data:

Your data is stored safely and kept secure by using authentication and encryption.

We protect our passwords using bcrypt and secure all of our API endpoints.

Enabling Users

Users can manage their data, checking what information they have, editing certain details, exporting it and deleting it.

Guarantees everyone stays aware and free from digital dependence.

Browsing and Exporting your Data are Simple:

App users are encouraged to learn more about the app and how it works by accessing their data in standard file formats.

Using a Modular System

Individual modules in the frontend, backend, database and mail system make updating each section relatively easy.

METHODS

The digital citizenship application was built step by step using the MERN stack, including MongoDB, Express.js, React and Node.js. It concentrates on safe data handling, separate modular design units and putting the user at the center of the system. Learn about the schemes below that are applied in the system.

1. Requirements Gathering:

Recognized needs of users include getting data, protecting privacy, removing data and communicating.

I checked and applied the requirements of data privacy laws such as the GDPR, to comply.

2. System Design:

I was responsible for user interface design of the login, registration, dashboard, contact form and data management on React.

I built RESTful APIs using Node.js and Express for a secure connection with the database from the frontend.

Storing user profiles, query data and logs requires using carefully designed schemas in MongoDB.

Middlewares that help with input input validation, authentication and route protection are built into the core.

3. Checking Users for Authorization:

Hashed passwords (bcrypt) are now used for both registration and login when users sign in.
Used JSON Web Tokens (JWT) to safely control user sessions.

4. Data Operations:

Users had the option to see, edit, delete and save their personal data.
I used MongoDB to efficiently handle all the basic operations of the application.

5. Connecting to Unsplash using Nodemailer:

Have a form on your website where users can submit messages and questions that are sent to you by email.
Sent out automatically to confirm that a user's submission was successful.

6. Testing :

Tests were done at the unit and integration level for each module.
I used Postman and developer tools in every browser for both API and frontend testing.

RESULTS

1. Functional User Login:

An easy way to safely set up an account, log in and control sessions is provided.
bcrypt is used to encrypt passwords and we guard protected routes with JWT.

2. Privacy Control:

Users can check, change or remove the information listed for them.
Updates to the data are put into the database right after they happen.

3. It is possible to delete data and to export it:

Users can now delete their accounts completely to meet the needs of the "Right to be Forgotten."
All users have the option to export their information in JSON format for easy viewing and storage.

4. Email is Made Safe:

By using Nodemailer, users can contact companies through a contact form.
A successful submission is confirmed to the user with an auto-reply email which helps increase their trust and makes the company more accessible.

5. Admin Features (These Can Be Skipped If Desired):

An admin panel allows you to check user-submitted forms and interact with user accounts when it is implemented.

6. Mobile-Responsive Interface:

Because the React frontend works well on any device or screen, accessibility is made easier.

7. **There is an increased awareness of users:**

There were educational messages and design elements to help users learn about digital rights and what's ethical with data.

CONCLUSION

The system introduced by Digital Citizenship – Personal Data Management System addresses the rising problems over user data privacy and conduct online in an efficient way. Because our information is often picked up, moved and saved by various digital systems today, users can now manage and control what is known about them online.

Through React, Express.js, MongoDB and Node.js, along with Nodemailer, it was possible to build a consistently functional, resilient and engaging web application. The platform allows users to register, log in, handle, export and safely erase their data.

When you use the project's main lessons on digital citizenship, it becomes both a helper and a place to learn about safe use of the internet and our rights to data. The user interface was built to be straightforward and understandable and the backend was built so that it would be secure and dependable.

REFERENCES

1. Ribble, Mike, What All Students Should Understand About Digital Citizenship in Schools: Nine Crucial Elements.ISTE, 2011.ISBN: 978-1564843012.A book that supports learning about using technology responsibly in schools and communities.
2. Daniel J. Solove has made a name for himself by writing about privacy.Understanding Privacy.From Harvard University Press, in 2008.ISBN: 978-0674035072.Provides a detailed investigation of privacy law and the ways personal data is used in society.
3. Schneier, Bruce.Data and Goliath: Inside the Bargains for Your Personal Data and What It Means for Your Life.Norton Company published this book in 2015.ISBN: 978-0393352177.Outlines the methods government and corporate groups use to collect data and suggests ways people can defend themselves.
4. Ohm, Paul.Responding to Privacy's Broken Promise: What Went Wrong with Anonymization.The issue of UCLA Law Review for 2010 was Volume .It is important to review risks to privacy as well as when data is anonymized—this helps us understand data protection.
5. Michael Darrell West Automation, Artificial Intelligence and Robots are Changing Our World of Work.Edited by Joel Charles Adams in 2018 for Brookings Institution Press.ISBN: 978-0815732938.Although the focus is on automation, the book also sheds light on how we handle data ethics and responsibility in coming tech environments.
6. Hitt, Laura W., Luke H. Johnson, Richard C. Boise and Richard O. Mason. Problems Related to Ethics in the World of Computers.1996, by Cengage Learning.ISBN: 978-0538880624. Learns about the ethical challenges involved in computer science, for example, related to privacy, data safety and security.