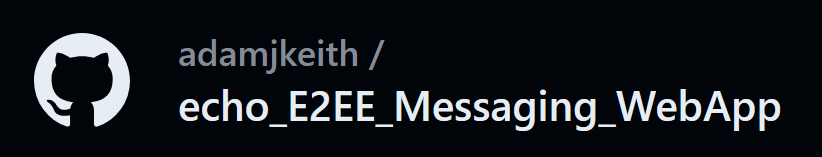
Adam Keith

Echo messenger Project

Final Report



Abstract

There are growing concerns over data privacy and security breaches in digital communication platforms. The development of an on-device end-to-end encrypted (E2EE) messaging application is a possible solution to securing sensitive information. This report presents a project to address the issue of distrust surrounding E2EE technologies through the creation of a robust, user-centric messaging web application. Drawing from the preliminary assignment's insights, the report navigates through the implementation and evaluation phases of the project, emphasising the importance of security, usability, and seamless communication. Key features such as OTP authentication and real-time on-device encrypted messaging are detailed, alongside critical reflections on challenges faced, successes achieved, and lessons learned. Professional issues, including data privacy considerations and code quality maintenance are addressed, showing the project's commitment to improving user trust. Through rigorous testing, iterative improvements and adherence to best practices, the report highlights the strides made in fostering a secure, user-friendly platform for private communication. Concluding with future project plans for secure communication technologies, the report shows the significance of user trust and data integrity in encrypting user messaging.

Table of Contents

[Introduction 2](#_Toc163068145)

[Implementation Summary 2](#_Toc163068146)

[User Registration and OTP Authentication: 2](#_Toc163068147)

[Home Page: 3](#_Toc163068148)

[Chat Interface: 3](#_Toc163068149)

[Security Features: 3](#_Toc163068150)

[Navigation and User Interaction: 3](#_Toc163068151)

[Critical Reflection 4](#_Toc163068152)

[Challenges: 4](#_Toc163068153)

[Security Implementation: 4](#_Toc163068154)

[Real-time Messaging: 4](#_Toc163068155)

[Cross-Browser Compatibility: 4](#_Toc163068156)

[User Experience: 4](#_Toc163068157)

[Successes: 5](#_Toc163068158)

[Functional Implementation: 5](#_Toc163068159)

[Security Measures: 5](#_Toc163068160)

[Responsive Design: 5](#_Toc163068161)

[Lessons Learned: 5](#_Toc163068162)

[Prioritise Security: 5](#_Toc163068163)

[Continuous Testing and Improvements: 5](#_Toc163068164)

[Flexible Architecture: 6](#_Toc163068165)

[Professional Issues and Solutions: 6](#_Toc163068166)

[Data Privacy: 6](#_Toc163068167)

[Code Quality and Review: 6](#_Toc163068168)

[Conclusion: 6](#_Toc163068169)

[Concluding Remarks 7](#_Toc163068170)

[References 8](#_Toc163068171)

# Introduction

This report builds on the work from the prior assignment, centring around the development of an end-to-end encrypted (E2EE) messaging application. In the preliminary assignment (CW1), attention was drawn to the prevalent issue of distrust surrounding E2EE technologies. This report aims to address these concerns by demonstrating the implementation and evaluation of an E2EE messaging web application which ensures user messages remain secure. As “the “end” in “end-to-end” encryption refers to the “endpoint,” which in the case of messaging is the client device of the user rather than the server.” (Ermoshina et al., 2016) along with E2EE, all messages are removed after the chat ends to ensure user privacy.

The increase of digital communication platforms has changed the way individuals and organisations interact. However, the threat of unauthorised access, data breaches, and surveillance has eroded trust in conventional messaging systems. In response to these challenges, this project endeavours to create a robust, user-centric solution that leverages the principles of E2EE to safeguard sensitive information. E2EE is used to do this because as stated by (Information Commissioner’s Office, 2021) “E2EE is a technical measure that encrypts content in communications channels so that only the sender or recipient can access it. This approach prevents third parties, including the provider of the communications platform service, from accessing the content. It is increasingly used to support secure communications and content sharing between users.” This should reinforce users trust in the security of encrypted messaging services.

Through critical reflection, the challenges and lessons learned throughout the project will be elucidated, providing valuable insights for future projects in secure communication technologies. This reflection will provide possible solutions to the norm of message applications of messengers using “a One-Pass Key Exchange (OPKE) protocol to establish a shared secret between parties.” (Len et al., 2023) and instead use a key that both users can generate on their device.

# Implementation Summary

The app is designed to provide a secure messaging platform with features including user registration, OTP (One-Time Password) authentication, home page with tabs for invites and chat creation, and a chat interface for messaging.

## User Registration and OTP Authentication:

* + The user registration involves generating a random secret for OTP generation. OTP was implemented because “Multi-factor authentication methods are more difficult to compromise than single-factor methods” (Abhishek et al., 2013)
  + This secret is encoded into a QR code and displayed to the user.
  + The user scans this QR code using an authenticator app to set up OTP authentication. An authenticator was chosen because a study by (Reese et al., 2019) found that “employees preferred the prior token-based system to using the Duo App”. Duo is an application that does not use token-based OTP.
  + Upon successful registration, phone number and encrypted secret are stored in a secure database for future authentication.
  + OTP validation is performed during login by comparing the input OTP with the OTP generated on device using the secret from the database after decrypting it on device.

A screenshot of a login screen

Description automatically generatedA screenshot of a qr code

Description automatically generatedA login screen with blue circle and text

Description automatically generated***Screenshots of the authentication process, including the index page (left), registration page (middle) and login page (right)***

***Diagram illustrating the encryption and storing of the login process***

A screenshot of a qr code

Description automatically generated

AES



AES



## Home Page:

* + The home page serves as the main dashboard for users after login.
  + It displays the user's username and app logo.
  + Tabs are implemented using HTML and JavaScript to provide a seamless navigation experience.
  + The Invites tab fetches and displays pending invitations, allowing users to accept or decline them.
  + The Create Chat tab provides a search functionality to find phone numbers, facilitating chat initiation.

A screenshot of a computer

Description automatically generatedA screenshot of a chat

Description automatically generated***Screenshot of the create chat (left) and invite (right) tabs, from the homepage.***

## Chat Interface:

* + The chat interface provides a real-time encrypted messaging experience between two users.
  + Upon opening chat, usernames of both participants are displayed.
  + Messages are exchanged and displayed in a scrollable container, allowing users to view the conversation history.
  + The input field enables users to type and send messages, which are then displayed in the interface in real-time using JavaScript and AJAX requests, utilising client-side encryption. “In client-side encryption, the user is responsible for the encryption and handling the encryption keys” (Marciano da Rocha et al., 2021), improving user trust in the encryption method used.

A screenshot of a computer

Description automatically generated***Screenshot of the chat interface, allowing users to chat in real time***

## Security Features:

* + Encryption is employed to store sensitive user data such as OTP secrets and conversations between the users securely.
  + OTP authentication adds an additional layer of security to user logins, mitigating the risk of unauthorised access.

## Navigation and User Interaction:

* + Navigation is facilitated through buttons and tabs, ensuring a smooth user experience.
  + User interaction is designed to be user-friendly and responsive, with clear prompts and feedback messages guiding users through various actions such as sending messages, accepting invites, or initiating chats.

Overall, the implementation prioritises security, usability, and seamless communication to provide users with a robust and enjoyable messaging experience, ensuring the privacy and confidentiality of user communications while offering convenient features for managing chats and invitations.

## Testing

Testing was done throughout the development process of the Web Application and examples are listed below.

### Encryption

To test the security of encryption, the encrypted secret from the database was logged to the console and then read to see if it was possible to understand the original secret. This test proved successful because the key had been encrypted multiple times using AES with a key only the user can generate. This made it impossible to determine what the original secret was without having access to the key. A similar method was tested on the encrypted messages.

To further the encryption security, the project could have tested using additional random keys and encrypting the messages multiple times as well.

### Table Removal

Table removal after users end a chat is an integral feature of the project. This was tested by monitoring the tables inside the project’s database and seeing if the table was deleted if either of the user ended the chat and this test was successful. Adding an automatic, timed table removal that removes an inactive table, would increase the security of data and could be considered as a future project improvement.

In conclusion, by testing these features, the application developed within this project can assure data security and provides a valuable insight into possible improvements.

# Critical Reflection

The development of the messaging application presented numerous challenges, successes, and lessons learned. This reflection will highlight the key aspects of the project implementation and the professional issues encountered along the way.

## Challenges:

### Security Implementation:

Implementing robust security measures was a priority to ensuring user data is kept secure. However, integrating encryption techniques and OTP authentication posed significant challenges. Complexities encountered in securely storing sensitive user information such as phone numbers and OTP secrets, while ensuring seamless authentication processes was challenging. (Imperial College London, 2024) states, applications should “not collect and store unnecessary sensitive or personal information.” Therefore, during the development process, this project needed to ensure only essential data is stored securely.

### Real-time Messaging:

Using real-time messaging functionality was a key feature of the application. However, achieving seamless messaging and synchronisation across devices required planning and development efforts. The project explored approaches, including AJAX-based communication, to ensure timely message updates without compromising performance. It is crucial these messages were synchronised between users as (Tang & Bradshaw, 2020) points out “students prefer instant messaging to face-to-face interactions.” This shows a need for the messages to appear on both devices instantly.

### Cross-Browser Compatibility:

Ensuring cross-browser compatibility was crucial to guaranteeing a consistent user experience across different browsers and devices. However, CSS and JavaScript inconsistencies across various platforms proved to be challenging, encountering multiple issues with layout rendering, CSS styling, and JavaScript functionality.

### User Experience:

Designing an intuitive and user-friendly interface was essential for enhancing user engagement and satisfaction. However, striking the right balance between simplicity and functionality posed challenges. Through iteratively refining the user interface, focusing on optimising navigation, message handling and feedback mechanisms, it was ensured a seamless user experience was delivered.

## Successes:

### Functional Implementation:

Although challenging, the project successfully implemented the core functionalities of the messaging application. From user registration and OTP authentication to chat creation and messaging, each feature was meticulously designed and tested to ensure functionality and reliability.

### Security Measures:

This project successfully integrated robust security measures to protect user data and privacy. Encryption techniques were used to securely store sensitive information, while OTP authentication added an additional layer of security to user logins. These measures reassure users regarding the safety of their personal information. The method of encrypting the user data was achieved by using AES. “By employing AES, a symmetric block cipher, to encrypt files with a 128-bit key randomly generated for each encryption instance.” (Srivastava & Kumar, 2023), for additional security, the secret is encrypted using AES with the seed of a randomly generated number before being encrypted again with a different seed to be stored.

### Responsive Design:

The commitment to responsive design was very successful, as the application seamlessly adapted to different devices and screen sizes. By leveraging CSS media queries and flexible layout designs, it ensured a consistent and user-friendly experience across desktops, tablets, and mobile devices.

## Lessons Learned:

### Prioritise Security:

The development process highlighted the importance of prioritising security from the project's inception. Moving forward, future projects must allocate sufficient time and resources to implement robust security measures effectively, ensuring the protection of user data and privacy. As stated by (Knowen et al., 2024) “personal data should be given the top security priority as we want to attain total security”.

### Continuous Testing and Improvements:

Incorporating continuous testing and creating a list of possible improvements throughout the development process proved invaluable. By identifying and addressing issues early on, the project was able to deliver a more polished and user-centric web application. Moving forward, projects should ensure continuous testing and keep track of improvements to drive iterative improvements for the overall application.

### Flexible Architecture:

Adopting a scalable architecture enabled the project to adapt to changing requirements and future feature enhancements seamlessly. During development, effective flexible, system design was essential to accommodate evolving requirements while maintaining stability and performance.

## Professional Issues and Solutions:

### Data Privacy:

As this project’s main focus was improving user trust in end to end encryption, it was essential to use robust encryption methods that can be made on device, therefore ensuring that users can trust that no one can access the messages. These challenges were addressed by conducting thorough research, and implementing encryption techniques and authentication protocols to protect user data.

### Code Quality and Review:

Ensuring code quality and reviewing the code regularly was a critical aspect of the project’s development process. By adhering to coding standards and reviewing the code, the project was able to identify potential vulnerabilities, optimise performance, and maintain a high level of code quality throughout the project lifecycle.

## Conclusion:

The process applied in developing the web-based messaging application was filled with challenges, successes and valuable lessons. Despite facing obstacles, the commitment to delivering a secure, user-friendly, and feature-rich product drove this project to overcome issues and achieve the goals of an encrypted messaging application that users can trust. Future projects will apply the insights gained from lessons learned, continually striving for excellence and innovation in development processes.

# Concluding Remarks

In conclusion, the development process of the end-to-end encrypted messaging web application has been both challenging and successful. Through an implementation process, this project has successfully tackled the prevalent issues of distrust surrounding E2EE technologies, offering users a robust and trustworthy platform for secure communication.

Commitment to prioritising security is evidenced at every stage of development, from the integration of robust encryption techniques to the implementation of OTP authentication, ensuring that user data remains secure against unauthorised access. By adhering to principles outlined by reputable sources such as the Information Commissioner’s Office and leveraging encryption methods such as AES, the project has instilled user confidence regarding the safety of their personal information.

Moreover, the emphasis on responsive design has resulted in a seamless user experience across various devices and screen sizes. By adopting flexible layout designs and employing CSS media queries, the application ensures that users can access the application effortlessly, irrespective of their preferred device.

The importance of continuous testing and improvement has been explored, driving a proactive approach towards identifying and addressing issues throughout the development process. Additionally, the necessity of prioritising security from the project's inception has been emphasised, with lessons learned for future projects regarding the importance of allocating sufficient time and resources to implement robust security measures effectively.

Professional issues, such as data privacy and code quality, have been addressed through thorough research and adherence to coding standards. By implementing encryption techniques and authentication protocols to protect user data and conducting regular code reviews, this demonstrates that the application meets high standards of data security and integrity.

Overall, the development of the end-to-end encrypted messaging web application shows dedication to building trust and confidence in end to end encryption with users. By applying the lessons learned and continuously striving for secure applications, user expectations for private data to be handled securely, without the need for third party access, has been successfully demonstrated.

# References

Abhishek, K., Roshan, S., Kumar, P., & Ranjan, R. (2013). A Comprehensive Study on Multifactor Authentication Schemes. *Advances in Computing and Information Technology*, 561–568. https://doi.org/10.1007/978-3-642-31552-7\_57

Ermoshina, K., Musiani, F., & Halpin, H. (2016). End-to-End Encrypted Messaging Protocols: An Overview. *Internet Science*, 244–254. https://doi.org/10.1007/978-3-319-45982-0\_22

Imperial College London. (2024). *Managing sensitive data*. Imperial College London. https://www.imperial.ac.uk/research-and-innovation/support-for-staff/scholarly-communication/research-data-management/data-storage-and-security/storing-sensitive-and-personal-data/

Information Commissioner's Office. (2021). *A Framework for Analysing End to End Encryption in an Online Safety Context v1 02/11/2021*. https://ico.org.uk/media/about-the-ico/documents/4018823/ico-e2ee-paper-02112021.pdf

Knowen, C., Ronoh, L., & Mugalavai, A. (2024). *View of Prioritizing Personal Data Protection in Insurance Organizations: A Review*. Nauss.edu.sa. https://journals.nauss.edu.sa/index.php/JISCR/article/view/2147/1276

Len, J., Tech, C., Ghosh, E., Grubbs, P., & Rösler, P. (2023). *Interoperability in End-to-End Encrypted Messaging*. https://eprint.iacr.org/2023/386.pdf

Marciano da Rocha, Cézane, D., Ângelo Perkusich, Kyller Costa Gorgônio, Rodrigo Tomaz Pagno, & Will, N. C. (2021). Trusted Client-Side Encryption for Cloud Storage. *Communications in Computer and Information Science*, 1–24. https://doi.org/10.1007/978-3-030-72369-9\_1

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). *A Usability Study of Five Two-Factor Authentication Methods This paper is included in the Proceedings of the Fifteenth Symposium on Usable Privacy and Security. A Usability Study of Five Two-Factor Authentication Methods*. https://www.usenix.org/system/files/soups2019-reese.pdf

Srivastava, A., & Kumar, A. (2023, November 16). *A Robust Approach to Secure Data Encryption: AES-RSA Hybrid with Kernel Key Protection*. Www.researchsquare.com. https://www.researchsquare.com/article/rs-3565782/v1

Tang, C. M., & Bradshaw, A. (2020). Instant messaging or face-to-face? How choice of communication medium affects team collaboration environments. *E-Learning and Digital Media*, *17*(2), 204275301989972. https://doi.org/10.1177/2042753019899724