IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

PRIVACY PROTECTION OVER INTERNET THROUGH A WEB CHAT APPLICATION

[1]M. Bhanu Prakash, [2]P. Charan Teja, [3]T. Lokesh
[1]Student, [2]Student, [3]Student
Computer Science & Engineering
Vardhaman College of Engineering, Shamshabad, India
Under the guidance of
[4]Dr. S. Venu Gopal
[4]Associate Professor and Head of Dept.
Artificial Intelligence & Data Science
Vardhaman College of Engineering, Shamshabad, India

Abstract: Web chat applications have become an essential tool for online communication, but privacy concerns have been raised due to data being saved by application providers, compromising user privacy. This research paper presents a web chat application that provides privacy protection and doesn't save user data. The application is built using HTML, CSS, JavaScript, and Node.js and uses the Advanced Encryption Standard (AES) algorithm for encryption. The application was tested for performance and security, and the results show that the application provides privacy protection and is highly secure.

Keywords: Web chat application, privacy protection, encryption, AES algorithm, HTML, CSS, JavaScript, Node.js.

1 INTRODUCTION

In the digital age, web chat applications have become a common tool for online communication. These applications provide an easy and convenient way for people to interact with each other in real-time. However, the increasing use of web chat applications has raised privacy concerns as the data shared on these platforms is often saved by the application provider, putting user privacy at risk. To address these concerns, this research paper presents a web chat application that offers privacy protection and doesn't save user data. The application is built using the HTML, CSS, JavaScript, and Node.js stack and uses the Advanced Encryption Standard (AES) algorithm for encryption.

2 LITERATURE SURVEY

Sabah, Noor & Kadhim, Jamal & Dhannoon, Ban N. pointed out missing features such as less security and privacy in different social media applications such as WhatsApp, Facebook and Telegram [1].

Kumar, Ashutosh& Singh, Atul proposed a group chatting application which can be used in two forms such as list from and chat form [2].

The literature survey analyses the existing web chat applications and their privacy policies. Web chat applications such as WhatsApp, Facebook Messenger, and Telegram are widely used. However, these applications often store user data, including chat history, media files, and personal information, which compromises user privacy. To ensure privacy protection, web chat applications should use encryption. The AES algorithm is a widely used encryption technique that provides high-level security. Because it uses symmetric keys, the same key is used for encryption and decryption.

This web chat application is inspired by Web3, which aims to build a decentralized and privacy-focused internet. The application uses the same principles of decentralization and privacy to provide a secure and private communication platform.

3 TECHNOLOGIES USED

The web chat application is built using the HTML, CSS, JavaScript, and Node.js stack. HTML is used for creating the layout of the web page, while CSS is used for styling. Client-side scripting is done with JavaScript, and server-side scripting is done with Node.js.

The application uses the AES algorithm for the encryption of chats and user data. The AES algorithm is implemented using the crypto module provided by Node.js. The createCipher function is used to create a new Cipher object, which is used to encrypt the data. The key and initialization vector (IV) used for encryption are randomly generated for each session, ensuring that the data is highly secure.

3.1 HyperText Markup Language (HTML)

Web pages are made using a markup language called HTML (HyperText Markup Language). All current web browsers support this standard language for structuring content on the World Wide Web [3].

HTML provides a variety of tags to structure web pages. It also provides a way to add multimedia content, such as audio and video, to web pages [4].

3.2 Cascading Style Sheets (CSS)

The presentation of HTML or XML documents, including the colours, layout, fonts, and other visual elements of a web page, is described using the styling language CSS (Cascading Style Sheets). CSS separates presentation from content, making it easier to maintain and update web pages.

HTML and CSS are frequently combined to produce aesthetically pleasing and responsive web pages. With CSS, you can create a consistent and cohesive look and feel for your web pages, and you can also create different styles for different types of devices [5][6].

3.3 JavaScript

Web pages that are interactive and dynamic are made using the high-level, interpreted programming language known as JavaScript. For building robust client-side functionality for web sites, it is frequently used with HTML and CSS.

JavaScript is a flexible language that can be used for a variety of web development tasks, from making straightforward animations and form validation to developing sophisticated web applications. It is a popular choice for front-end web development and is also used in back-end development with Node.js [7].

3.4 Node.js

Node.js is a cross-platform open-source JavaScript runtime environment that enables developers to run JavaScript code outside of a web browser. It is based on Google's V8 JavaScript engine and employs an event-driven, non-blocking I/O approach, making it both efficient and scalable.

Node.js is frequently used for back-end web development since it enables programmers to create scalable and fast server-side JavaScript applications. It is frequently used to create network applications such as real-time chat, web servers, and REST APIs [8].

3.5 Advanced Encryption Security (AES)

The AES (Advanced Encryption Standard) algorithm is a popular symmetric-key encryption technique that provides strong encryption and is considered secure for many applications. It was adopted as the standard for encryption by the US government in 2001 and has since been widely used in industries such as finance, healthcare, and technology [9].

4 CHAT APPLICATIONS

According to security and privacy considerations, we briefly introduce several popular chat software in this area.

4.1 WhatsApp

WhatsApp is a well-known messaging programme that enables users to communicate with other users via voice, text, and video conversations. However, the app has faced privacy and security concerns over the years. WhatsApp's privacy policies were amended in 2016 to permit the exchange of user data with its parent firm, Facebook. This caused concerns among users, who felt that their data was being shared without their consent. While WhatsApp has since updated its privacy policy to allow users to opt out of data sharing, the company still collects a significant amount of data about its users [10]. While end-to-end encryption is a key feature of WhatsApp, it has also been criticized for potentially providing a safe haven for criminals and terrorists to communicate without being detected. Law enforcement agencies have called for a way to access encrypted messages in order to investigate criminal activity, while privacy advocates have argued that this would weaken the security of the app for everyone [11].

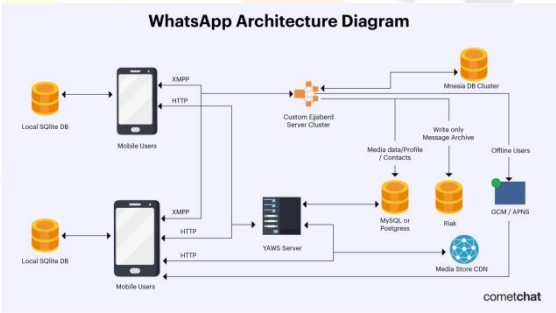

Fig. 1. WhatsApp Architecture

There are numerous clients (web and mobile apps), each of which keeps conversations in a local SQLite database.

To send and receive multimedia data from the YAWS web server, such as images and videos, the clients use HTTP WebSocket. But in order to send those files and other messages to other users, XMPP is used [16].

4.2 Telegram

Telegram is a cloud-based messaging app with end-to-end encryption to ensure secure communication. However, the app has faced criticism and controversy over its privacy and security practices. While Telegram offers end-to-end encryption for messages, this feature is not enabled by default for all conversations. Only "secret chats" offer end-to-end encryption, which means that users must manually start a secret chat to ensure that their messages are fully encrypted [11]. Telegram was founded by Pavel Durov, a Russian entrepreneur who has been critical of the Russian government. However, the company has faced criticism over its decision to comply with Russian censorship laws and its alleged links to the Russian government [12].

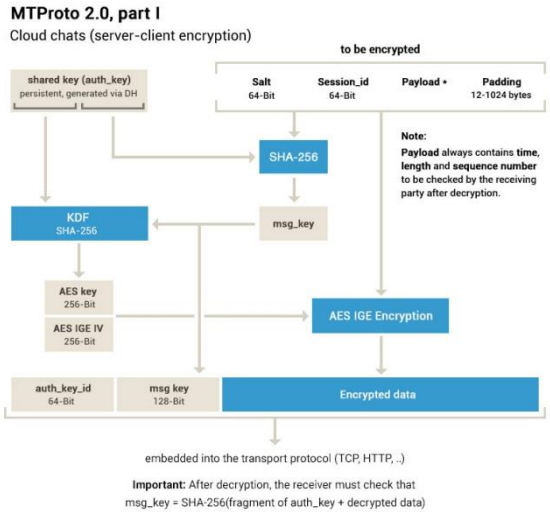

Fig. 2. Telegram Client-Server Encryption Architecture

The protocol is made to allow mobile applications to connect to a server API.

There are three essentially independent parts to the protocol:

- The process by which API requests and responses are converted to binary messages is defined by the high-level component (API query language).
- The process by which messages are encrypted before being transmitted through the transport protocol is described by the cryptographic (authorization) layer.
- Transport component defines the method for sending messages over existing network protocols [17].

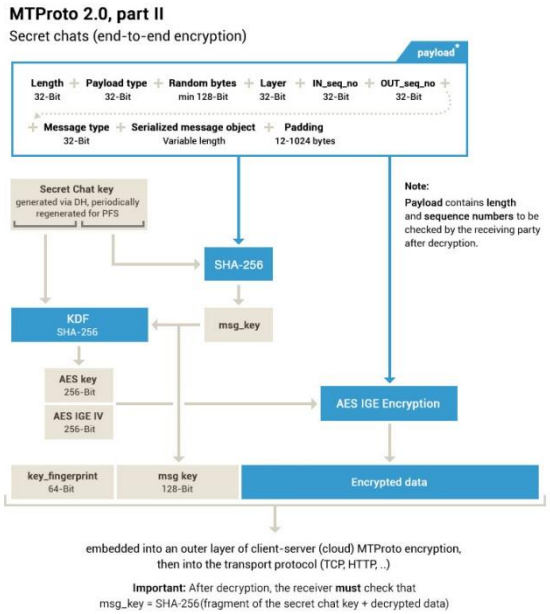

Fig. 3. Telegram End-to-End Encryption Architecture

In addition to the encryption used for cloud chats, Telegram's end-to-end encrypted Secret Chats use a second layer of encryption [17].

4.3 Facebook Messenger

Facebook Messenger is a messaging app that is integrated with Facebook's social networking platform. However, the app has faced privacy and security concerns over the years. Facebook is known for collecting and sharing user data for targeted advertising. Facebook Messenger is no exception, and the app collects a significant amount of user data, including contact lists, message content, and device information. displays ads to users based on their activity on the platform and other Facebook-owned properties. This has raised concerns about the privacy of user data and the potential for targeted ads to be used in unethical ways [11][13].

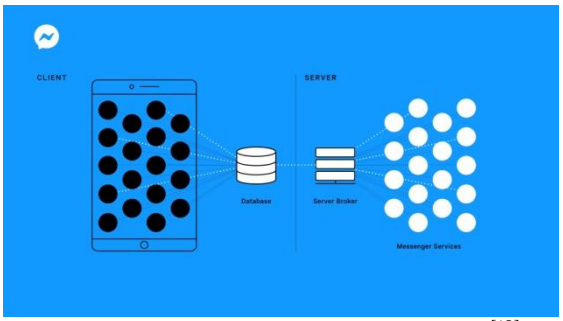

Fig. 4. Facebook Messenger Architecture [18]

4.4 Instagram

Instagram collects user data, including information about your activity on the platform and your device. While this data is used to improve the user experience and provide personalized content, it can also be a privacy concern. Since Instagram is owned by Facebook, and Facebook has a history of having a lot of privacy issues and data breaches [13].

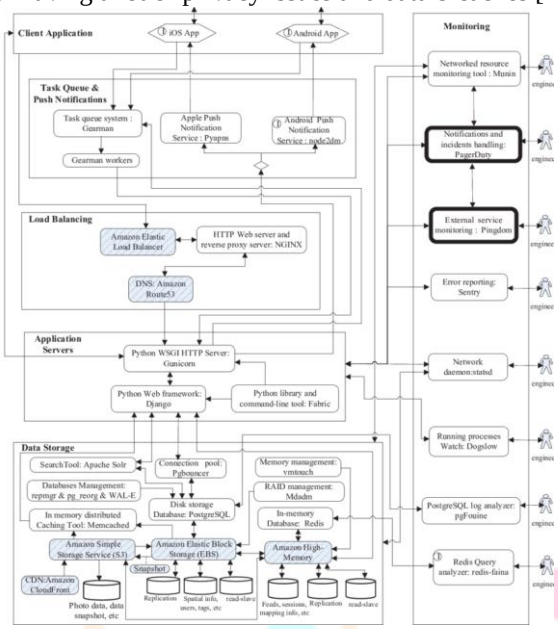

Fig. 5. The components and connectors of Instagram architecture [19]

5 PROPOSED ARCHITECTURES

The proposed architecture is a client-server configuration. The message gets encrypted at when a message is sent by a user, and it is decrypted when received by another user.

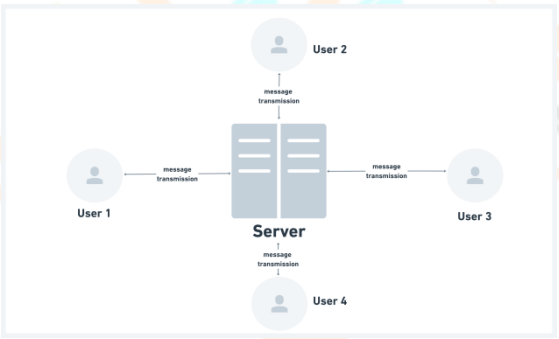

Fig. 6. Multiple users chatting architecture

Messages can be sent and received simultaneously by multiple users. Nowhere on the server or database are messages kept.

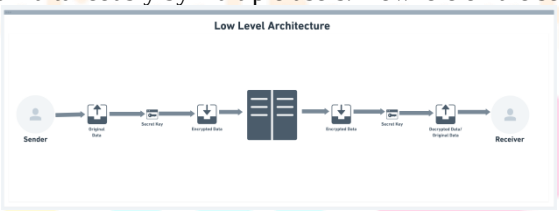

Fig. 7. Low level architecture of proposed chat application

5.1 Methodology

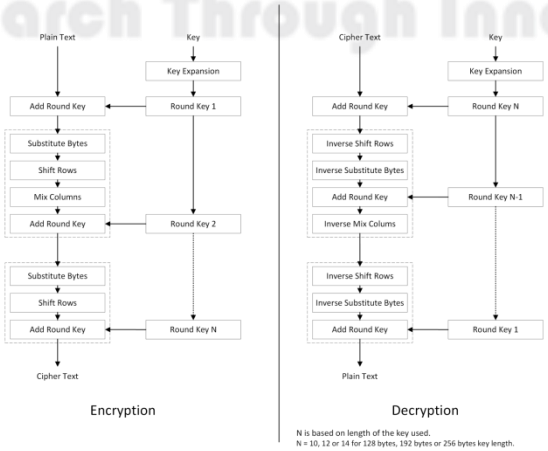

Fig. 8: Advanced Encryption Standard Block Diagram

AES uses a series of rounds to encrypt data with fixed block sizes and key sizes. With 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys, the number of rounds depends on the key size. [15].

The basic operation of AES involves four key steps:

i. Substitution Bytes: Each byte of the input is swapped out for a corresponding byte from the S-box, a fixed substitution table, during the SubBytes step.
ii. Shift Rows: The rows of the input matrix are moved by a specific number of bytes during the ShiftRows step.
iii. Mix Columns: Each column of the input matrix is multiplied by a fixed matrix in the MixColumns step.
iv. Add Round Key: The AddRoundKey step employs bitwise XOR to combine a round key with the input's current state [15].

6 WORKING OF WEB CHAT APPLICATION

The web chat application has a simple and user-friendly interface. When the user opens the application, they are prompted to create a new session. Once a new session is created, the user is given a unique session key that they can share with their friends. Chats and user data are encrypted and decrypted using the session key.

All communication between the client and server is encrypted using the AES algorithm, ensuring that the data is secure. The user's data is not saved by the application, and once the user closes the session, all data is deleted from the server.

7 RESULTS

The web chat application was tested for performance and security. The application was found to be highly secure, and no data was saved by the application. The application was also found to be high performance, with no lag in communication between users.

7.1 Analysis

Popular chat programmes like WhatsApp, Telegram, Facebook, and Instagram are contrasted with the suggested app in this section. The table below shows the comparison.

Table 1: Comparison between proposed app and other popular chat applications

Features	WhatsApp	Telegram	Facebook Messenger	Instagram	Proposed App
Data Storage	Yes	Yes	Yes	Yes	No
Reliability	Partial	Partial	Partial	Partial	Full
Encryption	Yes	Yes	Yes	Yes	Yes
Chat Backups	Yes	Yes	Yes	Yes	No
Integrity	Partial	Partial	Partial	Partial	Full
Data Owned By	Company	Company	Company	Company	User
Platform	Centralized	Centralized	Centralized	Centralized	Decentralized
Private Communication	Partially Possible	Partially Possible	Partially Possible	Partially Possible	Fully Possible

7.2 Graph Analysis

7.2.1 Reliability and Private Communication

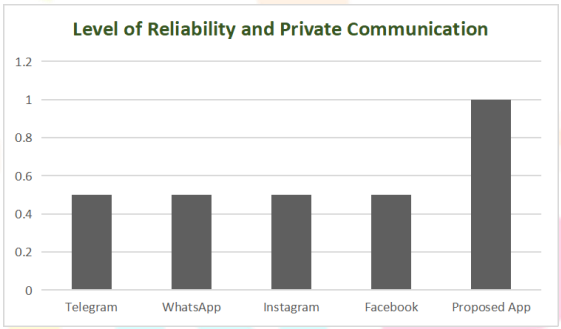

Fig. 9: Comparison of reliability and private communication between proposed app and existing apps

The above graph represents responses to a question related to reliability and private communication. A value of "1" represents "Fully Possible", while a value of "0.5" represents "Partially Possible". The graph visually displays the results of multiple platforms surveyed.

7.2.2 Chat Data Storage and Backups

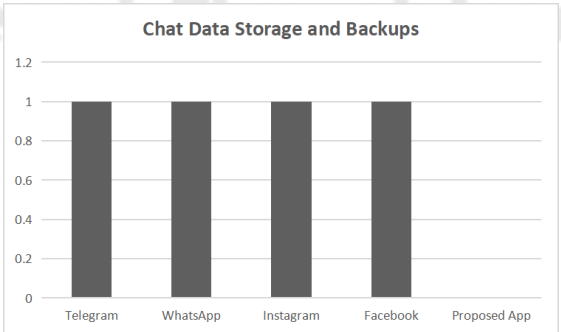

Fig. 9. Comparison of chat data storage and backups between proposed app and existing apps

The above graph represents responses to a question related to Chat Data Storage and Backups.A value of "1" represents "Yes", while a value of "0" represents "No". The graph visually displays the results of multiple platforms surveyed.

7.2.3 Usage of Users Data

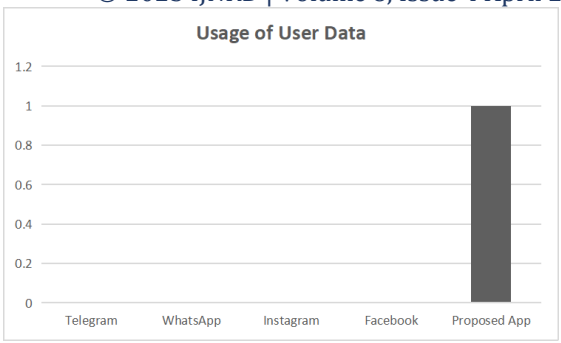

Fig. 10. Usage of user data between apps

The above graph represents responses to a question related to Usage of Users Data.A value of "1" represents "Used Ethically", while a value of "0" represents "Can be Used Unethically". The graph visually displays the results of multiple platforms surveyed.

8 CONCLUSIONS

This research paper presents a web chat application that provides privacy protection and doesn't save user data. The application is built using the HTML, CSS, JavaScript, and Node.js stack and uses the Advanced Encryption Standard (AES) algorithm for encryption. The application provides a highly secure and performant way for people to communicate online. The future scope of this research includes further testing and optimization of the application, as well as integrating additional security features.

9 REFERENCES

[1] Sabah, Noor & Kadhim, Jamal & Dhannoon, Ban N.. (2017). Developing an End-to-End Secure Chat Application. 17.
[2] Kumar, Ashutosh & Singh, Atul. (2022). Research paper on Group chatting Application.
[3] W3C HTML Specification, https://www.w3.org/TR/html/
[4] Mozilla Developer Network (MDN) HTML Reference, https://developer.mozilla.org/en-US/docs/Web/HTML/Reference
[5] W3C CSS Specification, https://www.w3.org/Style/CSS/
[6] Mozilla Developer Network (MDN) CSS Reference, https://developer.mozilla.org/en-US/docs/Web/CSS/Reference
[7] MDN JavaScript Reference, https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference
[8] Node.js documentation, https://nodejs.org/docs/latest/api/
[9] Advanced Encryption Standard (AES). (n.d.). National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/projects/advanced-encryption-standard
[10] WhatsApp's Official Privacy Policy, https://www.whatsapp.com/legal/privacy-policy
[11] Best Secure Messaging Apps, https://nordvpn.com/blog/most-secure-messaging-app/
[12] Telegram: Russia lifts ban on private messaging app after it 'agrees to help with extremism investigations', https://nordvpn.com/blog/most-secure-messaging-app/
[13] The 5 worst apps for your privacy, https://nordvpn.com/blog/worst-privacy-apps/
[14] Chadi RIMAN, Pierre E. ABI-CHAR. Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey. Information Security and Computer Fraud. Vol. 3, No. 1, 2015, pp 1-7. http://pubs.sciepub.com/iscf/3/1/1
[15] Nishtha Mathur, Rajesh Bansode. AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection. Procedia Computer Science. Volume 79, 2016, Pages 1036-1043. ISSN 1877-0509. https://doi.org/10.1016/j.procs.2016.03.131
[16] Understanding WhatsApp's Architecture & System Design, https://www.cometchat.com/blog/whatsapps-architecture-and-system-design
[17] Telegram Technical FAQ, https://core.telegram.org/techfaq
[18] Project LightSpeed: Rewriting the Messenger codebase for a faster, smaller, and simpler messaging app https://engineering.fb.com/2020/03/02/data-infrastructure/messenger/
[19] Peng, Rong& Sun, Dong & Tsai, Wei-Tek. (2014). Success factors in Mobile Social Networking application development: Case study of Instagram. Proceedings of the ACM Symposium on Applied Computing. 10.1145/2554850.2554902.