iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50633

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

E2EE Web Messaging Application Using Cryptography Techniques

Harshvardhan Bawake[1], Saideep Cholke[2], Atharv Dhole[3], Ankit Jadhav[4], Prof. Aarti Bhise[5]
[1, 2, 3, 4, 5]*Computer Dept. SKNCOE, Pune, Maharashtra*

Abstract: ***Instant messaging services on mobile devices, such as WhatsApp, have become immensely popular, largely due to their end-to-end encryption (E2EE) feature, which ensures user privacy. However, this has raised concerns for some governments who argue that E2EE makes it challenging to combat terrorism and organized crime. These governments have expressed the desire for a "backdoor" to access messages in cases of credible threats to national security. However, WhatsApp users have strongly opposed this idea, citing concerns about privacy infringement and potential exploitation by hackers. This paper presents the advantages of maintaining E2EE in WhatsApp and argues against granting governments a "backdoor" to access user messages. It highlights the benefits of encryption in safeguarding consumer security and privacy, while also acknowledging the challenges it poses to public safety and national security. In the realm of internet messaging security, cryptography plays a crucial role in protecting networks. This paper aims to raise awareness among common computer users about the importance of email security and its requirements. Several cryptographic techniques have been developed to achieve secure communication, and the proposed messaging system ensures security in accordance with standard security models.***
Keywords: Cryptography, Instant Messaging, WhatsApp, Signal, End-to-End Encryption, Security, Privacy, Web Based App.

I. INTRODUCTION

The world is ever changing due to the advancement in the realm of science and technology, and these days it seems hard to escape the presence of technology in our daily lives. Since Smartphones became popular, many messaging services have been launched. WhatsApp, which has more than 1.3 billion users in over180 countries today, is a free messaging service owned by Facebook Inc., and has become more popular than others. WhatsApp works with internet connectivity and helps its users to stay InTouch with friends and relatives on their contact list. Apart from making its users get, and stay connected with each other, it also helps them to create groups, send images, videos, documents, and audios. As more and more people use WhatsApp as a means of communication, the importance of securing its users' business or private communications has become more imperative [2].

Cryptography provides number of security goals to ensure of privacy of data, on-alteration of data and so on. The idea of encryption and encryption algorithm by which we can encode our data in secret code and not to be able readable by hackers or unauthorized person even it is hacked.

The evolution of encryption is moving towards a future of endless form of possibilities. As it is impossible to stop hacking, we can secure our sensitive data even it is hacked using encryption techniques and which protecting the information security.

In this paper we present a research paper on cryptographic techniques based on multiple algorithm and which is suitable for many applications where security is main concern. We have demonstrated the same through a Web Based messaging application called "DM-ME". We have used latest tech stack for both Front-End as well as Back-End.

II. NEED

The need for end-to-end encryption in messaging has become increasingly important due to the convenience and speed with which messages can be transmitted globally, regardless of geographical distance. In today's world, where national security relies heavily on the internet and its applications, cryptography plays a crucial role in ensuring the confidentiality, integrity, and authenticity of message contents. Cryptography provides various security goals, such as protecting the privacy of data, preventing unauthorized alteration of data, and verifying the authenticity of message senders and receivers. Encryption algorithms allow data to be encoded in secret codes that are unreadable by hackers or unauthorized individuals, even if the data is compromised.

The use of encryption in message communications, however, faces challenges such as the complexity of current email encryption solutions and the management of encryption keys. Nevertheless, encryption techniques are essential for promoting information security, particularly in sensitive communications such as those involving national security, business secrets, and personal data.

©IJRASET: All Rights are Reserved

Furthermore, encryption is a powerful tool that empowers individuals to maintain control over their own data and protect their privacy. End-to-end encryption, in particular, ensures that only the intended recipients can access the messages, and not even the service providers have access to the decrypted content. This provides users with a sense of trust and confidence in the security of their communications

III. LITERATURE SURVEY

Sr no	Author Name	Year of publications	Features and Techniques	Advantages
1	Joseph Amalraj, Dr. J. John Raybin Jose	2016	Encryption, Decryption, Computer Security, Cryptography, DES, AES, Blowfish, RSA, CL-PKC, Securing Data, Hacking.	• This paper provides detailed study of Cryptography Techniques like AES, DES, 3DES, Blowfish, RSA • In this paper it has been surveyed about the existing works on the encryption techniques. • This paper presents the performance evaluation of selected symmetric algorithms like AES, 3DES, Blowfish and DES. • We concluded that X-3DHE has the overall better performance than other algorithms.
2	Ganguly M.	2017	WhatsApp Design and features, Security, Chat and messaging app, Privacy	• In this paper different aspects of WhatsApp are discussed. This aspect increases convenience and reliability of message delivery at the cost of some security, is not inherent to the Signal protocol. Open Whisper Systems' messaging app – also called Signal – works differently. • If a recipient's security key changes while offline, an in-transit message will fail to be delivered and the sender will be notified of the change in security keys without the message having been resent automatically. • This re-encryption and rebroadcasting of previously undelivered messages could potentially allow a third party to intercept and read a user's undelivered messages.

3	Mohamed Nabeel	2017	E2EE, Algorithms, Security Analysis, Meta Data	• Many of the E2E systems we analyzed in this work are not secure against passive adversaries who have access to metadata. • Better designs considering strong encryption techniques, hiding metadata and access patterns, can help construct systems that are secure against strong adversaries.
4	Deepak Garg, Seema Verma	2009	Symmetric Key, Asymmetric Key, RSA, Cryptography	• In this paper, we were introduced to RSA cryptosystem and its improvements. • Many methods are discussed to improve the same, e. g., Batch RSA, MultiPrime RSA, MultiPower RSA, Rebalanced RSA, RPrime RSA.
5	Mohit D. Singanjude, Prof. R. Dalvi	2016	MANET, RSA, Performance Improvement	• In this paper we learned about the techniques used for secure and fast transmission of data in MANET. • An Indian Ancient Vedic method is known for its performance. • The Vedic method is very helpful to increase the speed of RSA to generate the public and private keys.
6	S. Blake-Wilson, D. Johnson, and A. Menezes	1997	Authenticated key, Conformation, Unified Model	• This paper has proposed formal definitions of secure Authenticated Key Exchange (AK) and Authenticated Key Exchange with conformation (AKC) protocols within a formal model of distributed computing. • The `unified model' of key agreement has been introduced, and several variants of this model have been demonstrated to provide provably secure AK and AKC protocols in the random oracle model. • Strong evidence has been supplied that practical implementation of the protocols

				also offer superior security assurances than those currently in use, while maintaining similar computational overheads.
7	Prasoon Varshney, Zubair Beg, Vishal Kumar Shaw and Dr. Ashish Chopra	2022	E2EE, Extended Triple Diffie Hellman Key Exchange Algorithm, Double Rachet Function	• This paper briefs that end-to-end encryption cannot be achieved by using any single standard algorithm. It can only be possible when one algorithm is mathematically integrated with another algorithm to remove limitations and use good properties of both the algorithms. • X3DH Protocol is used in signal Protocol even nowadays to achieve End- to - End Encryption and it is used by big companies like WhatsApp, Facebook. • It is also concluded that X3DH Protocol is not only sufficient, but it also must be mathematically integrated with Double Ratchet to get the best results.
8	T. Perrin	2016	Forward Secrecy, Double Rachet mechanism	• In this paper we learned about double rachet mechanism. Basically, it is a function that can turn only one way, i.e., it cannot move backward. It is called as KDF Rachet. • If the attacker gets one key, he/she will not be able to undo the operation performed by KDF Ratchet to figure out the input data, but he/she will only be able to access future messages. That's a huge problem. • To ensure future secrecy, we use a Diffie-Hellman Ratchet with the KDF Ratchet function forming a Double Ratchet.

IV. EXISTING SYSTEM

1) Initialize Signal Server Store before login.
2) On user Login, **Axios** calls are made to verify if the user exists, returning Users details as an object.
3) The Signal Protocol Manager is then initialized for each logged-in user, at App.js.
4) After login, the Chat Window appears, with two sub-components, Contact List and Message Box.
5) The Chat Window makes an Axios call to the server, to fetch all contacts except the logged-in one and which are not equal to the role of the logged-in user.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

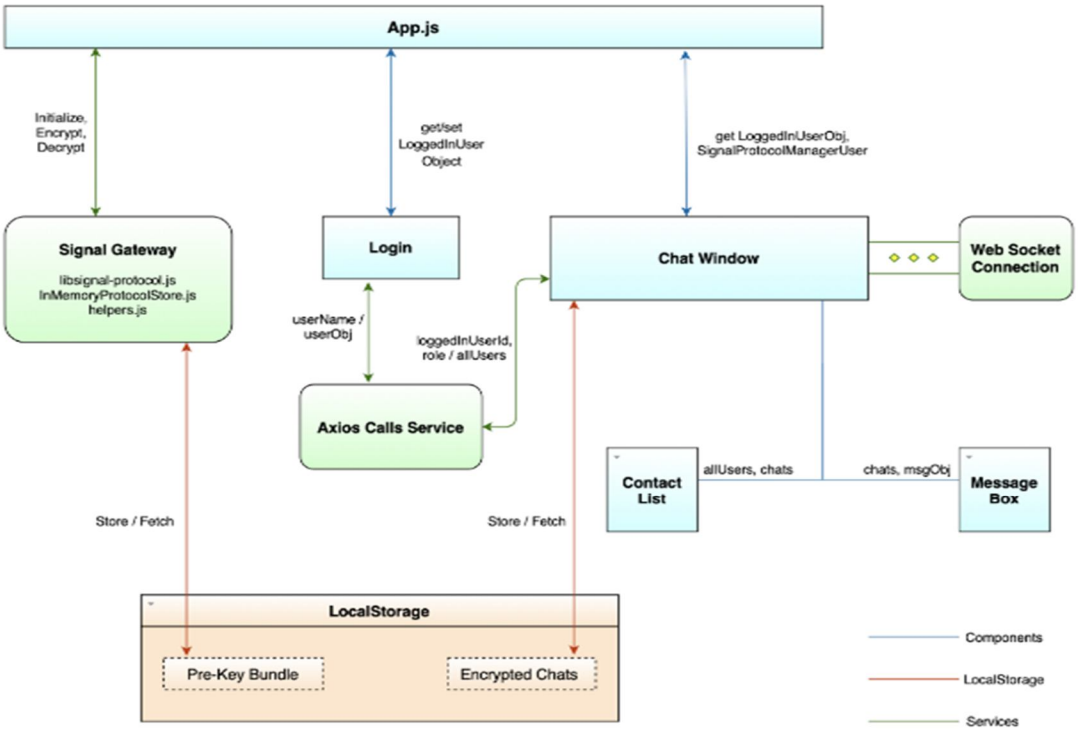


Figure 1: System Architecture

6) It then displays the contacts in the Contact List component.
7) A user can select a contact to Chat with; then the selected user Id is sent to the chat window to display its messages (if any) in the message box component, and for further communication.
8) When user hits enter to send a message, it is first encrypted using Signal, and then sent to the server using Web Socket.
9) On receiving a message, it is checked by the client if it is its message. If not then it is sent to Signal for decryption, else the last message is used.
10) The chats in the message box (decrypted) and local storage (encrypted) are updated with new message.

V. RESULT AND DISCUSSION

The Diffie-Hellman parameters play a crucial role in manipulating the Key Derivation Function (KDF) chain to reset the sending and receiving chains of both Alice and Bob, thereby synchronizing them once again. This ensures that if a key is compromised, the secrecy can be re-established from that point onward. For instance, Bob can send his Diffie-Hellman public key (dh2) to Alice's Diffie-Hellman ratchet, which will reset the sending and receiving chains on both ends. Additionally, a key practice in end-to-end encryption is to immediately and securely delete the decrypted messages after they are read, ensuring that the endpoints are safeguarded against future attacks.

This approach establishes robust end-to-end encryption, where even the system designers themselves cannot access the keys or messages. In the event that hackers or intermediaries gain access to any messages and are able to decode them by breaking the encryption, they will only be able to read that specific message, as each message is encrypted with a unique key. This is a significant advantage of the double ratchet mechanism, as it limits the potential damage of a security breach to a single message, ensuring the confidentiality and integrity of other messages exchanged within the system.

In conclusion, the use of Extended Diffie-Hellman parameters (X3DH) and the double ratchet mechanism in end-to-end encryption protocols provides a strong layer of security that protects against unauthorized access to messages and keys.

Proper implementation of these techniques ensures that even the system designers cannot access the encrypted data, maintaining the privacy and confidentiality of communications.

VI. CONCLUSION AND FUTUREWORK

Thus, through this application we have demonstrated the implementation of multiple encryption techniques sandwiched together in order to achieve an advanced E2EE. This technique ensures protection against cyber-attacks and hackers trying to gain access to sensitive or personal information. This application does not keep any record of user information. It also prevents any 3rd party organization from gaining access to user information even on government orders.

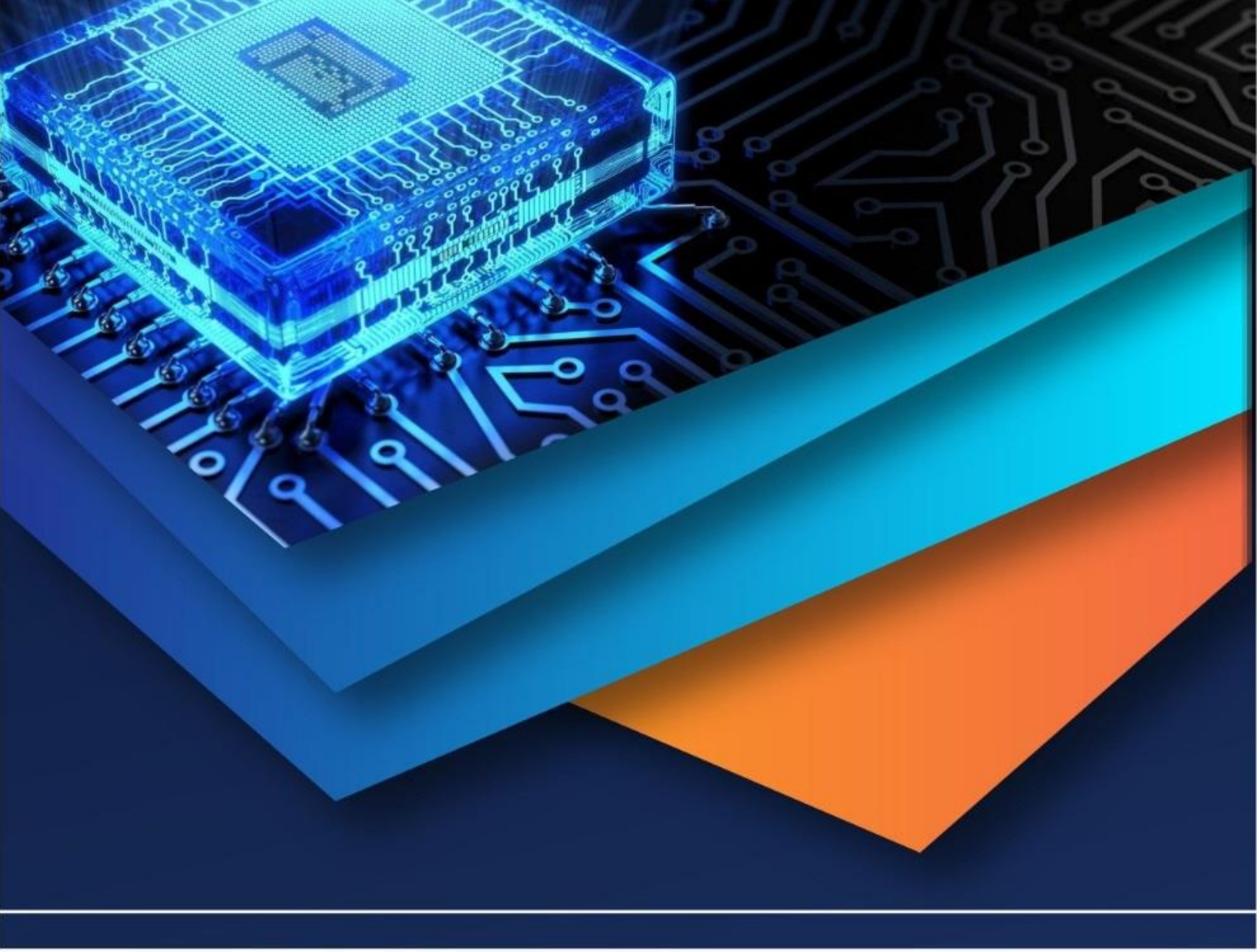
It is evident that if an intruder gains access to the private keys from a low-level device, they would not only be able to record the communication but also send messages on behalf of any party. This is due to the fact that in many devices, the data that is supposed to be erased is not completely wiped out, giving the intruder low-level access.

In conclusion, the use of end-to-end encryption in messaging is crucial for protecting the confidentiality, integrity, and authenticity of messages in today's digital world. While there may be challenges in implementing encryption solutions, the benefits in terms of information security and privacy outweigh the drawbacks. Therefore, encryption techniques should continue to be embraced and advanced to ensure secure and private communication in the face of evolving threats in the digital landscape.

REFRENCES

[1] Joseph Amalraj, Dr. J. John Raybin Jose, “A SURVEY PAPER ON CRYPTOGRAPHY TECHNIQUES”, International Journal of Computer Science and Mobile Computing, Vol. 5, Issue. 8, August 2016.
[2] Ganguly, M., “WhatsApp Design Feature Means Some Encrypted Messages Could Be Read by Third Party” ,2017
[3] Mohamed Nabeel, Qatar Computing Research Institute,” The Many Faces of End-to-End Encryption and Their Security Analysis”, IEEE 1st International Conference on Edge Computing, 2017.
[4] Deepak Garg, Seema Verma, “Improvement over public key cryptographic algorithm”, IEEE International Advance Computing Conference, 2009.
[5] Mohit D. Singanjude, Prof. R. Dalvi, “Secure transmitting of data using RSA public key implemented with Vedic method”, Volume 5–Issue 10, 675-677, 2016.
[6] S. Blake-Wilson, D. Johnson, and A. Menezes, “Key agreement protocols and their security analysis,” in Cryptography and Coding: 6th IMA International Conference Cirencester, UK, December 17–19, 1997 Proceedings, 1997.
[7] Prasoon Varshney, Zubair Beg, Vishal Kumar Shaw and Dr. Ashish Chopra,” SECURED END-TO-END ENCRYPTION USING X3DH PROTOCOL WITH DOUBLE RATCHET ALGORITHM AND ITS LIMITATIONS”, April 2022
[8] T. Perrin, “The Double Ratchet Algorithm (work in progress),” 2016.
[9] https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf
[10] https://signal.org/docs/specifications/x3dh/
[11] https://signal.org/docs/specifications/doubleratchet/

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)