iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.50805

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 V May 2023- Available at www.ijraset.com

A Secure Messaging Application with Unbreakable End to End Encryption

Bawake Harshvardhan[1] , Cholke Saideep[2], Dhole Atharv[3], Jadhav Ankit[4], Prof. Arti Bhise
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 messaging 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].

Users of the app expect a reasonable amount of privacy for all their communications. But Governments demanded for a "backdoor" into apps like WhatsApp, to use in accessing messages and emphasized that they will only use the "backdoor" if there is a credible threat to national security. Users of this apps argued against it claiming that it was infringement of their privacy.

To meet this expectation End-to-End Encryption (E2EE) technology was introduced. This allows for data between communicating parties to be secure, free from eavesdropping, and hard to crack. This technology offers peace of mind to end users because their data are safe in transit, and third parties thus, messages can only be decrypted by the recipient. 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 main reason for not using encryption in email communications is that current email encryption solutions and hard key management. Different encryption techniques for promoting the information security.

Based on a report by Javelin Strategy and Research, one out of every four individuals who experience an online data breach may fall prey to identity theft. End-to-End Encryption can serve as a powerful tool to thwart such attacks. If Yahoo Inc. had implemented it properly, it could have potentially avoided large-scale security breaches like those it experienced in 2013 and 2016, where over 1 billion and almost 500 million accounts were compromised, respectively. However, some governments and secret services are demanding access to users' data from encrypted messaging services such as WhatsApp.

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.

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 this 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. RELATED WORK

Joseph Amalraj, Dr. J. John Raybin Jose et al: This paper gives a detailed study of Cryptography Techniques like AES, DES, 3DES, Blowfish, RSA. Among those algorithms and concepts the security for the data has become incredibly important since the selling and buying of products over the open network occur very frequently. 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. The selected algorithms are AES, 3DES, Blowfish and DES. Firstly, it was concluded that 3DES has the overall better performance than other algorithms. In future we can use encryption techniques in such a way that it can consume less time and power of furthermore and high speed and minimum energy consumption.[1]

Ganguly M. et al: 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 approach is known as "blocking"; the WhatsApp approach is called "non-blocking". This re-encryption and rebroadcasting of previously undelivered messages could potentially allow a third party to intercept and read a user's undelivered messages in a situation where, for example, they had stolen a user's sim card. When the third party put the stolen sim card in another phone, they could then theoretically collect any messages that had not yet been delivered to the user in question.[2]

Mohamed Nabeel et al: In this paper many of the E2E systems are analyzed are not secure against passive adversaries who have access to metadata (POTM) or persistently monitor access patterns (PPER). Further, weak encryption techniques such as DET (non-unique fields), OPE, and SE (partial keyword search) leak information about the encrypted data. Systems employing
such encryption techniques are not secure against even the weakest POTD adversaries. Better designs considering strong encryption techniques, hiding metadata and access patterns, can help construct systems that are secure against strong adversaries. However, there are open issues in doing so. For example, porting existing systems such as web application frameworks while hiding metadata may not always be possible. Further, adding efficient and practical techniques to hiding access patterns remains an open issue as well.[3]

Deepak Garg, Seema Verma et al: In this paper, we have introduced RSA cryptosystem and its improvements. There are many cases when there is the need to enhance the decryption/signature generation speed at the cost of encryption/signature verification speed, e. g., in banks, signature generation can be in huge amount in a single day as compared to only one signature verification in the complete day at receiver side. Many methods are discussed to improve the same, e. g., Batch RSA, MultiPrime RSA, MultiPower RSA, Rebalanced RSA, RPrime RSA. [4]

Mohit D. Singanjude, Prof. R. Dalvi et al: 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. The RSA is so secure as compared to other cryptography techniques. In the MANET there is need to refresh key simultaneously so these methods will help to improve the performance of MANET.[5]

S. Blake-Wilson, D. Johnson, and A. Menezes et al: 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.[6]

Prasoon Varshney, Zubair Beg, Vishal Kumar Shaw and Dr. Ashish Chopra et al: 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. To achieve E2EE, a signed pre-key should be present in the local storage and the server should also have a key bundle so that when one device is offline, it can be used to share the key. 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.[7]

T. Perrin et al: In this paper we learned about double rachet mechanism. It is basically a function that can turn one way only, 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 of Alice and Bob, forming a Double Ratchet.[8]

IV. PROPOSED 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.
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.

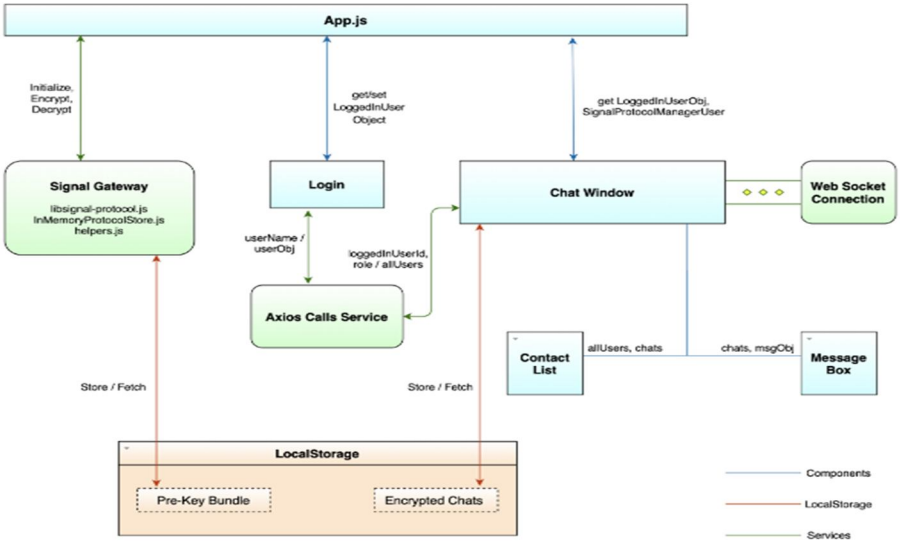


Figure 1: System Architecture

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

V. ALGORITHM

A. *Extended Triple Diffie-Hellman (X3DH)*

So here we will explain X3DH key agreement protocol in detail as it is being used in the Signal Protocol. This is useful in asynchronous communication as well as authentication. For example, Bob has published some information for Alice, but she is currently offline, then the server might temporarily hold the data or send a notification to Alice.

1) The Identity keys help in identifying where the message came from.
2) The Signed keys verify that only the user can control his/her respective identity key.
3) The One-time pre-keys make sure that no one can replay-attack the user by sending the whole conversation again later. These are deleted post X3DH.

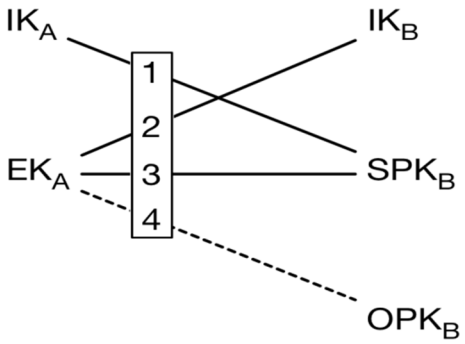


Figure 2: X3DH Exchange

This algorithm makes use of public components of identity keys (IK), ephemeral key (EK), signed pre-key (SPK), and one-time pre-key (OPK). The private components are stored at the respective user devices for computation and not shared.

1) Bob's device generates **IK_B**, **SPK_B**, and a set of **OPK_B** for its connections on App Installation (Login in our case of Web Browser).
2) The public components of these keys are then sent to the Signal Server and stored temporarily (Local Storage in our case) as a pre-key bundle.
3) When Alice installs the app (login in our case), she asks the server/local storage for their pre-key bundle of Bob.
4) She then performs Diffie-Hellman using the public components of her **IK_A** and **EK_A** (one-use session key) on her device.
5) Similarly, Bob performs steps 3 and 4 at his end.

The algorithm performs Diffie-Hellman four times, ensuring mutual authentication (DH1 & DH2) and Forward Secrecy (DH3 & DH4), using a Key Derivation Function or KDF which is quite similar to a hash function.
This produces one master secret key, **SK = KDF (DH1 || DH2 || DH3 || DH4)** at the client's respective devices, that can now be used by Alice and Bob to encrypt and decrypt the messages. To prevent man-in-the-middle attack, the Identity public keys are mathematically combined into a Safety Number using a hash function, which only the sender and receiver will have at their respective ends. This can be in the form of a QR code or fingerprint scan.

B. *What is Forward Secrecy?*

This ensures that future messages shall not be accessed by any third party even when he/she gets access to the public keys. We will discuss this in more detail in the next algorithm.

C. *Double Ratchet Mechanism*

DOUBLE RATCHET: - We got end-to-end encryption using X3DH, we also achieved forward secrecy and mutual authentication in asynchronous communication. Now, why does the Signal protocol still need another algorithm? When a user is offline, it gives an attacker a lot of time to find and use public keys available at the server. Since the key is always the same for a long period, it makes the messages vulnerable. You need to update the keys regularly! In messaging applications like Signal and WhatsApp, these keys are updated for every message. For implementing this, the Double Ratchet algorithm came into play.[7]

A ratchet function is a function that can turn one way only, i.e., it cannot move backward. What we will be using here is called a KDF Ratchet, since you cannot go back to figure out what the key was. This function works as follows-

1) A KDF key and some input data are taken as input to the KDF Ratchet function. This function generates an output key for data and another key for the next KDF Ratchet as input.

2) This creates a KDF chain, as presented in the diagram below, with three inputs being processed and producing three output keys.[7]

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 of Alice and Bob, forming a Double Ratchet. In such a session, we have three chains on both ends, i.e., a Root chain, sending chain, and Receiving chain.

The sending chain of Alice is synchronized with the receiving chain of Bob and vice versa. These start at the same time. In case of any asynchronous event like non-receival of messages or delay or misuse of keys, the receiver keeps a check on the key which is not deleted until all messages are received.

Steps for Double Ratchet mechanism

a) Alice sends a message to Bob by encrypting it using an output key A1 from her sending chain.

b) Bob's receiving chain decrypts this message using A1 and then deletes it later.

c) Steps 1 and 2 repeats when Bob sends a message to Alice.[8]

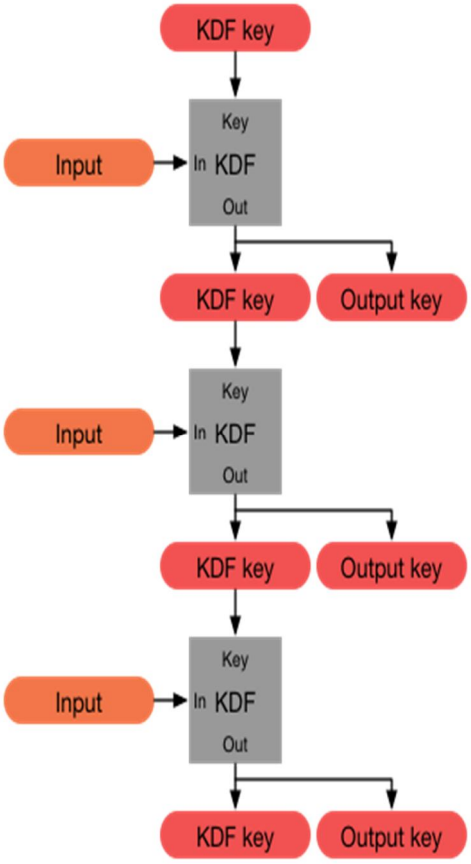


Figure 3: Double Rachet Mechanism

VI.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.

VII.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.

We discussed the importance of Web Sockets technology and end-to-end Encryption, and how these are implemented to develop a real-time secure chat application. The signal protocol, being the most secure and trustworthy protocol provides its code as open source. We also used REST APIs for login operations and to fetch contacts based on role. We implemented the WebSocket library, one of the many libraries available for implementing Web Sockets API in NodeJS.

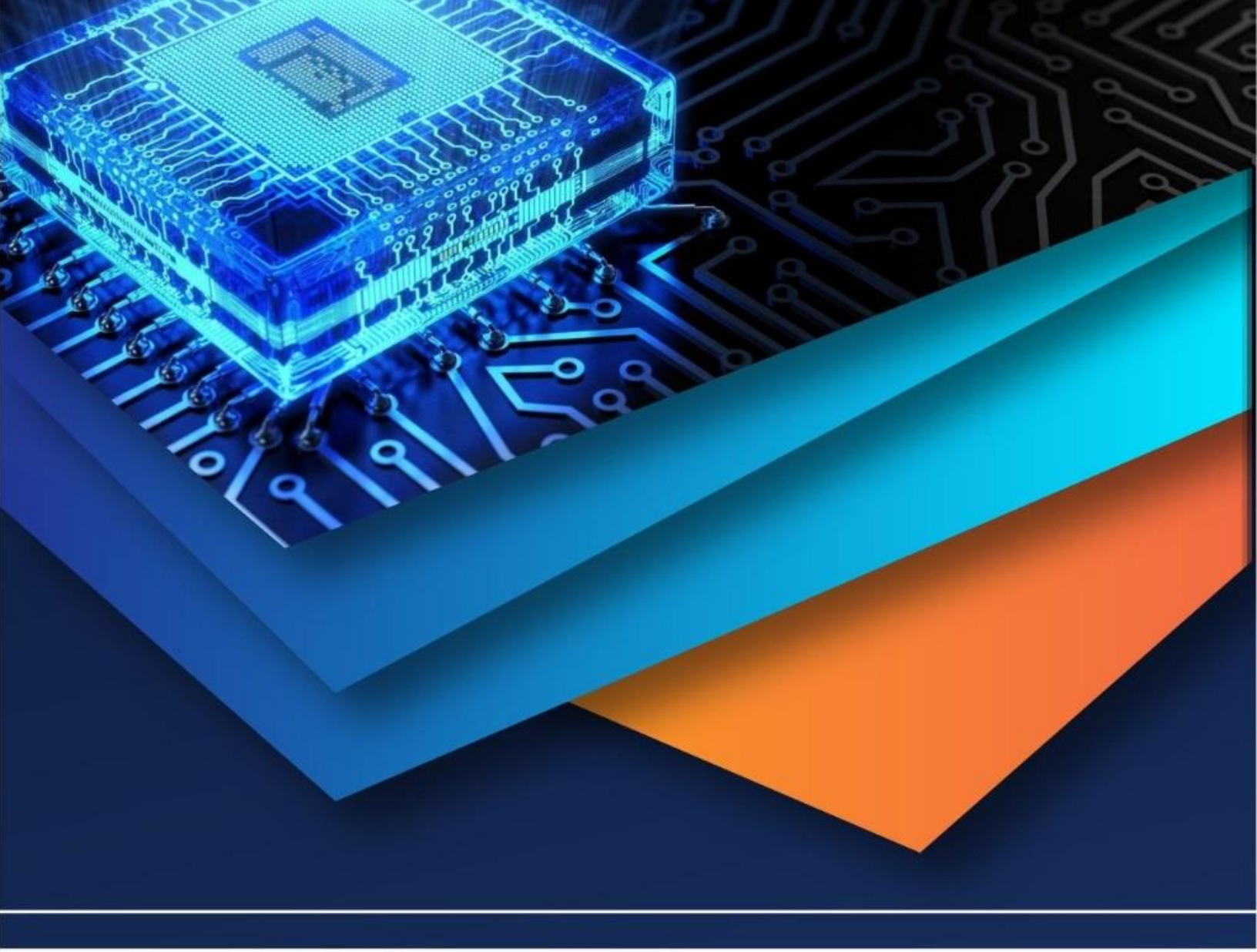
However, many more features can be added to our simple chat application. Such as group messages, online-offline features, guaranteed message delivery, temporary message storage at a separate server, load balancing, and much more that we discussed with the proposed architecture. Firebase can also be used for building a real-time chat application, which internally uses the concept of Web sockets.

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.

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.

REFERENCES

[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. (2017) WhatsApp Design Feature Means Some Encrypted Messages Could Be Read by Third Party.
[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.”
[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://signal.org/docs/specifications/x3dh/
[10] https://signal.org/docs/specifications/doubleratchet/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY