Advancements in Encryption Techniques for Enhanced Data Security Over Cloud

Rishu[1], Vijay Kumar Sinha[1], and Shruti Aggarwal[1]

[1] Department of CSE, Chandigarh University, Punjab, India

Emails: rishu.e10989@cumail.in ; prof.vksinha@gmail.com; drshruti.cse@gmail.com

Abstract

With the advancements in internet technologies and increased transactions over the internet the threats for data security increased many folds than ever. Nowadays message application services are in great demand, as they offered end-to-end encryption (E2EE) that is essential to provide security to the users while communication takes place between parties. Today messaging application service is in great use for communication. For making communication over the network. This paper presents that security is essential while communication takes place between users and how E2EE offers security to the users. Consumers' concerns related to the security and privacy of their data are growing day by day with increased inter-connectivity. We examine the existing mobile message service encryption protocols that provide security and the features which preserve privacy for messenger applications and also evaluate the technical challenges involved for its implementations.

Keywords: Quantum Key Distribution, Elliptic curve Diffie-Hellman key exchange , End-to-End Encryption , Advanced encryption standard, Data Encryption Standard

1. Introduction

The symmetric key algorithm is most simpler and less complex as stated in symmetric database encryption because the same key is used by the sender(to send the data) and the receiver(to receive the data) whereas in an asymmetric algorithm different keys are used i.e to encrypt the data sender used public key and to decrypt the data receiver used private key hence it becomes more complex. Quantum key distribution has come across all the words, the best encryption technique which works on physics principles of uncertainty. This QKD states that during transmission if any third party is trying to make a duplicate file and transfer it to the receiver then the receiver may determine the no. of bits and compare it with constant real bits. The transmission will be broken on the spot. In the quantum theory of encryption, the author had used photons individually for the transformation of the encryption key between the person.

DOI: https://doi.org/10.54216/JCIM.080202
Received: May 05, 2021 Accepted: October 13, 2021

With the enhancement in the field of science and information technology, the world is changing day by day and nowadays this is very difficult to hide the presence of technologies in our day-to-day life.

Now, communication becomes easier with these developing technologies and Whatsapp is one of the most popular message application services using today for means of communication so the security of the data of their user is their main concern [1]. So they introduced E2EE technology in their message application service through this no third party can access their data without authorization. This feature or technology provides its users to communicate securely and also ensures their users that the data is protected while transferring even no other party or Whatsapp itself able to see or access any message and also offers integrity, security and privacy during communication. While data transferring from the sender side it goes in the encrypted format in which no information can be read by anyone or can only be read or decrypted by the recipient which has that secret key. So for transferring the information over internet encryption is mostly used in technology[2]. While maintaining E2EE in Whatsappguarantees privacy and security in the conversations between the sender and receiver and it also assured users that no third party is monitoring their conversations, then the conversations tend to be like a real conversation(face to face) which is secure. Governments want"backdoor" into such applications, to have to access messages, in such a scenario where national security is at risk means somebody tried to threaten data but end-user of Whatsapp denied to build "backdoor" because they told that a "backdoor" will affect their privacy, as the hackers can also take advantage of it by making some attacks on our communication[3].

2. **Background**:

2.1 E2EE:- E2EE stands for End to End encryption that ensures security in message application services. In today's life, it is necessary to maintain the security between the two communicating parties so that their information will not steal or read by a third party[4].

2.2 QKD:-Quantum key distribution(QKD) ensures that no third party can read the messages or access any data. If any unauthorized person tries to do so the sender gets alert and the threat is broken in between.QKD is implemented and to generate a random secret key for a secure communication quantum mechanism is used. This random secret key is required for the encryption and decryption of messages[5].

2.3 ECDH:-E2EE is provided by ECDH key exchange that includes key pairs, that should be exchanged between two parties to create a secure shared key. This key can be used as an encryption key. Through this, no one can access the conversation going on between two parties so the personal information of the user is maintained secured[6].

2.4 Encryption: - It is the process of encoding your message into a form that is not readable by any other person or party, an encoding of that message will be done by the private or public key of the sender [7].

2.5 Decryption:- It is the process of decoding the message sent by the sender that decodes the message into a readable form and that will be done by the private or public key of the receiver[8].

DOI: https://doi.org/10.54216/JCIM.080202
Received: May 05, 2021 Accepted: October 13, 2021

3. Algorithm

There are many algorithms used for attaining E2EE in mobile chat applications to ensure the message send to the recipient is delivered securely or not or the data is both confidential and authenticated depends upon the encryption technique. So there are some important algorithms discussed in this paper.

a. ECDH: ECDH is a method of performing key agreements. The goal of this algorithm is to generate a secret key on both sides(receiver and sender side). The random key will be selected by both parties that will be considered as a private key. The working of the algorithm is given below:-

1. a. The sender will have a private key(d_A).
   b. The receiver will have a private key(d_B).
2. Now the sender will compute a public key:-$Q_A=d_A*G$-(1) and the receiver will compute public key $Q_B=d_B*G$ -(2).
3. Both parties will now exchange their public key with each other to compute the secret key.
   a. Sender computes secret key = d_A*Q_B _-(3)
   b. Alice computes secret key = d_B*Q_A -(4).
4. Put the value of equations 1 and 2 in equations 3 and 4 respectively. Now the shared key will be:-

a. at sender side= d_A* d_B*G

b. at receiver side= d_B* d_A*G .

5. Here both the party have the same secret key (symmetric)[9].

b. RC4: RC4 is an algorithm that uses a symmetric key that specifies the same key will be used for encrypting or decrypting the text as the XORing is performed between the data stream and generated key sequence in this case keystream is not dependent on the plain text that is being used. It makes use of a variable-length key that is from 1-256 to initialize the 256-bit state table, in this state table is utilized for pseudo generation for random bytes and also for a random stream. To get ciphertext XORing is done with the plain text and pseudo-random stream so that in-state table the elements are swapped at least once. Due to restrictions in export, the key is bounded to 40 bits but sometimes the key is used as 128 bit. The capability of RC4 is that it can use keys between 1-2048 bits. There are two phases in the algorithm that is ciphering and key setup. The key setup is a difficult phase. When the N-bit key setup starts (N is the length of the key), the generation of encrypting variable is done with the use of encryption key and by using 2 arrays, key & N-no. of mix operations. The mix operation includes swapping of bytes, modulo operation, etc [11].

c. AES: AES was created by the National Institute of Standards and Technology (NIST) which is known as the new Federal Information Processing Standard (FIPS) publication. It has described methods of encryption.AES has replaced DES as it is most powerful and it is a privacy transform for the IPSEC and Internet Key Exchange.AES had offered a very large key size that ensures only authorized members can decrypt messages and intruders will fail to decrypt the message. In 2001, the US government used asymmetric key encryption standard which was designed by Vincent Rijmen and Joan Daemen in the year 1998. Many security

DOI: https://doi.org/10.54216/JCIM.080202
Received: May 05, 2021 Accepted: October 13, 2021

mechanisms were performed and AES became most effective in May 2002.AES has three different keys 128,192 and 256 bit were used for encrypting 128-bit data. Different rounds depend upon key length that is for 128 bit key 10 rounds need to be done and similarly for 192 bit key -12 rounds, for a 256-bit key for 14 rounds[13].

4. Usage of security with applications:

Robert E. Endeley [2018]surveyed that due to enhancement in the field of science and information technology the world is changing day by day and nowadays this is very difficult to hide the presence of technologies in our day-to-day life. As Whatsapp is using as means of communication so for the security of its user, it has become more imperative. So for better security provided to its user by Whatsapp by introducing E2EE technology. This feature or technology provides its users to communicate securely. This feature ensures their users that the data is protected while transferring even no other party or Whatsapp itself can see or access any message. This technology also offers integrity, security, and privacy during communication[15].

Sagheer et al. [2018] have developed a secure chat application. The proposed application was tried on many devices like android phones which help users to communicate safely and provide E2EE secure communication. Through the encryption of data, the communication process is done and in the encrypted form, data is submitted to an internet server. After that encrypted data is retrieved by some queries and decryption is done. Then finally the result is shown to the client. The application comprises a set of interface designs, that allow the client to do chat with the other client. Here E2EE is provided by key exchange Which includes key pairs, that should be exchanged between two parties to create a key that is secure and must be shared with both. This would be used as an encryption key[16]. User's personal information is maintained secured, no one can have access to the chat. even the provider of service is not allowed to interrupt. only at server-side exchange data is stored and physical memory of phone stores nothing. AES provides high secure thou it is slow. Here RC4 algorithm is used for the encryption of voice and image. It is a fast encryption technique and mostly suitable for smartphone devices which is capable of encrypting the infinity sum of the data.
Many applications claim to give protection to administration but could not access the design freely. Ali Makki in 2013, introduced a crossbred cryptography plan (AES and RC4 for the key extension) For providing security to text data. The cryptographic algorithm was tried on different cell phones like Nokia 5233. The paper used public-key encryption that could save cost and also the time of encryption is minimized. Chen et al. [17], In 2014, reveal the idea of smartphone chats that utilizes a session key based on transposition.it accustoms the technologies of substitution & classical block cipher. With the use of network innovation, the key can be created for new sessions [18].

Galushka et al. [2018] have stated that almost all companies, industries use data warehouses or databases to store millions of data using SQL but at the same time security is also mandatory. For this, the company depends upon security tools for a database management system(DBMS). This includes some methods for access control and rights distribution for users and tools like dynamic data [19] masking or stored procedure encryption in SQL servers. Moreover, these methods would require one or more administrations that shall have complete access to the database and the capability to disable security mechanism configurations. This kind of operation features can be exposed that can lead to leakage of data and therefore for protecting databases an effective method of cryptography is used to

DOI: https://doi.org/10.54216/JCIM.080202
Received: May 05, 2021 Accepted: October 13, 2021

remove the access of the unauthorized person. Database E2EE involves data transfer & storage and the clients who are authorized and participating in exchange can have access to the database. With the use of the cryptographic algorithm, the E2EE technique ensures that the elements or the facts are maintained directly by the clients. Neither server that stores data and nor interceptors can decrypt messages. Encryption of the text data increases protection which reduces data loss possibility and it does not cancel control access. Suppose on computer database is installed and configuration was incorrect and confidential data was known by the attacker but the stolen data would be treated like garbage. If it was encrypted previously.

for eg:-In symmetric-key algorithm uses only the same or secret key to encrypt or decrypt the data but in asymmetric algorithm different keys are used i.e to encrypt the data different key is used by the sender(i.e private key) and to decrypt the data different key is used by the receiver(i.e public key). So due to the simplicity of symmetric encryption, the speed is best and a shorter key length ensures strength. To maintain true interaction of the client who is exchanging information with the database. One user should be allowed to decrypt data that was not only encrypted by him but also by another user. so one key must be provided to them[20].

Abirami N. [2018] has said that there are several portals in digital communication but the point is that if it's secure or not. lack of security will result in the loss of data that means no. of crime will increase if confidential data will be lost. As we come across algorithms like RSA, AES, ECDH key exchange which is used for security and they are useful too. Whatsapp uses the RSA algorithm that is an asymmetric key Algorithm but for quantum computers, this algorithm will not be efficient. To overcome this problem quantum cryptography is used. The author had used photons individually for the transferring of encrypted key data between the two-person. The photon itself will determine the value, it can be 1 or 2 series bit photon which is generated at the sender side whereas at receiver side photons divergence is calculated. During this process of transmission of data, if the third party tries to interfere, the cryptographic file is destroyed and it is returned to the sender. The physics had introduced the uncertainty principle on which QKD works which makes third-person impossible to determine the features of transmitted bits and also the third party can not make any duplicate file. if he tries to make a duplicate file and send it to the receiver, the receiver will get to know as bits would not be the same as constant bits[21].

Ganguli et al.[2017] surveyed that by using an acclaimed signal protocol, unique secret keys will be generated because as we know EC is the process of encoding the plain text message into a form that cannot be read by anyone and can only be read or decrypted by the recipient which has that secret key. So for transferring the information over internet encryption is mostly used in technology. For eg:- If any end-user re-install the application or gets a new phone, the message which is pending to be deliveredwhen the person used to be offline,then the message was encrypted and resent utilizingthe sender automatically without even sender didn't have an opportunity to verify that message received by the user is the one intended to receive that message. The sender will get notification only if the sender had opted for the notification in the setting, for generating the secret keys for making communication possible between two parties the protocols enable in E2EE. However in such a case where the user re-installs Whatsapp then-new secret keys get generated[22].

Lewis et. Al [2017] surveyed that according to end-user it is the first requirement of every end-user that their private information should be kept confidential and cannot be used or accessed by any other so E2EE is the better technology introduced by Whatsapp for securely transferring of data, the privacy for communication is a key element of human

DOI: https://doi.org/10.54216/JCIM.080202
Received: May 05, 2021 Accepted: October 13, 2021

rights as he surveyed that the developed encryption technique has not reached up to that level which justifies various restrictions like the re-encrypted and re-sending of undelivered message allows the third party to read or intercept undelivered messages of the user in a scenario where for Eg- User lost his sim card and that sim card had stolen by the third party and then they collect that messages theoretically, which is pending to deliver yet. Because by inserting that sim card the third party can intercept those messages and hence the confidential information will be lost[23].

Whittaker and Z. [2017]surveyed that by using E2EE technique helps government and secret services because with the use of E2EE it reduces efforts to organize combat against crime, child pornographers and terrorist to protect our data or confidential information. Governments wanta “backdoor” in those applications, to have access to the message and assuredthat they will use “backdoor” in such a scenario where national security is at risk means somebody tried to threaten data. But end-user of Whatsapp denied buildinga “backdoor” and argued because they told that a “backdoor” does not affect their privacy only, but the hackers can have benefited from it by making some attacks on our communication.

The government wants to access messages only to avoid or stop any type of attack on the network but as end-user of Whatsapp denied so conflict occurs between the government and users of Whatsapp for the security of their data,his research presents benefits of E2EE which provides security and privacy and allows communication securely and in July 2017 the senator said that “the US government does not need the approval of its secret surveillance court to ask a tech company to build an encryption backdoor”[24].

Michalas and A. [2017] surveyed that the removal of E2EE from Whatsapp is not a solution because criminals, attackers, or hackers can create a similar type of software that allows people to securely communicate, while any other ordinary person loses the ability for sending messages over the internet. While maintaining E2EE in Whatsapp, guarantees privacy and security in the conversations going between sender and receiver. and it also assured users that no third party is monitoring their conversations, then the conversations tend to like a real conversation(face to face) which is secure[25].

Berlin et al. [2017] have designed an algorithm for the encryption of text. In this approach, the input file was encrypted two times using a different algorithm that is a substitution approach and polyalphabetic cipher technique. With the help of double encryption, strong protection was provided to the data. For the protection of text messages, a new efficient cryptographic approach is used. For every new message, a new key was generated and time complexity was also efficient. The hybrid encryption technique was also used which includes both symmetric and asymmetric cryptosystem which means two algorithms participated is AES and Elliptic Curve Cryptography. US national cyber security states that 60 % of small scale or mid-level companies are been affected by different hackers which takes a long time to recover cost over $6,90,000 is need by small companies and $1million is need by corporate companies to get off from cyber attack problems.

To maintain security in companies:-

1. They should protect the system with high version antivirus software.
2. Also, they should avoid unwanted links so that hackers could not get a chance to interfere in the system.
3. Scan the USB with a malware detector.

DOI: https://doi.org/10.54216/JCIM.080202
Received: May 05, 2021 Accepted: October 13, 2021

4. Another encryption mechanism is LINE.LINE provides a letter sealing mechanism to create security along with multi-level platforms. It is used to encrypt both textual and multimedia data. LINE server gives the public key to all clients to initialize the message while installation of the LINE app. so the author suggests the best security aspects[26].

Krombholz et al. [2015]surveyed that E2EE is another gift from God". Criminal defendants across the United States are benefiting from E2EE while the safety of all other American communities is in peril. However, providing a backdoor would not only be a risk of privacy to Whatsapp users but creating a way for the hackers or attackers to read encrypted messages would also make the system vulnerable to cyber-attacks. Because by implementing backdoor into such app predict that there is no secure communication take place however Skype was a very popularly used app and in this backdoor was implemented by the Microsoft corporation even though its user base knew that Skype was fully endowed with end-to-end encryption technology. However, in 2013 government whistleblower Edward Snow-den revealed that the platform did in fact, have a backdoor and communication is not secure on that application. This revelation led to a protest of Skype users and an eventual loss of credibility of the application [27].

5. Discussion And Conclusion

While we discussed the need for security while communication takes place between the users. According to Robert Endeley government ask to put a backdoor in the messaging application services but the user of Whatsapp application services did not agree to have a backdoor in such application services and they argued that by putting backdoor it will not affect the privacy of their messages but the hackers or any third party can take advantage of it and can steal our confidential information. Because implementation of backdoor means the information does not end to end encrypted. According to Michalas, the implementation of E2EE provides the user peace of mind that their data or information is secure while transferring over the internet. This feature of Whatsapp provides integrity, confidentiality, and availability to the user. The text files were encrypted two times and for each message, new keys were also generated by the use of Elliptical curve cryptography and AES. Companies should also be aware of threats due to which company data get lost. They should ignore the spam links and the antivirus is the most necessary task for a computer system. The USB should be scanned before using it on computers. To provide security at multiple interfaces LINE app is used which can encrypt text and files of multimedia. Also, the RC4 Algorithm is used to encrypt voice messages and images.RC4 has the strength to encrypt the infinity group of data. Authentication, confidentiality, integrity, and nonrepudiation are key points that are essential for all applications to make them more secure. The database and Dataware house security are also important for every organization and industry. They use data warehouses to keep millions of data regularly. Database encryption involves the transfer and storage of data and the valid person can only have access to it. Data dynamic masking and access control mechanism plays a vital role. The encryption process like symmetric and asymmetric encryption has some complexity and simplicity. The symmetric key algorithm is most simpler and less complex as stated in symmetric database encryption because the same key is used by the sender(to send the data) and the receiver(to receive the data) whereas in an asymmetric algorithm different keys are used i.e to encrypt the data sender used public key and to decrypt the data receiver used private key hence it becomes more complex. Quantum key distribution has come across all the words, the best encryption technique which

DOI: https://doi.org/10.54216/JCIM.080202
Received: May 05, 2021 Accepted: October 13, 2021

works on physics principles of uncertainty. This QKD states that during transmission if any third party is trying to make a duplicate file and transfer it to the receiver then the receiver may determine the no. of bits and compare it with constant real bits. The transmission will be broken on the spot. In the quantum theory of encryption, the author had used photons individually for the transformation of the encryption key between the person. The photon would be able to detect 1 and 2 series bit(sender side) and divergence of a photon is calculated(on the receiver side).

References:

[1] Gopal Ghosh, et al. 'A Systematic Review on Image Encryption Techniques' Turkish Journal of Computer and Mathematics Education, Vol.12 No.10 (2021), 3055-3059 M. Balazinska et al., "Data management in the worldwide sensor web," IEEE Pervasive Comput., vol. 6, no. 2, pp. 30–40, 2007, DOI: 10.1109/MPRV.2007.27.

[2] Ghosh, Gopal; et al. 'Internet of Things based video surveillance systems for security applications' Journal of Computational and Theoretical Nanoscience, Volume 17, Number 6, June 2020, pp. 2582-2588(7) https://doi.org/10.1166/jctn.2020.8933

[3] Kaur Manjit; et al. "Flying Ad-Hoc Network (FANET): Challenges and Routing Protocols" Journal of Computational and Theoretical Nanoscience, Volume 17, Number 6, June 2020, pp. 2575-2581(7), https://doi.org/10.1166/jctn.2020.8932

[4] Greenberg, A. (2014). Hacker Lexicon: What Is End-to-End Encryption?. Ηλεκτρονικό]. Available: https://www. wired. com/2014/11/hacker-lexicon-end-to-end-encryption/.[Πρόσβαση Οκτώβριος 2017].

[5] Renner, R. (2008). Security of quantum key distribution. International Journal of Quantum Information, 6(01), 1-127.

[6] Durlanik, A., &Sogukpinar, I. (2005). SIP authentication scheme using ECDH. World EnformatikaSoc Trans EngComputTechnol, 8, 350-353.

[7] M. Kumar, P. Mukherjee, K. Verma, S. Verma, and D. B. Rawat, "Improved Deep Convolutional Neural Network-based Malicious Node Detection and Energy-Efficient Data Transmission in Wireless Sensor Networks," in IEEE Transactions on Network Science and Engineering, DOI: 10.1109/TNSE.2021.3098011.

[8] Decryption and how it works https://www.educba.com/what-is-decryption accessed on 20/11/2019 5:00 PM

[9] Kodali, R. K., &Sarma, N. N. (2014). Energy-efficient ECC encryption using ECDH. In Emerging Research in Electronics, Computer Science and Technology (pp. 471-478). Springer, New Delhi.

[10] ECDHhttps://www.google.com/search?q=ecdh&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjWiesxqjnAhWOHMBHR5lBEUQ_AUoAXoECBIQAw&biw=1366&bih=625#imgrc=CBGMJTG6tFUA2M

[11] Mousa, A., &Hamad, A. (2006). Evaluation of the RC4 algorithm for data encryption. IJCSA, 3(2), 44-56.

[12] A. Hussain et al., "A Resource Efficient hybrid Proxy Mobile IPv6 extension for Next-Generation IoT Networks," in IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2021.3058982.

[13] Rayarikar, R., Upadhyay, S., &Pimpale, P. (2012). SMS encryption using AES algorithm on android. International Journal of Computer Applications, 50(19), 12-17.

[14] Working of AES https://www.google.com/search?q=working+of+aes&source=lnms&tbm=isch&sa=X&ved=2ahUKEwir9I CEy6jnAhVJ6XMBHUy7CWcQ_AUoAnoECA4QBA&biw=1366&bih=625#imgrc=sm8AcLAns8mw8M: accessed on 3/12/2019 2:00 PM

DOI: https://doi.org/10.54216/JCIM.080202
Received: May 05, 2021 Accepted: October 13, 2021

[15] Endeley, R. E. (2018). End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. Journal of Information Security, 9(01), 95.

[16] Sagheer, A. M., Abdulhameed, A. A., &AbdulJabbar, M. A. (2013, December). SMS Security for Smartphone. In 2013 Sixth International Conference on Developments in systems engineering (pp. 281-285). IEEE.

[17] Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., ...& Philip Chen, C. L. (2014). SCADA communication and security issues. Security and Communication Networks, 7(1), 175-194.

[18] Mock, M., &Swedor, O. (2014). U.S. Patent No. 8,726,026. Washington, DC: U.S. Patent and Trademark Office.

[19] Shmueli, E., Vaisenberg, R., Elovici, Y., &Glezer, C. (2010). Database encryption: an overview of contemporary challenges and design considerations. ACM SIGMOD Record, 38(3), 29-34.

[20] Galushka, V. V., Aydinyan, A. R., Tsvetkova, O. L., Fathi, V. A., &Fathi, D. V. (2018, May). System of end-to-end symmetric database encryption. In Journal of Physics: Conference Series (Vol. 1015, No. 4, p. 042003). IOP Publishing.

[21] N.Abirami (2018) E2EE ENCRYPTION using QKD Algorithm, International Journal Of Trend in Scientific Research and Development , Vol-2.

[22] Lim, Y. Y., Messina, M., Kargl, F., Ganguli, L., Fischer, M., & Tsang, T. (2008, April). SNMP proxy for wireless sensor network. In Fifth International Conference on Information Technology: New Generations (it 2008) (pp. 738-743). IEEE.

[23] Lewis, J. A., Zheng, D. E., & Carter, W. A. (2017). The effect of encryption on lawful access to communications and data. Rowman& Littlefield.

[24] Whittaker, Z. (2017)US Says It Doesn't Need Secret Court's Approval to Ask for ENCRYPTION Backdoors.

[25] Mavroeidakos, T., Michalas, A., &Vergados, D. D. (2016, April). Security architecture based on defense in depth for Cloud Computing environment. In 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 334-339). IEEE.

[26] K. Berlin (2017)Adoption of Crypto ENCRYPTION Techniques in Different Scenario. International Journal of Advanced Research in Computer Science and Management Studies, Volume 5.

[27] Krombholz, K., Hobel, H., Huber, M., &Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

DOI: https://doi.org/10.54216/JCIM.080202
Received: May 05, 2021 Accepted: October 13, 2021