Analyzing Cryptographic Integrity and Security Challenges in WhatsApp, Telegram, and OpenSSL and Development of CipherX

*Arjun Verma[1], Falguni Sharma[2], Prashant Sharma[3], Ayush Choudhary[4], Jyoti Khemnani[5], Chirag Choudhary[6], Arvind Pal[7]
Department of Computer Science and Engineering, Vivekananda Global University, Jaipur, India
[1]23tec2cs769@vgu.ac.in, [2]falguni.sharma@vgu.ac.in, [3]prashant.sharma@vgu.ac.in, [4]23tec2cs307@vgu.ac.in, [5]23tec2cs496@vgu.ac.in, [6]23csa2bc008@vgu.ac.in, [7]23tec2cs797@vgu.ac.in

Abstract

This research aims at understanding the application of cryptography in the protection of communication, evaluating apps such as WhatsApp, Telegram, and OpenSSL. Despite using encryption methods including RSA, AES, ECC, such platforms possess risks including, metadata leaks, cryptographic deficiencies as well as insider's threats. It was found that although WhatsApp currently has strong end-to-end encryption, its backup features are inadequate and reveal metadata. Telegram has added 'Secret Chats' to improve security but its MTProto communication protocol and cloud storage raise risks to the security of its users. Secure communications app OpenSSL becomes a problem for complexity and key management as the Heartbleed exploit showed. The study also reviews the creation of CipherX –practical and efficient text encryption, the Chrome extension. Having been developed to meet the need of secure communication needs CipherX has a good interface and a solid keys management system. This feature of integration allows the users to safeguard their data properly while at the same time making use of the convenience of commonly used Google Chrome browser interface. CipherX is depicted as a means of secure encrypted communication service that is easily accessible and navigable. The paper presents a comparison of cryptographic protocols, and assessment of the merits and demerits of existing architectures and technologies, and shows how tools like CipherX can complement and strengthen user security. Ideas are provided to improve security issues related to familiar social applications like WhatsApp, Telegram, and OpenSSL.

Keywords: Cryptography, Encryption, Data security, Key management, Digital communication, Symmetric key encryption, Digital privacy, Information confidentiality.

1. Introduction

At the moment, encryption plays a vital role in protecting the vast amounts of data that are sent via communication channels. Secure communication techniques are more important than ever in the modern world, when practically all human interactions, including social interactions, corporate transactions, and financial dealings, take place online Applications like OpenSSL, Telegram, and WhatsApp rely heavily on cryptographic methods to safeguard user data. Despite the fact that these platforms have advanced encryption techniques, they are still made of humans and are therefore vulnerable to security flaws. For example, WhatsApp uses end-to-end encryption to secure chats, but users' backup files and information are left open to prying eyes. Though it has also drawn criticism for using the proprietary MTProto protocol and having default encryption, "Secret Chat" is a more secure messaging option. Although OpenSSL has contributed to the security of web communications by offering essential tools for

N. Vyas et al. (eds.), *Proceedings of the International Conference on Advancements in Computing Technologies and Artificial Intelligence (COMPUTATIA 2025)*, Advances in Intelligent Systems Research 189,
https://doi.org/10.2991/978-94-6463-700-7_38

cryptography, it has also given rise to some high-profile vulnerabilities, such as the Heartbleed problem. This essay seeks to explain the origins and evolution of cryptography, comprehend the operation of modern cryptographic algorithms like RSA, AES, and ECC, and point out the dangers and vices associated with Telegram, WhatsApp, and OpenSSL. The goal of the article is to compare various platforms and offer comprehensive information on the current status of cryptography and the ongoing need to improve cyber security in light of emerging cyber threats. The goal is to draw attention to the necessity of having more robust, tried-and-true cryptography protocols that are both simple to use and extremely safe.[1]

1.1 Motivation of Research

The need for secure security systems has grown significantly since digital communication and data exchange markets expanded dramatically. Encryption keeps emerging cyber threats at bay by maintaining user privacy along with enabling safe communication methods. Various encryption tools demand specific technical knowledge so they remain difficult for regular users to operate. The development of this research seeks to create an encryption solution which features easy usability along with secure performance in daily digital communication. The research identifies security vulnerabilities in communication tools to strengthen user privacy protection and makes private conversations accessible to non-cryptographic experts.

1.2 Objective of Research

A priority of this investigation lies in designing an end-to-end encryption tool which protects user operations while maintaining both convenience and effective performance. The research develops a Chrome extension that provides an easy method for encryption and decryption while creating secure communication options available for users at large. A robust symmetric key encryption algorithm serves as protection for text messages through its implementation to prevent unauthorized access. The system will use advanced key management security features which solve a major encryption application problem of unauthorized system entry. The tool integrates with multiple digital communication interfaces to maintain its operational capabilities while preserving easy user interactions. The security profile together with usability factors of the proposed system will receive comprehensive evaluation based on research and testing protocols. The proposed study aims to create usable encryption protocols which ensure digital privacy across all users.

2. Literature Review

2.1 Core Principles of Cryptography

Throughout its history, cryptography has been guided by three fundamental principles:

2.1.1 Confidentiality: The fundamental principle of cryptography relies on confidentiality because it enables authorized persons alone to view specific information. Sensitive data remains accessible only to authorized users because cryptography prevents various forms of unauthorized access or data exposure in digital communications. The safeguarding of security needs both symmetric and asymmetric encryption to ensure data confidentiality. Symmetric algorithms with encryption capabilities use the AES method which protects information through a shared

key that both sender and receiver must protect securely. Both RSA and other asymmetric encryption protocols implement a public-private key combination to let only authorized receivers access encrypted messages successfully. Network data transmission finds additional protection through secure communication protocols which implement SSL/TLS standards. The disclosure of important data including financial activities and corporate records becomes possible when confidentiality measures are not in place because eavesdropping attacks and data breach events can occur. Firmware remains a top priority in cybersecurity due to increasing complexity of cyberattacks while encryption and access controls and secure key management systems aim to protect confidentiality.[2]

2.1.2 Integrity: The essential principle of cryptography depends on integrity to maintain trustworthy data that stays unmodified throughout its journey from source to endpoint. This security measure protects data from alteration that may occur from unintentional or purposeful modification while data is stored or transmitted. The SHA-256 hash function together with other cryptographic functions serves to protect data integrity through its production of single fixed-length hashes for input data which changes upon any modification indicating tampering attempts. MACs and digital signatures operate as additional integrity mechanisms that verify both the authenticity of data and the identity of its source. Cloud computing depends on integrity protection for its remote-hosted data due to its critical importance in this environment. The protection of data from unauthorized modifications is achieved through user-end encryption techniques and hashing provides consistency verification for data. Strong cryptographic methodologies play an essential role in data protection because cybersecurity threats demand them to maintain accurate and trustworthy information throughout its entire lifespan. [3]

2.1.3 Authenticity: The fundamental principle of cryptography requires authenticity to verify proper identity of communicating entities while confirming messages came from valid sources without any modifications taking place during transfer. The widely used digital signature algorithm called ECDSA creates authenticity through verification so recipients can confirm both the message source and the content preservation. Post-quantum cryptography development focuses on creating new methods to protect digital communication's authenticity against quantum threats in order to secure communications through the quantum computing age. Strong cryptographic techniques represent the key requirement for maintaining secure communications because digital threats consistently advance in sophistication.[4][5]

2.2 How Cryptographic Algorithms Work

Investigating the inner workings of these fundamental cryptographic algorithms is crucial to comprehending the breadth and potency of contemporary cryptographic techniques.

2.2.1 The RSA Algorithm

Public key cryptosystems like the RSA method are frequently used to transmit data securely. It is protected by the factoring problem, which is the practical difficulty of factoring the product of two huge prime numbers.

2.2.1.1 How RSA Works:

(A) Key Generation:

Select Primes: Choose two large prime numbers, p and q. **Compute n:** Calculate $n=p\times q$. The different keys in this case entail a value n, which serves as the modulus, as will be explained later. **Compute (n):** Establish $\phi(n)=(p-1)\times(q-1)$. **Public Key:** Select an integer e with the conditions that $1 < e < \phi(n)$ and $\gcd(e, \phi(n))=1$. The

different keys in this case entail a value n, which serves as the modulus, as will be explained later 'e' and 'n'. **Private Key:** We therefore compute d as the modular multiplicative inverted value for e with respect to $\phi(n)$, that is, $d \times e \equiv 1 \pmod{\phi(n)}$. In these bases, the Otway and Dawson have set the private key as (d, n).

(B) Encryption:

To encrypt a message M using the RSA algorithm, it must first be converted into an integer m that falls within the range $0 \leq m < n$. This transformation is typically done using character encoding techniques such as ASCII or Unicode, ensuring that textual or binary data is properly represented as a numerical value suitable for encryption. Once m is obtained, RSA encryption is performed using the public key, which consists of two values: e (public exponent) and n (modulus). The encryption formula is:

$$c = m^e \pmod{n}$$

Here, cc represents the Ciphertext, which is the encrypted version of the original message. The modular exponentiation ensures that the encryption process remains computationally secure. Since only the intended recipient possesses the corresponding private key, decrypting the message without it is practically infeasible, making RSA a reliable method for secure communication.[6]

(C) Decryption:

The decryption process for Ciphertext cc under RSA requires the private key consisting of exponent d together with modulus n belonging to the recipient. To decrypt the message through the RSA algorithm one computes mm by using the following formula:

$$m = c^d \pmod{n}$$

Efficient calculation of this modular exponentiation becomes important because dd and nn represent large numbers created from multiplying two prime numbers pp and qq. To accomplish this process efficiently the square-and-multiply algorithm is usually used. Decryption efficiency improves with the implementation of the Chinese Remainder Theorem (CRT) because it reduces the magnitude of numbers used in computational operations. [7]

An integer mm after being obtained from decryption needs to be converted into its original format through ASCII or Unicode encoding schemes. The decryption process through M delivers a result that matches exactly with the message the sender originally transmitted. The encryption method of RSA depends on the factoring challenge of large composite numbers to ensure that only the recipient holding the d private key can successfully decrypt the message without compromising security.[8]

2.3 Advanced Encryption Standard (AES)

One of the primary symmetric key encryption algorithms is AES, which the US government approved in 2001. It is frequently used for safe data encryption and can accommodate key sizes of 128 to 256 bits.

2.3.1 How AES Works:

(A) Key Expansion:

The encryption procedure starts through key expansion by using the Key-Schedule method. The primary key expands during encryption to create various round keys which serve specific rounds in the process. Security against cryptanalysis improves because key expansion generates different keys for each round of the process. The Rijndael

key schedule implements byte substitution shifts XOR constant values to generate series of round keys for AES encryption operations. [9]

(B) Initial Round:

Add Round Key: The encryption process begins with the initial Add Round Key step after which AES enters its main rounds of encryption. An XOR operation connects the state input (128-bit block) exclusively to the first round key. The initial plaintext integrates with encryption key through this step which makes it difficult for attackers to uncover the original message. [9]

(C) Main Rounds:

Proceedings in each round of the main encryption phase require four vital transformations which run in a specific sequence:

i. Every byte in the state receives a value from the Substitution Box (S-Box) through its designated substitution mechanism which serves to introduce confusion for security reasons.[9]

ii. Each row of the state matrix receives cyclic repositioning during the Shift Rows transformation. With the first row remaining fixed the succeeding rows advance their byte positions one by one until the fourth row shifts its bytes by three byte steps. The data distribution reaches every section of the state through this method.[9]

iii. Each column within the state matrix undergoes matrix multiplication operations in Galois Field ($GF(2^8)$) to achieve the computational Mix Columns step. The encryption technique results in advanced diffusion since modifications made to any specific state area propagate throughout several bytes.[9]

iv. The state receives a fresh round key through an XOR operation which results in different transformations between rounds. [9]

(D) Final Round:

The last round duplicates the main rounds with the exclusion of Mix Columns operation in order to facilitate decryption. Round Key addition marks the process completion leading to encrypted ciphertext generation. AES accomplishes Its status as a universal encryption standard for sensitive data security through its formal transformation process that delivers robust protection and attack defense alongside excellent performance. [9]

2.3.2 Decryption:

During AES decryption the procedure works in reverse by applying the round keys that were previously used in encryption but in the opposite direction. The identical round keys from encryption enable decrypting the ciphertext to produce the original plaintext exactly. A set chain of reverse operations in the decryption procedure performs inverse transformations to undo the encryption process. An execution of the Add Round Key step is performed with the final round key during the first operation. The rows in the state matrix perform an Inverse Shift Rows movement by returning to their initial arrangement. The Inverse Sub Bytes operation performs byte replacement through the inverse S-Box to counter the encryption substitutions. The Inverse Mix Columns step applies to cases that are not the final round to recover mixed data into its pre-encryption state. The final addition of round keys through Add Round Key leads to the reformation of plaintext [10]

2.4 Elliptic Curve Cryptography (ECC)

The modern cryptographic method called Elliptic Curve Cryptography (ECC) delivers its secure functions through keys that require fewer digits than RSA cryptographic systems require. ECC establishes efficient operation by using elliptic curves over finite fields mathematics in environments with restrained power determination capabilities. The security advantages of ECC surpass RSA because it provides equivalent security using less key size (a 256-bit ECC key equals the protection level of a 3072-bit RSA key).[11]

2.4.1 How ECC Works:

ECC functions on elliptic curve structures which are defined by equations with the following form:

$$y^2=x^3+ax+b(\text{mod } p)$$

The equation selects p as a prime number together with fixed constant values a and b which construct the curve. The protection of ECC relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP) because solving this problem requires exceptional computational time which defends against attacks. [11]

(A) Key Generation:

The ECC key generation depends on scalar multiplication to create the public key using a random integer multiplying a point from the curve.[11]

1. Key generation starts with selecting an appropriate N curve E and defining G as generator point on that curve.
2. The selection of random integer d functions as the private key within this method.[11]
3. To obtain the public key Q this procedure performs scalar multiplication on the curve. [11]

$$Q=dG$$

Here, dG denotes repeated addition of the point G on the curve, which is computationally efficient but difficult to reverse, ensuring security.[11]

(B) Encryption (Elliptic Curve Diffie-Hellman - ECDH):

Although ECC is typically employed for security in the key exchange protocol because it enables two entities to build a shared encryption key across an unsecure connection.[11]

1. During public key exchange the parties independently create ECC key pairs then distribute their published keys to each other.[11]
2. The sharing of secrets proceeds by multiplying received public keys against each party's private key for creating the session key.[11]

$S=d_AQ_B=d_BQ_A=d_Ad_BG$

Since the calculations are based on scalar multiplication, both parties compute the same shared secret without directly transmitting it. This shared secret can then be used as a symmetric key for encrypting and decrypting communications.[11]

(C) Decryption:

By once the shared secret is established in Elliptic Curve Cryptography (ECC), it functions as a symmetric encryption key, enabling secure encryption and decryption of messages. Both communicating parties derive the same key independently, ensuring that only authorized users can access the encrypted information. Since this shared secret is never directly transmitted over the network, the risk of interception by attackers is significantly reduced.

This property enhances security, making ECC a robust choice for protecting sensitive data. Due to its strong security and smaller key sizes compared to traditional algorithms like RSA, ECC is widely used in SSL/TLS encryption, blockchain technology, secure messaging applications, and digital signatures**,** offering a highly efficient and scalable solution for modern cryptographic needs.[11]

3. The Need for Encryption in the Digital Age

The age of digital connectivity calls for urgent attention to sensitive data protection because secure information has become the paramount necessity. Online communication expansion combined with financial transactions growth and business operation expansion creates new cyber threats that are effectively defended using encryption as a vital cybersecurity measure. By using encryption technology companies and individuals protect their personal data and monetary records along with business information through obfuscation methods which create unrecognizable formats that need decryption key access approval. Vulnerable data often becomes the target of hackers who execute attacks through identification theft and cyber espionage and financial fraud efforts because proper encryption security measures remain unchecked. Encrypting sensitive information demands commitment from government institutions together with organizations and individuals while adopting powerful security techniques to stop unauthorized intrusion and improper usage of data. The General Data Protection Regulation (GDPR) alongside the Health Insurance Portability and Accountability Act (HIPAA) require organizations to implement encryption because it protects data according to their privacy requirements. Security experts have confirmed that encryption proves to be one of the most reliable means to fight against advanced cyberattacks and safeguard digital privacy. [12]

3.1 Proliferation of Digital Communication

Numerous digital platforms enable users to exchange personal messages while sharing their personal information with each other on a daily basis. Secure digital communications stay protected by encryption which blocks both criminals and governments and third persons from monitoring transmissions. The lack of encryption would allow attackers to intercept essential private messages plus financial data alongside personal information for destructive purposes. Communication channels which lack encryption security become prime targets for phishing attacks and man-in-the-middle tactics that result in both identity theft and financial fraud. Secure messaging software implements data encryption measures that safeguard user information no matter what security breaches occur. Digital communication growth demands organizations to implement encryption in their communication systems for protecting privacy and stopping unauthorized data access to personal information. [13]

3.1.1 Personal Communications

Corporate entities must use encrypted communication tools because cyber threats against businesses continue to grow in frequency. Websites maintain large amounts of sensitive corporate data which extends to proprietary trade data and financial details and customer-related information. Such breaches lead to financial losses and reputation death in addition to adverse legal results. Businesses can protect sensitive communication operations through encryption by using data encoding procedures that only recipients with the proper authorization can access. The protection of corporate communications against cyber threats relies on typical encryption methods including secured email encryption and encrypted cloud storage protocols together with secure file-sharing standards. Companies with

robust encryption systems achieve better outcomes in preventing cyber espionage along with insider threats and unauthorized data breaches. Businesses fighting advanced cybercrime must embed encryption as a core cybersecurity element to keep their data intact while safeguarding their most sensitive information. [14]

3.1.2 Business Communications

It's a fact that cyber threats are growing exponentially in corporate world and so, encrypted business communications are becoming very necessary. An organization also deals with an immense amount of confidential data such as trade secrets, financial records, and client information. Such a data breach can certainly lead to financial losses, reputational damage, and legal consequences. Encryption allows businesses to safely transmit sensitive data through encryption and will ensure only those people receive it who have been authorized to have access. Protecting information transmitted between companies and employees from cyber threats usually involves email encryption, encrypted cloud storage and secure file sharing protocols. However, companies that take strong steps and implement strong encryption are more capable to prevent cyber espionage, insider threats, and unauthorized data leaks. With advancing cybercrime, data integrity and protecting critical information can only be maintained through the integration of encryption into businesses' cybersecurity strategies.[13]

3.2 Rise in Cyber Threats

Cyber Modern cybersecurity depends entirely on encryption because cyber threats continue to advance in complexity. Cybercriminals take advantage of ransomware and phishing and spyware methods for unauthorized access of sensitive information with financial institutions, healthcare operations and governmental departments serving as their primary targets. The primary function of encryption is to establish defense through its capability to produce unreadable data till a valid decryption key appears. Financial operations require encryption as their primary protective measure to stop identity theft along with preventing payment details and banking credentials from falling into the wrong hands. Financial transactions stay secure with encryption protocols TLS and SSL because these protocols create difficult-to-twist protection for payment information.[15]

The major problem today involves cyber espionage because both criminal organizations and nation-sponsored actors gain access to networks in order to extract classified data which they use for disruptive activities and strategic gains. The high vulnerability of political bodies and corporate entities and research facilities exists because their information is highly classified. Conditional access by encryption protects valuable information since unauthorized users remain unable to decipher it. The combination of multi-factor authentication (MFA) and secure network protocols completes defense systems against Cyber espionage attacks. The growing geopolitical competition between nations and economic competition between nations pushes cyber warfare which makes encryption a critical protective measure for national security and personal privacy and corporate data preservation. Digital system security and worldwide interconnected trust requires that encryption be extensively adopted to stop the rapidly evolving cyber threats.[15]

3.3 Legal and Regulatory Compliance

Digital communication expansion required encryption to properly defend personal data and business and financial information against cyber dangers. The covert attempts of cybercriminals utilize superior methods of phishing alongside ransomware and spyware to infiltrate personal data illegally. Payment security depends heavily on the

encryption protocols TLS and SSL to protect financial details because these protocols defend e-commerce stores and online banking systems from fraud attacks. Cyber espionage creates substantial threats for both governments along with corporations and research institutions because attackers try to acquire confidential information. The protection of encryption makes intercepted information unreadable except when authorities use correct decryption keys which supports national security objectives.[15]

National governments together with regulatory authorities worldwide require substantial data protection through GDPR and HIPAA which establishes encryption as an essential way to secure sensitive information. Non-compliance leads to both severe financial consequences and harm to business reputation. User information protection becomes a business ethical obligation that includes deploying end-to-end encryption together with secure storage approaches and access controls designed to stop data breaches. The encryption process builds trust among customers while simultaneously reducing the chance of both identity theft and financial fraud. All organizations require encryption as their base cybersecurity standard due to constantly evolving cyber threats. The tool provides essential protection for privacy while complying with standards and ethics in current digital business practices to maintain secure confidentiality of crucial data across all industries.[15]

4. Comparative Analysis: WhatsApp, Telegram, and OpenSSL

Some well-known programs in the field of technological communication platforms, such as WhatsApp, Telegram, and OpenSSL, use cryptographic techniques to increase user security. Every platform has benefits and drawbacks that could be related to the various encryption and client safety strategies.

4.1 WhatsApp

4.1.1 Metadata Exposure: All WhatsApp messages are only encrypted in transit, and the way WhatsApp does it employs end to end encryption, so only the participants of a conversation can decrypt the message. However, none of the above is encrypted; they still keep the metadata like sender and receiver IDs, timestamps, etc. Exposure of metadata is a privacy issue since it reveals communication patterns without need for the access to content of the message. One such example would be such as analyzing metadata to draw conclusions about the behavior of users, such as who do they talk to most frequently, for when long-lived conversations do they last, and at what times are they the most active. This metadata is exploited by governments, advertisers and cybercriminals to track and monitor users, and infer sensitive personal detail. Although the message content is not present in metadata, it is valuable enough for surveillance and profiling activities. Although encrypted content, metadata analysis can still be used to predict user relationships, political affiliations, and even daily routines.[16]

4.1.2 Unencrypted Backups: The second vital security flaw in WhatsApp is its cloud backup feature. Messages are encrypted as they are sent, but can be unencrypted and stored in a non secure form on cloud storage services such as Google Drive or iCloud. That makes the cloud account a possible vulnerability as the unauthorized access to the chat histories exists. Let us consider an example, for instance, if a hacker compromises a user's cloud storage and breaches the bucket that contains the backup files, the unencrypted messages will get retrieved. While end to end encryption, protects user's communication by ensuring only the sender and recipient are able to read messages,

unencrypted backups make possible for service provider, government agency, or crims to read a user's private conversation. [17]

4.1.3 Potential Vulnerabilities: Part of the vulnerabilities in WhatsApp's security system stem from its encryption protocols as well as potential faults in software programming. The main security issue is unauthorized message monitoring through unknown system flaws and security weaknesses. A newly discovered zero-day vulnerability of WhatsApp in 2019 enabled attackers to secretly install spyware on user devices after one missed call from the attacker. This incident exposed weaknesses regarding the security measures implemented by the platform. The critics remain concerned about WhatsApp encryption security because it operates under Meta (Facebook) which has received many complaints about its user data management practices. The security risks increase because of government restrictions along with legal requirements that the service follows. Both WhatsApp users and messaging system providers must disclose information to authorized authorities within defined legal frameworks. Open backdoors found in the system would enable unauthorized entities to access WhatsApp's security measures. The security protection provided by WhatsApp encryption stands strong but users face risks because of the visible metadata combined with unsecured backups and identified system weaknesses. To ensure complete privacy users must activate backup disablement along with using strong authentication approaches and monitor potential privacy implications during platform usage.[18]

4.2 Telegram

Secret Chats on Telegram implement MTProto as their protocol by using AES-256 encryption with RSA 2048-bit key encryption and Diffie-Hellman key exchange. The Secret Chats function of Telegram provides users with two security-enhancing features including temporary-message destruction. The encryption features of Telegram only extend to Secret Chats thus making standard chat messages without end-to-end protection open to interception through unauthorized parties. Users' security is at risk because they might mistake unencrypted and encrypted communication to be equivalent. Researchers have uncovered various flaws which affect the MTProto secure communication system. A research paper found four severe issues which indicate that Telegram's encryption capabilities might be weaker than its intended standards. The protocol receives criticism from the security community because experts have fewer opportunities to examine it compared to widely tested security protocols. Inadequate thorough investigation of Telegram raises doubts about its ability to resist advanced attack methods.[19]

The cloud server-based data storage system used by Telegram creates security vulnerabilities in addition to data storage risks. The centralized storage model helps users access their data throughout all devices yet this structure makes their information vulnerable to unauthorized third parties as well as government agencies conducting surveillance operations. A review of cloud computing security documents revealed major threats that affect Telegram's cloud-based storage system particularly through data breaches and unauthorized access. Users must recognize the built-in security weaknesses of Telegram basics until they switch to Secret Chat mode for protected messaging.[20]

4.3 OpenSSL

4.3.1 Complexity: OpenSSL is a widely utilized open-source toolkit that integrates engineering and cryptography, offering a comprehensive suite of cryptographic functions. However, its command-line interface (CLI) presents a

significant barrier to entry for users lacking specialized encryption knowledge. The CLI demands familiarity with specific commands and parameters, which can be daunting for individuals not well-versed in programming or cryptographic concepts. This steep learning curve may lead to misconfigurations or improper implementations, potentially compromising security. A study analyzing OpenSSL's usability highlighted that even experienced developers can encounter challenges when navigating its complex CLI, underscoring the need for more user-friendly interfaces to enhance accessibility and reduce the likelihood of user errors.[21]

4.3.2 Key Management: A critical limitation of OpenSSL is its lack of integrated key management functionalities, such as key generation, storage, and distribution. Users are required to manage these aspects independently, which increases operational overhead and introduces potential security risks if not handled correctly. Effective key management is essential for maintaining the confidentiality and integrity of encrypted data. A comprehensive analysis of encryption key management systems emphasizes that inadequate key management can lead to vulnerabilities, as improper handling of keys may result in unauthorized access or data breaches. The absence of built-in key management in OpenSSL necessitates that users implement their own solutions or rely on third-party tools, further complicating the deployment process and potentially affecting the overall security posture.[22]

4.3.3 Security: Despite its extensive adoption, OpenSSL has experienced critical security incidents, most notably the Heartbleed vulnerability discovered in 2014. This flaw allowed attackers to exploit a buffer over-read, enabling access to sensitive data from the memory of affected systems. In the aftermath of Heartbleed, efforts were made to improve OpenSSL's code quality and reduce complexity. A study examining the impact of Heartbleed on OpenSSL revealed that the project adopted better software engineering practices, including code refactoring and increased code reviews, to enhance security and prevent similar vulnerabilities in the future. However, the incident underscores the necessity for continuous vigilance, regular updates, and proactive security measures to address potential weaknesses in widely used cryptographic libraries[23]

Table 1. Comparison Chart

Feature	WhatsApp	Telegram	OpenSSL
Messaging Encryption	Provides end-to-end encryption for messages using the open-source Signal Protocol.	Offers end-to-end encryption in "Secret Chats" using the MTProto encryption protocol.	Supports encryption and decryption of text files using symmetric (e.g., AES) and asymmetric (e.g., RSA) encryption algorithms.[24]
Encryption Protocols	Signal Protocol: Double Ratchet Algorithm, prekeys, Triple Diffie Hellman, Curve25519, AES, HMAC_SHA256.	MTProto: AES-256 encryption, RSA 2048-bit encryption, Diffie-Hellman key exchange.	Symmetric encryption (AES) and asymmetric encryption (RSA) algorithms.

Drawbacks	- Metadata such as message sender, receiver, and timestamps are accessible, compromising user privacy. - Unencrypted cloud backups pose security risks. - Concerns about potential vulnerabilities or backdoors due to Facebook's history with privacy issues.	- Default chats not end-to-end encrypted. - MTProto protocol criticism for lack of vetting compared to established protocols. - User data stored on servers poses hacking and data access risks.	- Complexity of commands requires technical understanding. - Lack of built-in key management features. - Susceptible to security vulnerabilities, requiring regular updates. Command-line interface may not be user friendly for non-technical users.

5. CipherX: A Modern Encryption Solution

5.1 Design and Integration

Users can obtain a secure encryption experience with CipherX through its Chrome extension functionality that functions independently from additional software requirements. Users can easily access secure communication with this extension because it seamlessly integrates within the Chrome browser framework. The implementation of browser extensions comes with security risks that occur when developers do not create proper secure designs. The examination of Chrome extensions security discovered that particular extensions led malicious websites to gain unauthorized access to user information. It is essential to implement strong security measures when integrating solutions similar to CipherX into system design.

5.2 User Interface and Experience

The encryption and decryption features of CipherX operate through an interface which makes the complete process effortless for users. The interface enables users from all technical backgrounds to start securing their messages without complex procedures. The usability of interfaces remains essential since complications within security tool interfaces often lead users to avoid adoption. Security applications achieve higher effectiveness rates when they demonstrate excellent usability because users tend to use tools which are easy to operate.

5.3 Key Management Features

Text encryption in CipherX uses symmetrical keys but users bear the responsibility of handling encryption key management. The management of encryption keys stands essential for protecting both the secrecy and whole integrity of protected information. Appropriate key management strategies serve as the essential base for symmetric key encryption to prevent unapproved access and protect data security according to research on encryption key methods. The system security depends on users to manage keys throughout their lifecycle starting from generation to storage and distribution.

5.4 Features of CipherX

Utilities of Chrome's broad support allows CipherX to present efficient encryption capabilities within an interface which users find easy to operate. The encryption and decryption features of the program use symmetric key cryptography to manage text operations. The encryption process becomes more efficient for users because the key functions to encrypt and decrypt messages using the same method. The keys used in CipherX need strict protection

due to possible unauthorized access that threatens communication confidentiality. Security and usability meet in the extension design which delivers operational efficiency to users in their professional and personal activities.

Chrome web browser. Here is a summary of CipherX's salient characteristics:

5.4.1 Text Encryption

Users have the ability to use CipherX to encrypt message texts by defining symmetric keys through the platform. The encryption process starts when users enter their text and choose or generate their symmetric key through the extension before applying the encryption algorithm. A person with the appropriate decryption key maintains the only possibility to read secure encoded content when it is shared. The encryption process through this method guarantees secure protection against unauthorized individuals gaining access to important data. The safety of encrypted information depends completely on key confidentiality according to studies focusing on symmetric key cryptography.

5.4.2 Text Decryption

Through its decryption mode, CipherX enables users to recover encrypted messages into plain text using the encryption key that was initially used for the process. Users submit encrypted information coupled with the correct symmetric key during this operation. The application decrypts encrypted content by extracting readable texts from it. The system maintains communication privacy through its encryption method because it requires users to provide a valid key for decryption access. The key management process requires proper implementation for symmetric key decryption because security breaches in this area can result in unauthorized entry to protected data.

6. Conclusion

An analysis of WhatsApp, Telegram, and OpenSSL reveals that many of the strategies used in today's beneficial smartphone applications are difficult to recognize and address. Even though the platforms are carefully chosen and employ advanced encryption techniques, each one contains flaws that could allow for a breach of user privacy. These incidents make it clear that more cryptographic protocols are required, as evidenced by the WhatsApp shared metadata leak, Telegram's poor default encryption, and OpenSSL's past weaknesses. This paper emphasizes the need of using clear, safe, and scientifically validated techniques to safeguard digital communication. In order to safeguard both functioning and safety in the largely networked world, our cyber security measures should also adjust to changes in threats.

References

[1] C. E. Bogos, R. Mocanu and E. Simion, "A security analysis comparison between Signal, WhatsApp and," *Cryptology {ePrint} Archive,* 2023.

[2] M. Zinkus, T. M. Jois and M. Green, "Cryptographic Confidentiality of Data on Mobile Devices," *IEEE Xplore,* 2020.

[3] S. A. Nooh, "Cloud Cryptography: User End Encryption," *2020 International Conference on Computing and Information Technology (ICCIT-1441),* 2020.

[4] B. JOVANOVIĆ, I. TOT and S. ILIĆ, "CONTEMPORARY CRYPTOGRAPHY: RECENT ACHIEVEMENT AND," *11TH INTERNATIONAL SCIENTIFIC CONFERENCE ON DEFENSIVE TECHNOLOGIES OTEH 2024,* 2024.

[5] G. S. Mamatha, N. Dimri and R. Sinha, "Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era," 2024.

[6] R. Imam, Q. M. Areeb, A. Alturki and F. Anwer, "Systematic and Critical Review of RSA Based Public Key Cryptographic

Schemes: Past and Present Status," *IEEE Access,* 2021.

[7] K. Somsuk, T. Chiawchanwattana and C. Sanemueang, "Speed up RSA's Decryption Process with Large sub Exponents using Improved CRT," *International Conference on Information Technology (InCIT),* 2018.

[8] R. Imam, Q. M. Areeb, A. Alturki and F. Anwer, "Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status," *IEEE Access,* 2021.

[9] S. Liu, Y. Li and Z. Jin, "Research on Enhanced AES Algorithm Based on Key Operations," *IEEE 5th International Conference on Civil Aviation Safety and Information Technology (ICCASIT),* 2023.

[10] W. Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education Limited, 2020.

[11] Z. Miao, "Elliptic curve cryptography: Theory, security, and applications in modern network security," *Theoretical and Natural Science,* 2024.

[12] V. Wylde, N. Rawindaran, J. Lawrence, R. Balasubramanian, E. Prakash, A. Jayal, I. Khan, C. Hewage and J. Platts, "Cybersecurity, Data Privacy and Blockchain: A Review," 2022.

[13] S. D. Sanap and V. More, "Analysis of Encryption Techniques for Secure Communication," *International Conference on Emerging Smart Computing and Informatics (ESCI),* 2021.

[14] S. K. Ghosh, S. Rana, A. Pansari, J. Hazra and S. Biswas, "Hybrid Cryptography Algorithm For Secure And Low Cost Communication," *International Conference on Computer Science, Engineering and Applications (ICCSEA),* 2020.

[15] K. I. Masud, M. R. Hasan, M. M. Hoque, U. D. Nath and M. O. Rahman, "A New Approach of Cryptography for Data Encryption and Decryption," *5th International Conference on Computing and Informatics (ICCI),* 2022.

[16] N. Rastogi and J. Hendler, "WhatsApp security and role of metadata in preserving privacy," 2017.

[17] G. T. Davies, S. Faller, K. Gellert, T. Handirk, J. Hesse, M. Horváth and T. Jager, "Security Analysis of the WhatsApp End-to-End Encrypted Backup Protocol," *Advances in Cryptology – CRYPTO 2023,* 2023.

[18] R. Khan, S. Barakat, L. AlAbduljabbar, Y. AlTayash, N. AlMussa and M. AlQattan, "WhatsApp: Cyber Security Risk Management, Governance and Control," *Fifth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU),* 2022.

[19] M. R. Albrecht, L. Mareková, K. G. Paterson and I. Stepanovs, "Four Attacks and a Proof for Telegram," 2023.

[20] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," *IEEE Access,* 2021.

[21] M. Ukrop and V. Matyas, "Why Johnny the Developer Can't Work with Public Key Certificates," *Topics in Cryptology – CT-RSA 2018,* 2018.

[22] I. Kuzminykh, M. Yevdokymenko and D. Ageyev, "Analysis of Encryption Key Management Systems: Strengths, Weaknesses, Opportunities, Threats," *IEEE International Conference on Problems of Infocommunications. Science and Technology,* 2020.

[23] J. Walden, "The Impact of a Major Security Event on an Open Source Project: The Case of OpenSSL," 2020.

[24] J. Viega, M. Messier and P. Chandra, Network security with openSSL: cryptography for secure communications, O'Reilly Media, Inc, 2002.