



Investigating the Performance of Messenger App Security for WhatsApp , Facebook and Instagram Among Indian Users

Vaibhav Mishra, Vivek Singh, Sakshi Kashyap and
Vinay Kumar Sharma

EasyChair preprints are intended for rapid
dissemination of research results and are
integrated with the rest of EasyChair.

July 9, 2023

Investigating The Performance Of Messenger App Security For WhatsApp , Facebook And Instagram Among Indian Users

Vaibhav Mishra

Student

Department of Computer Science and Engineering

Department of Masters In Computer Applications

Computer Applications

Email:vaibhav.22scse2030405@

@galgotiasuniversity.edu.in

Vivek Singh

Student

Department of Computer Science and Engineering

Department of Masters In Computer Applications

Galgotias University

Email:viveksinghkn2018@gmail.com

Sakshi

Student

Department of Computer Science and Engineering

Department of Masters In Computer Applications

Galgotias University

Email: sakshi.22scse2030234

@galgotiasuniversity.edu.in

Vinay Kumar Sharma

Professor

Department of Computer Science

and Engineering

Department of Masters In

Computer Applications

Email:-vinay.sharma@galgotiasuniversity.edu.in

Abstract—This study examines how well Indian consumers are protected by chat programmes based on whatsapp facebook and instagram to maintain the privacy and confidentiality of user data it is critical to assess the security aspects of the messenger apps that are increasingly used for personal and professional communication the study also emphasises how crucial user education and understanding of chat app security are many users may unwittingly expose themselves to hazards like identity theft and cyber assaults by sharing personal information and data on chat applications because they are ignorant of the potential risks involved the research concludes with a summary of the security issues surrounding these applications and the need for a performance-based evaluation strategy

Keywords: Feature extraction, Comparison.

INTRODUCTION

Messenger apps have become a crucial component of our personal and professional communications in the current digital age but as their use has increased worries about data privacy and security have also emerged this study examines the effectiveness of messenger app security for indian users with a focus on well-known apps like whatsapp facebook and instagram in addition to evaluating these apps

security features the study emphasises the need for user education and awareness regarding messenger app security the reports summary of the security issues with these apps and the significance of a performance-based evaluation strategy to guarantee the protection of users personal and professional data come to a conclusion

1.1 What is End-to-End Encryption

Only the sender and recipient of a message or other communication. communication may read or access its content thanks to end-to-end encryption (E2EE). End-to-end encryption makes it difficult for anybody else, including the service provider, to view or intercept the communication because the data is encrypted on the sender's device and can only be decoded by the recipient's device.

Other encryption techniques, such as transport encryption or server-side encryption, which encrypt the data only while it is in transit or kept on a server, are seen to be less safe than this sort of encryption. End-to-end encryption is frequently used in messaging apps, like WhatsApp, Facebook and Instagram, to safeguard users' privacy and prevent unauthorised access to their communications.




1.2 Other encryption standards

There are several encryption standards and protocols that are widely used in the field of information security. Here are some of the commonly known ones:

- **Standard for Advanced Encryption (AES):** The AES algorithm is a symmetric cypher is widely used for securing sensitive data. It supports 128, 192, and 256-bit key sizes and is considered secure against all known practical attacks.
- **RSA:** RSA is an asymmetric Encryption algorithm bearing the names of its creators, Ron Rivest, Adi Shamir, and Leonard Adleman. It is founded on the mathematical issue of factoring large prime numbers. RSA is widely used for secure data transmission and key exchange.
- **Diffie Hellman Key Exchange:** Diffie Hellman is a protocol for key exchange that permits two parties to establish a shared secret key over an insecure channel. It is commonly used in combination with symmetric encryption algorithms to establish a secure communication channel.
- **(ECC) Elliptic Curve Cryptography:** ECC is a family of cryptographic algorithms with public keys based on the mathematics of elliptic curves. ECC provides the same level of security as conventional asymmetric algorithms such as RSA, but with reduced key sizes, making it more suitable for environments with limited resources.
- **Transport Layer Security (TLS):** TLS is a cryptographic protocol used for securing communications over the internet. It provides encryption, data integrity, and authentication between clients and servers. TLS is commonly used to secure web traffic (HTTPS) and other network protocols.
- **Secure Sockets Layer (SSL):** SSL is the predecessor of TLS and is used for secure communication between clients and servers. However, SSL has been deprecated in favor of TLS due to security vulnerabilities in older versions of the protocol.

These are just a few examples of encryption standards and protocols used in information security. There are many more standards and algorithms, each with its own strengths, weaknesses, and areas of application.

1.3 Features Comparison

			
Cross-messaging	Yes, with Facebook Messenger	Yes, with Instagram	No
Advertising Tools	Yes	Yes	Yes
Customer Support Experience	One-on-one and public customer support	One-on-one and public customer support	One-on-one personalised experience
Third-party Chatbot Support	Yes (new feature)	Yes	Yes, with WhatsApp Business API
Content-type	Text and photos, videos, stories, IGTV, Story Highlights, Reels, Instagram Guides, Instagram Live, DMs (PDFs, Location, Quick Replies, Ice Breakers,)	Text-based posts, photos and videos, one-time notifications, message tags, sponsored messages	Text, photos, videos, catalogue, statuses, attachments (PDFs, Location), Interactive Messages
Labels	No	No	No
Privacy	No encryption	No encryption	End-to-end encryption (new feature)
Community and Engagement	No	Yes (Groups and Community Pages)	Yes (Broadcast and Group)
Native Mobile Optimisation	Yes, most users are on mobile	No, requires optimisation	Yes, most, if not all, are mobile users
Pricing	Free	Free	WhatsApp Business is Free, WhatsApp Business API has message-based pricing

2. Security

2.1 Forensics Analysis

Computer forensics, also known as digital forensics, is the gathering, analysis, and presentation of electronic evidence for the purpose of investigating and preventing digital offences. Computer forensics seeks to conduct a structured investigation and maintain a documented chain of evidence to determine precisely what occurred on a computing device and who is responsible.

In the section that follows, we will examine how effectively Instagram, WhatsApp, and Facebook conceal user data.

2.1.1 WhatsApp

Analysing WhatsApp requires specialised computer forensics tools and techniques, as well as digital forensics expertise.

To retrieve and analyse communications, forensics investigators must be aware of their storage locations. According to WhatsApp's Terms of Service, sent communications are temporarily stored on WhatsApp servers until the expiration of the recipient receives them, at which point they will be deleted. When a message is not delivered due to an inactive recipient, WhatsApp servers retain it for 30 days before erasing it. [1320]

WhatsApp offline backups are advantageous for consumers, but they are also useful for forensic investigation. The authors obtained WhatsApp database files comprising conversation session information by utilising UFED Physical Analyzer to extract the file system. Additionally, they utilised Xtract2.0 to organise these files in HTML format for easy analysis. [Tha13]

The authors discovered a vulnerability in the Android implementation of the AES cypher, allowing them to obtain the encryption key. By exploiting this vulnerability, they were able to access and view all WhatsApp-stored messages, phone numbers, and status updates.

2.1.2 Instagram

This research was effective in identifying Instagram applications that run on Android. These artefacts consist of user configurations that include account information, the number of followers, and the accounts of close acquaintances. Additionally, the chronology and message type, such as images, videos, and audio files, can be used to reconstruct the history of private and group messages exchanged between user accounts. Local storage allows the precise position of media files sent by a user to be determined. Finally, the device storage contains uploaded videos, images, and Instagram stories. According to research data, media attachments sent via direct messages are not stored locally on the device. The message column of the direct.db database contains information regarding URL addresses, the only way to access the received media message. The URL data for the link has an expiration date, which is unfortunate. Currently, no remarks or likes-related data are stored locally on the device. [1321]

2.1.3 Facebook

The fundamental building block of Facebook is a social graph, which includes items like people, images, and events as well as connections like friend connections, shared content, and photo tags. Sending HTTP calls to the Facebook Graph API can be used to obtain object properties, and all returns are JSON objects. These objects must be

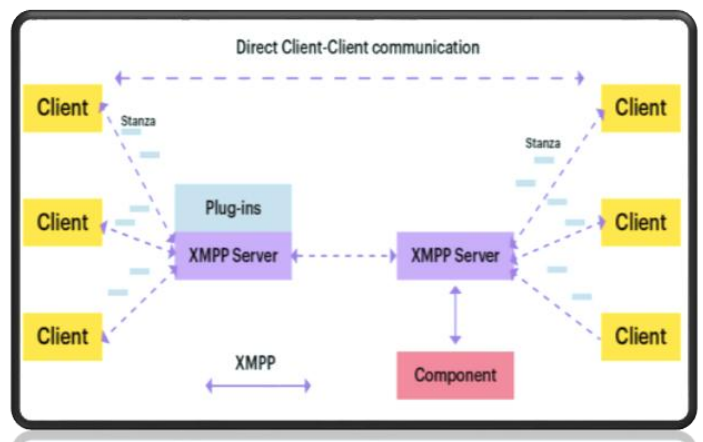
translated to HTML format with additional layout information in order to be viewed on a web browser. With the same key "text," Facebook comments and chats can be identified in JSON or HTML formats.

Additional signatures might be able to help distinguish the footprint as coming from Facebook and not another source, even though these forms may be too basic to be used by other programmes. Certainly, there is a possibility that the false negative rate of identifying footprints could increase. Furthermore, RAM or browser cache files can be examined to identify most of the valid Facebook footprints related to activities like comments, events, and chats. These footprints encompass details such as the Facebook user's profile ID, message content, and timestamps. Similar outcomes can be obtained from virtual machine image files. Moreover, data files bundled with the Facebook mobile app may contain footprints of Facebook activities. Nonetheless, it is essential to conduct further investigation to ascertain the potential involvement of the genuine account owner in the given case.

2.2 Protocol Models

2.2.1 WhatsApp

WhatsApp transmits data using the open-source, cost-free XMPP protocol. It is built on XML and enables the exchange of files, audio/video data, and text messages. Extensible Messaging and Presence Protocol (XMPP) is WhatsApp's platform's chosen messaging protocol. XMPP is an open standard for real-time communication that is used for online presence monitoring and instant chat. WhatsApp utilises an adaptation of XMPP that is designed for mobile devices and networks with limited bandwidth. The XMPP protocol is in charge of handling other functions like group chat, phone and video calls, and file sharing in addition to supporting the transmission of messages between users.



2.2.2 Facebook

We provided a formalisation of the protocol initially in AliceBob notation and then in HLPSSL. Two security issues, including a masquerade attack, have been discovered using AVISPA: an intrusion can capture cookies storing user session information and reuse them to access resources on the websites. In order to address this issue, we modified the protocol by including a message authentication mechanism that forbids an intrusive party from reusing cookies.

Finally, we have briefly discussed how this adjustment can be done in JavaScript. This method has been thoroughly confirmed using AVISPA.

We have utilised a common set variable to represent the SSL handshake and session key exchange, which is one component of our formalisation. Not all AVISPA backends currently support these variables. In fact, the AVANTSSAR project (the successor of AVISPA) has recently made some encouraging progress in order to support channels in addition to Dolev-Yao ones: in the new specification language (called HLPSSL++), it will be possible to precisely describe the security features of an SSL-like channel. As soon as the new platform is available, we want to modify our formalisations to work with it.

2.2.3 Instagram

- **Users:** Represents the individuals who use the Instagram platform.
- **Devices:** Represents the various devices through which users access Instagram, such as smartphones, tablets, and computers.
- **Instagram Servers:** Represents the backend infrastructure of Instagram, including multiple servers and data centers.
- **Instagram Mobile App:** Represents the Instagram application installed on users' mobile devices.
- **Instagram Web App:** Represents the web-based version of Instagram accessed through web browsers.
- **Instagram API:** Represents the Application Programming Interface that allows third-party developers to interact with Instagram's features and data.
- **Database:** Represents the central database that stores user profiles, posts, comments, likes, and other relevant information.
- **Authentication and Security:** Represents the authentication protocols and security measures implemented to ensure user privacy and data protection.
- **Content Delivery Network (CDN):** Represents the network of servers that cache and deliver media files, such as images and videos, to users quickly and efficiently.

2.3 Security Breaches

2.3.1 WhatsApp

- **Pegasus Spyware Attack (2019):**

In May 2019, it was discovered that Indian WhatsApp users had been the target of an attack using Pegasus, a spyware created by the Israeli business NSO Group. The spyware installed itself on targeted devices and gained access to user data by taking advantage of a flaw in WhatsApp's voice calling feature.

- **Issue with WhatsApp's Localization of Payment Data (2020):**

In October 2020, the Reserve Bank of India (RBI) looked into WhatsApp's localization and storage of payment data. WhatsApp was forced to adhere to the RBI's rules for payment service providers and store the data in India.

- **WhatsApp Privacy Policy Controversy (2021):** In January 2021, WhatsApp amended its privacy statement, raising a number of questions regarding the security of user data. The rule permitted WhatsApp to give its parent company, Facebook, certain user data. Many users looked into alternate messaging apps after the policy change drew criticism and a sizable response.

- **Sensitive records of over 280m Indian citizens exposed (2022) :**

The exposed data includes very sensitive personal information about Indian citizens, including their bank account numbers, income details, and government-issued Universal Account Numbers (UAN).

Earlier this week, two unprotected IPs hosting 'UAN'-themed Elasticsearch indexes were found. Over 280 million records were in the first cluster, while 8 million records were in the second cluster.

"Marital Status": "NEVER MARRIED",
"Nominee Gender": "MALE",
"Nominee DOB": [REDACTED],
"Gender": "MALE",
"dor": "[REDACTED]40:00Z",
"Consent Agreed": "YES",
"PermanentVsHome State Status": "NON MIGRANT",
"Guardian DOB": "1900/01/01",
"CurrentVsHome State Status": "NON MIGRANT",
"Is Active": "YES",
"Educational Qualifications": "GRADUATE",
"Father Name": [REDACTED],
"Bank Seeded Status": "NOT SEEDED",
"IFSC Code": [REDACTED],
"Disability": "NOT DISABLED OR NOT PROVIDED",
"Nominee Name": [REDACTED],
"Unicode Aadhaar Name": [REDACTED],
"Date Of Registration": "2022/01/07",
"Account Holder Name": [REDACTED],
"@timestamp": "2022-07-13T09:57:53.427971400Z",
"Guardian Name": "NOT PROVIDED",
"Occupation Name (Job Role)": "CULTIVATOR - GENERAL / FIELD CROP AN",
"4 Digits of IFSC Code": [REDACTED],
"CurrentVsPermanent State Status": "NON MIGRANT",
"Branch Name": "USUPUR",
"Guardian Address": "NOT PROVIDED",
"AdHash 256": [REDACTED],
"CurrentVsPermanent Address Pincode Status": "NON MIGRANT",
"Occupation Family": "AGRICULTURE",
"Relationship With User": "SON",
"Bank Account Number": [REDACTED],
"Social Category": "OBC",
"Aadhaar State": "TAMIL NADU",
"Income Slab": "10000 & BELOW",
"Current District": "CUDDALORE",
"Current State": "TAMIL NADU",
"Worker Status": "ORGANIZED WORKER",
"AadhaarVsPermanent Address Pincode Status": "NON MIGRANT",
"Aadhaar Name": [REDACTED],
"4 Digits of Aadhaar No": [REDACTED],
"Aadhaar DOB": "2000/08/31",
"Bank Name": "INDIAN BANK",
"Aadhaar Pin Code": [REDACTED],
"@version": "1"

5. Massive data breach discovered that affects 1.2 crore WhatsApp and 17 lakh Facebook users in India (2023):-

Cyberabad Police in this city discovered a significant data breach with implications for national security and detained Seven members of a gang suspected of obtaining and selling sensitive information from the government and other major organisations, including information on 2.55 lakh defence personnel and the private and confidential information of approximately 16.8 crore citizens, have been arrested. nationwide.

It was discovered that the accused had access to sensitive information about defence personnel, including their ranks, email addresses, locations of assignment, etc. Commissioner Raveendra stated. According to police, the data theft also included 17 lakh Facebook accounts and up to 1.2 crore WhatsApp users. Aside from Two million pupils, twelve million CBSE Class 12 students, forty million job-seekers, one and a half million car owners, information on eleven million government officials, and fifteen million IT professionals, to name a few, are included. other things, the police also discovered data.

2.3.2 Instagram

1. Instagram data breach: a Mumbai-based company divulges the personal information of social media influencers.(2019):

The data of nearly 5 billion Instagram influencers, including personalities, influencers, and brands, has been traced to Chtrbox, a social media influencer marketing agency based in Mumbai. The disclosure included both public and private user information. A cybersecurity researcher revealed the breach to TechCrunch first. The data was discovered unprotected on the AWS (Amazon Web Services) server.

2. Thousands of Instagram users' personal details exposed:(2020)

TechCrunch reported that Social Captain stored unencrypted plaintext credentials for linked Instagram accounts. A website flaw allowed anyone to view the profiles of all Social Captain users without requiring registration or Instagram credentials. According to the report, a security researcher who requested anonymity informed TechCrunch of the vulnerability and supplied a spreadsheet containing approximately 10,000 harvested user accounts. This is particularly unfortunate for affected users because not only have their Instagram passwords been compromised, but people frequently reuse passwords, which could lead to unauthorised access to additional accounts.

3.Instagram data exposure! 49 million users' private information exposed online:(2021)

- According to security researcher Anurag Sen, who discovered the breach and alerted TechCrunch, the database contained over 49 million documents that were publicly accessible online. The exposed data included users' biodata, profile pictures, the number of their followers, their city and country of residence, as well as the owner of the Instagram account's contact details like their phone number and email address.
- Anurag said that the breached database belonged to the social media marketing company Chtrbox, situated in Mumbai.

- Chtrbox stated that the database was removed offline and an investigation into the incident was initiated.

1. Data breach on Instagram, September 2, 2022

The European Union (EU) fined Instagram €405 million for allegedly processing children's data improperly. The penalties was imposed by the Irish Data Protection Commission, which oversees the EU's implementation of privacy laws. It ranks as the second-largest fine levied by the EU in accordance with the GDPR privacy rules.

2.3.3 Facebook

- **2018 Cambridge Analytica Data Scandal:** Although this was a global data breach, a sizable portion of Facebook users in India were impacted. In 2018, it came to light that Cambridge Analytica, a political consulting firm, had illegally collected the personal information of millions of Facebook users. A substantial number of Facebook users from India were among the approximately 87 million users globally whose data was exposed.

- **6 million Facebook users in India have had their personal information leaked, according to the latest news (2019):**

According to Facebook, the data breach exposed over 61 lakh Indian users' phone numbers, Facebook IDs, full names, current and past locations, birth dates, email addresses, account creation dates, relationship statuses, and biographical data.

Facebook said it discovered and corrected the vulnerability in August 2019 in response to the data breach.

According to the security researcher, a recent data breach globally impacts 533 million individuals.

The US is reported to have the largest data collection, with over 32 million user records.

The major data breach that exposed information about defence personnel also included email addresses, the most recent places of posting, and the ranks and designations of over 2.5 lakh people. The National Eligibility and Entrance Test (NEET) applications and student biographies were also included in this breach.

- **Facebook data leak: How are Indian users affected(2021):**

When the data was analysed, it was discovered that Delhi was the metropolis most severely affected, with more than 1,55,000 accounts hacked. Account information for more than 1,36,000 persons from Mumbai, more than 96,000 from Kolkata, and more than 39,000 from Chennai was also included in the hacked data.

3. Conclusion

In conclusion, when comparing the security of WhatsApp, Instagram, and Facebook among Indian users, it's important to consider their shared ownership by Facebook and the history of security breaches. While all three platforms have experienced security incidents in the past, it's worth noting that efforts have been made to improve their security measures over time.

- WhatsApp has implemented end-to-end encryption for all communications, ensuring that messages and calls remain private and inaccessible to anyone except the intended recipients. This level of encryption provides a high degree of security, making it difficult for unauthorized individuals or third parties to intercept or access user data.

- Instagram, as a photo and video sharing platform, also incorporates security measures to protect user information. However, it is worth noting that Instagram's focus on visual content sharing may pose additional challenges regarding user privacy and potential data breaches.
- Facebook, being the most widely used social media platform, has faced multiple security challenges in the past. However, it has taken steps to enhance its security infrastructure and implement measures to protect user data. These efforts include improved encryption protocols, stricter access controls, and regular security audits.
- While all three platforms have experienced security breaches, it is essential to recognize that no online platform is completely immune to potential vulnerabilities. Facebook, as the parent company, has been working to strengthen the security of all its platforms, including WhatsApp and Instagram.
- To determine which platform is better in terms of security among Indian users, it is recommended to assess individual preferences and priorities. Factors such as end-to-end encryption, privacy settings, data handling practices, and response to security incidents should be considered when making a decision. Additionally, it is crucial for users to stay informed about security updates and best practices to protect their personal information while using any online platform.

3. References

- [1320] A comparative study of WhatsApp forensics tools, [Khalid Alissa, Norah A. Almubairik, Lamyaa Alsaleem, Deema Alotaibi, Malak Aldakheel, Sarah Alqhtani, Nazar Saqib, Samiha Brahimi & Mubarak Alshahrani](#) Article number: 1320 (2019)
- [Tha13] Neha S Thakur. Forensic analysis of whatsapp on androids martphones ,2013.
- [1321] Forensic Analysis of Instagram on Android, Carolin Alisabeth and Yogha Restu Pramadi 2020
- [1081] <https://cybernews.com/news/sensitive-records-of-over-280m-indian-citizens-exposed/>
- [1082] <https://cybernews.com>
- [1083] <https://www.financialexpress.com/life/technology-massive-data-breach-targeting-1-2-crore-whatsapp-17-lakh-facebook-india-users-unearthed-details-3021310/>
- [1084] <https://www.indiatvnews.com/technology/news-instagram-data-breach-users-data-leaked-584582>
- [1085] <https://www.businesstoday.in/technology/news/story/instagram-data-breach-mumbai-based-chtrbox-leaks-private-data-of-social-media-influencers-201837-2019-05-22>
- [1086] <https://www.indiatvnews.com/technology/news-instagram-data-breach-users-data-leaked-584582>