JQCM
Journal Of Al-Qadisiyah For Computer Science And Mathematics
University Of AL-Qadisiyah

Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Instant Messaging Security: A Comprehensive Review of Behavior Patterns, Methodologies, and Security Protocols

***Ahmed R. AlMhanawi*[1]**, ***Bashar M. Nema**[*2]*

[1]Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq.
E-Mail: ahmedraai8@gmail.com
[2]Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq.
*E-Mail: bmn774@gmail.com, *Corresponding Author.*

ARTICLE INFO

Article history:
Received: 01 /02/2024
Rrevised form: 05 /03/2024
Accepted : 25 /03/2024
Available online: 30 /03/2024

Keywords:

Instant Messaging, Communication Security, End-to-End Encryption, Decentralized Authentication, Zero-Knowledge Proof, Privacy Measures, Behavioral Analysis.

Abstract:

This review presents a comprehensive analysis of contemporary scholarship pertaining to instant messaging (IM) user behavior and security protocols. Through meticulous selection, the authors highlight critical studies that illuminate optimized message consumption strategies and delve into the evolving landscape of IM security models. Focusing on the past four years, the review meticulously dissects cutting-edge advancements in this domain. A significant insight emerges: achieving optimal communication security necessitates the synergistic convergence of three fundamental techniques: end-to-end encryption for data confidentiality, decentralized authentication for independent user verification, and zero-knowledge proof for identity obscurity. The review postulates that the simultaneous integration of these elements within the application architecture is paramount for robust privacy and heightened security in the realm of IM.

https://doi.org/10.29304/jqcsm.2024.16.11440

1. Introduction

In this review, includes a detailed description of the most important research that has dealt with instant messaging applications during the past six years, as it indicates the features of instant messaging and the methods used to make instant messaging applications more secure and easy to use. The problem with the research lies in the fact that most instant messaging applications are low in security and vulnerable to hacking, in addition, the companies that own the applications can view all user information [1].

The importance of this research lies in that it proposes the use of modern methods to secure instant messages, which include the use of decentralized authentication in sending and receiving messages, the use of the zero-

Bashar M. Nema

E-Mail: bmn774@gmail.com

Communicated by 'sub etitor'

knowledge proof principle, which will be explained during the research, and the use of the Transport Layer Security (TLS) protocol, the instant messaging application to be Secure must achieve the three principles mentioned [2].

There is some research that has touched on how to make the transmission of instant messages secure, also most instant messaging applications have relied on the use of End-to-End Encryption, when the message is sent, the algorithm encrypts it directly so that it is transferred to the second party as an encrypted message. Some articles focus on analyzing the encryption protocol used by each of them, while applying the security features they provide, and through research it will give us the ability to choose a secure instant messaging service [3].

In the realm of instant messaging platforms, users encounter a plethora of options; however, not all platforms align seamlessly with users' preferences. Consequently, this investigation sought to delineate the pivotal user preferences, particularly from a security perspective, that users aspire to experience within an ideal instant messaging platform, emphasizing the amalgamation of comfort and security attributes [4].

The user wants applications that are easy to use. If there are two applications, one of which is safe but requires effort when used and the other is unsafe but does not require effort, the user will choose the site that does not require effort, Within the scope of our research endeavors, it was discerned that a prominent approach entails the development of an instant messaging platform leveraging blockchain technology integrated with machine learning algorithms. This fusion aims to reinforce confidentiality measures and ensure non-disclosure of user identities, thereby establishing a robust framework for enhanced security and privacy assurance [5].

Some researchers also used machine learning algorithms to monitor malicious activities resulting from unauthorized persons . The results of the researches that the instant messaging system applies the following steps, which are the use of decentralized authentication with Zero-Knowledge Proof technology for the purpose of not revealing identity and thus will achieving the best level of security and privacy in the proposed mobile phone application [6].

2. Instant messages:

Instant message is the exchange of near-real time between two or more users by using standalone or embedded application. Where right now more than 41 million messages are sending every minute with more than 80% of smartphone users are engagement [7].

2.1 Basic feature of Instant Messages:

provides most of these services [8]:

- Live chat or real-time chat: messages are sent and received directly between the two parties.
- Text-based communication: Text is the real mode of interaction because it allows fast writing and ease of reading.
- Presence awareness: Identifying people who are online or offline for the purpose of making contact at the appropriate time.
- Contact lists: Users organize contacts in the form of lists, which makes it easy to manage them or add them to groups.
- Private chats and group chats: The user can have private chats with one person or participate in group chats and talk to several people at the same time.
- File sharing: Files, pictures, and all types of documents can be easily exchanged.
- Sending multimedia: Instant messaging enables users to share photos, video clips, and voice messages for the purpose of enhancing communication and expressing feelings.

3. Secure Instant message

Achieve the data security by achieve CIA, which is confidentiality, integrity and availability through use *End-to-End encryption*, Attackers consider instant messaging programs to be rich in information because most users send their private information, including credit card numbers or any other personal information, via instant messaging programs. Therefore, it is necessary to use strong and modern security methods in order to protect this important information [8]. The security includes several aspects, including the use of data encryption when sending and receiving it. The encryption algorithm must also be strong and fast, so will use Base 64 algorithm, which uses upper- and lower-case letters and numbers. And some types of symbols when encoding texts, finally to create secure instant message must apply the CIA that include the End-to-End encryption with Decentralized Authentication and Zero-knowledge proof [9].

3.1 Decentralized Authentication

One of the most important security aspects is authentication, which is considered the first line of defense, but traditional (centralized) authentication mechanisms cannot provide a secure connection because they have weak points, the privacy problem, and a single point of failure. Also, distribution mechanisms fail when keys are distributed in the central structure, and therefore we cannot provide a connection. The safest solution for this solution is to use centralized authentication, which contains a set of features, including transparency and stability. When applying centralized authentication, it was found to be effective in the communication process and that it is approximately 70% superior and ten times faster than the central authentication process [10].

3.2 Zero-Knowledge proof:

Zero-Knowledge Proof (ZKP) is a protocol that allows a user to prove that they know some private and sensitive information without having to reveal that information. For example, a person can prove their identity without having to reveal it.[11].

The entire work with it will be encrypted, as if you want to add a new record to the database, it must be added encrypted, and if you want to search, it will be done within the encrypted data, and even if you have a desire to share part of the data, it must be shared while it is encrypted, meaning that zero-knowledge proof algorithms do not allow the transfer of any data. Keys or sensitive materials are not encrypted. At all times, files and keys are encrypted, and that no one can read our confidential communications, and that clients have means of communicating with each other and with the server as well. This indicates that the protection is working properly, and thus comprehensive trust is achieved without Leaking information [12].

4. Related work:

4.1. Instant messages

Christoph P., Florian B., Titilayo D. O., ‹Oluwafemi D., Urs G. and Ademola J. A., (2018) Instant messaging via mobile phone represents a huge communications phenomenon, as instant messages are sent very widely at a rate of more than 41 million messages per minute. It is used in many fields, including education, work, and others. The study examined young people’s use of instant mobile messaging to a large extent when they move around while working in the country. Other areas of life, which led to the acquisition of knowledge through people communicating with others directly or through groups in order to be aware of matters that concern them, such as work, study, etc[13].

Chih-Hung Yuan . Yenchun Jim Wu. (2020) In this study, the researchers found that instant mobile messages have a major role in students’ cooperation with others and solving the problems and difficulties they face in their studies. They proved this through a questionnaire the researchers conducted for 328 students in 6 different classrooms in a Chinese city. Most studies prefer using learning. Collaborative work conducted through temporary teams is conducting a study on a field. Researchers recommend that more attention be paid to learning resulting from groups based on the use of instant mobile messages.[14].

K. Paerata (2023) This research deals with the use of instant messages during the emergence of the Corona pandemic (COVID-19), due to the restrictions imposed for the purpose of achieving social distancing, as employees began working at home and communicating via instant messages instead of working in their departments and communicating face to face. The study also made a comparison between the use of instant messages for two years before COVID-19 and for two years After COVID-19, I concluded that in the two years after the COVID-19 people’s use of instant messages increased greatly and they began to use them in all their work and orientations [15].

N. S. Ahmad, S. Bahri, A. Fauzi (2023) Instant messaging applications are widely used in Malaysia, such as Telegram and WhatsApp for the purpose of communication and participation in decision-making. Most previous research on mobile instant messaging (MIM) focused on use and did not take into account the rest of the features. Also, this study was conducted on the use of MIM in managing. Working in a primary school, interviews were conducted with parents and teachers. The study found that the use of MIM expands the user's personal power and ability to make decisions in this institution. The analysis concluded that instant messaging has many advantages, including building relationships, personal control, and expanding the scope of knowledge [16].

4.2. Secure instant message:

Thomas P., and Hans-Joachim H., **(2016**) the researcher find that the users most often prefer instant messenger to be convenient in using and they prefers security but they don't want the security to be need effort from user for example if the user have to choose between two type of messengers the first secure but need effort and the second not secure but it's convenient the user will choose the convenient messenger although it's not secure [17].

Haibo Yi. (2019) In this research the proposed technologies are using block chain algorithms and machine learning. It is also known that the best thing is to use encryption when instant messaging, in addition to the blockchain algorithms, will include encryption. The proposed method uses machine learning algorithms to monitor instant messaging activity on the blockchain for the purpose of detecting anomalies. This system was designed on Linux platforms and the result showed that the instant messaging system is secure and can be applied to many instant messaging applications [18].

Anatoly K. and Sergey Z. (2020) The research indicates that there are major challenges in information security and suggests the use of blockchain technology in instant messages and transactions, as well as the application of modern security methods, including the use of mixed network technology and ring signature technology in order to achieve privacy. This article also discusses methods of proving zero knowledge for blockchain networks, and the idea is to use algorithms. Blockchain (decentralization) is for messages to be authenticated without the need for a third party. The use of blockchain algorithms represents the use of decentralized authentication technology[19].

R. M. Ali and S. N. Alsaad (2020): In this research, it is explained how to create a secure application for instant messaging, which uses modern encryption methods for the purpose of providing security and privacy to the users of this application, where encryption is fully implemented between the two communicating parties, taking into account the specifications of the mobile devices used by both parties. The application proposed in this research also provides many tasks, including creating a user profile, as well as allowing users to access and search for the purpose of finding friends [20].

Corina-Elena B., Razvan M. and Emil S. (2023) This research paper evaluates an analytical comparison between three of the most popular instant messaging applications, namely Signal, WhatsApp and Telegram. The comparison will also be made based on several aspects, including the encryption protocols used, and this research paper discusses the security features used for each application, and the work focused on how data is passed and packets sent from one party to another are analyzed, and the result of the research will enable the user to choose a secure instant messaging application, After comparing the three applications, it was found that Signal has the strongest security features, as it uses the Signal protocol, which is considered one of the strongest and most secure protocols, and one of its features is verifying the identity of users. As for the WhatsApp application, it uses encryption, but the protocol used is less proof of encryption, and WhatsApp contains many users, so it is more vulnerable to attack [21].

Table 1 - summary of related work:

#	Author Name	Year	Domain research	Methods & Results
1	Christoph P., Florian B., Titilayo D. O, Oluwafemi D., Urs G. and Ademola J. A. [13]	2018	IM	The study examined young people's use of mobile instant messages for work and other areas of life.[13]. The study found that using mobile instant messages acquires knowledge through people communicating directly with others in

				order to be aware of matters that interest them, such as work and study.[13].
2	Chih-Hung Yuan ,Yenchun Jim Wu [14]	2020	IM	The researchers conducted a questionnaire on 328 students in 6 different classrooms in one of the Chinese cities. [14]. The study found that mobile instant messages play a major role in the students' cooperation with others and solving the problems and difficulties they face.[14].
3	K. Paerata [15]	2023	IM	Compare between use instant messages before and after Corona pandemic (COVID-19). [15]. The study found that the use of mobile instant messages during the time of the Corona virus solved many problems, and it also increased significantly after the Corona virus [15].
4	N. S. Ahmad, S. Bahri, A. Fauzi [16]	2023	IM	The study found that the use of MIM expands the user's personal power and ability to make decisions in this institution [16].
5	T. Paul, Hans-Joachim Hof [17]	2016	Secure IM	The study found that which is security properties the user wants at instant messengers[17].
6	Haibo Yi. [18]	2019	Secure IM	The method uses machine learning algorithms to monitor instant messaging activity on the blockchain for the purpose of detecting anomalies. [18]. The result showed that the instant messaging system is secure and can be applied to many instant messaging applications
7	Anatoly K., Sergey Z [19]	2020	Secure IM	Use algorithms Blockchain (decentralization) for messages to be authenticated without the need for a third party [19]. It results in a secure instant messaging system [19].
8	R M Ali1, S N Alsaad [20]	2020	Secure IM	Use modern encryption methods in an instant messaging application [20]. As a result of the research, we obtain the security of messages when they are selected, as they are fully encrypted [20].
9	Corina-Elena B., Razvan M. and Emil S. [21]	2023	Secure IM	This research paper evaluates an analytical comparison between three of the most popular instant messaging applications, namely Signal, WhatsApp and Telegram [21]. The result of the research found that Signal has the strongest security features, as it uses the Signal protocol, which is considered one of the strongest [21].

5. Security Protocols:

There is a lot of sensitive information that is exchanged on the Internet every day, and it is possible for this information to be hacked by unauthorized people. To address this problem, protocols have been developed called security protocols, which are a set of rules that guarantee the confidentiality of data and help prevent the unauthorized person from accessing the data. Access to information [22].

The most important security protocols used to secure instant message and secure digital communications are: Secure Socket Layer (SSL), Transport Layer Security (TLS), Internet Protocol Security (IPSEC), Hypertext Transfer Protocol Secure. And Secure Simple Mail Transfer Protocol (SMTPs) [22].

Transport Layer Security (TLS): It is one of the best types of protocols used to secure communications over the Internet. It is suitable for use with decentralized authentication in instant messaging applications because it is used to create a secure link between two systems and encode data during transmission [22].

We conclude that these security protocols have a vital role in securing digital communications by transmitting instant messages in an encrypted manner. Therefore, we must use with them the central authentication method that was explained during the research, in addition to proving zero knowledge. The research concludes that combining these factors will achieve a secure communication that guarantees confidentiality. and the integrity and validity of the transmitted data, providing a secure environment for exchanging information [22].

6. Discussion and Recommendations:

The research on instant messaging and secure instant messaging presented in this literature review highlights the growing importance of these communication tools in various aspects of modern life. The studies discussed the widespread use of instant messaging for personal communication, collaboration, and even work-related tasks. However, the inherent security concerns associated with instant messaging have prompted researchers to explore alternative approaches for secure and private communication. We find that the following point very important in the process of designing and implementation of any Instant Messaging applications:

- Instant messaging applications have become ubiquitous, providing a convenient and accessible platform for communication.
- The emergence of the COVID-19 pandemic has further accelerated the adoption of instant messaging for remote work and social interactions.
- While instant messaging offers numerous benefits, concerns regarding security and privacy have led to the development of secure instant messaging applications.
- Blockchain technology and machine learning algorithms hold promise for enhancing the security and privacy of instant messaging.
- The balance between convenience and security remains a key challenge in the development of secure instant messaging solutions.
- Integrating explainable AI techniques into secure instant messaging applications can enhance user trust and understanding of the underlying security mechanisms.

References

[1] M. Iturralde. CI: A New Encryption Mechanism for Instant Messaging in Mobile Devices. Procedia Computer Science, Vol. 63,(2015). P 533 – 535.

[2] I. Makhdoom, M. Abolhasan, and J. Lipman. A comprehensive survey of covert communication techniques, limitations and future challenges. Computers & Security. Vol 120, September 2022.

[3] S. Bojjagania, D.R. Denslin Brabinb, P.V. Venkateswara Rao. PhishPreventer: A Secure Authentication Protocol for Prevention of Phishing Attacks in Mobile Environment with Formal Verification. Procedia Computer Science, 2020 P 171.

[4] I. Sukhodolskiy, S. Zapechnikov. Analysis of Secure Protocols and authentication methods for messaging. Procedia Computer Science, Vol 169, (2020). P407-409.

[5] G. S. Gaba , M. Hedabou , P. Kumar , An Braeken , M. Liyanage and M. Alazab. Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare. Sustainable Cities and Society, (2022). Vol 80.

[6] J. Wei , X. Chen , J. Wang , Willy Susilo and Ilsun You. Towards secure asynchronous messaging with forward secrecy and mutual authentication. Information Sciences Vol 626, (2023). P 114-116.

[7] M. Franco , O. Gaggi , B. Guidi , A. Michienzi and C. E. Palazzi. A decentralised messaging system robust against the unauthorised forwarding of private content. Future Generation Computer Systems. Volume 145, (August 2023) P 211-212..

[8] Kunpeng Liu, Chenfei Wang and Xiaotong Zhou. Decentralizing access control system for data sharing in smart grid. High-Confidence Computing. Volume 3, June (2023).

[9] D. E. Majdoubi , H. E. Bakkali , M. Bensaih and S. Sadki. A Decentralized Trust Establishment Protocol for Smart IoT Systems. Internet of Things. Volume 20, November (2022).

[10] M. T. HAMMI, P. BELLOT and A. SERHROUCHNI. BCTrust: A decentralized authentication blockchain-based mechanism. IEEE Wireless Communications and Networking Conference (WCNC). (2018)

[11] M. Kara, Hisham R.J. Merzeh , M. A. Aydın and H. H. Balık. VoIPChain: A decentralized identity authentication in Voice over IP using Blockchain. Computer Communications. Volume 198, January (2023) Pages 247-249.
[12] X. Yang and Wenjie Li. A zero-knowledge-proof-based digital identity management scheme in blockchain. Computers & Security. Vol 99. (2020).
[13] Christoph P. Florian B. Titilayo D. ‹Deborah O. Gröhbiel U, and Ajuwon A. Instant messaging and nursing students' clinical learning experience. Nurse Education Today**.** May (2018). Vol 64, P 119-121.
[14] Chih-Hung Yuan and Yenchun Jim Wu. Mobile instant messaging or face-to-face? Group interactions in cooperative simulations. Computers in Human Behavior. Vol 113. (2020) P1-9.
[15] K. Paerata. The use of workplace instant messaging since COVID-19. Telematics and Informatics Reports. (2023) Vol 10..
[16] N. S. Ahmad, S. Bahri, A. Fauzi. Does Mobile Instant Messaging (MIM) affect power redistribution? Evidence from a Malaysian school management organization. Social Sciences & Humanities. (2023). P 1-3.
[17] Thomas P., and Hans-Joachim H. An Empirical Survey on how Much Security and Privacy Customers Want in Instant Messengers. The Tenth International Conference on Emerging Security Information, Systems and Technologies. P 89. 2016.
[18] Haibo Yi. Securing instant messaging based on blockchain with machine learning. Safety Science. Volume 120, Pages 6-13, December 2019.
[19] A. Konkin, S. Zapechnikov. Privacy methods and zero-knowledge poof for corporate blockchain. Procedia Computer Science 190, (2021). P 471–472.
[20] R. M. Ali and S. N. Alsaad. Instant messaging security and privacy secure instant messenger design. 3rd International Conference on Sustainable Engineering Techniques ICSET. (2020). P 1-3.
[21] Corina-Elena B., Razvan M. and Emil S. A security analysis comparison between Signal, WhatsApp and Telegram. IACR Cryptology ePrint. January, (2023). P 1-4.
[22] Sabina Szymoniak. Security protocols analysis including various time parameters. Security protocols analysis including various time parameters. Vol 18(2). (2021). p1136–1153.