ITRC
ICT Research Institute
(Iran Telecommunication Research Center)

Journal of Information and Communication Technology

Iranian Society of Information and Communication Technology

Volume 17, Issue 66-67, Autumn and Winter 2025, pp. 87-101

Message Transfer Protocol Between Social Messengers

Hamzeh Sezavar[1], Hamed Monkaresi[1, 2*], Hassan Nikaein[3], Mehdi Mozaffari [2]

[1] Department of Computer Engineering and Information Technology, Razi University, Kermanshah, Iran
[2] Information Technology Organization of Iran, Tehran, Iran
[3] Department of Computer Engineering, Sharif University of Technology, Tehran, Iran

Received: 08 April 2025, Revised: 25 September 2025, Accepted: 27 September 2025
Paper type: Research

Abstract

The proliferation of social networking platforms has fundamentally transformed the way we communicate. The sheer number of these networks and the diversity of services they offer have led individuals to register on one or more platforms according to their personal preferences. However, this dispersion has made it difficult to interact with users of other social networks, forcing individuals to maintain accounts on multiple services merely to preserve connections with different social circles. This paper introduces a web-based protocol designed to enable seamless, unified message exchange across heterogeneous social networks, thereby eliminating the need for users to juggle multiple messaging applications. The proposed system supports both channels and groups and fosters interoperability among disparate platforms. European Union legislation governing social networks with over 45 million monthly users underscores the urgent need for such a solution to facilitate cross-platform messaging. As a few global networks have grown so dominant that they effectively stifle competition, our approach offers a means for emerging social platforms to compete on a level playing field, ultimately enhancing user experience while safeguarding privacy. In this study, the protocol was ultimately implemented across five popular messaging platforms in Iran, which collectively boast over 40 million monthly active users. Within less than three months of implementation, more than 1.5 million users had established communication with one another through different messaging applications using this protocol.

Keywords: Message Exchange Protocol, Interoperability, Social Messengers, Security, Privacy.

* Corresponding Author's email: h.monkaresi@razi.ac.ir

دوفصلنامه
فناوری اطلاعات و ارتباطات ایران

سال هفدهم، شماره‌های ۶۶ و ۶۷، پاییز و زمستان ۱۴۰۴، صفحه ۸۷ الی ۱۰۱

ارائه‌ی یک پروتکل تبادل پیام بین پیام‌رسان‌های اجتماعی

حمزه سزاوار[۱]، حامد منکرسی[۱،۲*]، حسن نیک آیین[۳]، مهدی مظفری[۲]

[۱] گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه رازی، کرمانشاه، ایران

[۲] سازمان فناوری اطلاعات ایران، تهران، ایران

[۳] گروه مهندس کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران

تاریخ دریافت: ۱۴۰۴/۰۱/۱۹ تاریخ بازبینی: ۱۴۰۴/۰۷/۰۳ تاریخ پذیرش: ۱۴۰۴/۰۷/۰۵

نوع مقاله: پژوهشی

چکیده

گسترش شبکه‌های اجتماعی، منجر به یک تحول اساسی در ارتباطات شده‌است .فراوانی این شبکه‌ها و تنوع سرویس‌هایی که به کاربران خود ارائه می‌هند، باعث شده تا اشخاص مطابق سلیقه و صلاحدید خود، در یک یا چند مورد از آن‌ها ثبت‌نام کنند؛ همین موضوع سبب شده تا ارتباط با اشخاصی که از شبکه‌های اجتماعی دیگری استفاده می‌کنند مشکل شود و جهت حفظ ارتباط با گروه‌های مختلف، کاربران را ملزم به ثبت‌نام در چندین پلتفرم، کرده‌است. این تحقیق، یک پروتکل مبتنی‌بر وب را معرفی می‌کند که باهدف تسهیل تبادل پیام یکپارچه بین شبکه‌های اجتماعی متفاوت، طراحی شده‌است و درنتیجه نیاز کاربران به نگه‌داری چندین پیام‌رسان را از بین می‌برد .این سیستم پیشنهادی، از کانال‌ها و گروه‌ها پیشتیبانی می‌کند و درعین‌حال، قابلیت همکاری بین شبکه‌های اجتماعی مختلف را ممکن می‌سازد. قانون اتحادیه‌اروپا، بر ضرورت چنین راه‌حلی برای شبکه‌های اجتماعی با بیش از ماهانه ۴۵ میلیون کاربر، جهت پشتیبانی از ارتباطات بین پیام‌رسانی، تاکید می‌کند؛ چرا که درحال‌حاضر، برخی از شبکه‌های اجتماعی جهانی، به حدی گسترش یافته‌اند که عملاً امکان رقابت در این حوزه را از بین برده‌اند. این تحقیق یک راه حل مناسب برای محدودیت‌های فعلی قابلیت همکاری شبکه‌های اجتماعی، بهبود تجربه کاربری و حفظ حریم خصوصی ارائه می‌دهد. پروتکل معرفی شده در این مقاله در نهایت توسط ۵ پیام رسان محبوب در ایران که در مجموع بیش از ۴۰ میلیون کاربر فعال ماهانه دارند پیاده سازی شده و در کمتر از ۳ ماه پس از پیاده‌سازی، بیش از ۱،۵ میلیون کاربر با استفاده از این پروتکل از طریق پیام‌رسان‌های متفاوت با یکدیگر ارتباط برقرار کرده‌اند.

کلیدواژگان: تبادل پیام بین شبکه‌های اجتماعی، قابلیت همکاری، پیام‌رسان اجتماعی، امنیت، حریم خصوصی.

* رایانامهٔ نویسنده مسؤول: h.monkaresi@razi.ac.ir

۱- مقدمه

انسان‌ها همواره به‌دنبال راه‌حل‌هایی برای ارتباط و انتقال پیام به یک‌دیگر هستند و در جهت افزایش فراوانی، دردسترس بودن وکاهش هزینه و... این راه‌های ارتباطی می‌کوشند. اینترنت و دنیای دیجیتال، تحولی عظیم در زمینه ارتباط و انتقال پیام ایجاد کرد و با ظهور شبکه‌های اجتماعی، این تحول به اوج خود رسید. شبکه‌های اجتماعی، یکی از پرمخاطب‌ترین سرویس‌های اینترنتی به‌شمار می‌روند. امروزه شبکه‌های اجتماعی، در ذهن ما، به اولین راه ارتباطی با دوستان ، آشنایان ، همکاران و... تبدیل شده‌است.

تا ماه جولای ۲۰۲۳، حدود ۵,۱۹ میلیارد کاربر اینترنت در سراسر جهان وجودداشت که ۶۴,۶ درصد از جمعیت جهان را تشکیل می‌داد[۱]. تا سال ۲۰۲۳، حدود ۴,۹ میلیارد نفر (۶۰ درصد از جمعیت جهان)، در سراسر جهان از رسانه‌های اجتماعی استفاده می‌کنند. انتظار می‌رود تعداد کاربران رسانه‌های اجتماعی در سراسر جهان تا سال ۲۰۲۷، به ۵,۸۵ میلیارد کاربر افزایش یابد[۲]. کاربران به‌طور متوسط، هر ماه در شش تا هفت پلتفرم فعال هستند[۳]. پرکاربردترین پلتفرم رسانه اجتماعی در جهان، فیس‌بوک با ۲,۹ میلیارد کاربر فعال ماهانه است[۳][۴].

امروزه برخی از شبکه‌های اجتماعیِ خاص، رشد بسیاری کرده‌اند و به غول‌هایی در این حوزه تبدیل شده‌اند؛ این شبکه‌های اجتماعی، با توجه به اینکه دارای منابع و سرورهای بسیار قدرتمندی هستند، عملاً امکان رقابت در این حوزه را از بین برده‌اند، حتی اگر یک شبکه اجتماعی جدیدی ایجاد شود که امکانات بیشتری را نسبت به این شبکه‌های اجتماعی خاص ارائه دهد ، و یا امکاناتی را عرضه کند که از دید برخی از کاربران مناسب و بهتر به نظر برسد. کاربر علی‌رغم میل‌باطنی خود، به‌دلیل عدم‌حضور دیگر مخاطبین که به‌طور روزمره با آن‌ها در ارتباط است، مجبور به مهاجرت به شبکه اجتماعی می‌شود که بیشتر مخاطبین مورد نظرش در آن حضور دارند. همچنین وضعیت موجود باعث شده‌است تا مصرف پهنای‌باند اینترنت کاربران، به علت نصب پیام‌رسان‌های متعدد افزایش پیداکند و گوشی‌های هوشمند کاربران، به علت نصب پیام‌رسان‌های متعدد، (افزایش سرویس‌های پس‌زمینه و مصرف حافظه اصلی و کاهش عمر باتری) کند شوند. این مسائل به یک چالش در اتحادیه‌اروپا تبدیل شده‌است. شورای قانون‌گذاری اتحادیه‌اروپا، برای بهبود این شرایط، با تصویب یک قانون، شبکه‌های اجتماعی را که ماهانه دارای بیش از ۴۵ میلیون استفاده‌کننده هستند، ملزم به ایجاد زمینه ارتباط و انتقال و دریافت پیام با سایر شبکه‌های اجتماعی کرده‌است[۶][۷].

در این پژوهش، یک پروتکل تبادل پیام بین شبکه‌های اجتماعی مبتنی‌بر وب را ارائه می‌گردد که می‌تواند با فراهم کردن امکان تبادل پیام بین پیام‌رسان‌های مختلف زمینه رقابت و رشد پیام‌رسان‌های نوظهور را فراهم آورد و همچنین وضعیت موجود و تجربه کاربری کاربران شبکه‌های اجتماعی استفاده‌کننده از راه‌حل پیشنهادی را ، بهبود بخشد.

۲- پیشینه پژوهش

در این بخش، به بررسی تحقیقات و طرح‌های پیشین دیگر پژوهشگران در زمینه انتقال پیام پرداخته می‌شود.

ری فلین[۸] در این گزارش رسمی که توسط شرکت اوپن‌مایند[1] منتشر شده‌است، طرحی را برای ایجاد یک هاب [2] RCS، معرفی کرده‌است. در RCS، هر اپراتور باید از طریق I-SBC[3] توسط یک ارتباط [4] NNI به اپراتور دیگر وصل‌شود.

هاب‌های RCS به‌طور ایده‌آل می‌توانند با ارائه دروازه‌های WebRTC[5] برای توسعه دسترسی RCS به VoIP[6] و ویدیو برای مرورگرهای وب استفاده‌شوند. درنهایت، رابط‌های مرکز پیام کوتاه[7] و مرکز سرویس پیام چندرسانه‌ای[8] در هاب RCS، امکان ارتباط متقابل با سرویس پیام‌کوتاه و سرویس پیام چندرسانه‌ای را فراهم می‌کنند.

پروتکل ماتریکس [۹]،یک استاندارد باز برای ارتباط متقابل، غیرمتمرکز و بلادرنگ از طریق IP است. از این پروتکل می‌توان برای تقویت پیام‌رسانی فوری، VoIP/WebRTC، ارتباطات اینترنت اشیا و یا هرجایی که به یک واسط برنامه‌نویسی کاربردی (API[9]) استاندارد HTTP[10] برای انتشار و اشتراک داده‌ها نیاز است، بهره برد. پروتکل ماتریکس، استانداردی را تعریف می‌کند و و در ادامه امکاناتی همچون پیاده‌سازی منبع باز سرورهای سازگار با پروتکل ماتریکس،

[1] openmind
[2] Rich Communication Services
[3] Interconnect Session Border Controller
[4] Network-Network Interface
[5] Web Real-Time Communication
[6] Voice over IP
[7] Short Message service center
[8] Multimedia Messaging Service center
[9] Application Programming Interface
[10] Hypertext Transfer Protocol

بسته توسعه نرم افزار سمت کاربر[1] و خدمات کاربردی[2] را به‌منظور کمک به ایجاد راه‌حل‌های ارتباطی جدید و یا گسترش قابلیت‌ها و دسترسی به راه‌حل‌های موجود، ارائه می‌دهد. هدف اولیه ماتریس، رفع مشکل پراکنده ارتباطات IP است، به بیان ساده‌تر، اجازه دادن به کاربران برای پیام دادن و تماس با یکدیگر بدون توجه به اینکه کاربر دیگر در چه برنامه‌ای حضور دارد.

جولیان اسپاربر[۱۰] یک سیستم پیشنهادی از نرم افزار Matrix را برای انتقال پیام بین کاربران مورداستفاده قرار می‌دهد و رمزگذاری پیام را از طریق قرارداد هوشمند و زنجیره بلوکی اتریوم پیاده‌سازی می‌کند. در این طرح، سیستم ایجاد شده از یک شبکه اتریوم برای ذخیره کلیدهای عمومی و خصوصی استفاده می‌کند. به طور خاص، کلیدها با استفاده از فناوری هسته OpenEthereum به نام Secret Store ذخیره می‌شوند. به کمک قرارداد هوشمندی که به عنوان قرارداد مجوز استفاده می‌شود، سیستم با یک فرآیند کنترل دسترسی پیشرفته، امکان دسترسی‌دادن یا لغو دسترسی به یک پیام را فراهم می‌کند. Secret Store از تعدادی گره اتریوم تشکیل شده‌است. در این طرح، هر کاربری که می‌خواهد از این سیستم رمزگذاری سرتاسری استفاده‌کند، نیازمند دسترسی به گره OpenEthereum است و برای این‌کار باید یک حساب اتریوم ایجاد کند.

بررسی نقاط و ضعف طرح‌های پیشین:

- پروتکل RCS:
  - نقاط قوت: امکان تعامل‌پذیری بین اپراتورها و ارائه خدمات اضافی مانند WebRTC.
  - نقاط ضعف: وابستگی شدید به اپراتورهای متمرکز و عدم ارائه معماری کاملاً غیرمتمرکز.
- پروتکل ماتریکس:
  - نقاط قوت: طراحی غیرمتمرکز، استاندارد باز و قابلیت استفاده در حوزه‌های مختلف (پیام‌رسانی، VoIP، IoT).
  - نقاط ضعف: چالش‌هایی در مقیاس‌پذیری در برخی موارد استفاده خاص.
- سیستم جولیان اسپاربر (رمزگذاری مبتنی بر زنجیره بلوکی):
  - نقاط قوت: استفاده از فناوری زنجیره بلوکی برای ذخیره کلیدهای رمزنگاری و پیاده‌سازی فرآیندهای پیشرفته دسترسی.
  - نقاط ضعف: وابستگی به حساب اتریوم و شبکه‌های زنجیره بلوکی که ممکن است منجر به افزایش هزینه‌ها یا محدودیت‌های مقیاس‌پذیری شود

جدول ۱ به بررسی و مقایسه استانداردهای موجود در حوزه تبادل پیام و مقایسه با پروتکل پیشنهادی را نشان می‌دهد.

۳- قانون بازارهای دیجیتال اتحادیه اروپا

قانون بازارهای دیجیتال (DMA)[۱۱]، یکی از قوانین اتحادیه اروپا است که هدف آن عادلانه‌تر کردن اقتصاد دیجیتال و رقابت‌پذیرتر کردن شرایط است. این قانون در ۱ نوامبر ۲۰۲۲ لازم الاجرا شد و در بیشتر موارد در ۲ مه ۲۰۲۳ به مرحله اجرا رسید[۱۲][۱۳]. هدف DMA، تضمین درجه بالاتری از رقابت در بازارهای دیجیتال اروپا، ازطریق جلوگیری از سوءاستفاده شرکت‌های بزرگ از قدرت خود در بازار و اجازه‌دادن به بازیگران جدید برای ورود به بازار است[۱۴]. این قانون، بزرگترین پلتفرم‌های دیجیتال فعال در اتحادیه اروپا را مورد هدف قرار می‌دهد. پلتفرم‌ها به دلیل موقعیت پایداری که در برخی از بخش‌های دیجیتال بازار دارند و به دلیل دارا بودن معیارهای خاص مربوط به تعداد کاربران، گردش مالی آنها یا سرمایه‌گذاری، به عنوان دروازه‌بان[3] شناخته می‌شوند [۱۵][۱۶][۱۷].

جدول ۱. بررسی استانداردهای موجود در حوزه تبادل پیام و مقایسه با پروتکل پیشنهادی

ویژگی/استاندارد	XMPP	SIP	Signal	Matrix	پروتکل پیشنهادی
رمزنگاری سرتاسری	اختیاری	ندارد	دارد	دارد	بهبود یافته (AES-256-GCM + RSA-4096)
معماری	متمرکز	متمرکز	نیمه-متمرکز	غیرمتمرکز	هیبرید (متمرکز برای تبادل، غیرمتمرکز برای احراز هویت)
پشتیبانی از چندرسانه‌ای	محدود	کامل	محدود	کامل	کامل + بهینه‌سازی ترافیک
تایید هویت دوطرفه	دارد	ندارد	دارد	دارد	دارد(هویت پیام رسان دیگر تایید می شود.)
تحمل خطا	متوسط	بالا	پایین	متوسط	متوسط

[1] Client Software Development Kit

[2] Application Services

[3] Gatekeepers

بیست و دو سرویس در شش شرکت (که دروازه‌بان تلقی می‌شوند) آلفابت، آمازون، اپل، بایت‌دنس، متا و مایکروسافت در سپتامبر ۲۰۲۳ توسط اتحادیه اروپا به عنوان سرویس پلتفرم‌های اصلی[1] شناسایی شدند[۱۸]. این شرکت‌ها تا ۶ مارس ۲۰۲۴ فرصت داشتند تا از تمام بندهای این قانون، پیروی کنند[۱۹]. یکی از بندهای این قانون، شامل ممنوعیت ترکیب داده‌های جمع‌آوری‌شده از دو سرویس مختلف متعلق به یک شرکت است (به عنوان مثال، در مورد متا، شبکه اجتماعی فیس‌بوک و پلتفرم ارتباطی آن WhatsApp مجاز به استفاده از داده‌های یکدیگر نیستند.)؛ [۲۰] در این قانون، مقرراتی برای حفاظت از تجارت پلتفرم‌های کاربران (از جمله تبلیغ‌کنندگان و ناشران) وجود دارد؛ این قانون در برابر روش‌های خودترجیحیِ پلتفرم‌ها برای تبلیغ محصولاتشان (مانند نتایج ترجیحی برای محصولات یا خدمات Google هنگام استفاده از موتور جستجوی Google) قرار دارد[۲۱]. مقررات مربوط به شیوه‌های بسته‌بندی و مقرراتی برای اطمینان از قابلیت همکاری، قابلیت دسترسی و انتقال داده برای مشاغل و کاربران نهایی پلتفرم‌ها[۶]، بخش‌های دیگر این قانون هستند. عدم رعایت این قوانین، می‌تواند منجر به جریمه تا ۱۰ درصد گردش مالی جهانی شرکت شود[۱۶][۱۷].

۴- وضعیت کنونی پیام‌رسان‌های جهانی

در این بخش، به بررسی آخرین وضعیت پیام‌رسان‌های بزرگ جهانی که مشمول قانون بازارهای دیجیتال اتحادیه اروپا می‌شوند خواهیم پرداخت. جدول ۲ آخرین وضعیت هر پیام‌رسان را در پیاده‌سازی قابلیت ارسال و دریافت پیام بین پیام‌رسانی نمایش می‌دهد.

جدول ۲. وضع پیاده‌سازی قابلیت ارسال و دریافت پیام بین پیام‌رسانی

پلتفرم‌های پیام‌رسان	قابلیت ارسال و دریافت پیام بین پیام رسانی
WhatsApp	تا حدی پیاده‌سازی شده‌است. ارسال و دریافت پیام کاربر به کاربر در پلتفرم‌های دیگر (به عنوان مثال، اینستاگرام، مسنجر) در اکوسیستم متا پشتیبانی شده‌است[۲۲][۲۳].
Messenger	تا حدی پیاده‌سازی شده است. مشابه واتس‌اپ، امکان ارسال و دریافت پیام کاربر به کاربر، در سایر پلتفرم‌های متا فراهم شده‌است[۲۲][۲۳].
Instagram	تا حدی پیاده‌سازی شده‌است. امکان ارسال و دریافت پیام کاربر به کاربر در سایر پلتفرم‌های متا فراهم شده‌است[۲۲][۲۳].
Signal	در حال پیاده‌سازی[۲۴][۲۵]
Telegram	در حال پیاده‌سازی[۲۶][۲۷]
Threema	در حال پیاده‌سازی[۲۸]

۵- طرح پیشنهادی

این بخش به بررسی بخش‌های مختلف طرح پیشنهادی می‌پردازد.

۵-۱- موجودیت‌ها

طرح پیشنهادی، از موجودیت‌هایی تشکیل شده‌است که ابتدا به معرفی آن‌ها پرداخته خواهد شد.

۵-۱-۱- پیام‌رسان

موجودیت پیام‌رسان، برای ثبت پیام‌رسان‌های موجود و به اشتراک‌گذاشتن اطلاعات عمومی آن‌ها با سایر پیام‌رسان‌ها است. پیام‌رسان شامل فیلدهای زیر می‌باشد:

id: شناسه یکتای پیام‌رسان که توسط متپ (مرکز تبادل پیام) در هنگام ایجاد پیام‌رسان تولید می‌گردد و به آن اختصاص می‌یابد.

Name: نام پیام‌رسان که یک رشته با حداکثر ۳۲ کاراکتر است.

server_url: آدرس پایه‌ی سرور پیام‌رسان می‌باشد، که سایر آدرس‌ها بر روی این آدرس تعریف شده‌اند.

sender_url: این آدرس endpoint پیام‌رسان است که پیام‌های سایر پیام‌رسان‌ها، به این آدرس ارسال می‌گردد. این آدرس در حالتی استفاده می‌شود که پیام‌رسان نیازمند ارسال داده توسط سرور متپ باشد و در صورتی که خود پیام‌رسان از سرور متپ داده‌ها را استخراج کند، این آدرس تعریف نمی‌گردد.

receiver_url: آدرس endpoint پیام‌رسان است که پیام‌های خود برای سایر پیام‌رسان‌هارا در این آدرس ارائه می‌دهد. این آدرس در حالتی است که پیام‌رسان نیازمند دریافت داده توسط سرور متپ باشد و در صورتی که خود، به سرور متپ داده‌ها را ارسال کند، این آدرس تعریف نمی‌گردد.

public_key_url: آدرس کلید عمومی پیام‌رسان است که بایستی بر روی دامنه‌ی خودِ پیام‌رسان، میزبانی شده باشد. کلید عمومی، باید یک کلید RSA با طول ۴۰۹۶ بیت باشد که با فرمت PEM ذخیره شده‌است.

file_size_limit: حداکثر اندازه فایلی است که این پیام‌رسان قابلیت دریافت آن‌را دارد (بر اساس بایت).

secret_key: کلید امن پیام‌رسان که برای ارتباط با متپ از آن

[1] Core Platforms Services

استفاده می‌کند. این کلید با فرمت base۶۴ ذخیره شده‌است.

۵-۱-۲- کاربر

موجودیت کاربر، نماینده وجود یک کاربر در متپ می‌باشد. در صورتی که کاربر، حساب کاربری خود را در پیام‌رسان حذف نمود، پیام‌رسان نیز بایستی نسبت به حذف کاربر از متپ اقدام نماید و درصورتی که کاربر فقط نسبت به غیرفعال‌سازی متپ اقدام نمود، پیام‌رسان بایستی نسبت به غیرفعال‌سازی کاربر در متپ اقدام نموده و از پاک کردن کاربر خودداری نماید. این موجودیت دارای فیلدهای شناسه، شماره‌تلفن متعلق به حساب کاربری، شناسه پیام‌رسانِ ثبت‌کننده کاربر، نام نمایشی کاربر و تصویر نمایه کاربر است.

۵-۱-۳- پیام

از پیام، به منظور ارسال یک پیام از یک کاربر به کاربر دیگر و همچنین برای ارسال خطا /ویرایش /حذف /خوانده‌شدن و... بین سرورهای پیام‌رسان‌ها استفاده می‌گردد. پیام از فیلدهای زیر تشکیل شده‌است.

Id: یک شناسه عددی ۸ بایتی یکتای پیام که توسط متپ در هنگام ایجاد پیام تولید می‌شود.

sender_id: شناسه کاربر فرستنده پیام؛ در هر حالتی این شناسه الزاما بایستی متعلق به پیام‌رسان فرستنده باشد. در صورتی که این پیام، به یک تغییر در اطلاعات گروه/ کانال مربوط باشد، این فیلد شناسه کاربر ایجاد کننده تغییر می‌یابد.

receiver_id: شناسه کاربر /گروه /کانال گیرنده پیام است. سرویس متپ بر اساس این شناسه، پیام‌رسان گیرنده را تشخیص می‌دهد. فقط مالک/ مدیران کانال اجازه ارسال مطلب به کانال را دارند.

category: این فیلد نشان‌دهنده نوع دریافت‌کننده است. اگر خالی باشد یعنی دریافت‌کننده، یک شخص است، اگر برابر«group» باشد یعنی دریافت‌کننده یک گروه است و اگر برابر «channel» باشد، یعنی دریافت‌کننده یک کانال است.

receiver_messenger_id: در صورتی که receiver_id شناسه یک گروه/ کانال را در خود داشته باشد، این فیلد نشان‌دهنده آن است که این پیام برای کدام پیام‌رسان مقصد ایجاد و رمزنگاری شده‌است.

send_time: زمان ایجاد پیام در پیام‌رسان فرستنده است.

message_sender_uid: یک عدد حداکثر ۱۲ بایتی، که به صورت یکتا توسط پیام‌رسان فرستنده ایجاد می‌گردد. این عدد در الگوریتم AES-GCM رمزنگاری encrypted_message هم به عنوان nonce استفاده می‌گردد (نکته‌ی امنیتی: برای یک کلید رمزنگاری یکسان برای AES-GCM، هیچ‌گاه نباید دو پیام مختلف با یک nonce رمزنگاری گردند. به همین علت، یکتا بودن این فیلد برای یک گیرنده ثابت، اهمیت امنیتی دارد.). این عدد بایستی به‌ازای تمامی پیام‌های ارسالی از سمت پیام‌رسان، یکتا باشد.

Encryption_key: محتوای این فیلد، کلید ۲۵۶ بیتی برای رمزنگاری AES-GCM مورد استفاده در این پیام است. این کلید توسط کلید عمومی گیرنده (که در داده پیام‌رسان وجود دارد) رمز شده است. جهت رمزنگاری، از الگوریتم OAEP با MGF۱ و SHA۵۱۲ (برای درهم‌ساز) و بدون برچسب، برای padding استفاده می‌شود. کلید پس از رمز شدن، توسط base٦٤ کدبندی می‌شود. هر فرستنده، بایستی این کلیدرا به ازای هر receiver_id ثابت نگه دارد و فقط در مواقع ضروری و در بازه‌های یک‌ماهه اقدام به تغییر این کلید بنماید. در صورت وجود encrypted_message، این فیلد نیز بایستی وجود داشته باشد و در صورت عدم وجود فیلد encrypted_message این فیلد هم نباید وجود داشته باشد.

Encrypted_message: محتوای این فیلد شامل پیام ارسال شده از سمت فرستنده است. این محتوا توسط الگوریتم AES-GCM با nonce برابر با فیلد sender_message_uid و تگ برابر با None (یا Null) رمزگذاری و سپس با استفاده از base۶۴ کدبندی شده است. طول پیام می‌تواند حداکثر ۴۰۹۶ کاراکتر باشد. زمانی که رشته‌ی ارسالی خالی است، این فیلد باید حضور داشته و با ترتیب بالا رمزنگاری گردد. در حالاتی که ۸ بیت اول message_type برابر با 0xFF است، این فیلد نباید وجود داشته‌باشد؛ در چنین حالتی در محاسبه‌ی sign، مقدار پیام، برابر با رشته‌ی خالی در نظر گرفته‌می‌شود.

Sign: محتوای این فیلد، مقدار امضای محتوای ذیل با استفاده از کلید خصوصی فرستنده است. جهت امضا بایستی از الگوریتم PSS به همراه MGF۱ (برای mgf) و SHA۵۱۲ (برای درهم‌ساز) و با طول بیشینه (۴۴۶ بیت) برای padding استفاده گردد. در نهایت مقدار امضا با استفاده از base۶۴ کدبندی می‌شود.

```
Sign_text = messsage_sender_uid +"|"+ message +"|"+ send_time +"|"+ message_type +"|"+ sender_id +"|"+ receiver_id
```

message_type: این فیلد، مشخص‌کننده نوع پیام ارسالی است. ۸ بیت راست آن مشخص‌کننده نوع محتوا (جدول ۳) و مابقی بیت‌ها، مشخص‌کننده عملیات می‌باشند (جدول ۴).

جدول ۳. معنای ۸ بیت اول (کم ارزشترین) نوع پیام

پیام متنی	0x00
پیام دارای فایل	0x01
پیام دارای فایل تصویری	0x02
پیام دارای فایل صوتی	0x03
پیام دارای فایل ویدئویی	0x04
پیام دارای فایل گیف	0x05
پیام دارای محتوای موقعیت مکانی	0x06
پیام دارای محتوای .contact	0x07
پیام دارای فایل وویس	0x08
پیام یک پیام خطا و یا نشان‌دهنده حذف یک پیام دیگر است	0xFF

جدول ۴. معنای ۸ بیت دوم (کم ارزش‌ترین) نوع پیام

پیام جدید	0x00
پیام خوانده‌شده. امکان ارسال خوانده‌شدن پیام فقط توسط گیرنده پیام وجود دارد.	0x01
پیام ویرایش‌شده. امکان ویرایش پیام فقط توسط فرستنده پیام وجود دارد.	0x02
پیام حذف شده. از این کد برای اعلان حذف یک پیام قدیمی استفاده می‌شود. پس از حذف شدن یک پیام، امکان ارسال هیچ‌گونه به‌روزرسانی بر روی آن وجود ندارد. امکان حذف پیام فقط توسط فرستنده پیام یا مدیر/ مالک گروه/ کانال وجود دارد.	0x06
فیلد encryption_key به درستی رمز نشده‌است (در صورتی که پیام‌رسان گیرنده، تغییر کلید داشته‌باشد و فرستنده همچنان با استفاده از کلید قبلی رمزنگاری انجام دهد، رخ می‌دهد.)	0x22
فیلد encrypted_message به درستی رمز نشده‌است.	0x26
امضا به درستی انجام نشده‌است.	0x2A
در سایر فیلدها عدم‌تطابق وجود دارد.	0x2E
پیام ارسالی پیاده‌سازی نشده است.(پیام‌رسان مقصد این نوع پیام را پشتیبانی نمی‌کند.)	0x32
خطا در دریافت پیام به دلایل دیگر	0x32
(ارسالی از سمت متپ) پیام‌رسان گیرنده در دریافت پیام به خطا خورده‌است.	0x52
(ارسالی از سمت متپ) پیام‌رسان گیرنده در حال حاضر پاسخ‌گو نیست. (و پیام، دیگر به گیرنده ارسال نمی‌گردد.)	0x56
در اطلاعات گروه/ کانال مقصد، تغییراتی داده شده‌است.	0x72
در فهرست مدیران و یا مالک گروه/کانال مقصد تغییراتی داده شده‌است.	0x76
در فهرست اعضای گروه/شنوندگان کانال مقصد، تغییراتی داده شده‌است.	0x7A

مثال:

۰x۰۰۰۰: این پیام، حاوی پیام جدید متنی است.

۰x۰۲۰۱: این پیام، یک ویرایش برروی پیام فایلی قدیمی است.

۰x۰۶FF: این پیام، نشان‌دهنده‌ی حذف شدن پیام تصویری قدیمی است.

۰x۲۲FF: این پیام، نشان‌دهنده‌ی وجود خطا از دید پیام‌رسان گیرنده بر روی فیلد encryption_key می‌باشد.

۰x۵۶FF: این پیام، نشان‌دهنده آن است که پیام‌رسان گیرنده در دریافت پیام، به خطا خورده‌است و متپ با ارسال پیام با این message_type به پیام‌رسان فرستنده، فرستنده را از این موضوع آگاه می‌کند.

از آنجایی که متپ یک پروتکل آسنکرون بین دو پیام‌رسان است، خطاهای رخ داده در پیام‌رسان گیرنده نیز به‌صورت پیام به پیام‌رسان فرستنده (توسط پیام‌رسان گیرنده یا متپ) ارسال می‌گردد MTPکه در آن message_type بیان کننده مشکل رخداده است.

original_message_id: در صورتی که این پیام، برای ویرایش یک پیام دیگر باشد، یا اطلاعات/ دستوری را در مورد یک پیام دیگر همانند حذف کردن، خوانده شدن، وجود خطا و ... داشته باشد، id پیام اصلی در این فیلد ارسال می‌گردد.

update_time: زمان انجام تغییر /دستور /اطلاعات بهTimestamp. این فیلد همزمان با original_message_id ،یا باید وجود داشته‌باشد یا نداشته‌نباشد. این مقدار برحسب میلی ثانیه است.

reply_to_message_id: درصورتی که این پیام، ریپلای به یک پیام دیگر باشد، id پیام اصلی در این فیلد ارسال می‌گردد. در صورت وجود این فیلد، sender_id و receiver_id این پیام و پیام ریپلای شده بایستی یکسان و یا برعکس باشند.

forwarded_from: این فیلد نشان‌دهنده آن است که پیام از فرد /کانال فوروارد شده‌است و نام فرد /کانال در این رشته وجود دارد.

file_id: شناسه فایل همراه پیام.

file_encryption_key: محتوای این فیلد، کلید ۲۵۶ بیتی برای رمزنگاری AES-GCM مورد استفاده برای رمزنگاری فایل اشاره شده در file_id است. این کلید همانند فیلد encryption_key رمزنگاری و کدبندی می‌گردد. در صورت وجود file_id، این فیلد نیز بایستی وجود داشته باشد و در صورت عدم وجود آن، این فیلد نیز نبایستی وجود داشته باشد.

۵-۱-۴- فایل

فایل از فیلدهای زیر تشکیل شده است:

Id: شناسه عددی ۸ بایتی یکتای فایل که توسط متپ در هنگام ایجاد فایل تولید می‌گردد و بازگردانده می‌شود.

file_name: محتوای این فیلد، برابر با نام فایل ارسال شده از سمت فرستنده است. این محتوا نیز همانند file_content رمزنگاری و کدبندی می‌گردد.

message_sender_file_uid: یک عدد حداکثر ۱۲ بایتی است، که به‌صورت یکتا توسط پیام‌رسان فرستنده ایجاد می‌گردد. این عدد در الگوریتم AES-GCM جهت رمزنگاری file_content هم به‌عنوان nonce استفاده می‌گردد.

file_content: محتوای این فیلد، برابر با محتوای فایل ارسال شده از سمت فرستنده است. این محتوا نیز مانند encrypted_message رمزنگاری و کدبندی می‌گردد.

شکل ۱ فرایند ارسال یک پیام دارای فایل را از ابتدای ایجاد تا خوانده‌شدن توسط کاربر مقصد نمایش می‌دهد.

۵-۱-۵- گروه

گروه‌هایی که در متپ ساخته می‌شوند فقط شامل افرادی هستند که در متپ وجود دارند. بنابراین به‌طور مثال در صورتی که فردی خواهان خروج از متپ بوده و در گروهی نیز عضویت داشته‌باشد، بایستی به اطلاع کاربر رسانده‌شود که خروج وی از متپ منجر به حذف کاربر از گروه خواهدشد. یا به‌طور مثال درصورتی که مالک گروه، تمایل داشت گروه خود را به گروه متپ تبدیل نماید، و در گروه، فردی خارج از متپ وجود داشت، فهرست افراد خارج از متپ، باید به مالک نمایش داده‌شود و به اطلاع وی رسانده‌شود که با حضور این افراد، امکان تبدیل گروه به گروه متپ وجود ندارد.

در صورتی که یک گروه، در متپ وجود داشته‌باشد، برای اضافه کردن فرد به گروه، مالک /مدیر گروه می‌تواند از فهرست کاربران خود، کاربران عادی و کاربران متپ را به گروه اضافه کند. همچنین روال‌های پیشینِ اضافه کردن عضو به گروه در پیام‌رسان‌ها (مانند لینک دعوت) برای گروه متپ نیز فعال می‌باشد. همچنین جهت اتصال یک پیام‌رسان جدید به یک گروه در متپ، هنگام ایجاد گروه در پیام‌رسان بایستی گزینه‌ای وجود داشته‌باشد که کاربر بتواند شناسه گروه متپ را به پیام‌رسان ارائه دهد و درنتیجه، گروه ایجاد شده، یک گروه متصل به متپ خواهد بود.

تغییرات در گروه، از طریق یک پیام به پیام‌رسان‌هایی که عضوی در members دارند، به‌وسیله‌ی پیام‌رسان تغییردهنده اطلاع داده می‌شود.

گروه از فیلدهای زیر تشکیل شده‌است:

Id: یک شناسه ۸ بایتی یکتا برای گروه، که توسط متپ در هنگام ایجاد گروه تولید می‌گردد.

name: نام گروه (رشته‌ای، الزامی، حداکثر ۲۵۵ کاراکتر)

description: توضیحاتی درباره گروه، که توسط ایجادکننده گروه نوشته شده‌است.

Members: فهرست شناسه کاربرانی که در گروه عضو هستند.

admins: فهرست شناسه کاربرانی که توسط ایجادکننده گروه به عنوان مدیران گروه انتخاب شده‌اند. این فهرست، زیرمجموعه‌ی فهرست members می‌باشد.

Owner: شناسه کاربر ایجادکننده گروه. ایجادکننده گروه الزاما باید عضوی از پیام‌رسان ایجادکننده گروه باشد و نمی‌تواند به عضوی که از یک پیام‌رسان دیگر هست، انتقال یابد. مالک یکی از اعضای admins می‌باشد.

Avatar: یک فایل با فرمت jpeg که توسط base۶۴ کدبندی شده است. حجم فایل حداکثر برابر با ۲۰۰ کیلوبایت می‌باشد.

group_type: بیت‌های مختلف این فیلد، مشخص‌کننده نوع گروه می‌باشد.

شکل ۲ مراحل ایجاد گروه ازطریق انتقال پیام‌های آن به‌صورت خودکار، در بستر متب به سایر پیام‌رسان‌ها را نمایش می‌دهد.

۵-۱-۶- کانال

کانال‌هایی که در متپ ساخته می‌شوند، ابزاری برای مدیریت محتوا بین کانال‌های مختلف، در پیام‌رسان‌های مختلف هستند. در واقع هدف از کانال‌ها در متپ، آن است که با مدیریت محتوا در یک پیام‌رسان، محتوا در پیام‌رسان‌های دیگر نیز به‌روزرسانی شود. از یک‌سو به‌دلیل تغییرات عضو زیاد در کانال‌ها و عدم‌اهمیت این موضوع برای کانال‌داران ، و از سوی دیگر جهت فراهم‌سازی امکان عضویت کاربران غیر متپ در کانال‌ها، اساسا اعضا در کانال‌های متپ نگه‌داری نمی‌گردند. با این‌حال، مدیران یک کانال متپ، باید در متپ حضور داشته‌باشند تا سایر پیام‌رسان‌ها بتوانند از تغییرات توسط آنها مطلع گردند.

شیوه‌ی کار کانال در متپ به این‌صورت است که یک شخص، کانالی را در متپ ایجاد می‌کند (مثلا از طریق یک دکمه در قسمت مدیریت کانال) و سپس کانال خود در سایر پیام‌رسان‌ها را ازطریق شناسه کانالِ ایجاد شده در متپ (با استفاده از کپی شناسه در قسمت مدیریت کانال)، به کانال متپ متصل می‌کند (مثلا از طریق یک

فیلد در مدیریت کانال، که شناسه کانال متپ را دربرمی‌گیرد.). در هنگام اتصال بایستی چک شود که کلیه مدیران کانال در متپ حضور داشته‌باشند.

تغییرات در کانال، ازطریق یک پیام به پیام‌رسان‌هایی که عضو listeners هستند، توسط پیام‌رسان تغییردهنده اطلاع داده‌می‌شود. همچنین پیام‌رسان‌ها باید در هنگام عضویت یک فرد در یک کانال، توجه کنند در صورتی که آن شخص عضو متپ نباشد، باید ابتدا به عضویت آن درآید.

کانال از فیلدهای زیر تشکیل شده‌است:

Id: یک شناسه ۸ بایتی یکتا که توسط متپ برای کانال در هنگام ایجاد کانال تولید می‌گردد.

name: نام کانال (رشته‌ای، الزامی، حداکثر ۲۵۵ کاراکتر)

description: توضیحاتی درباره کانال که توسط ایجادکننده کانال نوشته شده‌است.

admins: فهرست شناسه کاربرانی که توسط ایجادکننده کانال به عنوان مدیران کانال انتخاب شده‌اند.

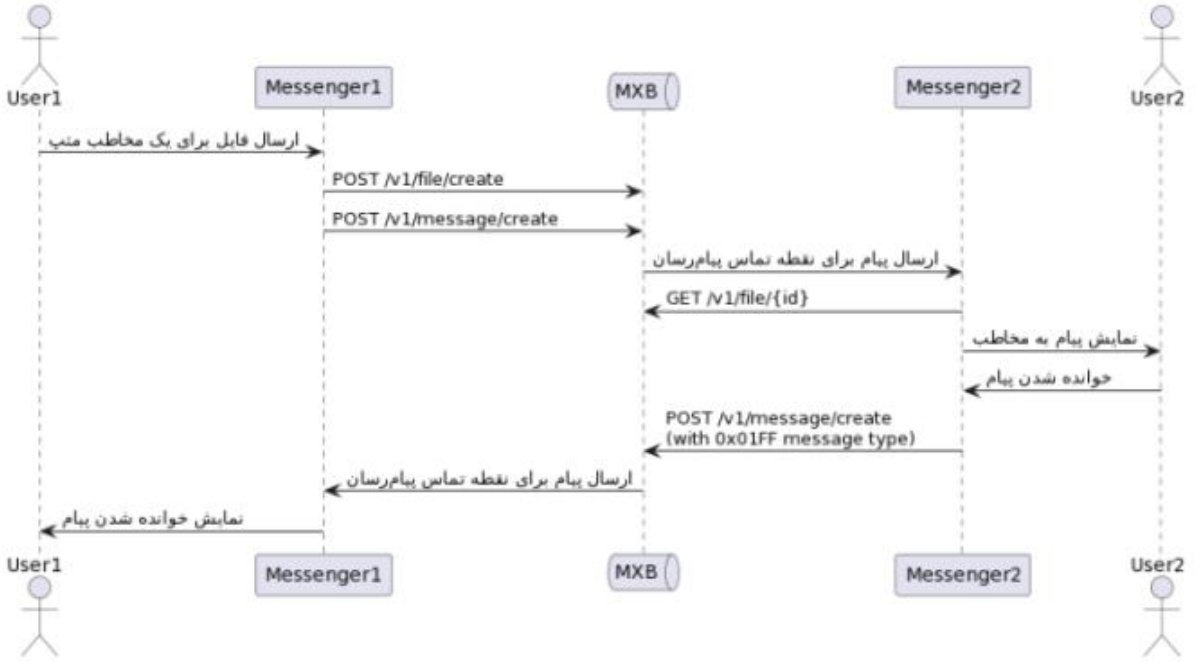
Owner: شناسه کاربر ایجادکننده کانال؛ ایجادکننده باید یکی از اعضای admins باشد.

listeners: فهرست شناسه پیام‌رسان‌هایی که به این کانال متصل هستند و تمایل دارند از تغییرات محتوا و نیز تغییرات خود کانال، مطلع گردند. پیام‌رسان ایجادکننده کانال همواره عضو اول این فهرست خواهد بود. با هر تغییر در این فهرست، پیام‌رسانِ تغییردهنده موظف است این تغییر را به تمامی اعضای این فهرست (به جز خود)، از طریق یک پیام، ارسال نماید.

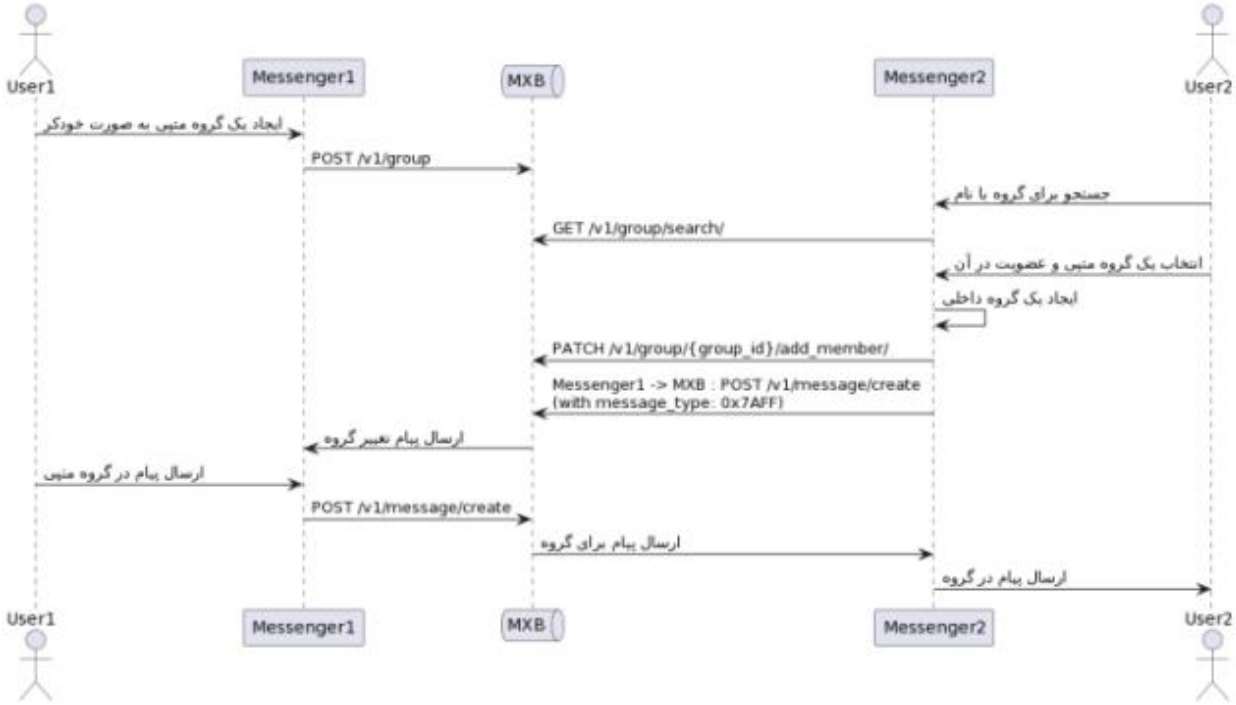
Avatar: یک فایل با فرمت jpeg که توسط base۶۴ کدبندی شده است. حجم فایل حداکثر برابر با ۲۰۰ کیلوبایت می‌باشد.

channel_type: بیت‌های مختلف این فیلد مشخص‌کننده نوع کانال می‌باشد.

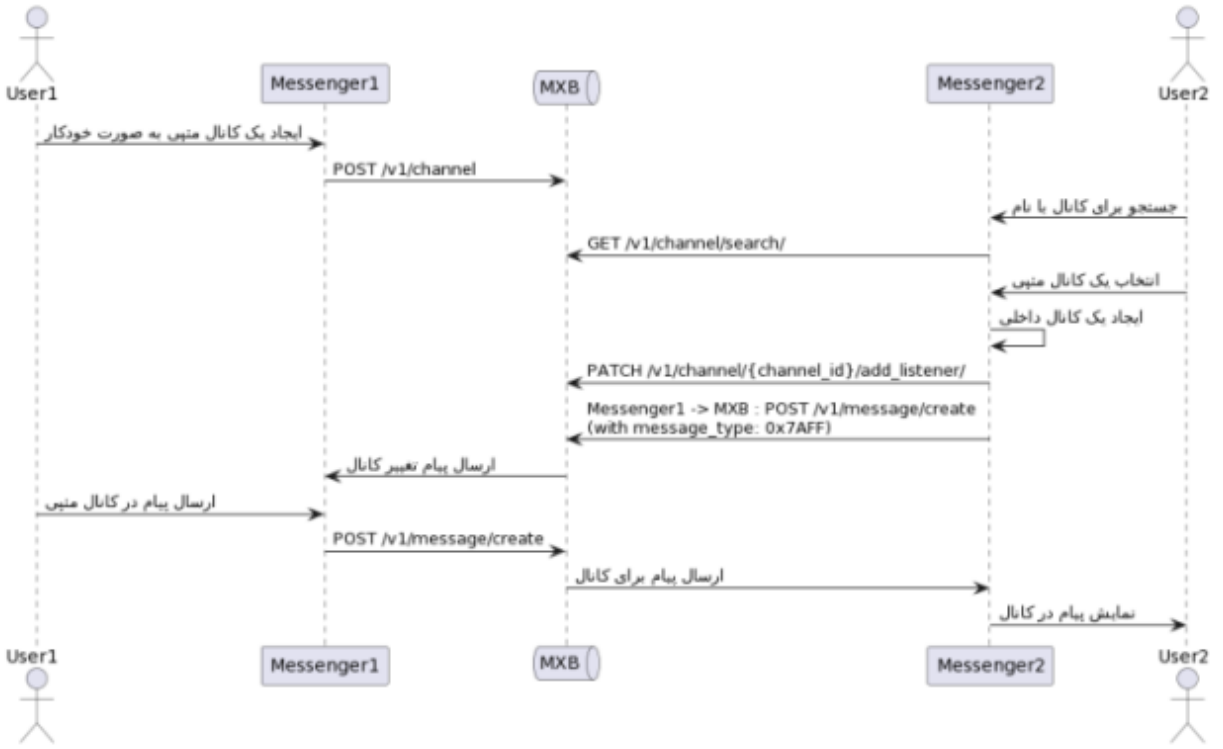
شکل ۳ فرایند ایجاد یک کانال و ارسال پیام‌های آن به‌صورت خودکار به دیگر پیام رسان‌ها را نمایش می‌دهد.



شکل ۱. فرایند ارسال یک پیام دارای فایل



شکل ۲. فرآیند ایجاد گروه با انتقال پیام‌های آن



شکل ۳. ایجاد یک کانال و ارسال پیام‌های آن

۵-۲- رابط کاربری

رابط کاربریِ طرح پیشنهادی ما، یک API تحت‌وب است که به بررسی endpoint های آن برای هر موجودیت خواهیم پرداخت.

۵-۲-۱- پیام‌رسان

دریافت فهرست پیام‌رسان‌ها

GET /v۱/messenger/info/all

در این endpoint، فهرست اطلاعات عمومی کلیه‌ی پیام‌رسان‌های موجود در متپ ارائه می‌گردد. این فهرست شامل موارد زیر است.

id, name, public_key_url, file_ size_limit

۵-۲-۲- کاربر

ایجاد کاربر

POST /v۱/user/create

با استفاده از این endpoint، یک پیام‌رسان می‌تواند یک کاربر را فعال نماید. بدین‌منظور، پیام‌رسان، فیلدهای nickname, avatar, phone, messenger_id را ارسال نموده و در جواب، id کاربر در متپ را دریافت می‌نماید.

دریافت اطلاعات کاربر با شناسه

GET /v۱/user/{id}

با استفاده از این endpoint، یک پیام‌رسان می‌تواند اطلاعات نمایه یک کاربر را با استفاده از شناسه کاربری دریافت نماید.

دریافت اطلاعات کاربر با شناسه پیام‌رسان و تلفن

GET /v۱/user/{messenger_id}/{phone}

با استفاده از این endpoint، یک پیام‌رسان می‌تواند اطلاعات نمایه یک کاربر را ازطریق از شناسه پیام‌رسان و شماره تلفن کاربر دریافت نماید.

غیرفعال‌سازی کاربر با شناسه پیام‌رسان و شماره تلفن

DELETE /v۱/user/{messenger_id}/{phone}/delete

با استفاده از این endpoint، یک پیام‌رسان می‌تواند کاربر خود را با استفاده از شناسه پیام‌رسان و شماره تلفن کاربر غیرفعال نماید.

به‌روزرسانی کاربر با شناسه پیام‌رسان و شماره تلفن

PUT /v۱/user/{messenger_id}/{phone}/update

با استفاده از این endpoint، یک پیام‌رسان می‌تواند نمایه کاربر خود را با استفاده از شناسه پیام‌رسان و شماره‌تلفن کاربر به‌روزرسانی نماید.

دریافت اطلاعات کاربر با شماره تلفن

GET /v۱/user/search/{phone}

با استفاده از این endpoint، یک پیام‌رسان می‌تواند اطلاعات نمایه مربوط به یک کاربر را با استفاده از شماره تلفن کاربر دریافت نماید. با توجه به اینکه ممکن است کاربر در چند پیام‌رسان عضو باشد، خروجی آن، فهرستی از داده‌های کاربر خواهد بود.

دریافت اطلاعات چند کاربر با شماره‌تلفن

POST /v۱/user/search/

در این endpoint، فهرستی از شماره‌تلفن‌های مورد جستجو ارسال می‌گردد و در جواب، یک شی با نگاشت هر شماره تلفن به فهرست جواب بر می‌گردد.

۵-۲-۳- پیام

ایجاد پیام

POST /v۱/message/create

این endpoint، برای ایجاد یک پیام، مورداستفاده قرار می‌گیرد؛ در ورودی فیلدها، مطابق با توضیحات پیام در یک شی ارسال می‌گردد و درخروجی آن، پیامِ ایجادشده به همراه شناسه بر می‌گردد.

دریافت پیام با شناسه

GET /v۱/message/{id}

این endpoint، برای دریافت اطلاعاتِ یک پیام خاص با ارائه‌ی شناسه‌ی آن پیام استفاده می‌گردد. هر پیام‌رسان صرفا به پیام‌های مرتبط با خود دسترسی خواهد داشت.

دریافت پیام‌های دریافتی از شناسه به میزان

GET /v۱/messenger/received/{id}/{limit}

با استفاده از این endpoint، یک پیام‌رسان می‌تواند پیام‌هایی را که برای او ارسال شده‌است، دریافت نماید. بدین منظور شناسه پیام، ابتدا و تعداد پیام‌های مد نظر را ارسال کرده و فهرستی از پیام‌ها را دریافت می‌نماید.

دریافت پیام‌های ارسالی از شناسه به میزان

GET /v۱/messenger/sended/{id}/{limit}

با استفاده از این endpoint، یک پیام‌رسان می‌تواند پیام‌هایی را که ارسال کرده‌است، دریافت نماید. بدین منظور شناسه پیام، ابتدا و

تعداد پیام مدنظر خود را به عنوان ورودی ارسال می‌کند و در پاسخ فهرستی از پیام‌هارا دریافت می‌نماید.

۵-۲-۴- فایل

ایجاد فایل

POST /v۱/file/create

با استفاده از این endpoint، یک پیام‌رسان می‌تواند فایل جدیدی را در متپ ایجاد نماید. برای ایجاد یک فایل، بایستی تمام فیلدهای فایل به جز id ارسال گردیده و در پاسخ، تمام فیلدها به جز محتوای فایل برگردانده شود.

GET /v۱/file/{id}

با استفاده از این endpoint، امکان دریافت فایل متناسب با یک id وجود دارد. در پاسخ این endpoint یک شی با کلیه‌ی فیلدهای فایل برگردانده می‌شود.

۵-۲-۵- گروه

ساخت گروه

POST /v۱/group

در این endpoint پیام‌رسان ایجادکننده گروه، با ارائه تمام فیلدهای گروه به جز شناسه(id)، گروه را در متپ ایجاد می‌نماید. خروجی این endpoint مقدار شناسه(id) گروه ایجاد شده می‌باشد .

ویرایش اطلاعات گروه

PUT /v۱/group/{group_id}

در این endpoint، پیام‌رسان ایجادکننده گروه، با ارائه‌ی تمام فیلدها، گروه را ویرایش می‌نماید.

تغییرات مجاز توسط مدیران: نام، آواتار، توضیحات گروه

تغییرات مجاز توسط مالک: نام، آواتار، توضیحات گروه، مدیران

دریافت اطلاعات گروه

GET /v۱/group/{group_id}

در این endpoint، یک پیام‌رسان با ارائه‌ی شناسه(id)، تمام اطلاعات یک گروه را دریافت می‌نماید.

پیام‌رسان‌هایی که در فهرست listeners یک گروه قرار دارند، موظف هستند به‌طور متناوب نسبت به دریافت اطلاعات گروه و به‌روزرسانی خود اقدام نمایند. این به‌روزرسانی بایستی حداکثر با فاصله زمانی یک ساعت انجام پذیرد. از سوی دیگر درصورت ارسال ویرایش یک پیام توسط کاربری که در فهرست admins قرار ندارد، پیام‌رسان باید مجددا اطلاعات گروه را دریافت کرده و بررسی نماید که فرد ویرایشگر در فهرست admins حضور دارد یا خیر.

در صورتی که این گروه حذف و یا غیرفعال شده‌باشد، خروجی این endpoint، کد خطای مربوط به وضعیت گروه خواهد بود.

جستجو در عنوان گروه‌ها

GET /v۱/group/search/

در این endpoint، یک پیام‌رسان با ارسال یک رشته، فهرست شناسه(id) گروه‌هایی که در name خود آن رشته را دارند، دریافت می‌نماید. حداقل طول ارسالی رشته برابر با ۳ کاراکتر خواهد بود.

اضافه کردن یک عضو به اعضای گروه

PATCH /v۱/group/{group_id}/add_member/{user_id}/

هر پیام‌رسان با استفاده از این endpoint می‌تواند یک عضو خود را در یک گروه عضو نماید.

حذف کردن یک عضو از گروه

PATCH /v۱/group/{group_id}/remove_member/{user_id}/

هر پیام‌رسان با استفاده از این endpoint می‌تواند یک عضو ثبت شده خود را از گروه حذف نماید.

غیرفعالسازی/فعالسازی گروه

PATCH /v۱/group/{group_id}/status/

پیام‌رسان ایجاد کننده گروه با استفاده از این endpoint و با ارائه شناسه(id) گروه می‌تواند اقدام به غیرفعال‌سازی و فعال‌سازی گروه در متپ نماید. با فراخوانی این endpoint، وضعیت گروه برعکس خواهد شد. گروه‌های غیرفعال‌شده در جستجوی گروه با عنوان و دریافت اطلاعات گروه نمایش داده نمی‌شود.

حذف گروه

DELETE /v۱/group/{group_id}/

پیام‌رسان ایجادکننده گروه با استفاده از این endpoint و با ارائه شناسه(id) گروه می‌تواند اقدام به حذف گروه در متپ نماید.

۵-۲-۶- کانال

ساخت کانال

POST /v۱/channel

در این endpoint، پیام‌رسان ایجادکننده کانال، با ارائه‌ی اطلاعات زیر (مطابق مدل دادگان)، کانالی را در متپ ایجاد می‌نماید.

name, admins, owner, avatar, description, username, channel_type

خروجی این endpoint مقدار id کانال می‌باشد.

ویرایش اطلاعات کانال

PUT /v۱/channel/{channel_id}

در این endpoint پیام‌رسان ایجادکننده کانال، با ارائه‌ی اطلاعات (مطابق مدل دادگان)، کانال را ویرایش می‌نماید. channel_id مقدار شناسه(id) کانال مورد ویرایش و موارد بعدی، فهرست تغییرات خواهد بود. لازم به ذکر است که همواره باید owner عضو پیام‌رسان ایجاد کننده کانال باشد.

تغییرات مجاز توسط مدیران: نام، آواتار، توضیحات کانال

تغییرات مجاز توسط کاربر ایجادکننده: نام، آواتار، توضیحات کانال، مدیران

دریافت اطلاعات کانال

GET /v۱/channel/{channel_id}

در این endpoint یک پیام‌رسان با ارائه‌ی شناسه(id)، اطلاعات کانال موردنظر را دریافت می‌کند.

پیام‌رسان‌هایی که در فهرست listeners یک کانال قرار دارند، موظف هستند به طور متناوب نسبت به دریافت اطلاعات کانال و به‌روزرسانی خود اقدام نمایند. این به روزرسانی بایستی حداکثر با فاصله زمانی یک ساعت انجام پذیرد. از سوی دیگر در صورت ارسال ویرایش یک پیام توسط یک کاربر که در فهرست admins وجود ندارد، پیام‌رسان بایستی مجددا اطلاعات کانال را دریافت کرده و بررسی نماید که کاربر ویرایشگر در فهرست admins قراردارد یا خیر.

همچنین درصورتی که یک ویرایش پیام از پیام‌رسانی غیر از پیام‌رسان ایجادکننده کانال انجام پذیرد، پیام‌رسان ویرایش‌کننده قبل از ارسال پیام ویرایش، بایستی مجددا فهرست admins خود را به‌روز نماید.

در صورتی که این کانال حذف و یا غیرفعال شده‌باشد، خروجی این endpoint، کد خطای مربوط به وضعیت کانال خواهد بود. تنها درصورت حذف شدن کانال از متپ و در صورتی که آخرین حالت کانال بر روی حالت انتقال خودکار بوده‌باشد، سایر پیام‌رسان‌ها نیز بایستی نسبت به حذف کانال اقدام نمایند.

جستجو در عنوان کانال‌ها

GET /v۱/channel/search/

در این endpoint، یک پیام‌رسان با ارسال یک رشته، فهرست شناسه(id) کانال‌هایی که در name خود آن رشته را دارند، دریافت می‌نماید. حداقل طول ارسالی رشته برابر با ۳ کاراکتر خواهد بود.

اضافه کردن یک پیام‌رسان به عنوان شنونده

PATCH /v۱/channel/{channel_id}/add_listener/

هر پیام‌رسان با استفاده از این endpoint می‌تواند خود را به عنوان listener به یک کانال اضافه کند.

حذف کردن یک پیام‌رسان به عنوان شنونده

PATCH /v۱/channel/{channel_id}/remove_listener/

هر پیام‌رسان با استفاده از این endpoint می‌تواند خود را به عنوان listener از یک کانال حذف کند.

غیرفعال‌سازی/فعال‌سازی کانال

PATCH /v۱/channel/{channel_id}/status/

پیام‌رسان ایجاد کننده کانال با استفاده از این endpoint و با ارائه شناسه(id) کانال می‌تواند اقدام به غیرفعال‌سازی و فعال‌سازی کانال در متپ نماید. با فراخوانی این endpoint وضعیت کانال برعکس خواهد شد. کانال‌های غیرفعال شده در جستجوی کانال با عنوان و دریافت اطلاعات کانال نمایش داده‌نمی‌شوند.

حذف کانال

DELETE /v۱/channel/{channel_id}/

پیام‌رسان ایجاد کننده کانال با استفاده از این endpoint و با ارائه شناسه(id) کانال می‌تواند اقدام به حذف کانال در متپ نماید.

۶- نتیجه‌گیری

دولت‌ها و سیاست‌گذاران فضای مجازی در دنیا، به این نتیجه رسیده‌اند که با توجه به رشد بیش از اندازه برخی پیام‌رسان‌های جهانی همچون فیسبوک، تلگرام، اینستاگرام و...، امکان رشد برای پیام‌رسان‌های نوپا و جدید بسیار کم است. بنابراین قوانینی برای رفع این مشکل تصویب کرده‌اند. به عنوان مثال شورای قانون‌گذاری اتحادیه‌اروپا، با تصویب یک قانون، شبکه‌های اجتماعی را که دارای ماهانه بیش از ۴۵ میلیون استفاده‌کننده هستند، ملزم به ایجاد زمینه ارتباط و انتقال و دریافت پیام به سایر شبکه‌های اجتماعی کرده‌است[۶][۷].

برقراری ارتباط بین پیام‌رسانی، خود یک چالش به‌شمار می‌رود؛ چرا که پیام‌رسان‌ها دارای ساختار متفاوت و روش‌های متفاوتی برای تبادل پیام کاربران هستند. همچنین تبادل امن پیام بین

پیام‌رسان‌های مختلف هم یک چالش است؛ چرا که این پیام‌رسان‌ها، دارای الگوریتم‌های متفاوتی برای رمزنگاری پیام‌های خود هستند. چالش بعدی، ارتباطات گروهی مانند تبادل پیام در گروه‌ها و کانال‌ها است.

در این پژوهش سعی گردید تا با ارائه پروتکل تبادل پیام بین شبکه‌های اجتماعی متپ، بر چالش‌های ذکرشده غلبه شود. در طرح ارائه‌شده، قابلیت رمزنگاری انتها به انتها بین پیام‌رسان‌ها وجود دارد و از ارتباطات گروهی مانند تبادل پیام در گروه‌ها و کانال‌ها پشتیبانی می‌شود. پژوهش‌های آتی می‌تواند بر چندین حوزه جهت تقویت سیستم پیشنهادی تمرکز کند. یکی از زمینه‌های مورد علاقه، توسعه روش‌هایی برای ارائه خدمات تماس صوتی و تصویری بین پلتفرم‌های پیام‌رسانی است. ارائه این ویژگی‌های ارتباطی، به طور قابل‌توجهی کارایی و تجربه کاربری سیستم پیشنهادی را افزایش می‌دهد.

علاوه‌بر این، می‌توان پژوهش‌هایی برای استفاده از پروتکل متپ برای زیرساخت اشتراک گذاری کلید عمومی انجام شود همچنین می‌توان پژوهش‌هایی برای پیاده‌سازی رمزنگاری انتها به انتها بین کاربران و استفاده از سیستم‌های غیر متمرکز مانند زنجیره بلوکی برای پیاده‌سازی سیستم مشابه انجام داد. به عنوان مثال می‌توان با ارائه یک مدل با استفاده از زنجیره بلوکی پروتکلی مانند متپ ارائه کرد که نیاز به سرور اضافی نداشته باشد و با استفاده از سرورهای موجود پیام‌رسان‌ها یک شبکه نظیر به نظیر برای تبادل پیام بین پیام رسانی بر بستر زنجیره بلوکی فراهم کرد این مدل چون به هیچ سرور خاصی وابسته نیست از مقاومت و پایداری بالاتری نیز برخوردار است.

مراجع

[1] J. Gottfried, “Americans’ Social Media Use,” Pew Research Center, Jan. 13, 2024. [Online]. Available: https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/. [Accessed: Aug. 22, 2024].

[2] M. Anderson, M. Faverio, and J. Gottfried, “Teens, Social Media and Technology 2023,” Pew Research Center, Dec. 11, 2023. [Online]. Available: https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/. [Accessed: Aug. 22, 2024].

[3] M. Nurudeen, S. Abdul-Samad, E. Owusu-Oware, G. Y. Koi-Akrofi, and H. A. Tanye, “Measuring the effect of social media on student academic performance using a social media influence factor model,” Educ. Inform. Technol., vol. 28, pp. 1165-1188, 2023. doi: 10.1007/s10639-022-11196-0.

[4] K. K. Kapoor, K. Tamilmani, N. P. Rana, P. Patil, Y. K. Dwivedi, and S. Nerur, “Advances in Social Media Research: Past, Present and Future,” Inf. Syst. Frontiers, vol. 20, pp. 531-558, 2018. doi: 10.1007/s10796-017-9810-y.

[5] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008, pp. 1-8.

[6] T. Madiega, “Digital services act,” European Parliamentary Research Service, PE, pp. 1-8, 2020.

[7] C. O’Halloran, “Social media giants face annual audits under new EU law,” The Journal.ie, Aug. 2023. [Online]. Available: https://www.thejournal.ie/social-media-audits-digital-services-act-6151679-Aug2023/. [Accessed: Nov. 20, 2023].

[8] R. Flynn, “RCS Interconnect Hub: Driving global interconnectivity of RCS,” Openmind Networks, pp. 3-10, 2013

[9] J. Simmons, J. Mackenzie, T. Martin, T. Ralston, and D. Almeida, “Matrix,” [Online]. Available: https://matrix.org/. [Accessed: Jul. 20, 2023], 2018

[10] S. Ferretti, M. Zichichi, and J. Sparber, “Blockchain-based end-to-end encryption for Matrix instant messaging,” 2021

[11] European Parliament and Council of the European Union, “Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act),” Official Journal of the European Union, L 265, pp. 1-66, Oct. 12, 2022.

[12] European Parliament and Council of the European Union, “Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector,” Official Journal of the European Union, L 265, Oct. 12, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/1925/oj. [Accessed: Aug. 22, 2024].

[13] F. Liberatore, “DMA: EU Publishes The New Digital Markets Act,” [Online]. Available: https://www.privacyworld.blog/2022/10/dma-eu-publishes-the-new-digital-markets-act/. [Accessed: Aug. 22, 2024].

[14] S. Amaro, “EU announces sweeping new rules that could force breakups and hefty fines for Big Tech,” [Online]. Available: https://www.cnbc.com/2020/12/15/digital-markets-act-eus-new-rules-on-big-tech.html. [Accessed: Aug. 22, 2024].

[15] European Commission, “Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act),” EUR-Lex, Nov. 25, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0842. [Accessed: Aug. 22, 2024].

[16] F. S. Morton and C. Caffarra, “The European Commission Digital Markets Act: A translation,” Jan. 5, 2021. [Online]. Available: https://cepr.org/voxeu/columns/european-commission-digital-markets-act-translation. [Accessed: Aug. 22, 2024].

[17] M. Mariniello and J. Anderson, “Regulating big tech: the Digital Markets Act,” [Online]. Available: https://www.bruegel.org/blog-post/regulating-big-tech-digital-markets-act. [Accessed: Aug. 22, 2024].

[18] K. Holt, “EU confirms the six tech giants subject to its strict new competition laws,” [Online]. Available: https://www.engadget.com/eu-confirms-the-six-tech-giants-subject-to-its-strict-new-competition-laws-161917822.html. [Accessed: May 22, 2024].

[19] European Commission, “Commission Proposes New EU Cybersecurity Strategy,” [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423. [Accessed: Aug. 22, 2024].

[20] M. Murgia, “Facebook Fined €110m by European Commission over WhatsApp Deal,” Financial Times, [Online]. Available: https://www.ft.com/content/a2dadc48-3bb1-11e7-821a-6027b8a20f23. [Accessed: Aug. 22, 2024].

[21] A. Satariano, “Google Fined $5.1 Billion by E.U. in Android Antitrust Case,” The New York Times, [Online]. Available: https://www.nytimes.com/2018/07/18/technology/google-eu-android-fine.html. [Accessed: Aug. 22, 2024].

[22] D. Brouwer, “Making messaging interoperability with third parties safe for users in Europe,” Mar. 6, 2024. [Online]. Available: https://engineering.fb.com/2024/03/06/security/whatsapp-messenger-messaging-interoperability-eu/. [Accessed: Aug. 22, 2024].

[23] K. Holt, “Meta explains how third-party apps will hook into Messenger and WhatsApp,” Mar. 6, 2024. [Online]. Available: https://www.engadget.com/meta-explains-how-third-party-apps-will-hook-into-messenger-and-whatsapp-192532065.htm. [Accessed: Aug. 22, 2024].

[24] B. Vigliarolo, “Meta killing off Instagram, Messenger cross-platform chatting,” Dec. 5, 2023. [Online]. Available: https://www.theregister.com/2023/12/05/meta_instagram_messenger. [Accessed: Aug. 22, 2024].

[25] “WhatsApp, Instagram, and Messenger will be integrated: cross-chatting option will be available,” Joy of Android, Sep. 29, 2021. [Online]. Available: https://joyofandroid.com/news/whatsapp-instagram-and-messenger-will-be-integrated-cross-chatting-option-will-be-available/. [Accessed: Aug. 22, 2024].

[26] N. Sarwar, “WhatsApp Cross-Chat With Messenger & Instagram Will Be Optional... For Now,” Sep. 28, 2021. [Online]. Available: https://screenrant.com/whatsapp-cross-chat-facebook-messenger-instagram-optional-interoperability/. [Accessed: Aug. 22, 2024].

[27] “An Update on How We’re Building Safe and Secure Third-Party Chats for Users in Europe,” Sep. 6, 2024. [Online]. Available: https://about.fb.com/news/2024/09/an-update-on-how-were-building-safe-and-secure-third-party-chats-for-users-in-europe/. [Accessed: Aug. 22, 2024].

[28] P. Sawers, “Inside Matrix, the protocol that might finally make messaging apps interoperable,” TechCrunch, Dec. 30, 2022. [Online]. Available: https://techcrunch.com/2022/12/30/inside-matrix-the-protocol-that-might-finally-make-messaging-apps-interoperable/. [Accessed: Aug. 22, 2024].