

TELEGRAM



АРХІТЕКТУРА ТА ПОБУДОВА
СИСТЕМИ TELEGRAM

ВЕРЯСОВ ВЛАДИСЛАВ ПЗПІ-22-2

Про Telegram

Telegram — це багатоплатформовий месенджер, створений для забезпечення швидкої, безпечної та надійної комунікації. Засновниками є брати Павло та Микола Дурови, які раніше створили соціальну мережу «ВКонтакте». Після конфліктів з російською владою щодо контролю над «ВКонтакте», Павло вирішив розробити незалежний месенджер, який би гарантував високий рівень приватності та захисту даних користувачів. Микола Дуров розробив протокол шифрування MTProto, який став основою для Telegram.

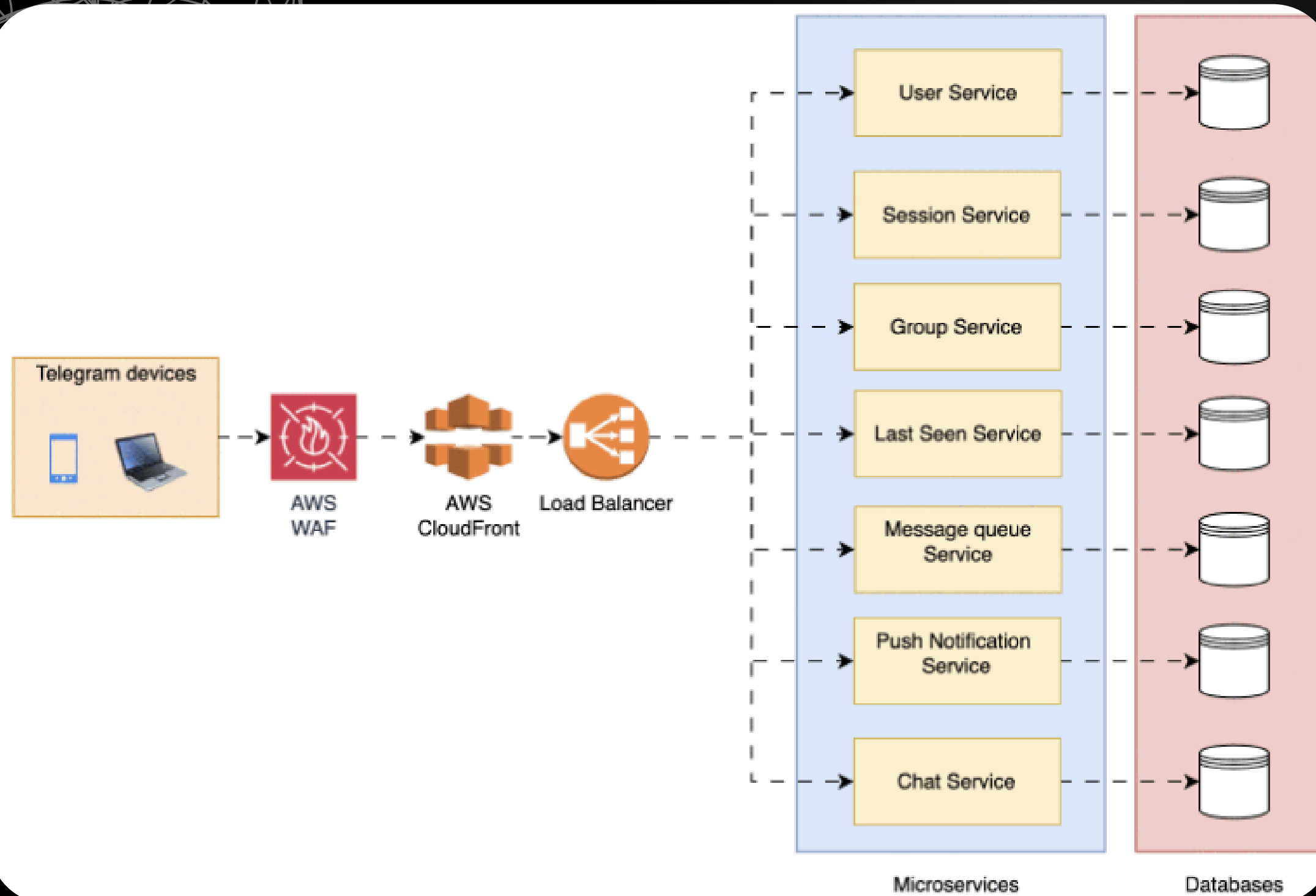
Масштаби застосування:

- Загальна кількість користувачів: Станом на 2023 рік Telegram має 250 мільйонів щоденних активних користувачів (DAU).
- Обсяг повідомлень: Telegram обробляє понад 1 мільярд повідомлень щодня.
- Використання даних: Орієнтовне щомісячне споживання даних Telegram становить близько 50 петабайтів.
- Географічне охоплення: Telegram має глобальну присутність, з користувачами у понад 200 країнах та територіях.

Розробка Telegram

Розробка Telegram розпочалася у 2011 році, коли Павло Дуров задумав створити «вільний месенджер». У серпні 2013 року було презентовано перший клієнт для iOS, а в жовтні того ж року — для Android. У листопаді 2013 року кількість установок програми досягла одного мільйона. У жовтні 2014 року було впроваджено підтримку нікнеймів, що дозволило спілкуватися без розкриття номера телефону, а в січні 2015 року — підтримку стікерів.

АРХИТЕКТУРА TELEGRAM



Архітектура Telegram побудована на клієнт-серверній моделі з використанням хмарного зберігання даних. Це забезпечує швидкий та надійний обмін повідомленнями, а також доступ до них з різних пристроїв. Основою безпеки є протокол MTProto, розроблений Миколою Дуровим, який використовує кілька рівнів шифрування для захисту даних під час передачі.

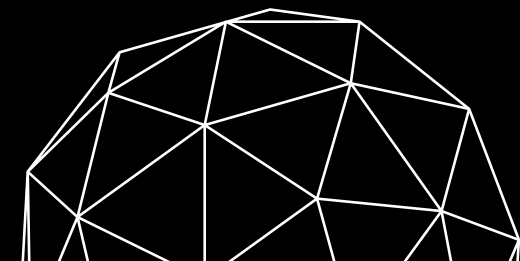


СЕРВЕРНА ІНФРАСТРУКТУРА



Telegram використовує децентралізовану серверну архітектуру. Це означає, що дані користувачів не зберігаються в одному місці, а розподіляються між дата-центрами в різних частинах світу. Основні сервери Telegram розташовані в Європі, Америці та Азії, що дозволяє зменшити затримку при передачі повідомлень.

Кожен регіон має власні дата-центри, які взаємодіють один з одним через зашифровані канали. Завдяки такій системі Telegram може ефективно балансувати навантаження та забезпечувати безперебійну роботу навіть при високих пікових навантаженнях.





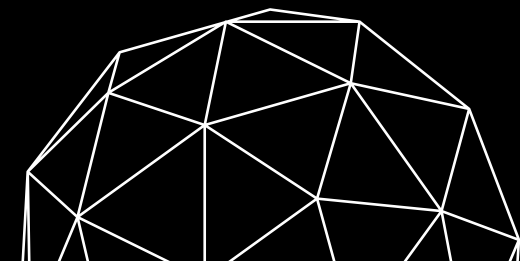
ЗБЕРІГАННЯ ТА ОБРОБКА ДАНИХ



Telegram використовує гібридну модель зберігання даних:

- Хмарне зберігання: Використовується для звичайних чатів, групових повідомлень, медіа та документів. Дані розміщуються на серверах Telegram і доступні з будь-якого пристрою користувача.
- Локальне зберігання: Використовується для секретних чатів, які шифруються наскрізно та не залишаються на серверах. Повідомлення зберігаються тільки на пристроях відправника та отримувача.

Завдяки такій системі Telegram забезпечує швидкий доступ до повідомлень, знижуючи навантаження на сервери за рахунок кешування найбільш популярних запитів.



ВИКОРИСТАНІ МОВИ ПРОГРАМУВАННЯ ТА ФРЕЙМВОРКИ

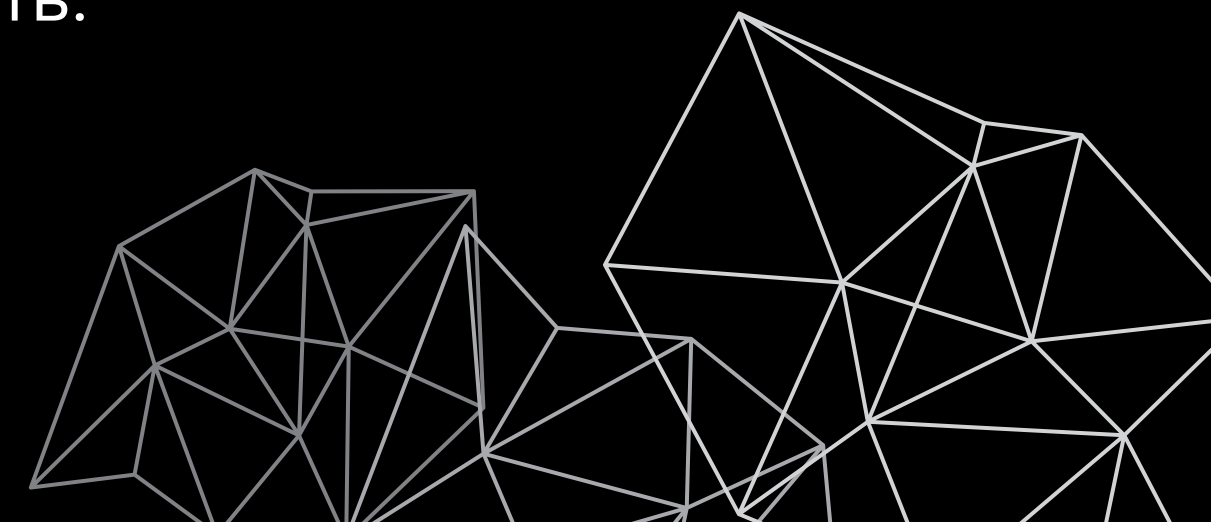
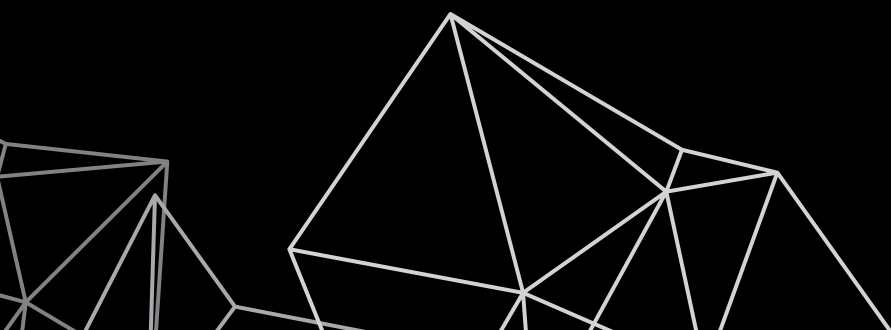
- Серверна частина: Написана переважно на C++ та Java. C++ забезпечує швидкість та ефективність, а Java використовується для обробки бізнес-логіки.
- Клієнтські додатки:
 - iOS – Swift, Objective-C
 - Android – Java, Kotlin
 - Web – JavaScript, TypeScript (React, Vue.js)
- Бази даних: Telegram використовує комбінацію SQL та NoSQL баз даних для зберігання різних типів даних. PostgreSQL застосовується для структурованих даних, а NoSQL рішення, такі як Redis і MongoDB, використовуються для кешування та швидкого доступу до тимчасових даних.
- Черги повідомлень: Використовуються брокери повідомлень, такі як RabbitMQ або Kafka, які допомагають забезпечити асинхронну обробку запитів та рівномірний розподіл навантаження між серверами.



API ТА МОЖЛИВОСТІ ІНТЕГРАЦІЇ

Telegram пропонує потужні API для розробників, що дозволяють створювати боти, додатки та інтегрувати Telegram з іншими сервісами:

- Telegram Bot API – дозволяє розробникам створювати ботів, які можуть автоматизувати процеси, взаємодіяти з користувачами та обробляти запити в реальному часі.
- Telegram MTProto API – надає доступ до внутрішньої архітектури Telegram, що дозволяє розробникам створювати власні клієнти для месенджера.
- Telegram Payments API – використовується для здійснення платежів безпосередньо в месенджері.
- Telegram Passport API – система ідентифікації, яка дозволяє користувачам безпечно передавати свої документи та особисті дані сервісам, що їх потребують.

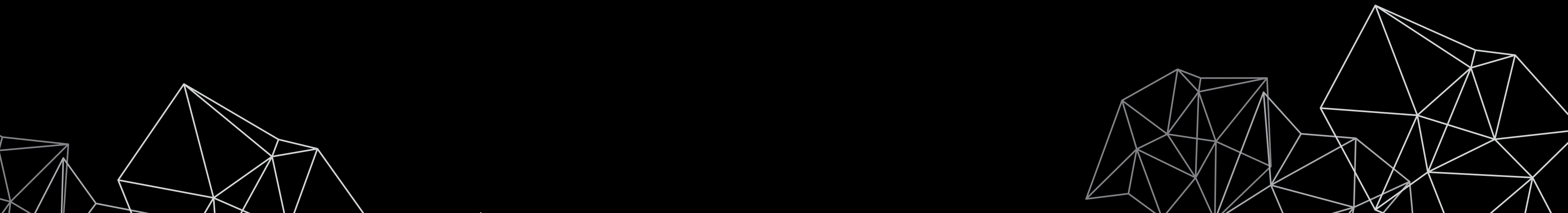


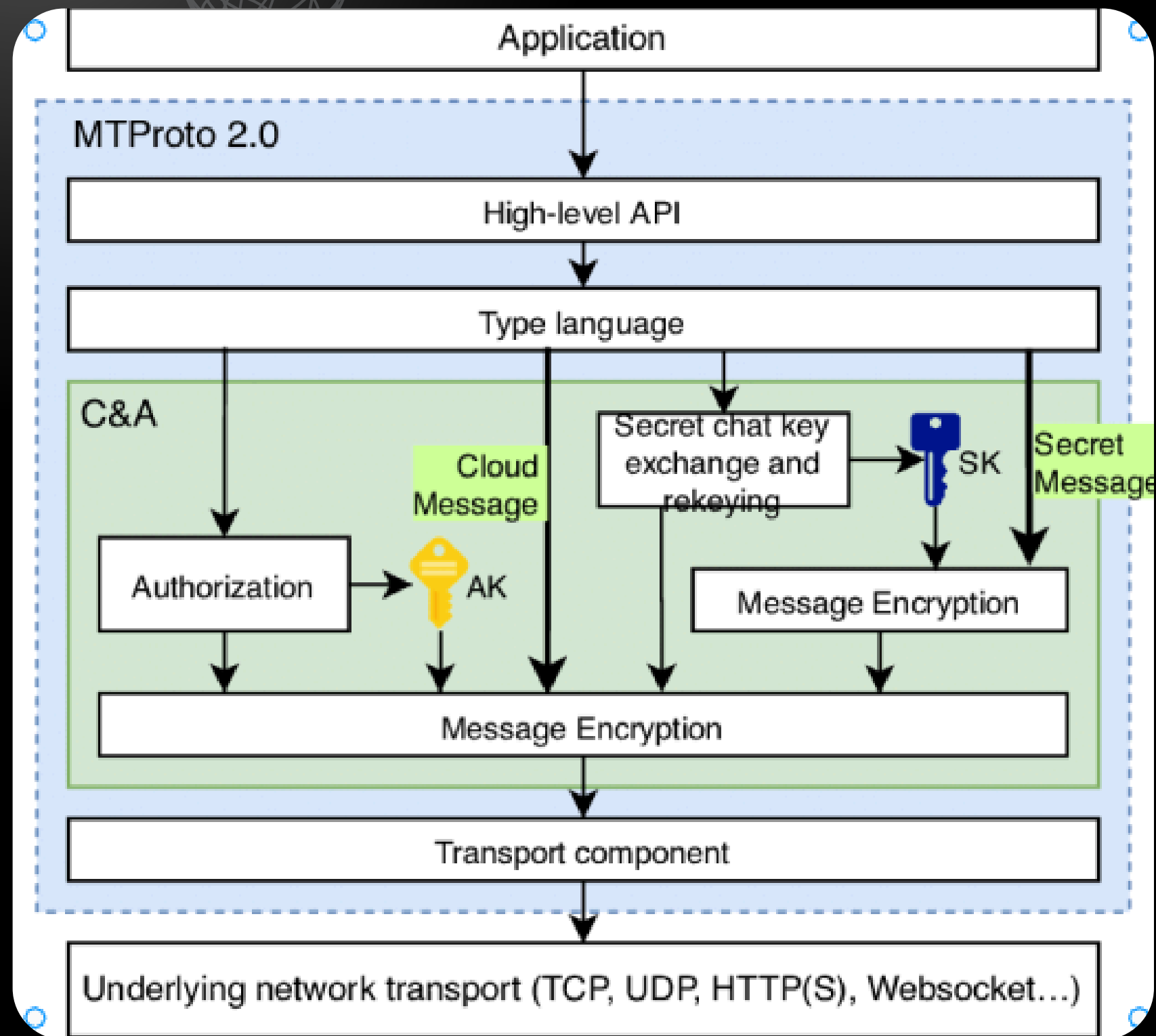
СИСТЕМА БЕЗПЕКИ ТА ШИФРУВАННЯ

Безпека є одним із головних пріоритетів Telegram. Месенджер використовує власний протокол шифрування MTProto, який складається з трьох рівнів:

1. Транспортне шифрування: Дані передаються через HTTPS-з'єднання.
2. Серверне шифрування: Повідомлення в хмарних чатах шифруються на серверах Telegram.
3. Наскрізне шифрування: Використовується в секретних чатах, забезпечуючи максимальний рівень захисту.

Крім того, Telegram застосовує двофакторну аутентифікацію (2FA) та унікальні алгоритми хешування для зберігання паролів, що робить злом акаунтів практично неможливим.



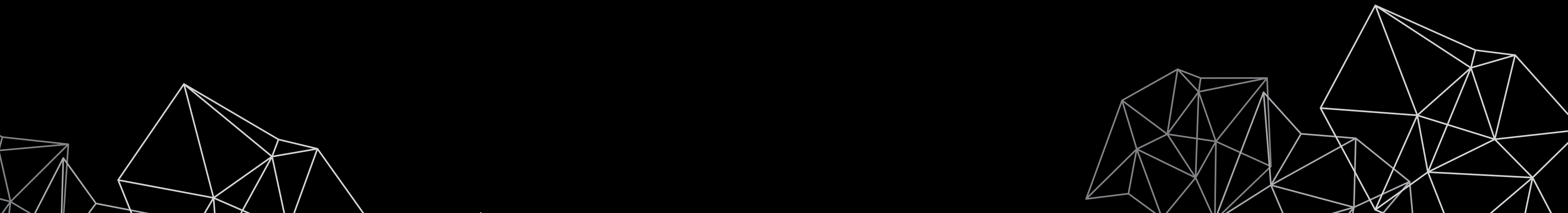


MTProto (Mobile Telegram Protocol) — це криптографічний протокол, розроблений для Telegram, який забезпечує швидку та безпечну передачу даних. Протокол складається з двох основних рівнів: Transport (мережевий рівень) і High-Level Protocol (високорівневий рівень). На мережевому рівні MTProto використовує декілька методів транспортування (TCP, HTTP, UDP), що дозволяє йому працювати в умовах поганого інтернет-з'єднання. Високорівневий рівень забезпечує шифрування через AES-256 у режиміIGE, а також обмін ключами через Diffie-Hellman. Передача даних здійснюється у вигляді серії запитів та відповідей між клієнтом і сервером, де кожне повідомлення має унікальний ідентифікатор та часовий штамп для захисту від атак повторення. Також MTProto підтримує секретні чати, в яких використовується end-to-end шифрування, що робить повідомлення доступними тільки для відправника і отримувача.

МАСШТАБОВАНІСТЬ ТА ПРОДУКТИВНІСТЬ

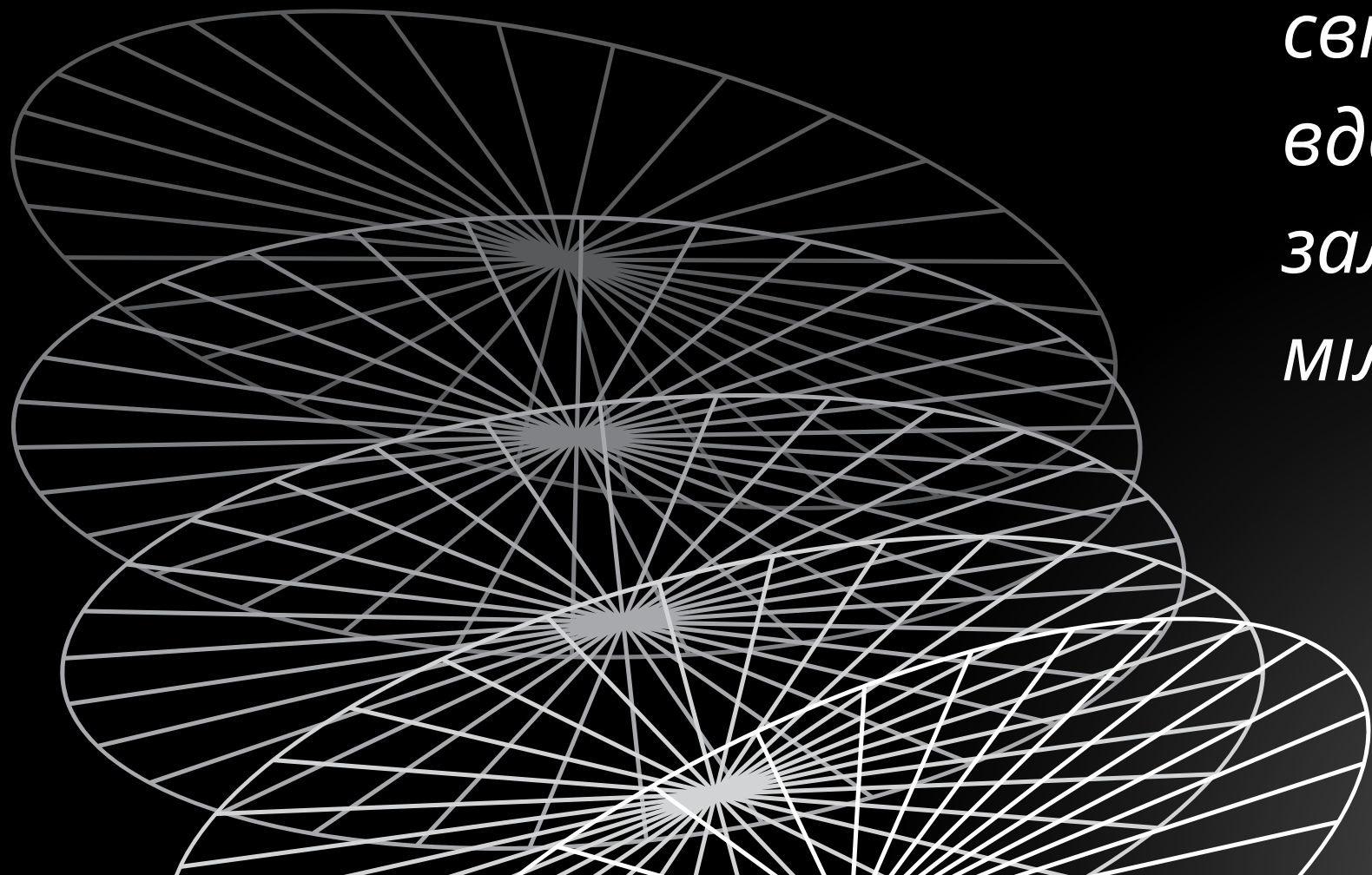
Telegram може обробляти величезну кількість запитів одночасно завдяки оптимізованій серверній архітектурі. Основні аспекти продуктивності:

- Горизонтальне масштабування: Telegram може легко додавати нові сервери без зміни основної архітектури.
- Розподілені обчислення: Дані обробляються паралельно на кількох серверах для швидкого виконання запитів.
- Кешування: Активно використовується кешування на рівні серверів та клієнтів для зменшення навантаження на бази даних.



ВИСНОВОК

Архітектура Telegram є потужною та гнучкою, що дозволяє месенджеру працювати швидко, безпечно та масштабовано. Використання сучасних технологій, розподілених серверів, потужного API та ефективних алгоритмів обробки даних робить Telegram одним із найкращих месенджерів у світі. Завдяки постійним оновленням та вдосконаленням Telegram продовжує залишатися надійним засобом комунікації для мільйонів користувачів.





THANK YOU