Facebook

- Data Management
  - How is data stored, transmitted and secured
- Ethical Concerns
  - Data privacy, security and misinformation
- Automation and AI
  - AI feed algorithm, targeted ads, Meta AI chatbot
- User Connections
  - Social media network map
- Presentation
  - PowerPoint explaining my findings

A picture of Facebook (now Meta) CEO, Mark Zuckerburg.

Christos Makrypodis

Q4, 2025

www.ChristosM.net

Index:

Note: Facebook (www.Faceboook.com) is a social-media platform whose parent company is Meta. Meta has a marketcap of $2.846 trillion AUD (as of 26 October 2025) and a total of 3.35 billion daily active users. Out of these, 3 billion of them are Facebook users.

How does Facebook store, transmit and secure data?

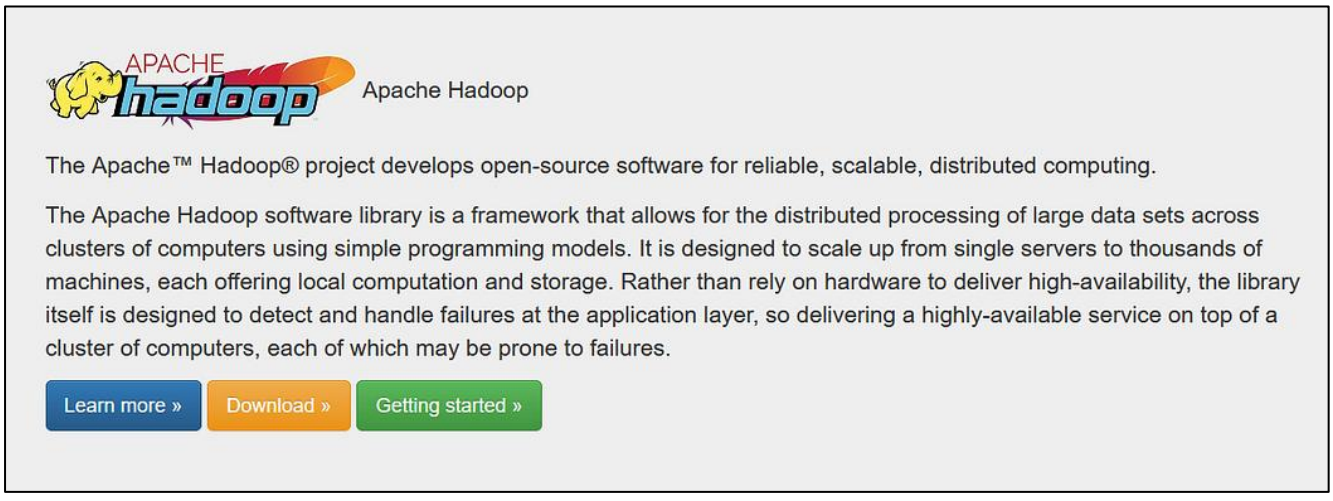
Facebook runs on its parent companies' data centres, Meta. This means that all Meta services including Facebook, WhatsApp and Instagram are run on the same data centres.

Meta has many data centres all across North America, Europe and Asia.

(https://datacenters.atmeta.com/all-locations/ | Accessed 2025-10-21)

Facebook on its own generates 500+ TB of data every day! This is a lot of data for Meta's datacentres to handle.

To manage all this data effectively, a software called Apache Hadoop is used.



This software effectively allows the data to be processed by using a method known as “Distributed Computing”, which is the practice of using a network of multiple computers to work together, rather than relying on a single machine.

(https://medium.com/@helloakashdas/how-does-facebook-manage-so-much-of-data-d500fdf1269a | Accessed 2025-10-21)

Facebook uses TLS (transport layer security) to transmit user data. This ensures that data is not intercepted during transmission.

Facebook also uses 2FA (2-factor-authentication) to ensure that only authorised users log into accounts.

(https://www.efani.com/blog/how-secure-is-facebook#content_3rd | Accessed 2025-10-23)

Another security measure used by Facebook is ‘Login Alerts’, which is a feature that alerts you when someone signs in or attempts to sign in to your account

(https://www.facebook.com/help/162968940433354 | Accessed 2025-10-23)

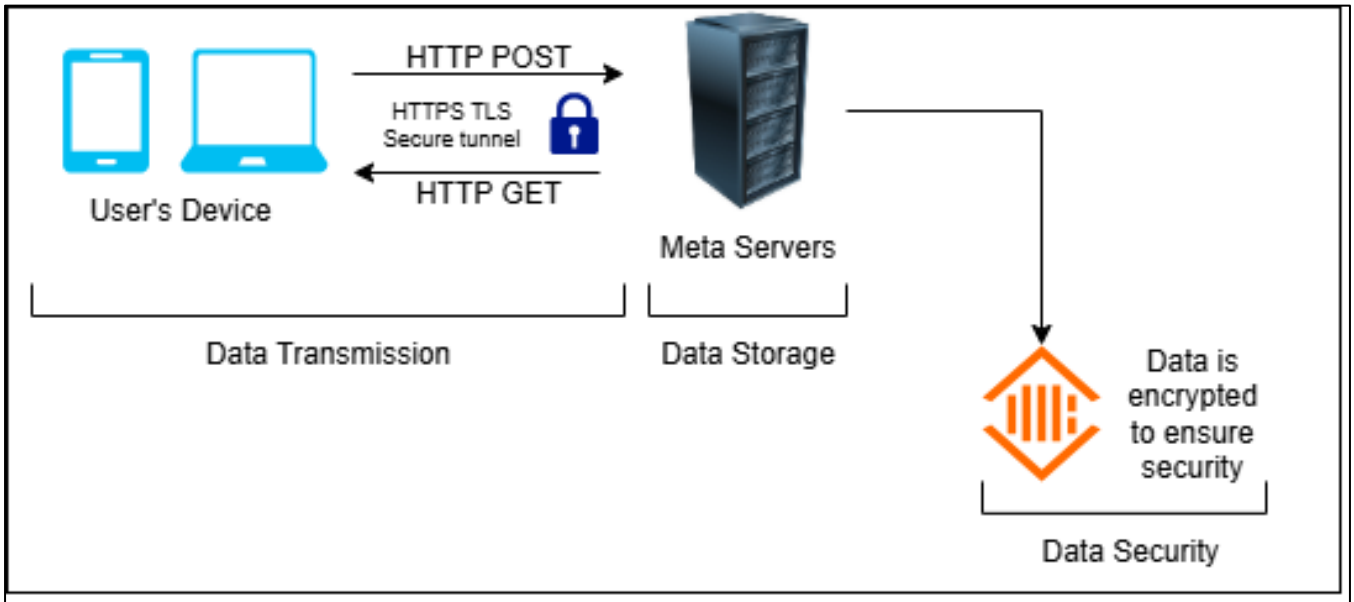
Facebook now stores user information encrypted and passwords hashed on their servers, however in 2019 they were caught storing user passwords in plaintext!

(https://www.theguardian.com/technology/2019/mar/21/facebook-admits-passwords-unprotected | Accessed 2025-10-23)

All these practices ensure that data on Facebook is securely transmitted and stored.

A diagram explaining how data is transmitted, stored and secured on Facebook using Meta's servers.

3 examples are provided.



Example 1: User adds a friend

1. User's device sends POST request to meta servers over HTTPS TLS
2. Meta servers process request
3. Output (updated friends list) is stored in the meta servers encrypted

Example 2: User makes and views a post

1. User's device sends POST request (post contents) to meta servers over HTTPS TLS
2. Meta servers process request
3. Output (post) is stored in the meta servers encrypted
4. When a user views the post, their device sends a GET request and meta's servers respond with the post over HTTPS TLS

Example 3: User likes a post

1. User's device sends POST request (what post to like) to Meta's servers over HTTPS TLS
2. Meta servers process request (update list of liked posts and like count of the post)
3. Output (updated like count) is sent to users device
4. Updated like count is displayed, as well as list of liked posts being updated.

Ethical concerns of Facebook

While Facebook does have strict measures to protect its users, ethical challenges are inevitable.

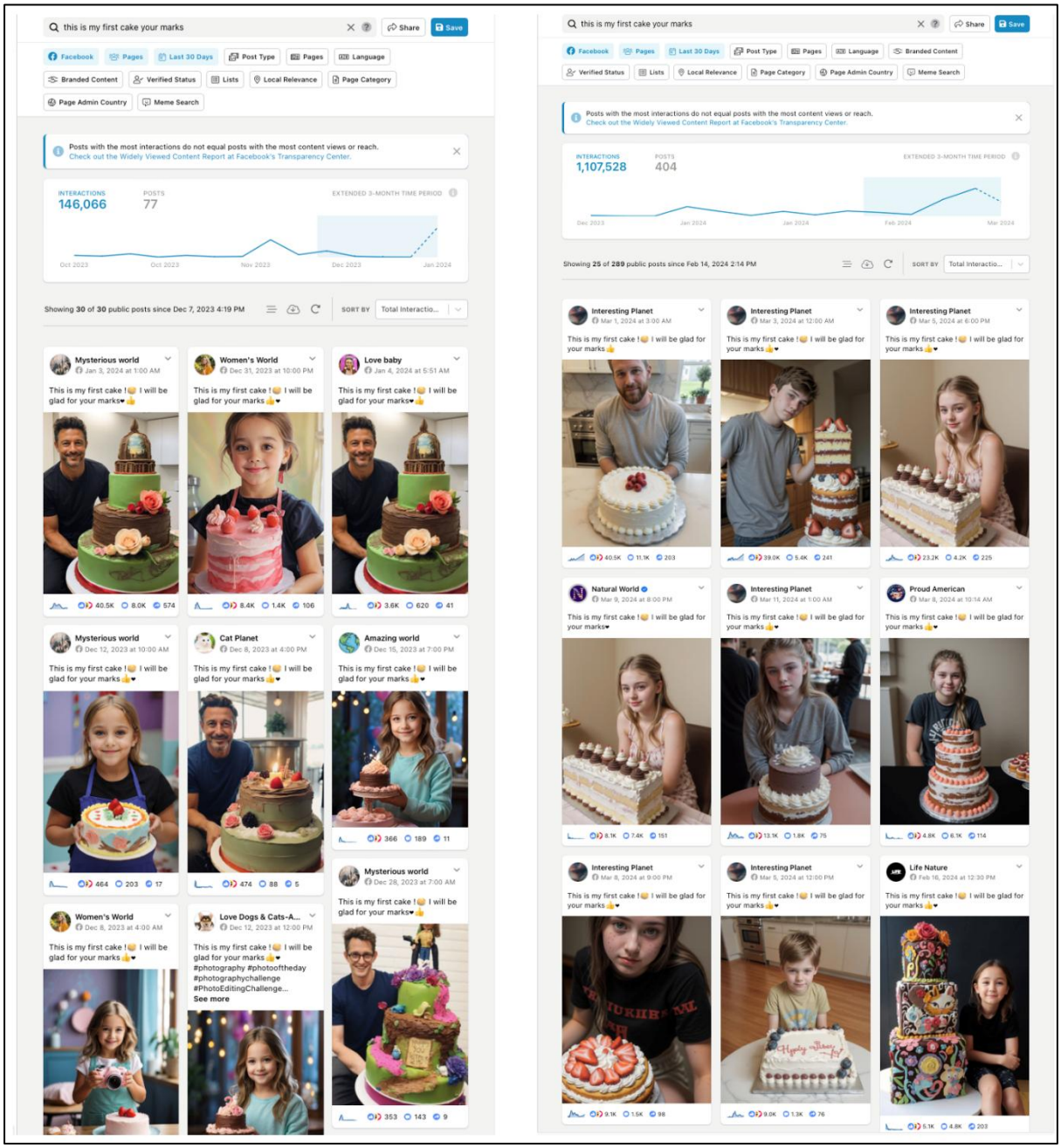
These issues can have the following consequences:

- Identity Theft
- Harassment/Stalking
- Targeted Advertising
- Misinformation/Disinformation
- Weak Account Security

A major ethical concern on Facebook is misinformation. This is obviously an ethical issue as it is spreading false information in a deceptive manner. A major cause of this information is AI-generated content being passed on as human-made. A report from the Harvard Misinformation Review (https://misinforeview.hks.harvard.edu/article/how-spammers-and-scammers-leverage-ai-generated-images-on-facebook-for-audience-growth/ | Written by Renée DiResta and Josh A. Goldstein on 2025-08-15 | Accessed 2025-10-24)

states “images from AI models are already being used by spammers, scammers, and other creators running Facebook Pages”.

A particular example featured in the report:



These are AI-generated images of people claiming to have made these amazing cakes, however they are being passed on as real. This is deceiving the public and getting lots of undeserved attention for the “creator”, taking away attention from legitimate cake makers.

Another particular example from the report:

This is a screenshot of a page sharing an AI-generated image of crab Jesus. The creator claims to have made it with their own hands, however it was actually generated with AI. This resulted in undeserved attention and praise for the “faker”. Unfortunately, as more AI art is being shared and people realise it is merely a computer generated image, the work of real artists will also come under suspicion. This may even lead to demotivation of real artists due to questions about their credibility.

Another major ethical concern on Facebook is data breaches. Facebook has faced many data breaches during its lifetime, exposing confidential information of its users.

This article from NordVPN (https://nordvpn.com/blog/facebook-data-breach/ | Written by Violeta Lyskoit on 2024-07-16 | Accessed 2025-10-24) states:

“Facebook’s digital walls have been breached more than once, exposing the personal information of millions of users. These incidents not only undermine trust in the social media giant but also pose significant risks to user privacy and security.”

A specific data breach the article mentions is one in October 2023, where 200,000 user records, personal information (including phone numbers and email addresses) were leaked on a hacker forum. This was a result of a threat actor named “algoatson” stealing the database from a contractor responsible for managing Facebook’s cloud services. The incident was only made public in February 2024, 4 months after the incident occurred.

Another data breach the article calls *“One of the most significant Facebook data leaks ever”* occurred in April 2019, when more than 540 million user records were exposed.

The data was compromised after being shared with third-party apps that used unsecured servers.

Two third-party Facebook app developers, Mexico-based “Cultura Colectiva” and L.A.-based “At The Pool”, stored about half a billion Facebook user data entries on unsecured servers. After the scandal, it took “Cultura Colective” almost 3 months to secure its users’ data, while “At The Pool’s” data was secured much quicker.

However, the data had been left unsecured for about 5 years prior, leaving it exposed to hackers.

A picture of Facebook (now Meta) CEO, Mark Zuckerburg.

(Extracted from https://www.theverge.com/2016/11/13/13613566/mark-zuckerberg-facebook-misinformation-hoax-media | Accessed on 2025-10-24)

Automation and AI

Facebook uses automation and AI throughout their platform. The primary uses are the:

- ❖Feed Algorithm
- ❖Friend Recommendations
- ❖Targeted Ads

Feed algorithm

The Facebook feed algorithm uses machine learning and AI to deliver the user videos/posts that they are most likely to watch and engage with.

"As of 2025, the Facebook algorithm has transformed into a sophisticated, AI-driven system focused on delivering content that resonates with users' preferences. "

The 4 ranking factors that the algorithm uses for content evaluation are:

- → Inventory *(posts by friends, followed pages, relevant groups)*
- → Signals *(numerous and diverse, such as timing of the post, identity of the poster, content type, user engagement with similar posts, user's local time)*
- → Predictions *(Using signals, the algorithm makes personalised predictions about what content is relevant and valuable to the user)*
- → Relevance *(Each piece of content is assigned a relevance score. Content with higher scores gets priority in the feed)*

(Information from https://socialbee.com/blog/facebook-algorithm/ | Written 2025-01-07 | Accessed 2025-10-24)

Friend Recommendations

Facebook has an algorithm which suggests friends for you to add on Facebook.

Facebook's algorithm is designed to make it easier to find friends and connections.

The algorithm is a machine learning algorithm which predicts who they might want to add as friends.

Some factors the algorithm uses are:

- Friends you add
- Friends of friends
- Bio
- Likes and comments
- Profiles you visit
- Facebook searches
- Google searches
- Contacts on your mobile smartphone

This algorithm is called a "K-nearest neighbours" algorithm (KNN algorithm).

"To put it simply, KNN uses a voting mechanism to determine the class of an unseen observation. This means that the class with the most votes will become the data point's class."

(https://medium.com/@shreyash9m/facebook-friend-suggestion-algorithm-ff9319e2ad7f | Accessed 2025-10-26)

Targeted Ads

Facebook uses automation to automatically serve the right ads to the right people. This is called *targeted advertising.*

The Facebook targeted ads algorithm works in the following way:

1. Ads are fetched from a database
2. The ads are ranked according to the likelihood of the user clicking on the ad.

In the database, there is typically 10-100 million ads. To only serve relevant ads to the user, an automated filter is used.

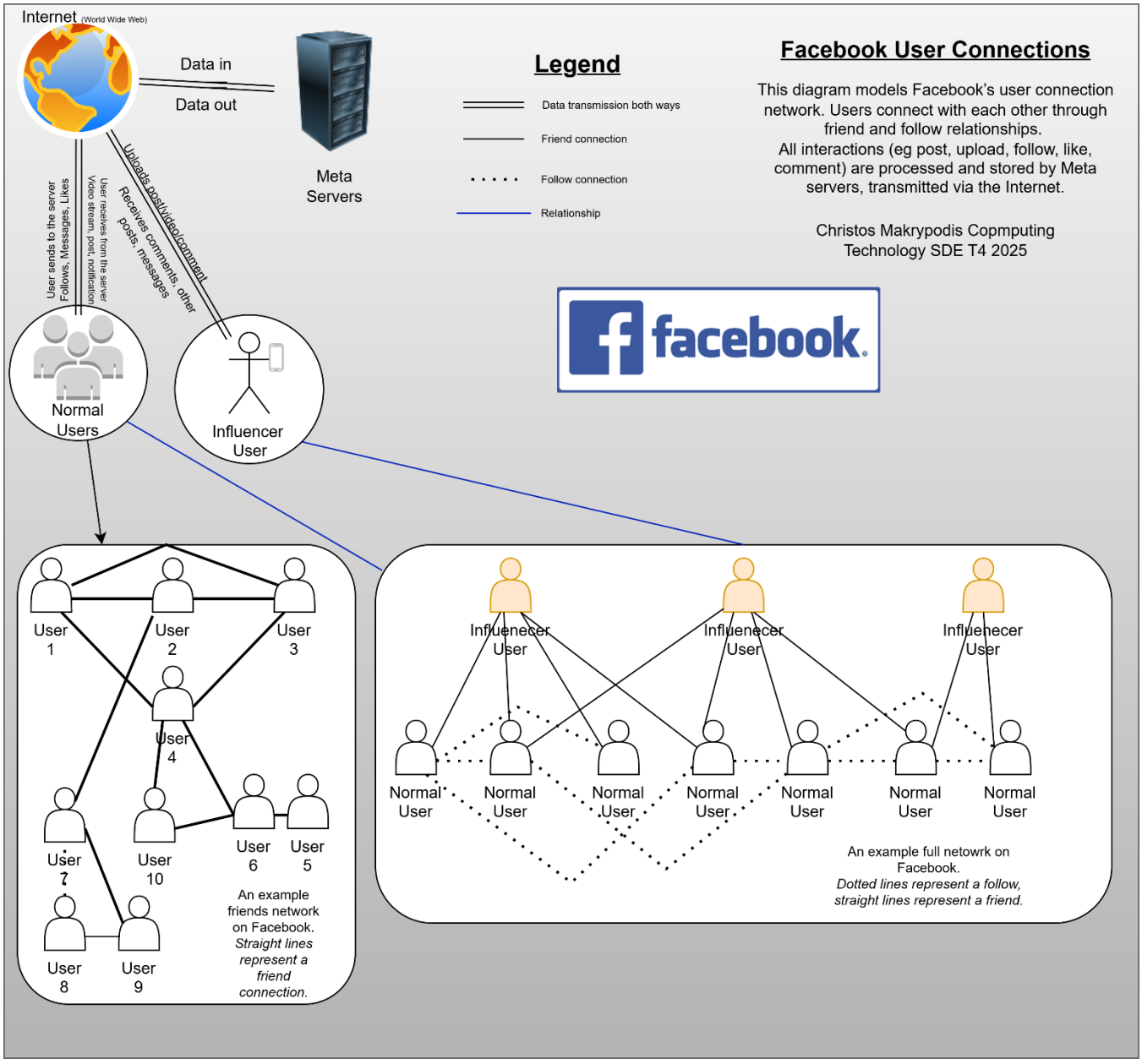
The following user information is used for this filter:

- Age
- Gender
- Language
- Location
- Number of friends
- Liked pages
- Interests
- Number of friends with the same interest
- Previous ad engagement

(https://datascientest.com/en/how-does-the-facebook-ads-algorithm-work | Accessed 2025-10-26)

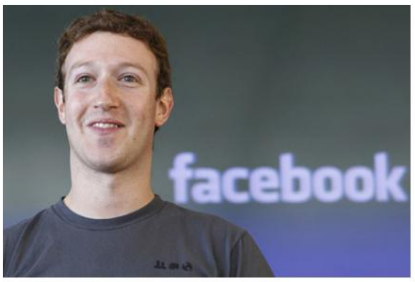
User connections

A model of the Facebook social network



Presentation:

Below: Mark Zuckerburg, the CEO of Meta, Facebook's parent company



Facebook

-Data Management
-Ethical Concerns
-Automation and AI
-User Connections

Christos Makrypodis Year 9
Computing Technology Assignment, Term 4, 2025
Sydney Distance Education High School

The scale of Facebook

- *Facebook (www.Faceboook.com) is a social-media platform whose parent company is Meta.*
- *Meta has a marketcap of $2.846 trillion AUD (as of 26 October 2025) and a total of 3.35 billion daily active users.*
- *Out of these, 3 billion of them are Facebook users.*

facebook

How does Facebook store data?

- Facebook stores data on its parent company, Meta's servers. This means that all Meta services including Facebook, WhatsApp and Instagram are run on the same data centres.
- Meta has many data centres all across North America, Europe and Asia.
- Facebook on its own generates 500+TB of data every day! To manage this effectively, a software called Apache Hadoop is used.

Apache Hadoop

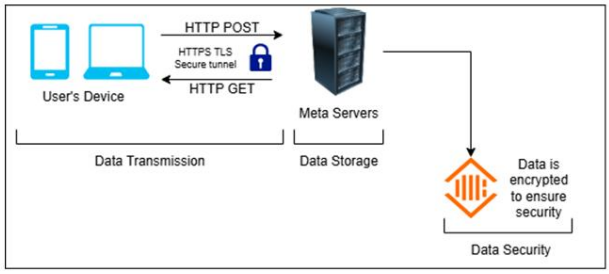
- Apache Hadoop is a software used by Facebook, which allows data to be processed using a method known as "Distributed Computing".
- Distributed Computing is the practice of using a network of multiple computers to work together, rather that relying on a single machine.
- This allows large amounts of data to be processed effectively.

Security practices used on Facebook

Security Practice	Use case
HTTPS TLS (Transport-Layer-Security)	All Data Transmission
2FA (2-Factor-Authentication)	User Login
Login Alerts	User Security
Storing passwords hashed	Data Storage Security

Not so fun fact: In 2019, Facebook was caught storing user passwords in plaintext! This would allow for a hacker to get access to user passwords without decoding them.

How is data transmitted, stored and secured on Facebook?



- Devices connect through the internet to Meta's servers through the secure HTTPS TLS protocol.
- Once the data reaches Meta's Servers, it is encrypted to ensure security.

Example 1: User adds a friend
1. User's device sends POST request to meta servers over HTTPS TLS
2. Meta servers process request
3. Output (updated friends list) is stored in the meta servers encrypted

Example 2: User makes and views a post
1. User's device sends POST request (post contents) to meta servers over HTTPS TLS
2. Meta servers process request
3. Output (post) is stored in the meta servers encrypted
4. When a user views the post, their device sends a GET request and meta's servers respond with the post over HTTPS TLS

Example 3: User likes a post
1. User's device sends POST request (what post to like) to Meta's servers over HTTPS TLS
2. Meta servers process request (update list of liked posts and like count of the post)
3. Output (updated like count) is sent to users device
4. Updated like count is displayed, as well as list of liked posts being updated.

Ethical concern 1 of Facebook: AI

- A major ethical concern on Facebook is AI(Artificial Intelligence)-Generated images are being passed off as real.

- For example, this artwork of Crab-Jesus is being passed off as handmade, however it was actually made with AI.
- This leads to real artists losing attention
- As more AI-generated content gets spread around, concerns about the legitimacy of real artworks will be raised.
- Real artists will possibly face demotivation due to "fakers" gaining popularity instead of real "makers", as well as their real works being perceived as AI-generated, when in reality the artist has put time and effort in to produce it.

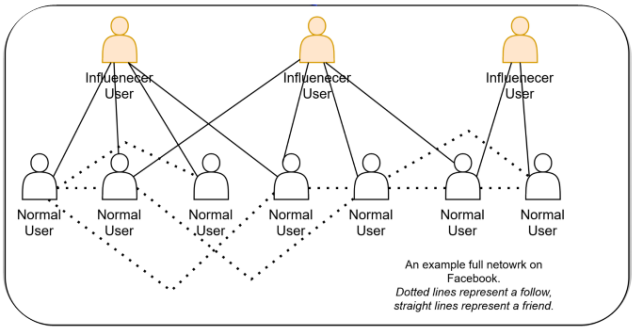
Ethical concern 2: Data breaches

- Facebook has faced many data breaches during its lifetime.
- A significant example occurred in April 2019, where more than 540 million user records were exposed.
- This was due to two third-party app developers storing Facebook data entries on unsecure servers.
- The data was unsecured for 5 years.

Automation and AI on Facebook

- Facebook uses Automation and AI for the following uses:
  - Feed Algorithm
  - Friend Recommendations
  - Targeted Ads
- Inputs for the algorithms include:
  - Friends and friends of friends
  - Likes, comments, followed pages, joined groups
  - Searches on Facebook and on Google
  - Age
  - Gender
  - Location
  - Previous engagement

User connections on Facebook model



- Users connect with other users, as well as with influencer users, forming a network.
- This is done through “friends” and “follows”

Citations/sources

- Image on Slide 1 downloaded from: https://www.csmonitor.com/USA/Latest-News-Wires/2010/1215/Mark-Zuckerberg-Facebook-founder-named-TIME-Person-of-the-Year-2010 | Accessed 2025-10-30
- Image on Slide 2 downloaded from: https://www.facebook.com/ | Accessed 2025-10-30
- Image on Slide 3 downloaded from: https://commons.wikimedia.org/wiki/File:Datacenter_de_ARSAT.jpg | Accessed 2025-10-30
- Image on Slide 4 (Apache Hadoop logo) downloaded from: https://commons.wikimedia.org/wiki/File:Hadoop_logo_new.svg | Accessed 2025-10-30
- Image on Slide 4 (Distributed computing) downloaded from: https://cloudxlab.com/blog/introduction-to-big-data-and-distributed-computing/| Accessed 2025-10-30
- Image on Slide 5 downloaded from: https://icomppayroll.com/data-security-for-small-and-medium-sized-businesses/ | Accessed 2025-10-30
- Image on Slide 8 downloaded from: https://www.idagent.com/blog/data-breach-duplicate/ | Accessed 2025-10-30
- Image on Slide 9 downloaded from: https://plat.ai/blog/ai-classification/ | Accessed 2025-10-30