End-to-End Encryption

Why in news?

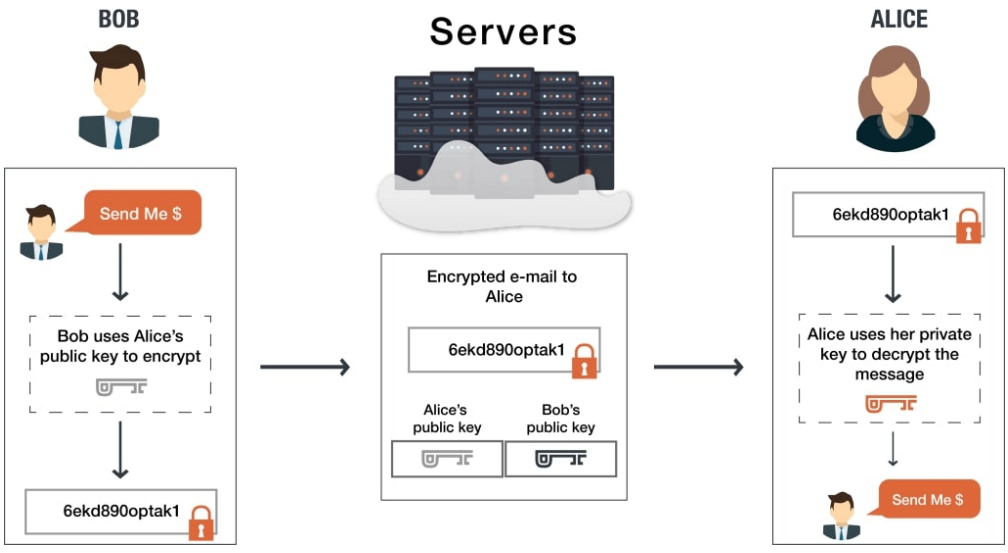
A recent announcement by messaging apps and technology giants to use end-to-end encryption to secure more user data has disappointed the government agencies.

What is the issue?

- Apple has recently announced that it will be increasing the number of data points protected by end-to-end encryption on iCloud from 14 to 23 categories.
- Similarly, Elon Musk, also said that he wanted Twitter DMs to be encrypted.
- However, government agencies are not happy with the development.
- According to the “Rising Threat to Consumer Data in the Cloud”, the total number of data breaches more than tripled between 2013 and 2021.

What is End-to-End Encryption?

- End-to-end encryption (E2EE) is a communication process that encrypts data being shared between two devices.
- It prevents third parties like cloud service providers, internet service providers (ISPs) and cybercriminals from accessing data while it is being transferred.
- The process of end-to-end encryption uses an algorithm that transforms standard text into an unreadable format.
- This format can only be unscrambled and read by those with the decryption keys.
- These keys are only stored on endpoints and not with any third parties including companies providing the service.
- End-to-end encryption has long been used when transferring business documents, financial details, legal proceedings, and personal conversations.
- It can also be used to control users’ authorisation when accessing stored data.



Where is it used?

- End-to-end encryption is used to secure communications.
- Some of the popular instant-messaging apps that use it are Signal, WhatsApp, iMessage, and Google messages.
- It is also used to secure passwords, protect stored data and safeguard data on cloud storage.

What is the difference between E2EE and TLS?

- Transport Layer Security (TLS) is an encryption protocol that, like E2EE, uses public key encryption and ensures that no intermediary parties can read messages.
- However, TLS is implemented between a user and a server, not between two users.
- This keeps data secure in transit to and from a server, but the data on the server itself is in decrypted form.

What are the advantages of E2EE?

- **Protection of Privacy** - With end-to-end encryption, user data will be protected even in case data is breached in the cloud.
- **Integrity of data** - With E2EE, malicious actors do not have the necessary key to access data in transit, so the integrity of data is maintained.
- **Protect from state agencies** - End-to-end encryption is also seen as a technology that secures users' data from snooping by government agencies.

What are the cons of E2EE?

- **Cyber-attacks** - E2EE hinder the government agency's ability to protect citizens from cyber-attacks, violence against children, and terrorism.
- **Inability** - Attempts by government agencies across the globe, in the past, to access encrypted data have met with strong resistance.
- **Criminal activities** - Terrorists and other serious criminals exploited this end-to-end encryption and hide from the law enforcement agencies.
- **Meta data** - End-to-end encryption does not protect metadata which includes information like when a file was created, the date when a message is sent.

References

1. The Hindu | What is end-to-end encryption?
2. Cloud Fare | Learning privacy
3. CIO Insight | Important Pros and Cons