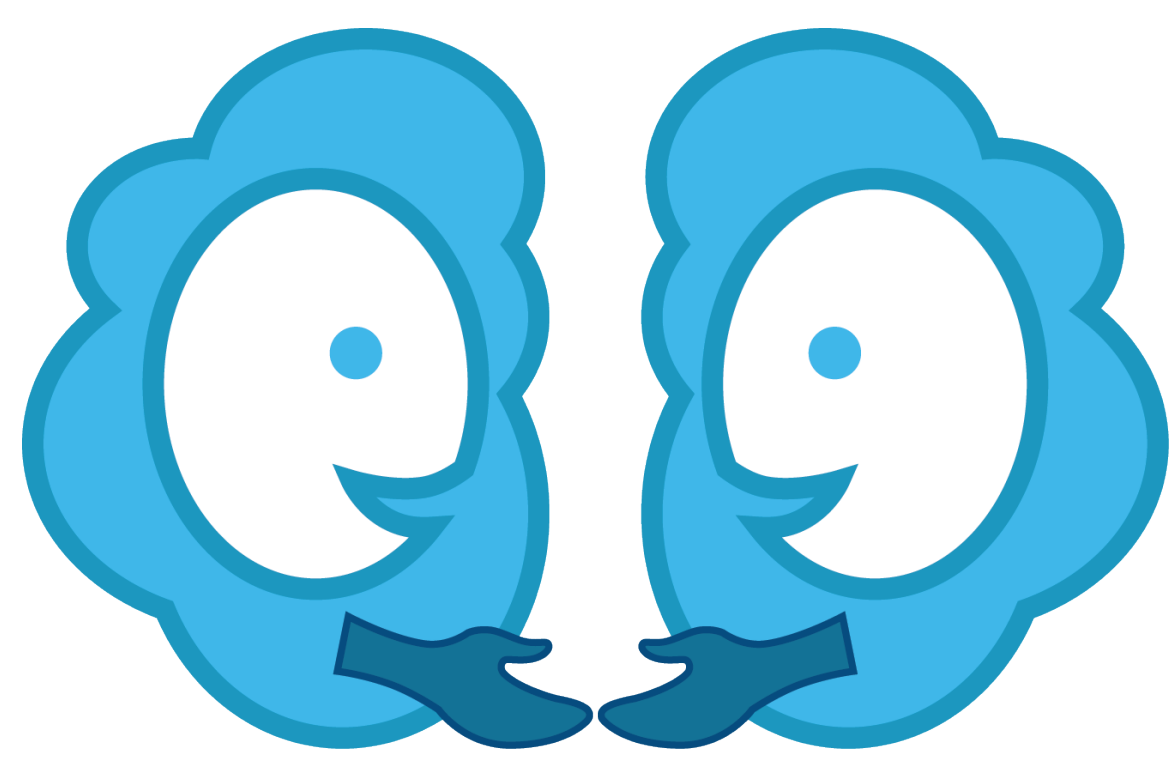


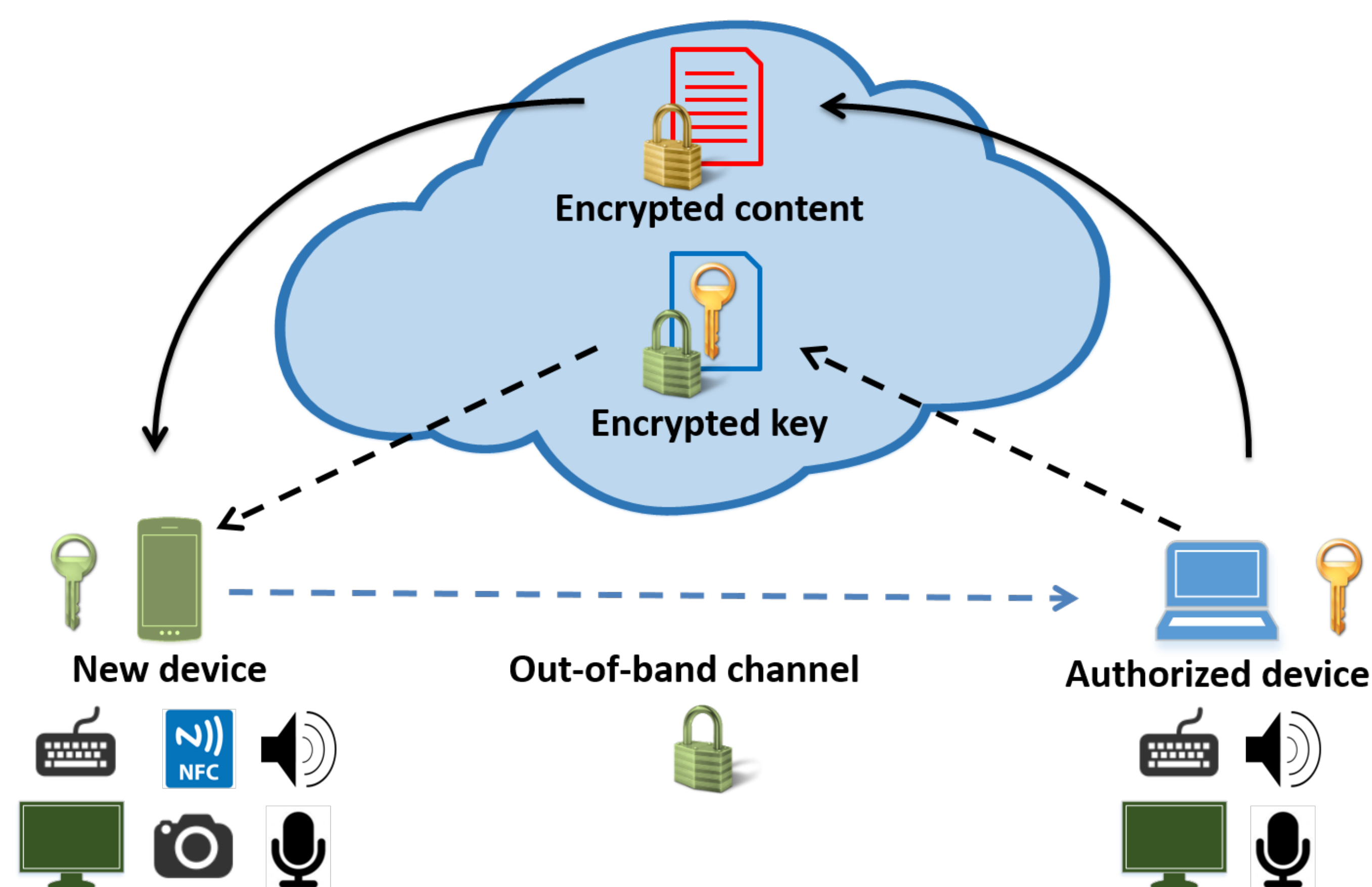
Andrew Paverd, Sandeep Tamrakar, Praveen Pendyala, Thien Duc Nguyen,
N. Asokan, & Ahmad-Reza Sadeghi (*)



OmniShare

Encrypted Cloud Storage For All Your Devices

- To defend against **cloud data breaches** and **insider threats**, your data should be encrypted on-device before being uploaded to the cloud.
- However, all your devices must have the decryption key, so current solutions use **password-derived keys**, which are much easier to guess.
- **OmniShare** combines strong client-side encryption using high-entropy keys, with secure yet intuitive key distribution mechanisms.

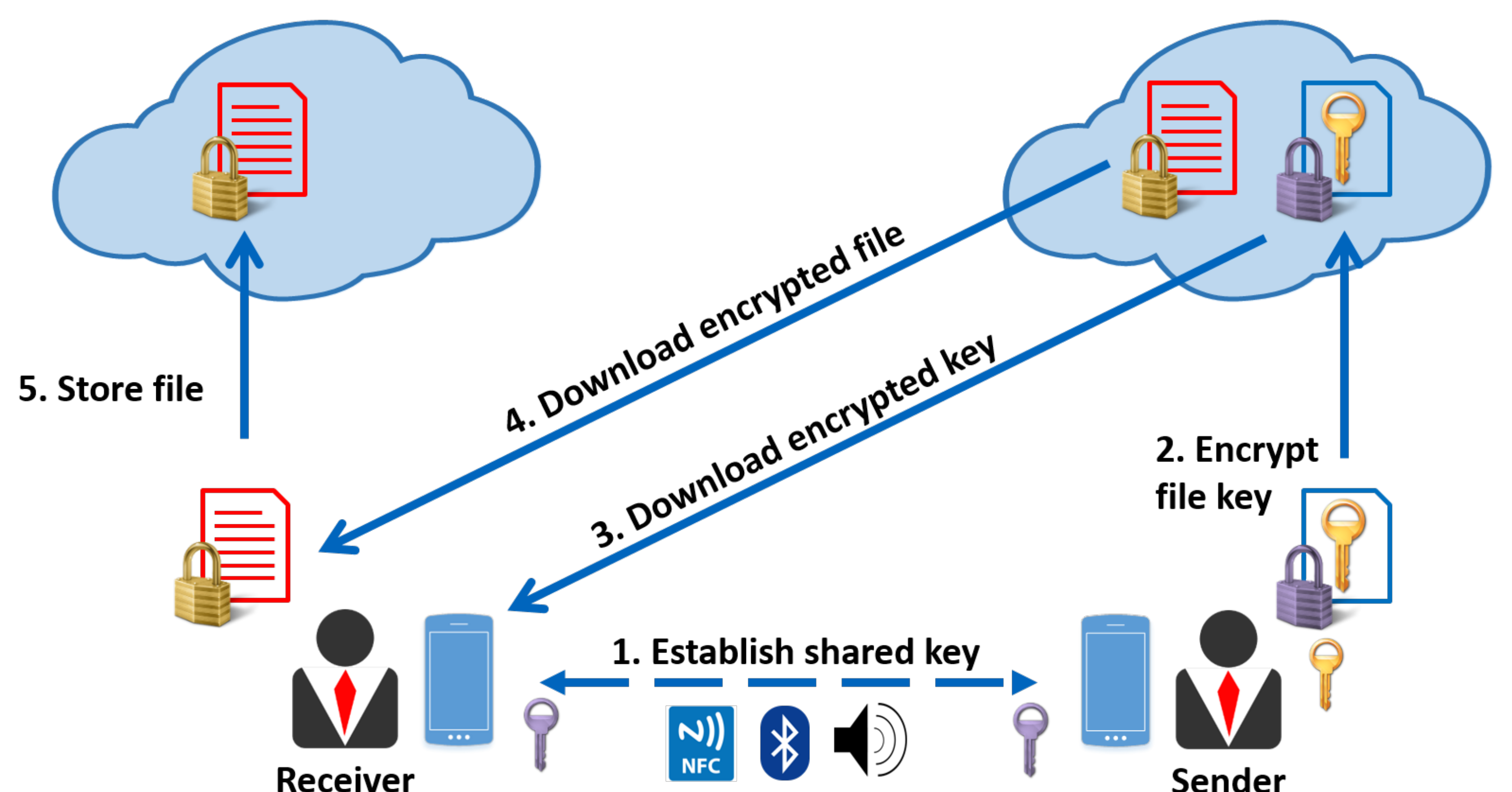


Intuitive Key Distribution

- **Deployable** – Keys distribution via QR codes, Bluetooth, NFC or ultrasonic communication.
- **Usable** – Minimal and consistent user interaction for each channel.
- **Secure** – Keys can be managed by secure hardware or Trusted Execution Environments.

Secure Efficient Sharing

- **Secure** – Shared files remain encrypted.
- **Efficient** – No re-encryption of files.
- **Usable** – Users meet for initial setup but can then share files from anywhere.



(*) The original OmniShare concept was the subject of Long Nguyen's MSc thesis. Binghui Liu and Mihai Bucioiu also contributed to this project. OmniShare was awarded development funding and exhibited at CeBIT 2016 as the winner of the MAPPING app development competition.

