PAROMA-MED

Privacy Aware and Privacy Preserving Distributed and Robust Machine Learning

Detecting&Preventing Data Leaks through Watermarking

A Secure Medical Data Sharing Solution in a Federated Learning Environment

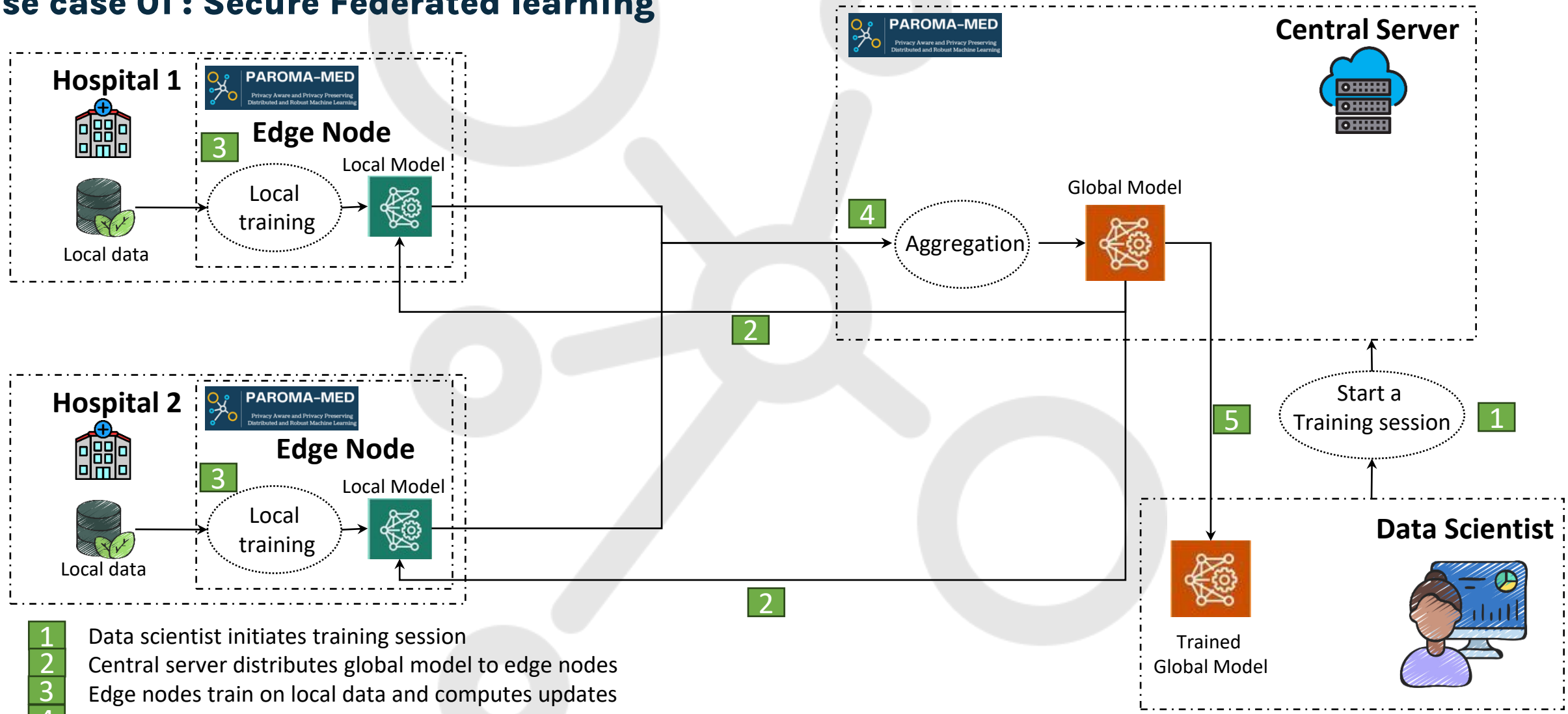
Reda Bellafqira, Gouenou Coatrieux, Chloé Berton.

IMT Atlantique, Inserm, UMR 1101 LaTIM, 29238 Brest, France.

Cross-Talk, 21/10/2024, Brussels, Belgium.

Paroma-Med Framework

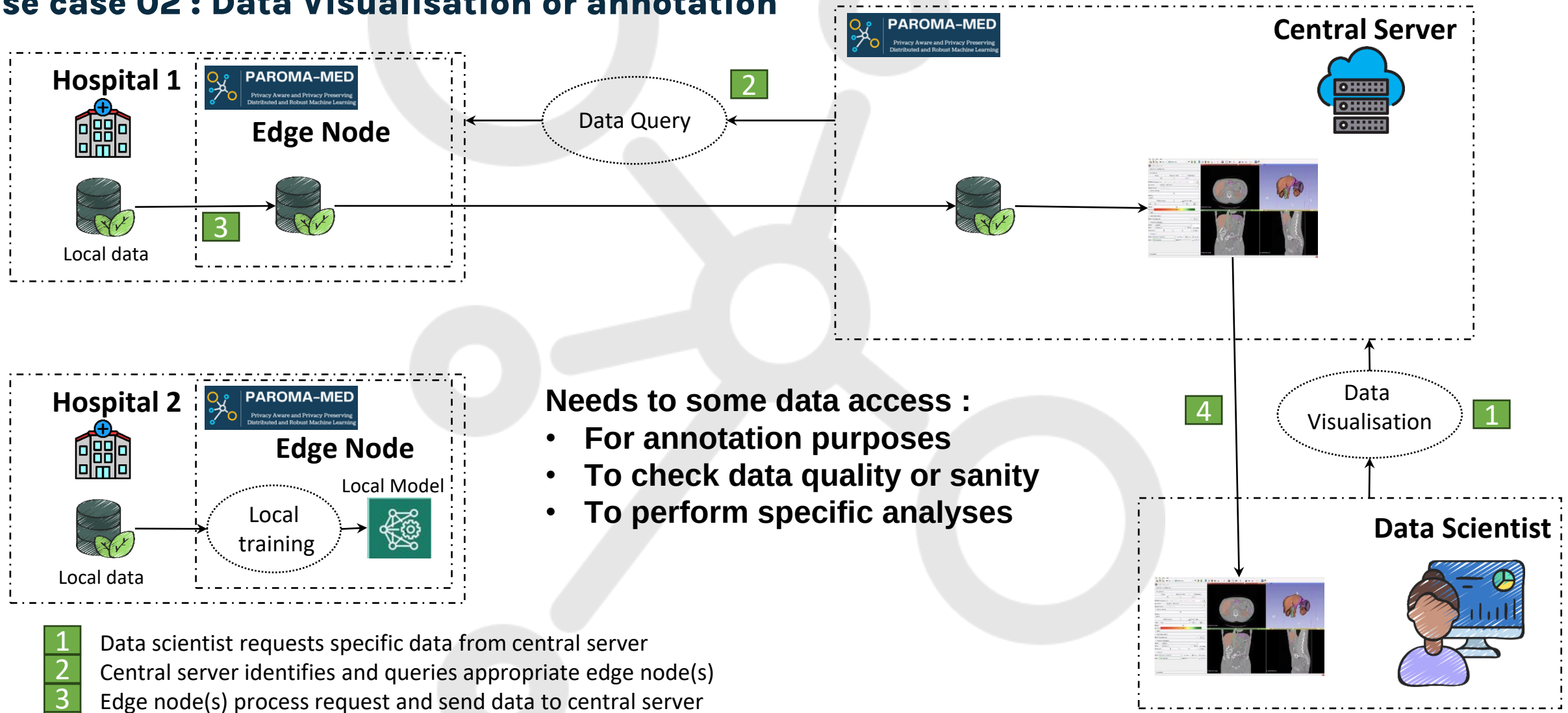
Use case 01 : Secure Federated learning



1. Data scientist initiates training session
2. Central server distributes global model to edge nodes
3. Edge nodes train on local data and computes updates
4. Nodes send updates to central server to aggregate them (Repeat steps 2-5 for multiple rounds)
5. Final global model sent to the data scientist

Paroma-Med Framework

Use case 02 : Data Visualisation or annotation



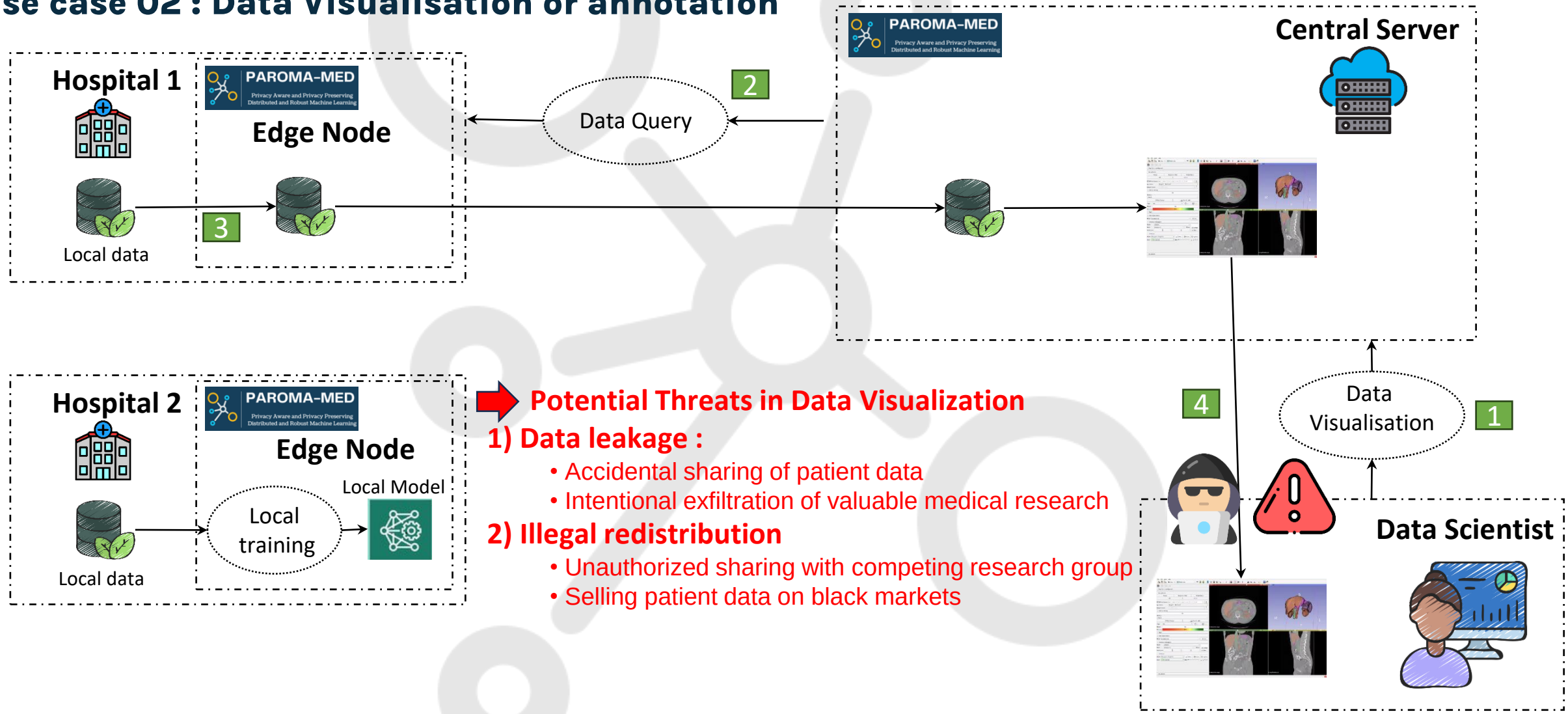
Needs to some data access :

- **For annotation purposes**
- **To check data quality or sanity**
- **To perform specific analyses**

1. Data scientist requests specific data from central server
2. Central server identifies and queries appropriate edge node(s)
3. Edge node(s) process request and send data to central server
4. Central server grants data scientist to visualize data using tools (e.g., Slicer 3D)

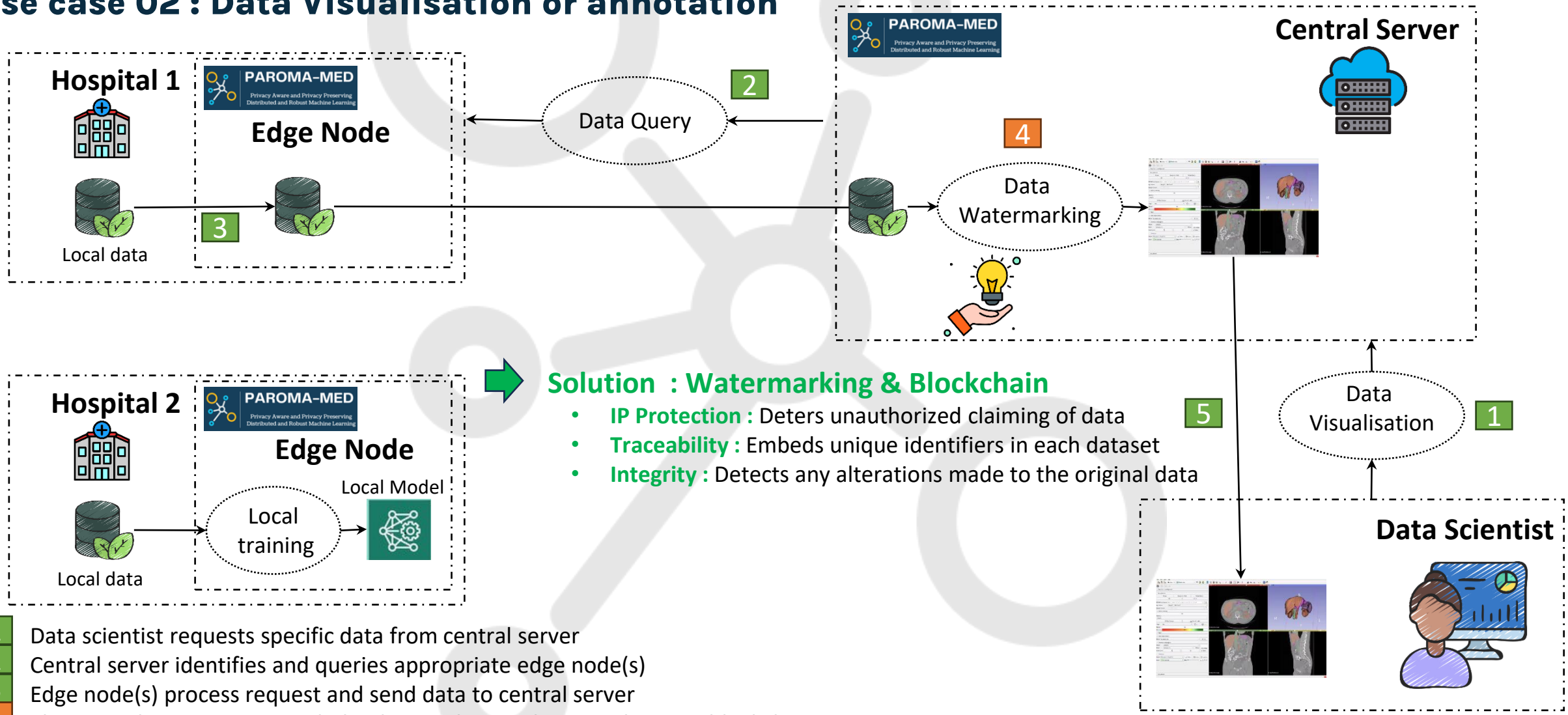
Paroma-Med Framework

Use case 02 : Data Visualisation or annotation



Paroma-Med Framework

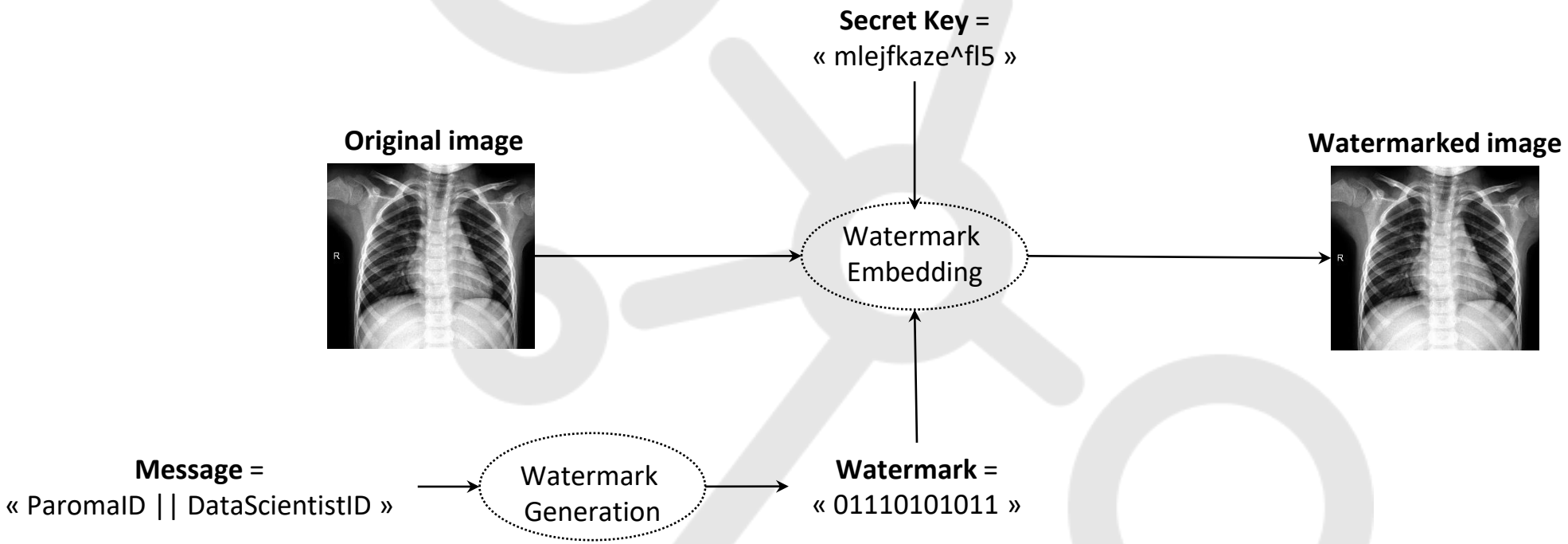
Use case 02 : Data Visualisation or annotation



1. Data scientist requests specific data from central server
2. Central server identifies and queries appropriate edge node(s)
3. Edge node(s) process request and send data to central server
4. **The central server watermark the data and store the metadata in a blockchain**
5. Central server grants data scientist to visualize data using tools (e.g., Slicer 3D)

Principle of image watermarking

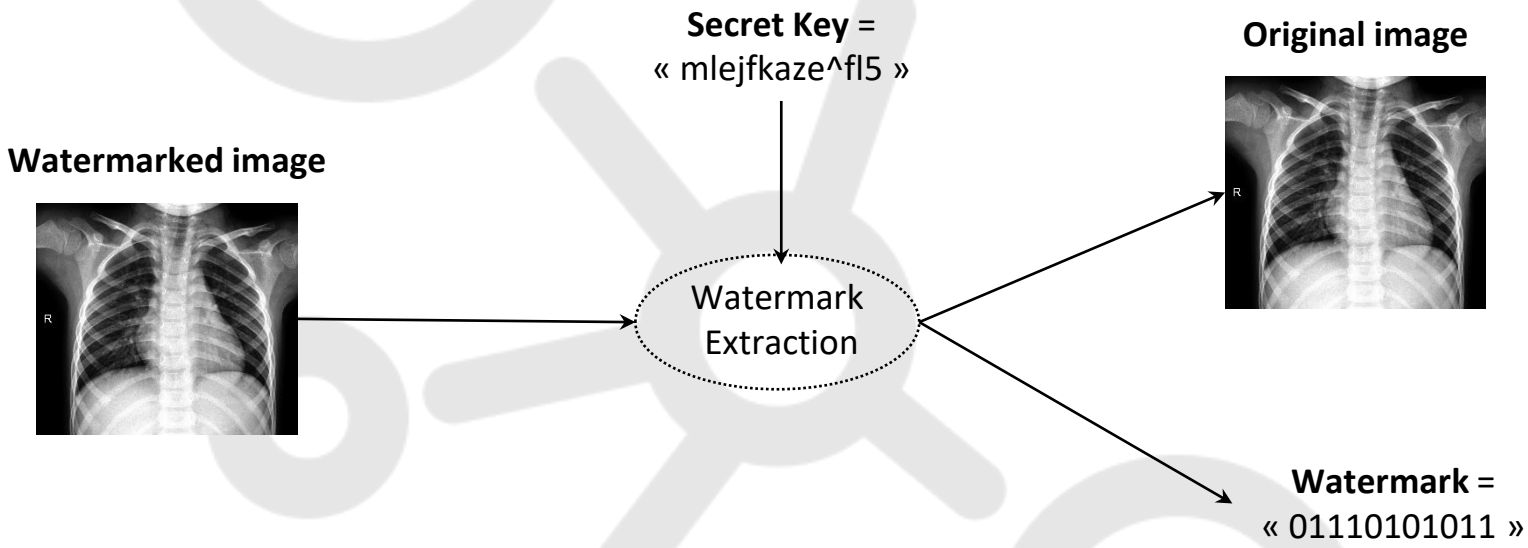
1. Embedding Stage



https://github.com/Bellafqira/histogram_shiffting_predictions

Principle of image watermarking

2. Detection/Extraction Stage



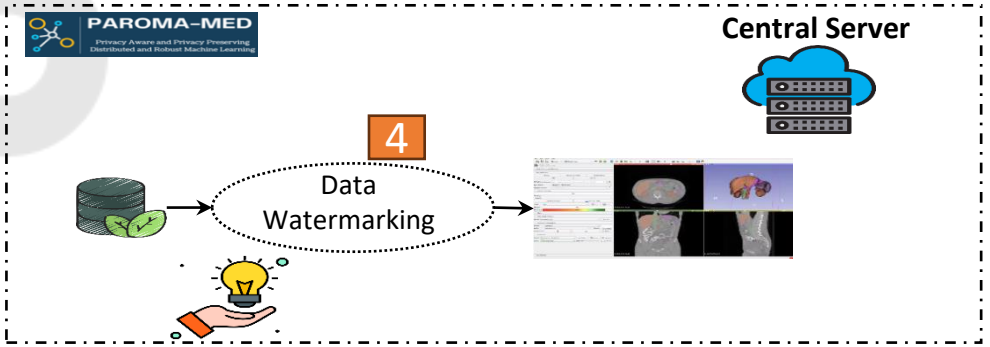
Why Reversible Watermarking?

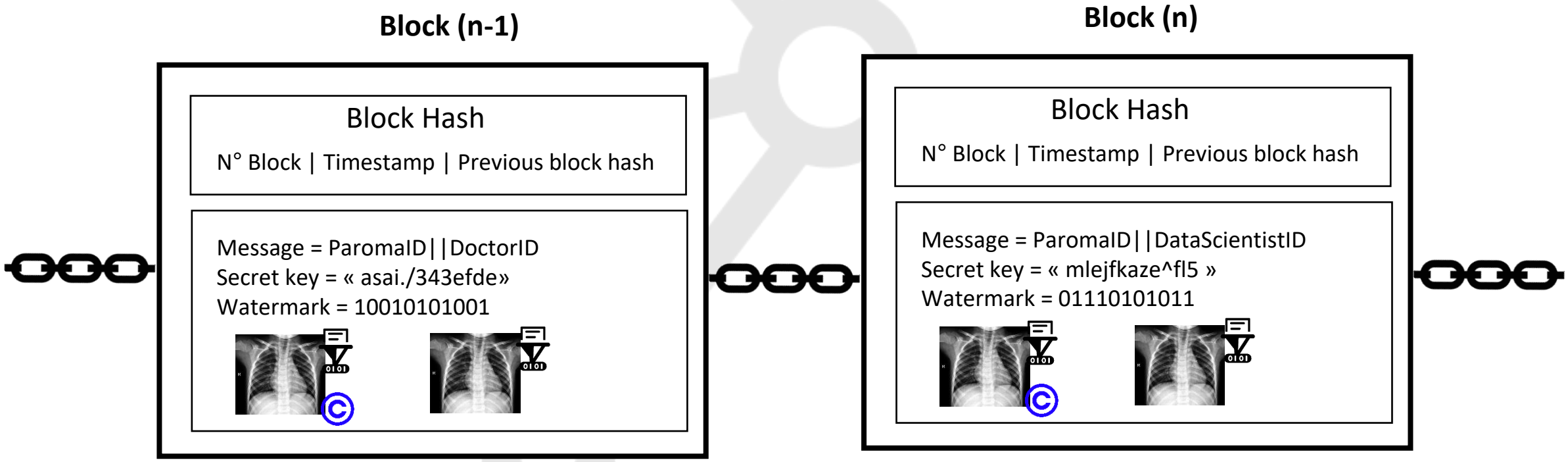
- Preserves data integrity for medical diagnosis and research
- Allows complete removal of the watermark when needed
- Ensures no loss of original data quality
- Critical for maintaining the accuracy of AI model training
- Complies with medical data regulations requiring data preservation

Watermarking & Blockchain

Blockchain Integration Benefits

- Immutable record of all data access and watermarking operations
- Enables quick verification of data ownership and integrity
- Decentralized storage enhances security and reliability
- Supports transparent data sharing in research collaborations

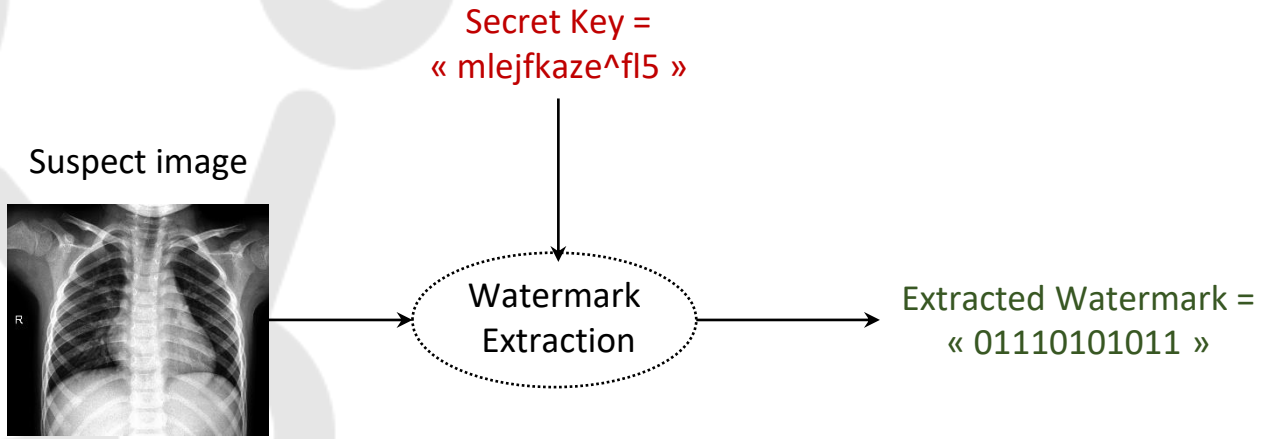




: Hash Function : Watermark

Principle of image watermarking

2. Detection/Extraction Stage



Block (n)

Block Hash

N° Block | Timestamp | Previous block hash

Message = ParomaID||DataScientistID
Secret key = « mlejfkaze^fl5 »
Watermark = 01110101011

1. **Compute the hash of the suspect image**
2. **For each** block in the Blockchain:
    1. If the **computed hash** exists in the current block:
        1. Return the **message** stored in the block
    2. **Extract** the **watermark** from the image using the block's **secret key**
        1. If the **extracted watermark** equals the **watermark in the block**:
            1. Return the **message** in the block
    3. If **no match**, continue to the **next block**
3. If **no matching** block is **found**:
    1. Return "**No watermark detected**"

Demo!

https://github.com/Bellafqira/histogram_shiffting_predictions

Conclusion: Securing Medical Data Sharing

- Watermarking provides robust protection against data leaks and misuse
- Blockchain integration ensures transparency and traceability
- Next steps: Large-scale implementation and real-world testing

Acknowledgement and disclaimer

- This project is funded by the European Union under Grant Agreement 101070222, project PAROMA-MED.

- Views and opinions expressed, are those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission (granting authority). Neither the European Union nor the granting authority can be held responsible for them.

PAROMA-MED partners

EURESCOM

agentscape

ERICSSON

Institut Mines-Télécom

Qualtek
Thinking Forward

THALES
Building a future we can all trust

UBITECH
ubiquitous solutions

UNIVERSITÉ DE RENNES 1

6G Health Institute

PAROMA-MED

Privacy Aware and Privacy Preserving Distributed and Robust Machine Learning

Thank you!

Reda Bellafqira – reda.bellafqira@imt-atlantique.fr