S4 – Privacy-preserving Cloud Data Access

- We had two talks:
  - **Searching Encrypted Data in the Cloud: the Quest for Practical Security**
  - Bernardo Ferreira, Universidade Nova de Lisboa
- and
  - **Architecture-aware privacy-preserving DNA Filtering and Alignment**
  - Paulo Esteves-Veríssimo, University of Luxembourg
- that further evidenced the tension between the need to outsource data processing to the cloud and the non-disclosure requirements of the data owners.
- Both presentations targeted medical data and considered similar threat models: malicious attackers and always curious cloud providers

Bernardo Ferreira

- Bernardo considered **multimodal medical databases** (image, audio and text) stored in untrusted clouds for data search.
- Searchable Preserving Encryption defend against snapshot attackers and partially against cloud providers
- Bernardo's recent research explored **Distant Preserving Encryption** schemes that further defend against the cloud provider by reducing the leakage of search patterns.
- By enabling to outsource much of the computation, DPE allows to leverage the cloud computation power and therefore can be much faster than previous approaches. Both for searching and training...

Paulo Veríssimo

- Paulo taught us about DNA sequences' sensitivity that need to be preserved right from the output of the DNA sequencers
- The presentation led us through standard processing techniques:
  - homomorphic cryptography
  - hashed k-mers
  - cloud burst (unsecure)
- and presented performance results of ongoing work of combining these three techniques into a hybrid **distributed read alignment** approach leveraging a private/public cloud architectures at the core of our community work

Discussion

- Considerations on the state of the art of homomorphic cryptography and what actually is being used as partial homomorphic techniques.