(Relazione da consegnare al Direttore del Dipartimento almeno un mese prima della scadenza annuale del contratto)

Relazione Scientifica Annuale sull'attività svolta nell'ambito dell'assegno di ricerca

Nominativo dell'assegnista di ricerca: Maryam Sepehri

Titolo dell'assegno di ricerca: The implications of Leakages on searchable encryption schemes supporting queries

Specificare se si tratta di assegno di ricerca di tipo A o di tipo B: Type A

Docente referente: Prof. Goffredo Haus

Durata del contratto da June 2018 **a** May 2020

Periodo di riferimento della relazione da May2019 **a** May 2020

Obiettivi della ricerca:

The objectives of the candidate's research are as the following:

- **To optimize exiting Oblivious RAM method for users with large trusted storge in terms bandwidth and delay**

It is possible to recover data if you are able to observe (enough) queries and their responses, even when both the queries and the responses are encrypted and opaque. This is called access leakage. You can even learn a lot from communication volume leakage i.e. how much data is returned. In the case of access leakages, reconstruction attacks are able to recover the secret attribute of every record in the database. Hiding these patterns incurs a high cost making most database systems impractical. For example, Oblivious RAM (ORAM) can hide the access and query pattern, but incurs a logarithmic overhead in the database size, i.e. the larger the database, the slower each ORAM query. To this purpose, the candidate addressed this issue by presenting a low-cost ORAM. The appraoch makes significant contributions as the follows:

- Provides an ptimized a tree-base ORAM algorithm in terns of bandwidth.
- Improves turn-around-time delay for getting/putting buckets from/to data storage server using batch processing model.

- **To create a big data governance platform allows for sensitive data querying without revealing any private information beyond set policies**

The aim is ti enforce policies that apply anonymization when answering queries. The policies are user and data adaptable that are applied on-the-fly during query answering phase. This ensures that only compliant views are retrieved from the users, while maximizing the utility of the answers.

The platform allows for sensitive data querying without revealing any privacy information to users beyond set policies. To this purpose, the candidate addressed this issue by adopting ARX anonymization algorithms for data transformation to fullfill a given privacy model while resulting in maximal utilitty to a given measure. The appraoch makes significant contributions as the follows:

- Creates a platform that applies possible de-identification policies used to transform input dataset while minimizing the loss of infromation.

Risultati della ricerca:

Here, the candidate briefly explain a technique proposed to achieve the mentioned beforehand objectives:

Objective 1: Towards this objective, the candidate applied a bandwidth-efficient ORAM technique called Ring ORAM to the data stored in key-value storage with the assumption that user has large data storage at trusted side. Ring ORAM is the first tree-based ORAM whose bandwidth is independent of the ORAM bucket size, a property that unlocks multiple performance improvements. It also supports client with large storage budget that was one of our assumption for the product. Moreover, she used batch processing to decrease the length of time it takes for a block access to be read from and written to the key-value storage. This work is still under progress and will practically apply to a start-up product as a service.

Objective 2: Towards this objective, the candidate used k-anonymity technique and identified attributes that have less influence on the classification of the data records and suppress them in order to comply with k-anonymity. Further, she assessed the risk of re-identification and estimitating the risk i.e., determining the probability that an intruder would discover the correct identity of a single record. All the experiments have done using ARX anonymization tool.

Attività svolte:

Prodotti della ricerca conseguiti: (in termini di pubblicazioni, brevetti, …)

International Journal

- G. Gianini, S. Cimato, M. Sepehri, E. Damiani, and R. Asad. “A Cryptographic Cloud-based Approach for the Mitigation of the Arline Cargo Cancellation Protection.”, J. Inf. Secur. Appl.51: 102462 , 2020.
(Published)

International Peer-Reviewed Conferences

- B. Kacsmar, B. Khurram, N. Lukas, A. Norton, M. Shafieinejad, Z. Shang, B. Baseri, M. Sepehri, S. Oya, and F. Kerschbaum. Differentially Private Two-Party Set. The 5th IEEE European Symposium on Security and Privacy, Genova, Italy, 2020. (Published)

- M. Sepehri, and F. Kerschbaum. Low-Cost Hiding of the Query Pattern. The 25th European Symposium on Research in Computer Security (ESORICS), 2020. (Submitted)

International School Attendance

- Waterloo.ai Reverse Co-op Natural language Processing”, 17-19 October, 2019, University of Waterloo, Canada.
- ML+Security+Verification Workshop, 26-30 August, 2019, University of Waterloo, Canada.

Ongoing papers

- An Oblivious Proxy-Based Scheme for Equality Query Search on the Cloud.

- Efficient Equality Search over Encrypted Data through a Proxy Server.

Descrizione dell’attività di ricerca svolta all’estero (eventuale; specificare: periodo, luogo, affiliazione):

- Visiting researcher in TandemLaunch Inc., Montreal, Canada (Winter 2020)

The candidate collaborated with a start-up team working on Share, Analyze and Monetize Sensitive Data with the following objectives:

- Researching new cutting-edge privacy techniques and methodologies.
- Optimizing an existing method for privacy provisioning of sensitive data for the purpose of AI and big data analytics.
- Enforcing policies that apply anonymization techniques when answering queries.

Further, she gave two seminars on the invistigation of optimizing PathORAM algorithm in terms of network bandwidth and latency. The aim was to address how to apply an optimized pathORAM algorithm that is called Ring ORAM to the start-up’s product. In addition, she worked with ARX tool to anonymize sensitive personal data. She also got an idea how to develope our last published paper “A proxy-based scheme for fast equality queries over encrypted data” in terms of query processing search on the cloud using a tree-based indexing structure, and how to preserve pattern privacy using Oblivious RAM algorithm.

Note that this visiting opportunity have provided the candidate to see the value of research through a lens of commercial develpement.

La presente relazione, non contiene dati sensibili e dati giudiziari di cui all’art. 4, comma 1, lettere d) ed e) del D.Lgs. 30.6.2003 n. 196.
Si autorizza la pubblicazione della relazione annuale sul sito web del Dipartimento.

Firmato(In Stampatello) NOME **Maryam** COGNOME **Sepehri**

Data **2020–05-04**

Il Responsabile Scientifico

____
(Firma)

L’ Assegnista di Ricerca

M. Sepehri

____
(Firma)