Use of Homomorphic Encryption to protect sensitive data

The internship carried out with the company "Ericsson Telecomunicazioni" in the center of Pagani (Salerno), directed a study and implementation work in the area of cybersecurity for the homomorphic encryption technology. The activity was carried out with the support of a company tutor. The internship was divided into progressive phases of study and analysis, in order to prepare an implementation experimentation phase. The first phase was aimed at learning the techniques necessary for the execution of the basic activity, through the study of the algorithm for homomorphic encryption and evaluated the various libraries that allow to improve data security with the use of this technology. An implementation phase then followed which saw the definition of an operational scenario in which to apply the techniques and systems studied in the first phase. In this context, a comparison of some tools available on the Internet was conducted in order also to identify the one to be used on a real application to be developed. The primary objective pursued throughout the course of the activity was to create two applications with two different encryption technologies, one with homomorphic encryption and one with end-to-end encryption, able to support arithmetic operations and then insert this data into a database, taking into account the execution times to evaluate the efficiency of the two types of encryption. Among the various libraries taken into consideration are to be mentioned: OpenSSL, Concrete, SEAL, Palisade and Lattigo. Palisade was selected for the application that uses homomorphic encryption. I then integrated C ++ applications comparing the performance results with the encryption created with the OpenSSL library. Everything was then integrated with a MySQL back-end creating a database prototype that stores homomorphically encrypted data.
All the objectives foreseen for this work have been designed to improve the skills and the level of autonomy in the definition of software architectures.