Processing a vast volume of data generated by web, mobile and Internet-enabled devices, necessitates a scalable and flexible data management system. Database-as-a-Service (DBaaS) is a new paradigm offered by cloud computing, promising a cost-effective and fully-managed database functionality that flexibly scale to meet the requirements of online data processing. Although there are many benefits to adopt DBaaS, however, it also introduces new threats and vulnerabilities. While many traditional data processing threats remain, DBaaS introduces new challenges such as confidentiality violation and information leakage in the presence of privileged malicious insiders and adds new dimension to the data security. We consider the problem of building a secure DBaaS on top of a public cloud infrastructure where, the Cloud Service Provider (CSP) is not completely trusted by the data owner. We present a high level description of several architectures that combines recent and modern cryptographic primitives to achieve our goal.

In this dissertation, a novel searchable security scheme is proposed to leverage secure query processing in presence of a malicious cloud insider without disclosing sensitive information. A holistic database security scheme comprised of data confidentiality and information leakage prevention is proposed in this dissertation. The main contributions of our work are:

- Searchable security scheme for non-relational databases of the cloud DBaaS;
- Leakage minimization in the untrusted cloud.

The analysis of experiments that employ a set of established cryptographic techniques to protect databases and minimize information leakage, proves that performance of our solution is bounded by communication cost and not cryptographic computation.