

# Security-as-a-Service for Column Oriented NoSQL Databases in Cloud



By

**Faria Mehak**

**NUST2012-60806-MSEECs-61312F**

Supervisor

**Dr. Muhammad Awais Shibli**

**Department of Computing**

A thesis submitted in partial fulfillment of the requirements for the degree  
of Masters in Computer Science (MS CS)

In

School of Electrical Engineering and Computer Science,  
National University of Sciences and Technology (NUST),  
Islamabad, Pakistan.

(February, 2015)



# Abstract

Database-as-a-service (DBaaS) or Database outsourcing in Cloud Computing supports data management on centralized Cloud servers. It provides a wide range of benefits such as multi-tenancy, resource sharing, scalability and many more. DBaaS has garnered a lot of hype, but while it is promising, it is also a mine-field of issues. Many challenges lie ahead in Cloud computing as a whole and in DBaaS model particularly. Security is one of the most critical challenges in this domain, which has only begun to earn the academic attention that it needs. There is a serious lack of research in this area that collectively covers the security of DBaaS, from its various problems to the possible solutions. Moreover, one of the types of Cloud databases is NoSQL (Not only SQL), which have flexible data model and are meant to provide elastic scaling for the management of big data. Such databases are ascertaining growing and significant industry in real-time web 2.0 applications but unfortunately, future generations of NoSQL databases in Cloud environment need considerable enhancement and development to assure secure environment for storing sensitive data.

To that end, we have carried out research in two major folds, where firstly we provide a holistic survey on the security aspects of the Cloud DBaaS, including its key features, advantages and storage architectures for managing data in the Cloud DBaaS. We identify challenges and classify the security limitations in DBaaS paradigm according to CIA (Confidentiality, Integrity, Availability) properties. Security requirements that are being fulfilled by state-of-the-art mechanisms along with their in-depth description are also presented. Additionally, we provide insight to the future security prospects. Our work acts as a comprehensive guideline for both developers and researchers to understand the domain, inherent security issues and the existent countermeasures in the DBaaS domain.

In the second fold of our research, we address major security requirements of column-oriented NoSQL databases in Cloud by proposing a comprehensive

and feasible solution in the form of Security-as-a-Service. Our solution caters the problem of how outsourced data can be secured, how access control can be enforced at fine grained level and how communication can be secured in order to avoid data breaches. Major features provided by our proposed system are secure data storage/retrieval, fine grained column-level access control, effective key management and SSL based secure communication. Granular level authorization (column level) is based on OASIS Extensible Access Control Markup Language (XACML) and Security Assertion Markup Language(SAML) technology as well as Advanced Encryption Standard (AES) based sensitive data at rest encryption has been provided to ensure confidentiality. Cassandra is one of the column-oriented NoSQL database, which is considered as a case study during this research work. Moreover, we have rigorously evaluated our work through different test scenarios as well as using security evaluation tool AVISPA which helped us to analyze the security aspects of the developed system.

