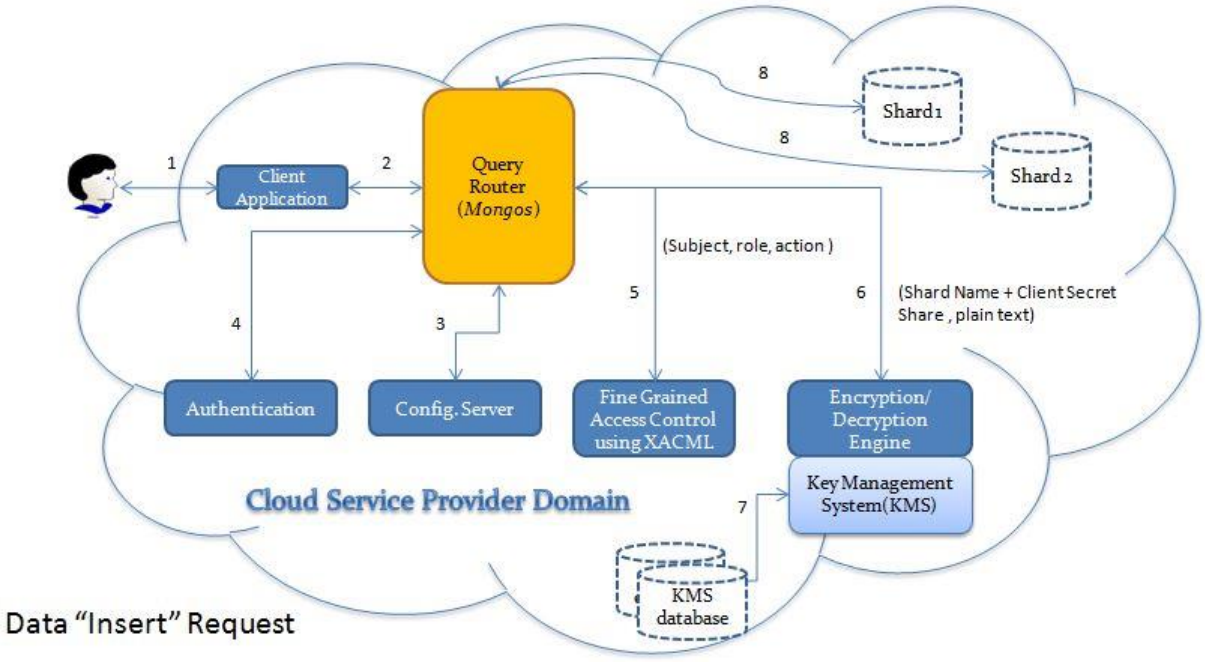
Research Title: Secure Sharding and Key management in Cloud based NoSQL database

Summary

NoSQL data stores are non-relational databases specially designed to provide high availability, reliability and scalability with big data processing capabilities. Additionally, sharding is one of the main advantages of NoSQL databases. Database Sharding is a highly scalable approach for improving the throughput and overall performance of high-transaction, large database-centric business applications hosted specially on Cloud platform. These sharded NoSQL databases when deployed on Cloud as Database as a Service (DBaaS) service model impose challenges of security and privacy besides managing their own core functionalities.

In our thesis, we have explored and addressed above mentioned issues by first structuring the knowledge in the domain of Sharded Cloud databases into a well organized taxonomy. Secondly, we have made use of the concept of secure NoSQL sharding to horizontally scale large amount of data securely among various nodes or shards on Cloud platform. Sharded data needs to be protected using various security controls of confidentiality and data protection. Particularly, the security controls like data encryption, key management and access controls are the critical requirements of many regulatory compliance like HIPAA_HITECH, PCI_DSS, FERPA and EU data Protection Directive etc. In this thesis, we have proposed secure sharding architecture of NoSQL database MongoDB, which makes use of encryption scheme to encrypt chunks of data before saving it into the shard while keeping track of their encryption keys efficiently. Moreover, attribute based fine grained access control is implemented for guaranteed data integrity and authorized access in the Cloud environment. Our model has also performed automatic key management of the cryptographic keys produced and saved on our platform. Hence, our proposed method has helped the NoSQL databases to provide data confidentiality to its users while providing high throughput due to sharding capabilities.



Data "Insert" Request