



ECHAHID HAMMA LAKHDAR UNIVERSITY - EL-OUED
Under the Supervision of the **DGRSDT** and in collaboration with the **CRTI**
International Pluridisciplinary PhD Meeting (IPPM'20)
23-26, 2020 1st Edition, February
Theme: Modern Technology and Fineness Life



Secure management of autonomous cloud entities in a distributed system

Student: Mr. Kara Mostefa

Thesis Director: Dr. Laouid Abdelkader MCA Univ Eloued

Co-director: Dr. Ahcène Bounceur HDR UBO

Exact Sciences Faculty, Computer Sciences Department
Operator theory laboratory and its applications (LABTHOP)
El-Oued University, Algeria

Email: karamostefa@univ-eloued.dz

Abstract

In recent years, Cloud Computing and Big Data have been considered as the most attractive areas that are revolutionizing the IT world. Cloud Computing paradigm has recently appeared that allows running proprietary or difficult portable applications outside their original software environment on one or more virtual hardware platforms.

Therefore, we are to developing such techniques which makes it possible to secure communication between the communicating Cloud entities. These techniques must take into account several factors due to the data transmitted in this type of environment is proprietary and of significant size. Conventional data security techniques are not suitable for today's cloud usage. Hence, the main research of this thesis is to define an adaptable architecture with the aim to propose a scalable system that supports cloud services.

The main objective of this thesis is to define feasible security solutions dedicated to the Cloud computing context in order to robustly protect data stored in the Cloud. We are more precisely looking for working on NoSQL databases.

Keywords: Cloud Computing, Data Protection, Secure Communication, Middleware, Protocols

Approach

The data Security process goes through many steps, starting from access control (Authentication, Authorization, and Audit) by using different mechanisms (LDAP, PKI and roles management) and ending with our main interest which is data encryption in storage.

Most of NoSQL data bases don't support any security function integration, despite the fact that there are other data bases that uses techniques such as « Transparent Data Encryption (TDE) » and « Third Party Storage Encryption » (e.g Linux Unified Key Setup, IBM Guardium Data Encryption, Vormetric Data Security Platform, Bitlocker Drive Encryption), which applies an encryption approaches; whether Symmetric (DES and AES Algorithms) or Asymmetric (RSA Algorithm).

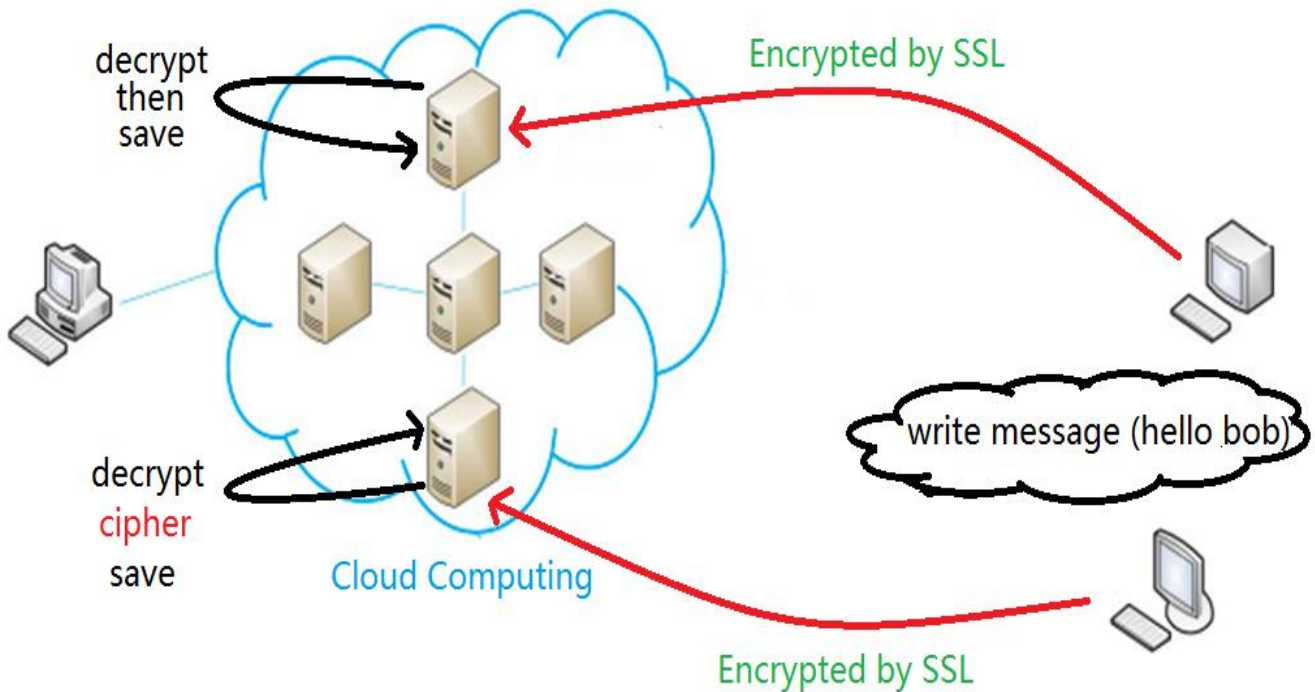
Based on these techniques and approaches, this work attempts to develop another approach that is more confidential and more robust against attacks.

Obstacles encountered

The difference between traditional and NoSQL DB shows several obstacles:

- The kind of NoSQL DB types (key-value, document-oriented, column-oriented, graph-oriented) :
- The choice of which one of these types we will working on.
- NoSQL DB is designed to provide real-time performance while managing a large amount of data poses a challenge for encryption operations.
- NoSQL DB couldn't assure ACID properties (atomicity, consistency, isolation and durability).
- Few open source NoSQL DB available.

Graphical Abstract



References

- [1] Stergiou, Christos, et al. "Secure integration of IoT and cloud computing." *Future Generation Computer Systems* 78 (2018): 964-975.
- [2] Balmakhtar, Marouane, Carl J. Persson, and Arun Rajagopal. "Secure cloud computing framework." U.S. Patent Application No. 10/243,959.
- [3] Oppermann, Alexander, et al. "Secure cloud computing: Reference architecture for measuring instrument under legal control." *Security and Privacy* 1.3 (2018): e18.
- [4] Darwazeh, Nour S., Raad S. Al-Qassas, and Fahd AlDosari. "A secure cloud computing model based on data classification." *Procedia Computer Science* 52 (2015): 1153-1158.
- [5] Benzekki, Kamal, Abdeslam El Fergougui, and E. A. Elbelrhiti. "A secure cloud computing architecture using homomorphic encryption." *International Journal of Advanced Computer Science and Applications (IJACSA)* 7.2 (2016): 293-298.
- [6] Carroll, Mariana, Alta Van Der Merwe, and Paula Kotze. "Secure cloud computing: Benefits, risks and controls." *2011 Information Security for South Africa*. IEEE, 2011.
- [7] Bugiel, Sven, et al. "Twin clouds: An architecture for secure cloud computing." *Workshop on Cryptography and Security in Clouds (WCSC 2011)*. Vol. 1217889. 2011.
- [8] Yagoub, Mohammed Amine, et al. "An Intelligent Cloud Data Protection Technique Based on Multi Agent System Using Advanced Cryptographic Algorithms." *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*. ACM, 2019.