Safe Control of Autonomous Cloud Entities in Distributed Systems

Mostefa Kara
LIAP Laboratory, University of El Oued, PO Box 789, El Oued 39000, El Oued, Algeria
E-mail: karamostefa@univ-eloued.dz
International Pluridisciplinary PhD Meeting (IPPM)
ECHAHID HAMMA LAKHDAR UNIVERSITY - EL-OUED

January 29, 2023

Abstract

In recent years, Cloud Computing and Big Data have been considered 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 make 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.

We will 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. We also intend to propose a secure solution based on the blockchain that has powerful features like decentralization, autonomy, security, reliability, and transparency.

keywords : Cloud Computing, Data Protection, Secure Communication, Middleware, Protocols.

1 Introduction

The Internet revolution and the increasingly massive creation of data in digital form facilitate communications and exchanges and therefore weaken the information stored.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 January 2023 doi:10.20944/preprints202301.0335.v2

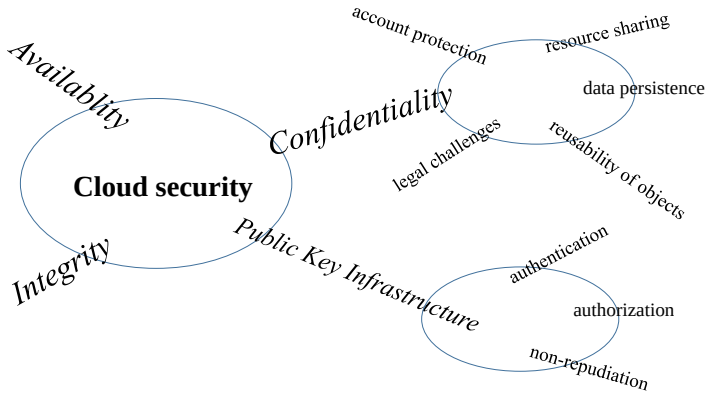

Figure 1: Cloud security

Indeed, public networks including distributed systems and cloud computing create security breaches also in terms of privacy and it is more manageable for an attacker to access data [1–4]. Similarly, the replacement of human beings by machines and programs makes relations much more anonymous even though access to this information requires strong authentication methods [5, 6].

In addition, the dematerialization and creation of other means of legal proof such as digital signatures instead of handwritten ones, all contributed to the increase in these security breaches. Thus, the digital revolution in the world of communication and information has opened many areas of security investigation as our daily lives have been invaded by smart cards, banking transactions, internet, mobile phone, etc.

There are many techniques to combat attacks targeting information in general and personal life in particular. These techniques are distributed on different levels such as networks, applications, storage devices, etc. However, one of the most important means of protection remains to keep this data with its original owner. The great development of technology such as IoT, cloud, speed of the internet, and the opening of the world to some of it led to the production of a huge amount of data, which led to the need to store data in a place other than the place of its production, we mean usually the Cloud.

2 Approach

Security is an important part of many areas [7–10]. 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 NoSQL databases don't support any security function integration, despite the fact that there are other databases that use 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 approach; whether Symmetric (DES and AES Algorithms) or Asym-

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 January 2023 doi:10.20944/preprints202301.0335.v2

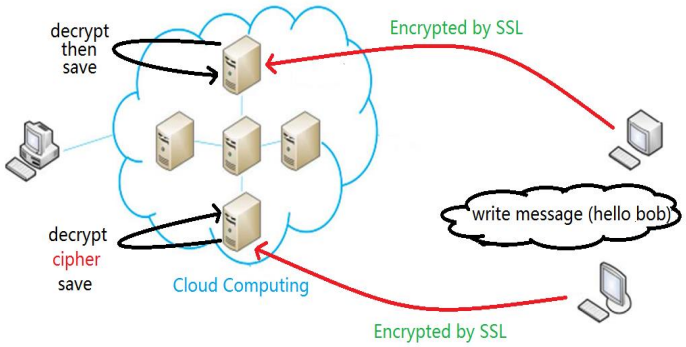

Figure 2: Data Encryption-Decryption in cloud computing

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

3 Encountered obstacles

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 be 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 sources NoSQL DB available.

4 Model

When this data is personal or sensitive, the cloud cannot be trusted and the client can not store data in a readable way (in clair), so the client will have to encrypt it. On the other hand, the client not only uses storage service but may ask the cloud to perform operations on this encrypted data such as addition and multiplication. It is obvious to know that not any encryption method will allow these operations to be performed, meaning that the cloud entities will ask the client to decrypt the data before performing the operation, and this is exactly what happens with the classic encryption methods.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 January 2023 doi:10.20944/preprints202301.0335.v2

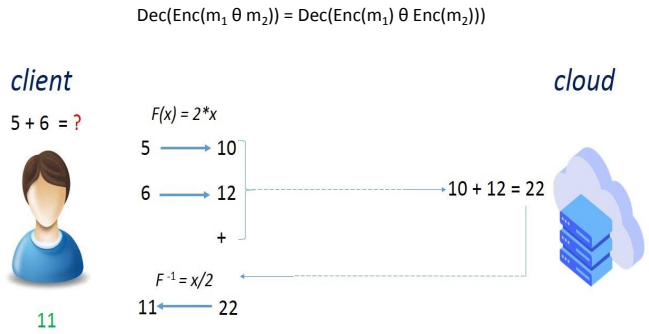

Figure 3: Homomorphic encryption

That is, the cloud entities are not autonomous, and therefore privacy cannot be preserved.

In our work, we want to add autonomy to the cloud entities and make them process the encrypted data without the need to decrypt it by its original owner, which is called homomorphic encryption [11, 12]. On the other hand, distributed systems may suffer, whether at the level of IoT or at the level of cloud entities, from some security problems that homomorphic cannot solve, such as domination, when these systems depend on the current leading technology in collecting and storing data, which is the blockchain. In order to raise the level of security in the cloud and distributed systems in terms of collecting and storing data, as well as giving autonomy, flexibility, and confidence to the cloud entities, we will develop security mechanisms using blockchain. Therefore,

This solution consists in developing consensus algorithms [13–15] that can be used in many domains [16, 17].

References

[1] N. S. Darwazeh, R. S. Al-Qassas, F. AlDosari *et al.*, "A secure cloud computing model based on data classification," *Procedia Computer Science*, vol. 52, pp. 1153–1158, 2015.

[2] A. Oppermann, F. G. Toro, F. Thiel, and J.-P. Seifert, "Secure cloud computing: Reference architecture for measuring instrument under legal control," *Security and Privacy*, vol. 1, no. 3, p. e18, 2018.

[3] A. E. Youssef and M. Alageel, "A framework for secure cloud computing," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 4, p. 487, 2012.

[4] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of iot and cloud computing," *Future Generation Computer Systems*, vol. 78, pp. 964–975, 2018.

[5] M. Kara, A. Laouid, M. AlShaikh, A. Bounceur, and M. Hammoudeh, "Secure key exchange against man-in-the-middle attack: Modified diffie-hellman protocol," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, vol. 7, no. 3, pp. 380–387, 2021.

[6] M. KARA, A. LAOUID, A. BOUNCEUR, M. HAMMOUDEH, and M. ALSHAIKH, "Perfect confidentiality through unconditionally secure homomorphic encryption using otp with a single pre-shared key," *Journal of Information Science and Engineering*, vol. 39, no. 1, pp. 183–195, 2023.

[7] M. Kara, A. Laouid, A. Bounceur, M. Hammoudeh, M. Alshaikh, and R. Kebache, "Semi-decentralized model for drone collaboration on secure measurement of positions," in *The 5th International Conference on Future Networks & Distributed Systems*, 2021, pp. 64–69.

[8] M. E. Kahla, M. Beggas, A. Laouid, M. Kara, and M. AlShaikh, "Asymmetric image encryption based on twin message fusion," in *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)*. IEEE, 2021, pp. 1–5.

[9] A. Habib, A. Laouid, and M. Kara, "Secure consensus clock synchronization in wireless sensor networks," in *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)*. IEEE, 2021, pp. 1–6.

[10] K. Chait, A. Laouid, L. Laouamer, and M. Kara, "A multi-key based lightweight additive homomorphic encryption scheme," in *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)*. IEEE, 2021, pp. 1–6.

[11] M. Kara, A. Laouid, M. A. Yagoub, R. Euler, S. Medileh, M. Hammoudeh, A. Eleyan, and A. Bounceur, "A fully homomorphic encryption based on magic number fragmentation and el-gamal encryption: Smart healthcare use case," *Expert Systems*, vol. 39, no. 5, p. e12767, 2022.

[12] M. Kara, A. Laouid, R. Euler, M. A. Yagoub, A. Bounceur, M. Hammoudeh, and S. Medileh, "A homomorphic digit fragmentation encryption scheme based on the polynomial reconstruction problem," in *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*, 2020, pp. 1–6.

[13] M. Kara, A. Laouid, M. Hammoudeh, M. Alshaikh, and A. Bounceur, "Proof of chance: A lightweight consensus algorithm for the internet of things," *IEEE Transactions on Industrial Informatics*, 2022.

[14] M. Kara, A. Laouid, A. Bounceur, F. Lalem, M. AlShaikh, R. Kebache, and Z. Sayah, "A novel delegated proof of work consensus protocol," in *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)*. IEEE, 2021, pp. 1–7.

 doi:10.20944/preprints202301.0335.v2

[15] M. Kara, A. Laouid, M. AlShaikh, M. Hammoudeh, A. Bounceur, R. Euler, A. Amamra, and B. Laouid, "A compute and wait in pow (cw-pow) consensus algorithm for preserving energy consumption," *Applied Sciences*, vol. 11, no. 15, p. 6750, 2021.

[16] M. Kara, A. Laouid, A. Bounceur, and M. Hammoudeh, "Secure clock synchronization protocol in wireless sensor networks," 2023.

[17] M. Kara, "A lightweight clock synchronization technique for wireless sensor networks: A randomization-based secure approach," 2023.