# Data Alteration: A Better Approach to Securing Cloud Data with Encryption

Sara Rhazlane[*,**] , Amina El Ouazzani[*], Nouria Harbi[**], Nadia Kabachi[**], Hassan Badir[*]

[*]LabTIC laboratory, ENSA Tanger, Abdelmalek Essaadi University, Tangier, Morroco
sara.rhazlane@eric.univ-lyon2.fr ; a.elouazzani2000@gmail.com
hbadir@uae.ac.ma
[**]ERIC Laboratory, University of Lyon, Lyon 2, France
nouria.harbi@univ-lyon2.fr ; nadia.kabachi@univ-lyon1.fr

**Abstract.** With the emergence of new technologies and the ubiquitous connectivity, large amounts of data are being generated everyday with the need to be stored properly and explored rapidly. In this context, the cloud computing services have been adopted to face these rising challenges. But in a cloud environment, data and the application are controlled by the service provider and the customer does not always have the possibility to increase the security level imposed. This leads users to apply encryption mechanisms before storing their data in the cloud. In this paper we propose a new approach that combines the strengths of both steganography and cryptography called Data Alteration. The technique aims to hide the data by modifying it completely as it remains readable, meaningful and therefore shows no suspicions to malicious cloud providers and pirates. The proposed appoach was implemented in Java and tested on realistic datasets in a multi agent systems based architecture.

## 1 Introduction

Every day quintillion bytes of data are generated and transferred due to the fast-growing number of users connected, and yet constantly increasing. With this rising amount of data, comes the need for storage solutions and affordable large capacity servers. One of the solutions is using a cloud computing environment. However, the challenge is how to analyze and interpret this data in a secure manner, more specifically securing the data itself. When storing data on cloud servers, two security concerns raises: First, the risk of a data misuse from an untrustworthy cloud provider and secondly, the attempt from the attackers and the hackers to collect sensitive information. Customers sometimes decide to entrust sensitive data as well as strategic ones to cloud service providers, that is why they usually have a policy of security and confidentiality encompassing all these data and the flexibility available to the client for securing its data can be limited by the nature of the proposed offer. Moreover, the data being accessed via Internet, hacking risks are more present than on local use.

In order to ensure the confidentiality and security of data stored in the cloud, several solutions have been proposed in the literature, Abdul Alsahib S.Aldeen et al. (2015). The most common solutions to address these concerns and benefit from the potential of cloud while having visibility and control over data privacy, are cryptography and steganography, Zielinska et al. (2012). However, both of them have their weaknesses. Steganography fails when the malicious user is able to access the content of the cipher message, while cryptography fails when the user detects that there is a secret message present in the steganography medium.

Therefore, we present in this paper a proposal that can be considered as a first step to implementing a privacy preserving solution for hosted data in the cloud. The solution proposes a new encryption approach combining the strengths of both steganography and cryptography, that could change the actual data by preserving their type while changing their value: The Alteration. The goal here is to give hackers an illusion on the veracity of the data and thus reduce the risk of piracy.

Our work will be structured as follows: in section 2, we will start our proposal with an explanatory state of the art and discussion of research studies related to this work. This section will be followed by a detailed description of our global architecture and contribution accompanied by a performance test and the results of our proposal detailed in section 4 , and finally conclusions and prospects.

# 2 State of the art and synthesis

With the rapid development of cloud technologies, more and more multimedia data (text, video, image, sound) are generated and transmitted in the medical, educational, commercial and other private sectors, that may include sensitive information which should be secured. The communication media through which we send data does not provide data security mechanisms and concerns about security risks remain the main barrier to cloud adoption by companies regarding the fact that data is distributed over individual computers in different geographical storage locations and the risk of data misuse is constant.

These security issues represent real concerns for companies, which find it an obligation to seek for effective solutions, particularly the implementation of encryption solutions. Over the last few years, several data security solutions have been proposed. The table below (Table 1) shows recent works and solutions that has been proposed in the field of data security in the cloud computing environment.

## 2.1 Data protection and security solutions in the Cloud

In 2016, the authors in G.Korde (2016) propose a new method based on the combination of both cryptography and steganography known as Crypto-Steganography. The algorithm that has been implemented hide first the input message in an image called "Stego image", and then encrypt the stego image using a cryptography technique. In the same year, Kini et al. (2016) provide an efficient data hiding technique and image encryption in which the data and the image can be retrieved independently. The aim or objective of the project was to overcome the existing system of watermarking by implementing a reversible data hiding technique in encrypted images.

In 2013, Singla and Singh (2013) deals with the methods of providing security using data encryption and ensuring that an unauthorized intruder can't access your file or data in the cloud. Data is encrypted by a symmetric block cipher cryptography algorithm called "Rijndael" before being stored in a cloud environment. Sachdev and Bhansali (2013) use the same approach but

| Author | Paper's title | Date of publication |
|---|---|---|
| Aparna G.Korde | Crypto-Steganography :An Information Security Tool for a Cloud Environment | 2016 |
| Kirti Kini, Meera Mithani, Rinali Naik, Divyata Raut and M.K. Kumbar | Securing Cloud Data using Crypto-Stegno based Technique | 2016 |
| Sanjoli Singla and Jasmeet Singh | Implementing Cloud Data Security by Encryption using Rijndael Algorithm | 2013 |
| Abha Sachdev and Mohit Bhansali | Enhancing Cloud Computing Security using AES Algorithm | 2013 |
| Deyan Chen and Hong Zhao | Data Security and Privacy Protection Issues in Cloud Computing | 2012 |
| Uma Somani, Kanika Lakhani and Manish Mundra | Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing | 2010 |
| Zunera Jalil and Anwar M. Mirza | A Review of Digital Watermarking Techniques for Text Documents | 2009 |

TAB. 1 – *Table summary of the recent proposed data security solutions.*

data is encrypted using "Advanced Encryption Standard (AES)" before being launched in the cloud.

In 2012, the authors in Chen and Zhao (2012) provide a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle.

In 2010, the authors in Somani et al. (2010) tried to assess cloud storage methodology and data security in the cloud by the implementation of digital signature with the "RSA" cryptography algorithm. In 2009, Jalil and Mirza (2009) discussed in a review the main contributions, advantages and drawbacks of different past methods used for text watermarking. Through this table it appears that the much used techniques in the data security field, proposed in the literature are:

— Cryptography: the science of using mathematics to encrypt and decrypt data. Cryptography enables to store or transmit sensitive information across insecure networks in a way that cannot be read by anyone except the intended recipient.
— Steganography: is an ancient art and practice, it is a branch of information hiding and its main goal is to communicate or transmit data securely in a completely undetectable manner. This practice hides messages within other messages in order to conceal the existence of the original message.
— Watermarking: is a method to achieve the copyright protection of multimedia contents. Because the multimedia presents several types of content such as text, image, video, audio, and graphic content, and they reveal very different characteristics in hiding information inside them, different watermarking algorithms appropriate to each of them should be developed, Jalil and Mirza (2009).

## 2.2 Comparison and analysis between Cryptography, Steganography and Watermarking

Cryptography hides the contents of the message from an attacker, but not the existence of the message. Steganography/watermarking techniques even hide the very existence of the message in the communicating data.

Steganography is often confused with cryptography, due to their common purpose of providing confidentiality. The difference becomes visible once the etymology of these words is known. Steganography is derived from the Greek: "covered writing", whereas cryptography stands for "secret writing". While the first describes the techniques to create a hidden communication channel, the latter is a designation of ongoing overt message exchange where the informative content is unintelligible to unauthorized parties and even hide the very existence of the message in the communicating data. Table 1 in Zielinska et al. (2012) summarizes the differences between cryptography and steganography.

Steganography and watermarking bring a variety of techniques on how to hide important information in an undetectable and/or irremovable way, in audio and video data. They are main parts of the fast developing area of information hiding.

In watermarking the important information is in the cover data, the embedded data is added for protection of the cover data. While in steganography the cover data is not important, it mostly serves as a diversion from the most important information that is in embedded data. Steganography tools typically hide relatively large blocks of information while watermarking tools place/hide less information in images or sounds.

In comparison to watermarking, the main goal of steganography is to hide a message *m* in some audio or video (cover) data *d*, to obtain new data *d'* practically indistinguishable from d, in such a way that an eavesdropper cannot **detect** the presence of *m* in *d'*.

The main goal of watermarking is to hide a message *m* in some audio or video (cover) data *d*, to obtain new data *d'* practically indistinguishable from *d*, in such a way that an eavesdropper cannot **remove or replace** the presence of *m* in *d'*. Table 2 in Zielinska et al. (2012) summarizes the differences between watermarking and steganography.

## 2.3 Discussion

As mentioned above, encryption is the process of converting plain text "unhidden" to a cryptic text "hidden" to secure it against data thieves. This process has another part where cryptic text needs to be decrypted on the other end to be understood. The majority of encryption algorithms converts plain text to cipher text in which we lose the data type to get crypted text. This solution is certainly effective but has its limits. Indeed, the data obtained after encryption is unreadable and therefore attracts the attention of hackers, so hardened to be able to decipher it.

Among all the text steganography methods, each one has respective capability to hide data in text. However, if those algorithms are found or if data is examined by a smart detector then the hidden data can be found and security destroyed.

On the other hand, watermarking main benefits are in copyright protection and related issues. It gives an idea about the possible unauthorized replication and manipulation of electronic data. It can protect the intellectual property rights specifically the digital rights management systems necessities. Also, the amount of work done on text watermarking is very limited and specific. Text watermarking algorithms using binary text image are not robust against reproduction attacks and have limited applicability. Similarly, text watermarking using text syntactic and semantic structure is not robust against attacks, with limited applicability and usability. Watermarking techniques are computationally expensive and non-robust and efficient text watermarking algorithms are still required.

After analyzing all these methods, from different limits observed, none of these solutions offers a possibility to "*alter*" the data, neither cryptography, steganography nor watermarking are suitable for our purpose. Cryptography fails when the malicious user is able to access the content of the encrypted message, while Steganography fails when the malicious user detects that there is a secret message present in the steganography medium. However, Alteration could be inspired by some strengths of the combined steganography and cryptography methods to achieve the alteration process.

# 3 Global Architecture

Our proposal is taking part of a cloud data security preserving solution architecture that we proposed on a previous work (Rhazlane et al. (2016)) , that exploits the characteristics of multi agent systems to deliver an optimal and secure solution for data storage and exploration in the cloud. The data storage aspect of the solution was based on an encryption process to secure the data before storage, as well as an intelligent multi agent system that was designed to optimize the data exploration.

The architecture of the global solution (See Fig 1) has a set of four actors: The data owners and administrators (A); The Client (B); The Cloud server (C) and the multi-agent system (D) including the "Main Agent", the "Query Translator agent" and the "Query Executor agent".

Each agent is responsible of performing a role including the data encryption and decryption intermediate operations. Given the existing architecture, the aim of the present paper is to improve the encryption and decryption operations (See the data owners and administrators (A) section in red) by providing an alteration process of the data before storing it in the cloud and a reverse alteration operation (decryption) before sending clear data to the client.

## 3.1 Actors

**The data owners and administrators:** They are responsible for defining the data (which columns of the table) to encrypt, and the keys used for encryption (encryption metadata). This metadata is used thereafter, on one side, to encrypt the data before storing it on the database hosted by the cloud provider, and on the other hand, by the tool for the exploration of the database. The administrators can update the metadata, perform the encryption/decryption and the deployment of the database in the cloud.

**The client:** Explore the database, through its application, can send the request to the "Main agent" and receive results as decrypted data.

**The cloud server:** Receives the query in its server version, run the query and send the results to the "Main agent".

**The multi-agent system:**

1. **Main Agent**: Plays an intermediary role between the client and the database, and coordinates the sending and receiving of messages between the client, the agents and the database server in the cloud;

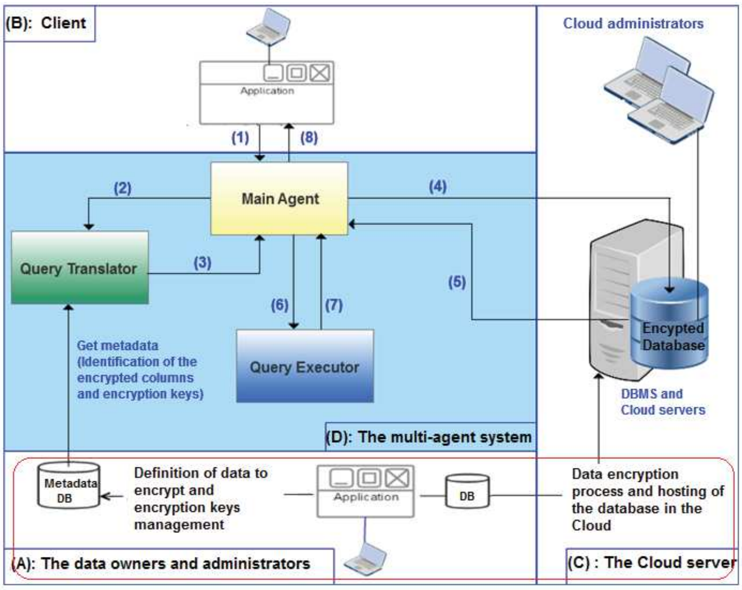


FIG. 1 – *Architecture of the proposed cloud data security preserving solution, Rhazlane et al. (2016).*

2. **Query Translator Agent**: Receives the original query sent by the "Main Agent", conceive the server version of the query and returns the server version of the query to the "Main Agent";
3. **Query Executor Agent**: Receives the original query and the encrypted results sent by the "Main Agent", decrypts the data, performs the calculations, applies the restriction conditions on the decrypted data and then returns the results (decrypted data) to the "Main Agent".

## 3.2 Functioning

In the initial deployment phase (see Fig 1), the data owner encrypts its database before hosting it in the cloud. This must always be possible even after the first deployment; the encryption is always based on one or more keys managed by the owners and the administrators of data. The multi-agent system (See steps from *(1)* to *(8)* in Fig 1), which plays the role of mediation between the client (using an application) and the server, must intercept and analyze the query sent by the client *(1)* with the help of the "Main Agent". The agent must identify the encrypted columns and send the query to the "Query Translator Agent" *(2)*, which is responsible for the translation of the query to its server version (a new version of the query that can be understood by the server, since the data is altered and therefore query conditions on altered column cannot be applied). The "Main Agent" then receives the server version of the query returned by the "Query Translator Agent *(3)*. The "Main Agent", sends the server version of the query to the server that hosts the database in the cloud, for execution *(4)*. The "Main Agent" subsequently receives the encrypted results of the execution of the query by the server *(5)*. The "Main Agent" sends the original query and the encrypted results to the "Query Executor Agent" that performs the decryption with the help of the data administrators *(6)*. The main agent finally receives the decryption results (decrypted data) *(7)* and sends the final results (decrypted data) to the client *(8)*.

The tasks of translation and execution of queries are performed based on specific algorithms. The encryption and decryption (Alteration of data) are executed through customized functions that we will discuss in the following section.

# 4 Proposition

## 4.1 Data Alteration

As seen in the state of the art section, the two important aspects of security that deal with transmitting information data using the cloud are steganography and cryptography. Steganography deals with hiding the presence of a message and cryptography deals with hiding the content of a message. Both of them are used to ensure data security. However, none of them can simply fulfill the basic requirements of security, G.Korde (2016). This need was behind our motivation to propose a new approach to "encrypt" and safely transmit data based on the combination of both cryptography and steganography and overcome their weaknesses, that we named: *Data Alteration*.

The alteration is inspired much of steganography, in the sense that it also aims to hide the data. It changes the meaning and value of the data while preserving their type, to give the impression that this data is real and thus limit the risk of ciphering and cloud providers malicious use. The fundamental difference between alteration and steganography, is that the last one uses the data to hide other data while the alteration changes the data itself based on cryptography concepts.

To understand the differences and similarities between Steganography, Alteration, and Cryptography , Table 2 shows the behavior of the three data security techniques (Shirali-Shahreza (2008)) when applied on the same data (Input data: *Mohamed*, Output data: *O*). Through this table we can see that:

— In terms of visual appearance, the hidden data using steganography method may be unreadable or not depending on the algorithm used. In case they are, it would be the same case for data encrypted by the cryptography technique. Thus, as the result is not readable, data will attract the attention of hackers who may suspect their non-veracity. The alteration corrects this weakness, indeed the altered output remains readable and meaningful whatever the case. Also, according to the context of data used as input during the alteration, it is possible to build a dictionary in accord with this context in order to make sure that the result relates to the same context. For example, if we want to alter a city's name the output will still remain a city's name but the value will be changed.

— The size of the data results after applying steganography increases, which remains a disadvantage in terms of memory consumption. However, in the case of cryptography, it could either increase or decrease depending on the used algorithms. The alteration is exactly in the middle. In the case of number's alteration, there is no risk of increasing the volume of data results. In the strings case we can see a slight increase due to the words contained in the dictionary, still this problem can be solved.

— In terms of conservation of data type result, neither steganography nor cryptography conserve type of the input data. Steganography could hide a string in an image or a text file which is not a string while cryptography returns a result that combined both numbers, strings and special characters. These two techniques could attract the attention of clever hackers. The alteration has improved this defect: the input data type is the same output data type .The alteration of a string would give a string as a result and no modification of the data will be detected.

| Output comparison criteria | Steganography | Alteration | Cryptography |
|---|---|---|---|
| Visual appearance of the data | Readable data (almost similar to the input data) or not (depending on the algorithm) O : Moohameet | Readable data (but different from the input) O : Abdoulatif | Unreadable data O : #K8Z5U7 |
| Size results | Increases | May decrease or remain unchanged for numbers and slightly increase, decrease or remain unchanged for Strings | May slightly increase, decrease or remain unchanged |
| Visual type (Eg : String) | Can be changed or not depending on the stegofile O : Moohamet (String) | Remains unchanged O : Abdoulatif (String) | Changed |
| Value (Eg : Mohamed) | Can be changed or not (depending on the algorithm) | Changed | Changed |

TAB. 2 – *Comparison results between Stenography, Alteration and Cryptography.*

## 4.2 Formalism

The development of this solution aims to achieve the alteration of numbers, strings, and also data files or datasets combining both numbers and strings. To ensure complexity and safety of this alteration technique, it was important to base the alteration algorithm on mathematical based functions. So we proposed 4 functions to encrypt and decrypt data as they are numbers or strings. The algorithm was also based on 2 tables: the ASCII table and the SSCE Table, which is a Secret Code for Steganography Embedding (SSCE) for encoding ASCII numbers (See Fig 7 in Banerjee et al. (2011) ). This table gives for each value encoded in ASCII, a corresponding value between 1 and 255. The use of the table was inspired from the authors in Banerjee et al. (2011) which proposed a steganography solution for data security.

### 4.2.1 Principles and functions of the proposed algorithm

**Number's alteration.** The alteration of numbers takes place according to the following process (See Fig 2):

— **Part 1:** The operations will be applied on each digit of the number. Each number is converted to ASCII (a). The ASCII value resulting from the previous conversion is then converted to SSCE (b). The SSCE value resultant between [1 - 255] is then encrypted by the function *(1)* (c). The result obtained by the alteration function is a decimal number (N) in the range [48-57] (The 0-9 number's range in the ASCII table) and we recover only the integer part of this number (N) into a number (N2) that we will use in the next step of the algorithm (d). This number (N2), is then converted from ASCII to normal to obtain finally a number with digits in the range [0-9] as a final result (e)(f).

$$X = [(n \div 256) \times 10] + 48 \textit{ (1)}$$

— **Part 2:** At this level all the digits of the number are altered, so we have therefore a new number (Q). The number (Q) is then divided by 2 if it is a peer number, if not we add 1 and divide the number by 2: we get a number Q2. Then the number Q2 is subject to a permutation 2 by 2 of his digits and thus we obtain a final number Q3 which is the final result of the alteration.

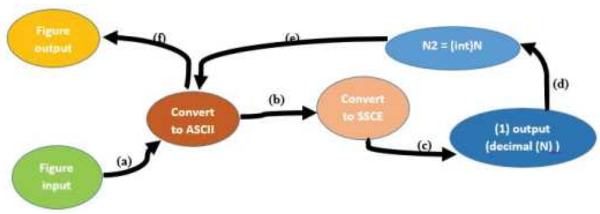


FIG. 2 – *The numbers and strings alteration process.*

**String's alteration.** The alteration of the words and characters takes place according to the same numbers alteration process (See Fig 2):

— **Part 1:** The operations will be applied on each character of the string. Each character is converted to ASCII (a). The ASCII value resulting from the previous conversion is then converted into SSCE (b). The SSCE resultant value between [1-255] is then encrypted using the strings alteration function (2) (c). The result obtained by the encryption function is a decimal number (N) in the range of [97-122] (The a-z character's range in the ASCII table), and we recover only the integer part of this number (N) into a number (N2) that we will use in the next step of the algorithm (d). This number (N2), is then converted from ASCII to normal to obtain finally a set of characters in a word format with digits in the range [a-z] as a final result (e)(f).

$$X = [(n256)26] + 97 \textit{ (2)}$$

— **Part 2:** After applying the first part of the algorithm on all the characters of the string , we have as a result a pre-altered string. This string will be different from the starting string and will have no meaning. Now our goal when doing the alteration is to give meaning to altered results, this why the chain of characters obtained in "part 1" will be send to a Spellchecker who will select the closest word to the string according to a dictionary. The result returned by the Spellchecker will be the final altered string.

The decryption functions for numbers *(3)* and strings *(4)* are the inverse of the functions *(1)* and *(2)* and the process of the algorithm is the reverse process of the algorithm process illustrated in Fig 2.

$$N = 256(X - 48)10 \textit{ (3)}$$
$$N = 256(X - 97)26 \textit{ (4)}$$

**Number's and string's desalteration.**

— **Number's desalteration:** At this level we have a number completely altered. First, we swap the digits of the altered number 2 by 2. Then, the result of the permutation is multiplied by 2 if it is a peer number or multiplied by 2 and then decreased by 1 if not. The algorithm below is applied to each digit of the number obtained in the previous step. The decimal digits (N) obtained by the alteration function (1) and corresponding to each digit of the original number are saved for a later use in the desalteration phase (For example the digit 51.2421875 in Fig 3). These values are passed as a parameter to the desalteration function (3) in order to obtain a desaltered value in SSCE. This value is then converted into ASCII using the ASCII table and we finally obtain the original value in the range [0-9] from the corresponding value between [48-57] in the ASCII table.

— **String's desalteration:** When a string is altered, for each character, the decimal value obtained (N) by the function (2) and the value returned by the spellchecker are stored in a file and used in the desalteration phase following the same process as the desalteration of numbers.

## 4.3 Example of application

In order to illustrate the complexity of the proposed algorithm, we choose two examples of two data types: numbers and strings. Our prototype was realized and tested under Java and tested on numbers and strings and combined datasets.

### 4.3.1 Number's alteration

For the numbers example, the input data was "14750". The result after applying the alteration function was the output "92538". The steps and the intermediate results are listed in the table below (See Fig 3). The usage of the floating number is to keep for a reuse as mentioned above, while applying the alteration reverse operation.

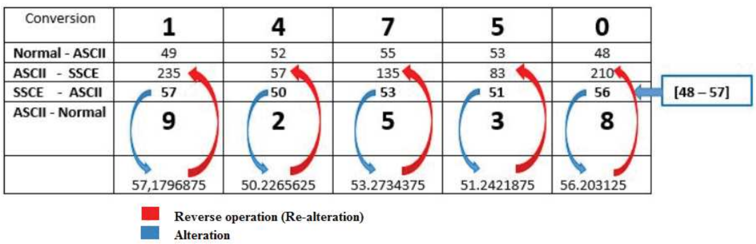


FIG. 3 – *The numbers alteration application example.*

### 4.3.2 String's alteration

Working with strings is much more difficult than working with numbers specially since that our proposal aims to get the same input type while changing its meaning and value. Changing the value is easy but changing the meaning and staying in the same context is much harder.

In the following example, the input data is "Sonia" and the resulted output of the part1 of the algorithm is "odbot". The resulting string has no meaning, this is where the use of a spell checker carefully chosen is necessary. As similar to the alteration of numbers, the floating point number is kept for use in the reverse strings alteration operation.

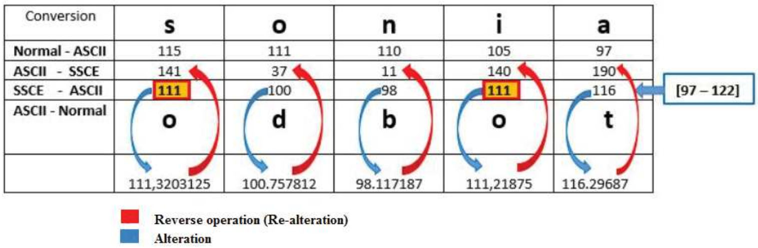


FIG. 4 – *The strings alteration application example.*

# 5 Conclusion and perspectives

As part of this work, we proposed a preliminary prototype of an alteration solution based on a multi-agent system architecture for the protection of data stored in the cloud. We conducted a state of the art combining recent works related to cloud data security , taking into account the analysis and comparison of 3 methods to position our approach regarding previous works.

This work was discussed in three main axis, the cloud environment, data encryption and decryption process and the development of a novel solution, with tests and results under Java.

However future perspectives may complement and develop this work, namely designing a more robust encryption system that fully meets safety requirements, and strengthen the multi-agent system by the exploitation of all its features and conceive a more configurable multi-agent system, and finally complete the translation and query execution algorithms to support a wide range of SQL queries.

# References

Abdul Alsahib S.Aldeen, Y., M. Salleh, and M. A. Razzaque (2015). State of the art survey on security issue in cloud computing architectures, approaches and methods. *Journal of Theoretical and Applied Information Technology 75*, 53–61.

Banerjee, I., S. Bhattacharyya, and G. Sanyal (2011). Novel text steganography through special code generation. *International Conference on Systemics, Cybernetics and Informatics*, 298–303.

Chen, D. and H. Zhao (2012). Data security and privacy protection issues in cloud computing. *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on Computer Science and Electronics Engineering 1*, 647–651.

G.Korde, A. (2016). Crypto-steganography : An information security tool for a cloud environment. *Epitome Journals 2*, 126–132.

Jalil, Z. and A. M. Mirza (2009). A review of digital watermarking techniques for text documents. *2009 International Conference on Information and Multimedia Technology*, 230–234.

Kini, K., M. Mithani, R. Naik, D. Raut, and M. Kumbar (2016). Securing cloud data using crypto-stegno based technique. *Journal of Insect Behavior 5*, 178–180.

Rhazlane, S., N. Harbi, N. Kabachi, and H. Badir (2016). Intelligent multi agent system based solution for data protection in the cloud. *13th ACS/IEEE International Conference on Computer Systems and Applications AICCSA 2016*.

Sachdev, A. and M. Bhansali (2013). Enhancing cloud computing security using aes algorithm. *International Journal of Computer Applications 67*, 19–23.

Shirali-Shahreza, M. (2008). Text steganography by changing words spelling. *2008 10th International Conference on Advanced Communication Technology 3*, 679–696.

Singla, S. and J. Singh (2013). Implementing cloud data security by encryption using rijndael algorithm. *Global Journal of Computer Science and Technology Cloud and Distributed 13*, 19–22.

Somani, U., K. Lakhani, and M. Mundra (2010). Implementing digital signature with rsa encryption algorithm to enhance the data security of cloud in cloud computing. *2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)*, 211–216.

Zielinska, E., W. Mazurczyk, and K. Szczypiorski (2012). Development trends in steganography.

# Résumé

Avec l'émergence des nouvelles technologies et de la connectivité omniprésente, de nombreuses quantités de données sont générées avec la nécessité d'être stockées correctement et explorées rapidement. Dans ce contexte, les services de cloud computing ont été adoptés pour relever ces défis croissants. Mais dans un environnement cloud, les données et les applications sont contrôlées par le fournisseur du service et le client n'a pas toujours la possibilité d'augmenter le niveau de sécurité imposé. Cela conduit les utilisateurs à appliquer des mécanismes de cryptage avant de stocker leurs données chez un fournisseur cloud. Dans cet article, nous proposons une nouvelle approche qui combine les points forts de la stéganographie et de la cryptographie nommée «Altération de données». La technique vise à cacher les données en les modifiant complètement tout en restant lisibles, significatives et par conséquent ne montrent aucun soupçon aux fournisseurs cloud malveillants et pirates. L'approche proposée a été implémentée en Java et testé sur un ensemble de données au sein d'une architecture basée sur les systèmes multi-agents.