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

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

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
Lumière Lyon 2 University
Lyon, France
nouria.harbi@univ-lyon2.fr
nadia.kabachi@univ-lyon1.fr

Résumé. 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. 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. 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 : we will start our proposal with an explanatory section of the state of the art and a 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, 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 mecanisms 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.

Author	Paper's title	Date of publication
Mrs. Aparna G.Korde	Crypto-Steganography :An Information Security Tool for a Cloud Environment	2016
Kirti Kini, Meera Mithani, Rinali Naik, Divyata Raut and Prof. M.K. Kumbar	Securing Cloud Data using Crypto-Stego based Technique	2016
Sanjoli Singla and Jasmeet Singh	Implementing Cloud Data Security by Encryptionusing 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 CloudComputing	2012
Uma Somani, Kanika Lakhani and Manish Mundra	Implementing Digital Signature with RSA Encryption Algorithmto Enhance the Data Security of Cloud in CloudComputing	2010
Zunera Jalil and Anwar M. Mirza	A Review of Digital Watermarking Techniques for TextDocuments	2009

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

In 2013, Singla et 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 et Bhansali (2013) use the same approach but data is encrypted using "Advanced Encryption Standard (AES)" before being launched in the cloud.

In 2012, the authors in Chen et 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 et 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 : Is 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 : The word steganography is derived from a Greek word meaning "covered writing". It is an ancient art or practice. Steganography 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 represents several type of content such as text, image, video, audio, and graphic content, and they reveal very different characteristics in hiding in-

formation inside them, different watermarking algorithms appropriate to each of them should be developed, Jalil et 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 and hides the contents of the message from an attacker, 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. The table (Fig 1) below summarizes the differences between cryptography and steganography.

		Cryptography	Steganography
Goal		Obfuscate the content of communication	Hide the fact of communication
Characteristics	Secrecy	Ciphertext is illegible	Embedded information is "invisible" to an unaware observer
	Security of communication	Relies on the confidentiality of the key	Relies on the confidentiality of the method of embedding
	Warranty of robustness	Complexity of the ciphering algorithm	Perceptual invisibility / statistical invisibility / compliance with protocol specification
	Attacks	Detection is easy / extraction is complex	Detection is complex / extraction is complex
Countermeasures	Technical	Reverse engineering	Constant monitoring and analysis of exchanged data
	Legal	Cryptography export laws	Rigid device / protocol specification

FIG. 1 – *Comparison of cryptography and steganography characteristics, Zielinska et al. (2012).*

Steganography and watermarking bring a variety of techniques 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 an image or sounds.

In comparaison 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*, by people in such a way that an eavesdropper cannot **remove or replace** the presence of *m* in *d'*. The table (Fig 2) summarizes the differences between watermarking and steganography.

		Watermarking	Steganography
Goal		Protect the carrier	Protect secret information from disclosure
Characteristics	Secrecy	Invisibility or perceptual visibility depending on the requirements	Embedded information is "invisible" to an unaware onlooker
	Type of robustness	Robustness against tampering or removal	Robustness against detection
	Effect of signal processing / random errors / compression	Must not lead to the loss of the watermark	May lead to the loss of hidden data
	Type of carrier	Digital files – audio, video, text or images	Any service, protocol, file, environment employing digital representation of data

FIG. 2 – *Comparison of watermarking and steganography characteristics, Zielinska et al. (2012).*

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 datacan be found and security destroyed.

On the other hand, watermarking main benefits can be 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. Text encountering massive insertion, deletion and reordering attacks need to be protected, and efficient text watermarking algorithms are still required.

After analyzing all these methods, from different limits observed, we can see that none of it offers an approach 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 altering process.

3 Global Architecture

Our proposal is tacking part of a previous 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 3) 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 this paper is to improve the encryption and decryption operation of the process (See the data owners and administrators (A) section in red) by providing an alteration process of the data before storing the data in the cloud and a reverse alteration operation (decryption) before sending clear data to the client.

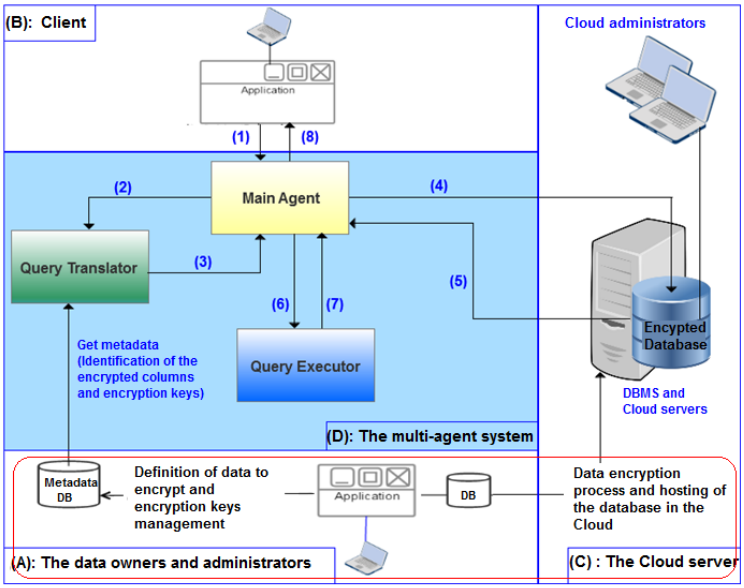

FIG. 3 – *Architecture of the cloud data security preserving solution.*

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 customer and the database, and coordinates the sending and receiving of messages between the client, the agents and the database server in the cloud ;
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, perform the calculations, applies the restriction conditions on the decrypted data and then return the results (decrypted data) to the "Main Agent".

3.2 Functionning

In the initial deployment phase (see Fig 3), 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 3), 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 contents 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 appoach and method to "encrypt" and safely transmit data based on the combination of both cryptography and steganography and overcomes 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 , the table (Tab 4.1) below summarizes the results of the three techniques, Shirali-Shahreza (2008), applied on the same data (Input data : *Mohamed*, Output data : *O*). This table summarizes the behavior of the three data security techniques when applied on the same data. 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 after having obtained them. Thus 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 same context context. For example, if we want to alter a city's name the output will still remain a city's name but output 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. Indeed, 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. 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 data type input is the same data type output.The alteration of a String would give a String as result, the hacker will have no idea of any modification of the data.

Output comparaison 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 depend on the stego file 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 – *Results comparaison beetween 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 combinig 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 4). 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.

Secret Steganography Code for Embedding(SSCE) Table

ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE	ASCII	SSCE
10	1	1	26	2	52	3	78	4	104	5	130	6	156	7	181	8	206	9	231
20	2	11	27	12	53	13	79	14	105	15	131	16	157	17	182	18	207	19	232
30	3	21	28	22	54	23	80	24	106	25	132	26	158	27	183	28	208	29	233
40	4	31	29	32	55	33	81	34	107	35	133	36	159	37	184	38	209	39	234
50	5	41	30	42	56	43	82	44	108	45	134	46	160	47	185	48	210	49	235
60	6	51	31	52	57	53	83	54	109	55	135	56	161	57	186	58	211	59	236
70	7	61	32	62	58	63	84	64	110	65	136	66	162	67	187	68	212	69	237
80	8	71	33	72	59	73	85	74	111	75	137	76	163	77	188	78	213	79	238
90	9	81	34	82	60	83	86	84	112	85	138	86	164	87	189	88	214	89	239
100	10	91	35	92	61	93	87	94	113	95	139	96	165	97	190	98	215	99	240
110	11	101	36	102	62	103	88	104	114	105	140	106	166	107	191	108	216	109	241
120	12	111	37	112	63	113	89	114	115	115	141	116	167	117	192	118	217	119	242
130	13	121	38	122	64	123	90	124	116	125	142	126	168	127	193	128	218	129	243
140	14	131	39	132	65	133	91	134	117	135	143	136	169	137	194	138	219	139	244
150	15	141	40	142	66	143	92	144	118	145	144	146	170	147	195	148	220	149	245
160	16	151	41	152	67	153	93	154	119	155	145	156	171	157	196	158	221	159	246
170	17	161	42	162	68	163	94	164	120	165	146	166	172	167	197	168	222	169	247
180	18	171	43	172	69	173	95	174	121	175	147	176	173	177	198	178	223	179	248
190	19	181	44	182	70	183	96	184	122	185	148	186	174	187	199	188	224	189	249
200	20	191	45	192	71	193	97	194	123	195	149	196	175	197	200	198	225	199	250
210	21	201	46	202	72	203	98	204	124	205	150	206	176	207	201	208	226	209	251
220	22	211	47	212	73	213	99	214	125	215	151	216	177	217	202	218	227	219	252
230	23	221	48	222	74	223	100	224	126	225	152	226	178	227	203	228	228	229	253
240	24	231	49	232	75	233	101	234	127	235	153	236	179	237	204	238	229	239	254
250	25	241	50	242	76	243	102	244	128	245	154	246	180	247	205	248	230	249	255
		251	51	252	77	253	103	254	129	255	155								

FIG. 4 – *The SSCE Table, Banerjee et al. (2011).*

4.2.1 Principles and functions of the proposed algorithm

Number's alteration. The alteration of the numbers takes place according to the following process (See Fig 5) :

- **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 into 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).

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

- **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.

Word's alteration. The alteration of the words and characters takes place according to the same numbers alteration process (See Fig 5) :

- **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

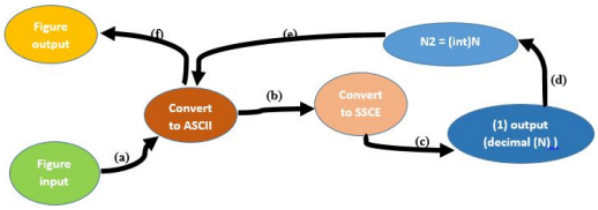

FIG. 5 – *The numbers and strings alteration process.*

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).

$$X = [(n \div 256) \times 26] + 97 \; (2)$$

– **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 in 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 5.

$$N = 256(X - 48) \div 10 \; (3)$$
$$N = 256(X - 97) \div 26 \; (4)$$

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.

4.3.1 Numbers 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 intermidiate results are listed in the table below (See Fig 6). The usage of the floating number is to keep for a reuse, while applying the alteration reverse operation.

4.3.2 Strings 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 at the same context is much harder.

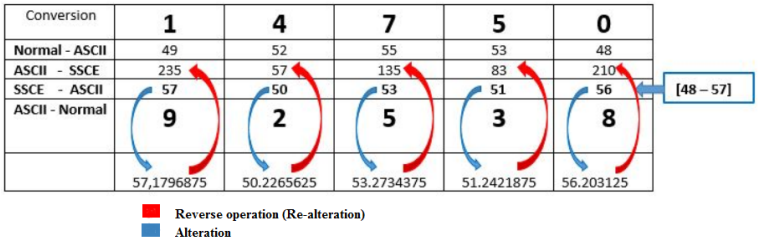

FIG. 6 – *The numbers alteration application example.*

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 necessery. As similar to the alteration of numbers, the floating point number is kept for use in the reverse strings alteration operation.

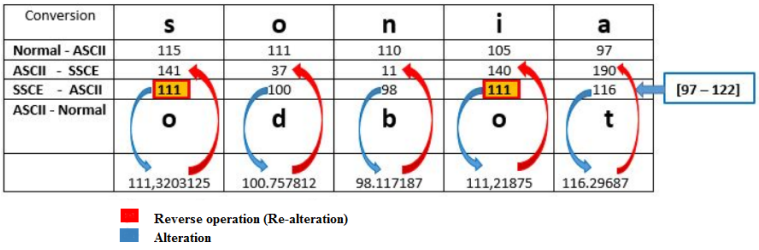

FIG. 7 – *The strings alteration application example.*

5 Conclusion and perspectives

As part of this work, we proposed a preliminary prototype of an alteration solution based on a multi-agent systems 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 comparaison of 3 methods to position our appoach regarding previsous 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 cryptographic system based on an encryption function 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.

Références

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

Chen, D. et 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. et 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, et M. Kumbar (2016). Securing cloud data using crypto-stegno based technique. *Journal of Insect Behavior 5*, 178–180.

Rhazlane, S., N. Harbi, N. Kabachi, et 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. et 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. et 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, et 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, et K. Szczypiorski (2012). Development trends in steganography.