A Data Security Algorithm for the Cloud Computing based on Elliptic Curve Functions and Sha3 Signature

Sonia KOTEL
ISITCom of Hammam Sousse
University of Sousse
Sousse, Tunisia

Fatma SBIAA
Faculty of Sciences of Monastir
University of Monastir
Monastir, Tunisia

***Abstract*—The rapid development of distributed system technologies enforces numerous challenges. For example, one of the most critical challenges facing cloud computing is ensuring the security of confidential data during both transfer and storage. Indeed, many techniques are used to enhance data security on cloud computing storage environment. Nevertheless, the most significant method for data protection is encryption. Thus, it has become an interesting topic of research and different encryption algorithms have been put forward in the last few years in order to provide data security, integrity, and authorized access. However, they still have some limitations. In this paper, we will study the security concept in Cloud Computing applications. Then, an ECC (Elliptical Curve Cryptography) based algorithm is designed and tested to ensure cloud security. The experimental results demonstrate the efficiency of the proposed algorithm which presents a strong security level and reduced execution time compared to widely used existing techniques.**

***Keywords*—Cloud; IaaS simulation upon SimGrid (SCHIaas); elliptic curve encryption; one-time pad symmetrical encryption method (OTP); confidentiality; integrity**

I. Introduction

Nowadays, cloud computing is satisfying the huge need for operating the large amounts of data that is stored and exchanged daily in cloud servers. Cloud storage covers the requirement of the growing demand for storage and decreases the charge of maintaining huge volumes of data. Despite the various benefits of the cloud, security remains the main problem. Indeed, the cloud storage server can be untrusted while the transmitted data includes sensitive information. Therefore, any transmitted information can be captured or modified by a malicious user. In this context, the Cloud poses security problems [1], mainly for confidentiality and data integrity since the data are managed outside the governance framework of the cloud users and the service provider can access the data at any time [2]. In order to ensure the data confidentiality, it is crucial to use an efficient encryption scheme to achieve secure control in the cloud storage server. Various cloud data security schemes have been developed and proposed to address data privacy and integrity issues [3-5], including RSA-based cryptosystems, elliptic curves [6], and hash functions [7]. In fact, all encryption systems are based on complex mathematical functions. The symmetric cryptosystem is based on the Secret Key using simple mathematical functions such as substitution and permutations. However, asymmetric cryptosystem requires likewise factoring big prime numbers (RSA) or it used the discrete log problems (DLP). Moreover, the public key cryptosystem is also famous as a holomorphic encryption scheme. Key size raises a plenty in public key cipher. Because of this huge key size, asymmetric cryptosystem needs much computational power. Recently, hybrid cryptosystems based on asymmetric cipher for key exchange and symmetric cipher for data confidentiality. Therefore, Elliptic curve encryption has settled the issue of big key size. ECC employs small key size to decrease the computational power and this can be performed in a cloud environment or IoT devices [6]. Moreover, the cloud provider service should ensure the secret data authentication and guarantee the robustness of the proposed cryptosystem against any process to reveal or change the data. Otherwise, there are an important requirement of a digital signature to ensure the data integrity.

The main contribution in this work is to propose a new security design for cloud computing architecture that reviews the different security deficiencies. Compared with related works, the proposed design offers a new hybrid technique which is faster and more secure. The present approach combines both the elliptic curve cryptographic (confidentiality issue) and the hash function SHA3(integrity issue).

This paper is organized as follows. The first section will introduce the cloud security issues. In the second section, we will study the cloud computing security overview. Section 3 will describe the proposed hybrid cryptosystem. Finally, we will discuss the experimental results and the security analysis results by comparing them to related works.

II. Cloud Security Issues

Commonly speaking, there are various kinds of security attacks in a cloud. This section presents an overview of the most important ones. Therefore, there are novel security requirements in the cloud compared to traditional environments. In fact, NIST is accountable for preserving security over the cloud computing environment and developing standards and rules which provides a precious involvement that gives a better knowledge of cloud applications and computing techniques [4]. The famous three cloud user service models in cloud architecture are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These service models required various levels of security over the cloud environment. The cloud service provider is compiled to gives services, resource distribution management, and security. The cloud computing architecture, shown in Fig. 1, details the five essential modules which are composed of services that are employed in the cloud. Cloud security is a large and complicated task when the data is transferred to the cloud among the client-server frameworks. Indeed, the principle of trust in the cloud architecture can be overfed as the clients ensure the capacities of the infrastructure that it offers the essential services reliably and faithfully.

There are various issues in cloud computing security as listed below [9-13]. The main contribution deals with data integrity and data confidentiality issues.

- Confidentiality: Confidentiality in cloud data storage relates to ensuring the user's data is secret and only the approved users can manipulate the data [1]. Indeed, the data is ciphered before it is deployed. The service provider obtains ciphered data. Then, it is deemed insignificant. But the user is responsible for processing the access control rule, ciphering the data, deciphering it, and exploiting the encryption keys. The traders of cloud computing are widely used the two basic techniques such as physical isolation and cryptography to reach the confidentiality [2].

- Integrity: data integrity is the preservation of the data to check that is not modified or missed by using the services of the third party. Hence, the Cloud service provider must put forward protection against insider attacks on data. Therefore, any modification to the stored data must be identified using techniques having higher visibility to define what or who can edit the data that possibly impact their integrity. Further, computation integrity should be verified at the data stage and computation stage. Also, the data integrity service could assist in picking up lost data or detecting if there is data exploitation.

- Trust: The cloud service provider is required to put forward an adequate security policy to reduce the threat of information loss or data management [3].

- Privacy: is specified as the forwardness of a user to have power over the disclosure of secret information. An illegal admittance to client's confidential data will make security issues [5] [13].

- Reliability and Availability: Trustworthiness of cloud service provider declines when a client's data get dripped [8].

- Authentication and Authorization [14]: To inhibit unauthorized access, software is needed beyond the organization's firewall.

In the next section, we will present an overview of existing encryption schemes over cloud computing.

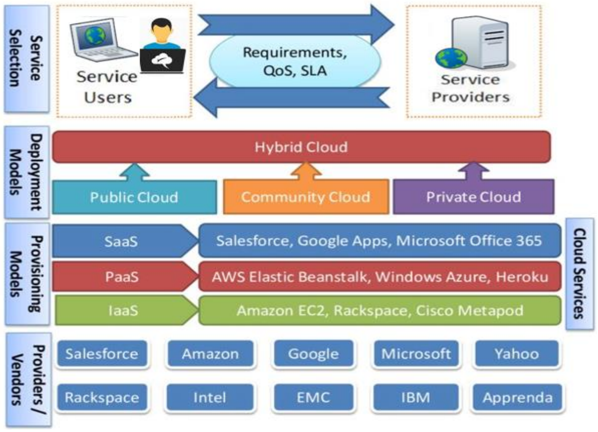

Fig. 1. Cloud Computing Infrastructure.

III. Related Work

Various related works about improvement the infrastructure security issues through data sharing in cloud computing have been proposed. Precisely, we select the methods that have been proposed to secure data transaction, access management and user authentication in the cloud. Indeed, authors in [15] presented virtual private storage services that gratify the standard requirements (authentication, integrity confidentiality, etc.). Most of these requirements are done by ciphering the files stocked in the cloud. But similar ciphering drives to complicate the search operation through documents and to hardness the collaboration operation in real-time modification. Furthermore, Farash MS and Attari,MA proposed in [16] an enhanced authentication design based on elliptic curve cryptographic functions (ECC) to offer a password authenticated key for swapping authentication method. The major drawback of this design is that it does not ensure the anonymity of clients and it does not resist against the man-in-the middle attack.

Moreover, in [17] Xie Q et al. proposed an authenticated key exchange method using a two-factor anonymous dynamic identification. This suggested protocol is suitable to smart card repudiation and password update unless centralized memory space. This solution does not ensure security against man-in-the-middle attack.

Furthermore, in [18] Chang CC et al. put forward a security method that would satisfy basic security requirements and offer mutual authentication among the cloud and its hardware equipment. This proposed method was mainly based on ECC functions to offer secure communication among the cloud and its linked machines. The main limitation of this method is that is vulnerable to the known-key-security attack, and it does not provide a good forward secrecy feature.

In addition, the authentication scheme proposed in [19] would satisfy the security demands and resist different attacks. The suggested method connects the cloud with its devices using ECC cryptographic functions. The principal drawback of this proposed scheme is that it does not ensure client untraceability and it is not secure against the known-key attack.

Also, the approach presented in [20] is based on an unidentified and efficient two-factor authentication protocol that correctly authenticates employers to the mobile cloud service. The proposed approach uses the ECC cryptographic method to offer mutual authentication among mobile phones devices and cloud services. However, it does not ensure user untraceability.

Our work is notably different from the existing schemes. We focus on both data storage confidentiality and integrity in Cloud Computing services. Indeed, the contribution is based on proposing a hybrid design using both the ECC functions and SHA-3 algorithm to ensure data security and integrity. The proposed design is presented in the next section.

IV. Proposed Crypto-System

In this section, we will describe the proposed encryption scheme. Indeed, in order to resolve the data security problems in the Cloud's data centers, we will study the two fundamental services which are confidentiality and integrity. We propose three different scenarios: the first one uses the simple mapping method (M1) while the second implements the double mapping architecture (M2). The main contribution consists in the hybrid approach that combines the simple mapping method to the OTP process. The final comparison will allow us to validate the appropriate scenario.

Thus, the third scenario of the proposed crypto-system is based on the combination of elliptic curve cryptography and the one-time pad symmetrical encryption method (OTP) as well as the hash function SHA3. For the data privacy, we will use a list of elliptic curve points which represent the OTP encryption keys. Therefore, each block of the confidential data will be ciphered using a different key. Moreover, to guarantee the integrity of the treated data we will apply the SHA3 hash function on the encrypted data in order to have a signature which can be verified during the data deciphering. The following Fig. 2 illustrates the proposed crypto-system.

In the following subsections, we will describe the elementary functions that constitute the designed system.

A. Elliptic Curve Cryptography

Cloud computing confidentiality can be ensured using encryption schemes based on Elliptical curve cryptography (ECC). This public key encryption technique is based on elliptic curve theory. It is used in order to design faster, smaller, and more efficient cryptographic keys. Indeed, the best assured group of new public key methods is built on the arithmetic of elliptic curves. It has been contended that elliptic curves are a foundation for future internet security, given the relative security level and the performance of these algorithms. Moreover, according to some researchers, ECC based schemes are more computationally efficient than the first-generation public key systems, RSA and Diffie-Hellman. It can provide an efficient security level with a 164-bit key while other systems require above 1024-bit key [3]. Therefore, ECC helps to establish equivalent security with lower computing power and battery resource usage. Thus, it is becoming widely used in various domains such as mobile applications.

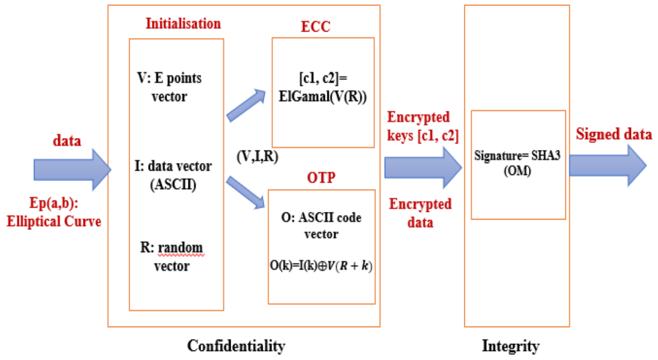

Fig. 2. Proposed Crypto-System Architecture.

B. OTP Encryption Technique

OTP is a symmetric cryptography technique, which uses randomly generated keys (see Fig. 3). It was created by G.Vemam in 1917. The encryption and decryption process uses XOR operators on the keys and secret messages. This technique is very powerful and resists brute force attacks under duress of using a random key just once.

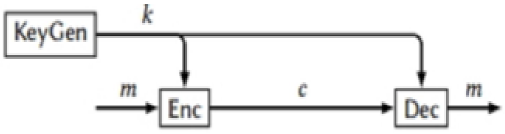

Fig. 3. OTP Encryption.

C. SHA3 Function

Hash functions produce a reduced and unique digest (of fixed size) as representation of data of any size. They calculate a message identification code which is called a hash value.

H: $\{0,1\}^* \rightarrow \{0,1\}^n$

M→ H(M)

The most common hash functions are MD52, SHA1, SHA2, SHA3. These algorithms are usually very fast since the generated hash value can be very small while ensuring that the transmitted message has not been altered or modified by a third party by sending the message along with its signature. The SHA-1 and SHA-2 hashing algorithms are very essential and widely used to secure communications such as wireless communications. But, they present many weaknesses and limitations which necessitated finding another replacement. NIST held a three-round competition to find a new secure hashing algorithm. This new algorithm "SHA3" exceeds the limits of the security presented in the previous hashing algorithms. Thus, SHA-3 is a cryptographic hash function that has four versions which allow to calculate signatures of different sizes: 224, 256, 384 and 512 bits. It is not intended to replace SHA-2 because until now no attack on SHA-2 has been demonstrated, but to provide another solution following the possibilities of attacks against MD5 standards, SHA-0 and SHA-1. Moreover, it is totally different since it is built on a completely different principle.

The Keccak algorithm is a cryptographic hash function designed by Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. It is the best algorithm among all applicants that was chosen for the SHA3 hash function. Thus, the SHA-3 (Keccak) scheme consists in two main stages which are the absorbing and the squeezing phases (see Fig. 4). During absorption, the original message M is subjected to the permutation f. In the squeezing phase, the output hash value is truncated from the first r-bit and further transformations are done if the required output bit is not obtained. Thus, it calculates the output of the resulting permutations of the value Z. The main objectives of using this construct are to have effective security against generic attacks and to make the use of the compression function simpler and more flexible.

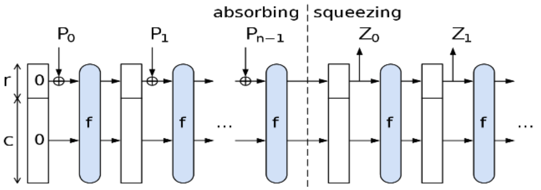

Fig. 4. Hashing Algorithm.

D. Proposed Hybrid Crypto-System Design

We propose, in the present paper, a hybrid crypto-system which is based on the combination of the elliptical curve cipher, the symmetric "OTP" encryption method and the SHA3 hash function. Fig. 5 illustrates the activity diagram that describes the data encryption process.

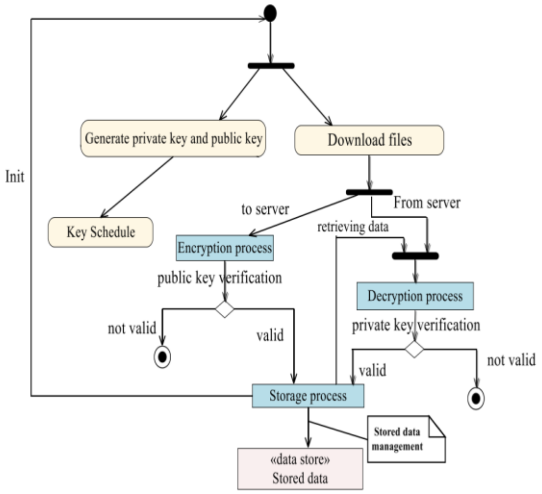

Fig. 5. Activity Diagram.

The proposed crypto-system based on the elliptic curve cryptography. In particular, we used Elgamal for data encryption and decryption. The public key PK is the result of multiplication of Prk with the generating point of the curve G.

Each user must generate its own private and public key couple. The private key PrK is just an integer chosen such that PrK <= P. The public key PK is the result of multiplying PrK with the generating point of the curve G. Algorithm 1 details the generation function of these two keys. Considering that:

$E_P(a,b)$ an elliptic curve in the form $y^2 = x^3 + ax + b$

G(x,y) the generating point of the curve E

Algorithm 1. Couple Key Generation (Private, Public)

```
1: Output {PrK, PK}
2: PrK: private key random value ( between 0 and P)
 PK: public key a point of the curve E
3: PK=PrK *G
4: Return (PrK, PK)
```

In order to use the points of the curve as the encryption key for the OTP method, the system starts by generating a vector that contains these points. Algorithm 2 details the curve points generator process.

Algorithm 2. Curve Points Generator

```
1: Output V: points vector of the curve E
2: For i=0 to P do
3: y2=$i^3$ + a * i + b mod P
4: if y2 is perfect square then
5:  add y2 to V
  end if
 end for
6: Return V
```

Algorithms 3 and 4 illustrate the ELGamal encryption and decryption processes respectively.

Algorithm 3. ElGamal-Encryption

```
1: Input: Plain Data , PK
 with Plain: point to encrypt
2: Output: {c1,c2}
 with c1, c2 two points of the curve
3: k random value (between 0 and P)
4: c1= k * G
 with G : the generating point of the curve
5: c2= Plain + k * PK
6: Return {c1, c2}
```

Algorithm 4. ElGamal-Decryption

```
1: Input: Data {c1,c2} , PrK
2: Output: Decrypted point
3: Sub point= Prk * c1
4: Decrypted = c2 - Sub
5: Return Decrypted
```

In Simple Mapping technique, for an elliptic curve E, the cipher generates a vector V containing the list of points of this curve. For a message m $(m_1,m_2,.....,m_n)$ and for each block m_i, the crypto-system looks for the corresponding point P in the vector V where $P=V[m_i]+256*i$. The encrypted message is the set of all the founded points where each is encrypted by ElGamal encryption. When encrypting a message M of n blocks $(m_1, m_2, ..., m_n)$, for each block m_i is associated a point of the curve so Encrypted value of m_i is only the result of encryption of the associated point.

The Double Mapping method is a simple optimization of the previous method where instead of encrypting a block salt at a time; we perform the encryption of two blocks. Hence for a message m $(m_1, m_2, ..., m_n)$ and for each pair of points (m_i, m_{i+1}), the crypto-system looks for the point that corresponds to the value $C = m_i + m_{i+1} * 256$ in vector V. The encrypted message is only the set of found points where each one is encrypted by ElGamal encryption.

V. Experimental Results

We implemented the proposed crypto-system using the Java language as well as the "Bouncy Castle" library which provides a set of classes and methods for different fields of cryptography such as elliptic curves and hash functions.

In order to evaluate the proposed solution, we used the SCHIaaS simulation environment that provides the IaaS model simulation with the SimGrid library which implements hypervisor level functionalities (see Fig. 6) [21]. SCHIaaS implements cloud-level functionality such as running and stopping instances. It also supports the main management functions of virtual machines (VMs), namely, run, terminate, suspend, resume and describe instances. Moreover, it allows the description of available resources, the management of image and instance types and the management of cloud storage. The SimSchlouder was used for the assessment since it supports the main cloud agent management functions for scientific computing. The type of application can be the execution of tasks and workflows. There is no limit to the number of tasks that can be simulated. These tasks can be heterogeneous and may require heavy CPU or I / O usage.

For both Calculation and Storage interface, SCHIaaS provides two implementations of both calculation and storage engines: these are RICE (Reduces Implementation of Compute Engine) and RISE (Reduces Implementation of Storage Engine). Fig. 7 describes how we can add simulation entity in SCHIaaS environment.

In order to realize the simulation, the RISE storage engine has been modified while allowing data to be encrypted before storage and decrypted before loading. For storing or loading data the "Storage" interface uses the RISE storage engine. The latter uses the "Encryption Task" task to encrypt or decrypt the processed data.

We took into consideration the execution time which represents a fundamental criterion for the Cloud applications. So to verify the reliability of the proposed crypto-system in terms of security, we carried out so many security tests on images such as the histogram analysis, the calculation of correlation and entropy, PSNR, NPCR and UACI.

In order to verify the reliability of the proposed crypto-system, we carried out several security analyzes. Thus, we calculated entropy, PSNR and correlation values between adjacent pixels on standard images. We have also taken into consideration the execution time which represents a fundamental criterion in the evaluation of such a technology. In this context, we compared the execution times obtained for different file sizes.

A. Execution Time

In this section, we will evaluate the speed of the selected encryption methods using images sized 1.2 Mo. All tests are performed on an HP PC with CPU: Intel (R) Core (TM) i7-4500U @ 1.80GHz, 2401 MHz, 2 core (s), 4 logic processor (s), installed memory (RAM): 8 GB. We will compare two different mapping methods (M1, M2) with the hybrid approach that combines mapping and OTP method. Table I represents the encryption and decryption execution time.

The execution time is computed in milliseconds. We note that the used elliptical curve "secp256k1" is tested using the following parameters (previously detailed in section IV.D) described in Table II.

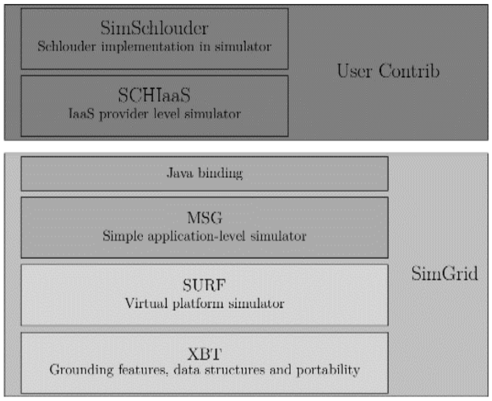
SimSchlouder
Schlouder implementation in simulator
SCHIaaS
IaaS provider level simulator
User Contrib
Java binding
MSG
Simple application-level simulator
SURF
Virtual platform simulator
XBT
Grounding features, data structures and portability
SimGrid

Fig. 6. SCHIaaS Simulation Environment.

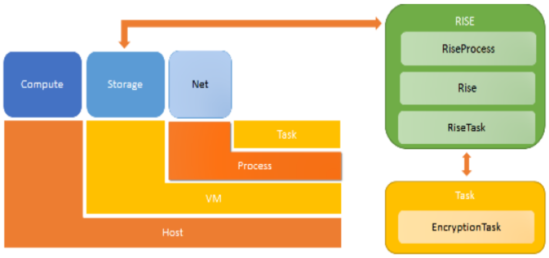

Fig. 7. SCHIaaS Simulation Entity Added.

TABLE I. Execution Time Results (MS)

Encrypted image (512x512	**simple mapping E.T**		**double mapping E.T**		**simple mapping combined to OTP E.T**		**SHA-3**
	Encryption	***Decryption***	***Encryption***	***Decryption***	***Encryption***	***Decryption***	***Encryption***
Lena	10256	10556	9614	9955	291	240	72
Baboone	9652	10215	8649	8896	323	235	68
Barbara	9577	11994	9073	10790	346	250	75
Peppers	10125	10869	9399	10260	332	231	76

TABLE II. “SECP256K1” ELLIPTICAL CURVE PROPERTIES

Elliptical Cuve parameters	Values
a	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
b	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007
P	2^{256}-2^{32}-2^{9}-2^{8}-2^{7}-2^{6}-2^{4}-1
Gx	0x79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B16F81798
Gy	0x483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08FFB10D4B8
N	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8CD0364141
H	01

It is clear that the execution times of the simple and the double mapping methods are very high, which means that they cannot be used for Cloud applications. However, hybrid method is faster. This approves its use for cloud computing security. In addition, we note that the execution time can vary, for the same processed data, from one encryption or decryption operation to another. This is due to the random variable generated during the ElGamal encryption operation.

B. Discussion

Here, in this section, we will compare the experimental results analysis with related works. Fig. 8 and Fig. 9 illustrate the encryption time analysis for the proposed hybrid cryptosystem. Here, the evaluation experiments are based on 400 kb size of data. Authors in [23] proposed a new data security algorithm based on RSA and HMAC. The data is encrypted using RSA and the HMAC code was generated for integrity check when the data is transferred to the cloud server. Moreover, Amalarethinam, I. George, and H. M. Leena presented in [24] an enhanced RSA algorithm. In addition of the two large prime numbers P and Q two other prime numbers are selected. So, the private key and the public key are composed of a distinct couple of numbers. Therefore, in [25] proposed a secured storage algorithm for cloud and IoT based on elliptic curve-based key generation algorithm.

From Fig. 7 and Fig. 8, it can be observed that the proposed cryptosystem takes less encryption and decryption time than the existing schemes in [23], [24] and [25].

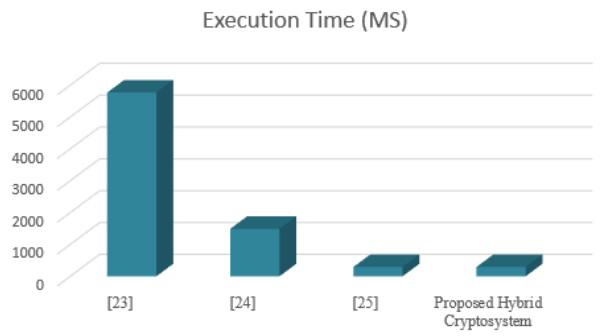

Fig. 8. Encryption Time Comparative Analysis.

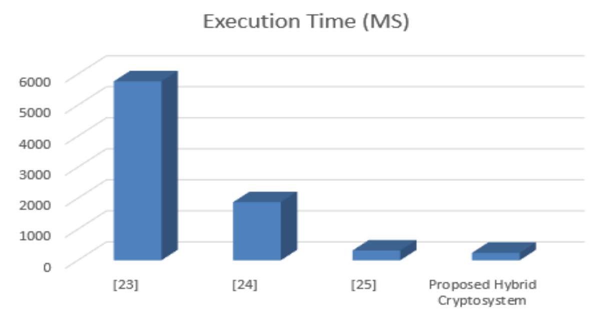

Fig. 9. Decryption Time Comparative Analysis.

C. Security Analysis

According to Claude Shannon, if the cryptographer has information on the statistics of the plain message (frequency of letters or sequence of letters), he can break the encryption method. Thus, to analyze the security level of the ECC algorithm against this category of attacks, we will apply different tests on encrypted standard images [22]. Considering the similarity between the methods M1 “simple mapping” and M2 “double mapping”, we limit ourselves to analyzing the results resulting from the methods M2 and M3.

1) Histogram analysis: A histogram shows how the pixels in an image are distributed; it represents the distribution of the intensities of the image by associating each intensity value with the number of pixels taking this value. The analysis of the histograms of the original and encrypted images is shown in the Fig. 10.

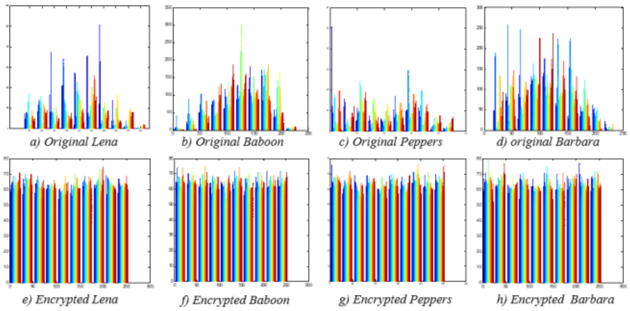

Fig. 10. Histograms of Plain Images and Ciphered Images (Image à Traduire).

As illustrated in Fig. 10, the pixels in the histogram of the encrypted image are uniformly distributed; each intensity is almost the same. Hence, the encrypted image does not reflect any information about the original image.

2) Correlation coefficient analysis: It is well proven that the less correlation value between two adjacent pixels the higher ability to resist to statistical attacks. In this sub-section, we computed the correlation coefficient between two adjacent pixels in plain image and ciphered image. The correlation between horizontally, vertically, and diagonally adjacent pixels is calculated using the following equations:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (1)$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{2}$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{3}$$

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{4}$$

Where x and y are the intensities of two adjacent pixels in the image and N is the total number of pixels.

Table III represents the obtained results of horizontal, vertical and diagonal correlation coefficients between two adjacent pixels in the original and encrypted test images using the crypto-system.

Obtained results indicate that the correlation coefficients for the various encrypted images are very close to zero. This means that the two methods M1 and M2 are good at hiding the details of the original images.

3) Entropy analysis: Information entropy is the most significant property of randomness. In practice, the probability p_i is approximated by a statistical count, which obviously leads to approximations of the amount of information. The average amount of information in an image can be calculated by taking a weighted arithmetic average of the amounts of information provided by each level (with p_i coefficients). The result is called the entropy of the image:

$$H(m)=\sum_{i=0}^{2^n-1}p(m_i)\log_2\frac{1}{p(m_i)} \tag{5}$$

Where *m* is the information source, *p(m)* defines the probability of symbol *m*. Considering that there are 2^8 information source states and they perform with the same probability, using Equation (5), we achieve the best entropy value when H (m) = 8, which illustrates that the origin is certainly random. Therefore, the encrypted image information entropy should be close to 8. The closest value to 8, the smaller chance for the crypto-system to disclose information.

Table IV details results of the encrypted images entropy using the two encryption methods M1 and M2. Obtained entropy values using M2 are closer to the ideal value than those obtained using M. Hence, the probability of fortuitous information leakage is minor.

4) Peak Signal-to-noise ratio (PSNR): The most common measure used to assess the confidentiality of an image is the peak signal-to-noise ratio (PSNR) which is a criterion for measuring image distortion given by the following formula:

$$PSNR=10\log_{10}(\frac{p_{\max}^2}{MSE}) \tag{6}$$

Where P_{max} is the maximum pixel value of the image and the MSE is the pixel-to-pixel mean squared error which presents the error between the original image and the encrypted one.

As illustrated in Table V, PSNR values, using the two encryption methods, between the encrypted image and the plain image are small. Indeed, the lower value of PSNR denotes better cipher quality. Therefore, obtained results prove that the encryption quality of each test image is quite good.

TABLE III. CORRELATION COEFFICIENTS RESULTS OF ORIGINAL AND ENCRYPTED TEST IMAGES USING M1 AND M2 METHODS

	Plain Image (512×512)				**Encrypted Image (512×512)**			
	Lena	***Baboon***	***Barbara***	***Peppers***	***Lena***	***Baboon***	***Barbara***	***Peppers***
Horizontal M1	0.9719	0.8665	0.8597	0.9792	0.0009	0.0031	0.0012	0.0009
Horizontal M2					0.0021	0.0014	0.0027	0.0013
Vertical M1	0.9850	0.7586	0.9591	0.9826	0.0034	0.0065	0.0048	0.0051
Vertical M2					0.0032	0.0028	0.0024	0.0072
Diagonal M1	0.9593	0.7261	0.8418	0.9680	0.0001	0.0002	0.0018	0.0006
Diagonal M2					0.0013	0.0007	0.0031	0.0010

TABLE IV. THE INFORMATION ENTROPY OF ORIGINAL IMAGES AND CIPHERED IMAGES

	Plain Image (512×512)				**Encrypted Image (512×512)**			
	Lena	***Baboon***	***Barbara***	***Peppers***	***Lena***	***Baboon***	***Barbara***	***Peppers***
H-M1	7.4456	7.3579	7.4664	7.5715	7.9217	7.9224	7.9219	7.9201
H-M2					7.993	7.9993	7.9992	7.9992

TABLE V. PSNR VALUES BETWEEN PLAIN IMAGE AND CIPHERED IMAGE

	Lena	**Baboon**	**Barbara**	**Peppers**
PSNR-M1	9.2302	9.5219	9.1636	8.4925
PSNR-M2	9.2481	9.5384	9.1628	9.2813

VI. Conclusion and Perspectives

Although, several initiatives had been made in order to provide a secured Cloud environment, Elliptic Curve Cryptography (ECC) is considered to be one of the most efficient solutions with improved performance in computing power and battery resource requirements. Recently, ECC had provided a robust and secured model for the development and deployment of secured application in the Cloud. In the present work, we proposed an efficient crypto-system to ensure the data security in cloud Datacenters. The main contribution of the present work consists in designing a hybrid scheme using a new implementation of ECC functions combined with OTP and SHA-3 algorithm. Finally, the proposed cryptosystem was implemented on the SCHIaaS Cloud simulator to better test its performances. We evaluated the execution time of the proposed crypto-system and we noticed that by increasing the size of the elliptical curve parameters the execution time increases while remaining an acceptable time. Moreover, the security level ensured by the designed system has been proven with a set of security tests which were applied on standard images. As future work, we propose to implement several attacking scenarios in order to evaluate the efficiency of the proposed approach that should meet all security requirements.

References

[1] C. Wang, Q. Wang, K. Ren, N. Cao, Wenjing, “Toward Secure and Dependable Storage Services in Cloud Computing”, IEEE Transactions on Services Computing, vol. 5, no. 2, pages 220–232, April 2012.

[2] A. Alharbi, H. Zamzami and E. Samkri “Survey on Homomorphic Encryption and Address of New Trend”, International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 11, No. 7, 2020.

[3] D. Adrian, S. Creese, M. Goldsmith, “Insider attacks in cloud computing. Trust”, Security and Privacy in Computing and Communications (TrustCom) IEEE 11th International Conference, 2012.

[4] Getov, Vladimir. "Security as a service in smart clouds--opportunities and concerns." 2012 IEEE 36th Annual Computer Software and Applications Conference. IEEE, 2012.

[5] Abuhussein, Abdullah, et al. "Evaluating security and privacy in cloud services." 2016 IEEE 40th annual computer software and applications conference (COMPSAC). Vol. 1. IEEE, 2016.

[6] R. Yadav, S. Srinivasan, S. Gupta, “Security Analysis of RSA and ECC in Mobile Wimax”, International conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016.

[7] National Institute of Standards & Technology (NIST), “Secure Hash Standard (SHS)”, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, 2015.

[8] Mushtaq, M. Faheem, et al. “Cloud computing environment and security challenges: A review”, International Journal of Advanced Computer Science and Applications (IJACSA), 8.10 (2017): 183-195.

[9] Aldossary, Sultan, and William Allen. “Data security, privacy, availability and integrity in cloud computing: issues and current solutions”, International Journal of Advanced Computer Science and Applications (IJACSA), 7.4 (2016): 485-498.

[10] Victor S. Miller, “Use of Elliptic Curves in Cryptography”, Conference on the Theory and Application of Cryptographic Techniques, 1985.

[11] B.Thirumala, R. Naresh, “A Study on Data Storage Security Issues in Cloud Computing”, International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016), pages 128–135, 2016.

[12] A. Mohammed, A. Ben Soh, E. Pardede, “A Survey on Data Security Issues in Cloud Computing : From Single to Multi-Clouds”, JOURNAL OF SOFTWARE, vol. 8, no. 5, May 2013.

[13] Sherman S. M. ChowYi-Jun HeLucas C. K. HuiSiu Ming Yiu. SPICE–Simple Privacy-Preserving Identity-Management for Cloud Environment, In International Conference on Applied Cryptography and Network Security, volume 7341, pages 526–543, 2012.

[14] H. Guiqiang, D. Xiao, T. Xiang, S. Bai, Y. Zhang, “A Compressive Sensing Based Privacy Preserving Outsourcing of Image Storage and Identity Authentication Service in Cloud”, Information Sciences, September 2016.

[15] Kamara and Lauter . CS2: A Searchable Cryptographic Cloud Storage System,IJSIR,2012.

[16] Farash MS, Attari,MA (2014) A secure and efcient identity-based authenticated key exchange protocol for mobile client-server networks. J Supercomput 69(1):395–411.

[17] Xie Q, Wong DS, Wang G, Tan X, Chen K, Fang L (2017) Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model. IEEE Trans Inf Forensics Secur 12(6):1382–1392.

[18] Chang CC, Wu HL, Sun CY (2017) Notes on “secure authentication scheme for IoT and cloud servers”. Pervasive Mob Comput 38:275–278.

[19] Kumari S, Karuppiah M, Das AK, Li X, Wu F, Kumar N (2018) A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. J Supercomput 74(12):6428–6453.

[20] Mo J, Hu Z, Chen H, Shen W (2019) An efcient and provably secure anonymous user authentication and key agreement for mobile cloud computing. Wireless Commun Mob Comput. https://doi. org/10.1155/2019/4520685.

[21] Schiaas. SCHIaaS : IaaS simulation upon SimGrid. http ://-schiaas.gforge.inria.fr/simschlouder.html, June 2017.

[22] S. Somaraj, M. Ali Hussain, “Performance and Security Analysis for Image Encryption using Key Image“, Indian Journal of Science and Technology, vol. 8, no. 35, December 2015.

[23] Sharma, Tejinder. "Proposed hybrid RSA algorithm for cloud computing." 2018 2nd international conference on inventive systems and control (ICISC). IEEE, 2018.

[24] Amalarethinam, I. George, and H. M. Leena. "Enhanced RSA algorithm with varying key sizes for data security in cloud." 2017 World Congress on Computing and Communication Technologies (WCCCT). IEEE, 2017.

[25] Malarvizhi Kumar, Priyan, et al. "Cloud-and IoT-based deep learning technique-incorporated secured health monitoring system for dead diseases." Soft Computing 25.18 (2021): 12159-12174.