Securing Data Storage in Cloud Computing

H. Guesmi, C. Ghazel and L. A. Saidane
Cristal Lab, National School of Computer Sciences.
University of Manouba – Tunisia

***Abstract*— This paper addresses the need for users to trust the commercial cloud providers and the security issues of storing data in a cloud storage service. The cloud storage is one of the prominent services offered in cloud computing. Data stored over cloud in the plain text format is a security threat. This paper proposes a method for cloud storage that allows user to store and access the data securely. It also guarantees that no one can access the data neither the cloud storage provider except the authenticated user. This method provides security and privacy for data stored in public servers.**

Keywords*— *Cloud Computing Security, Cloud Storage Security, Elliptic Curve Cryptography

I. INTRODUCTION

Cloud Computing is a technology that uses central remote servers and the internet to maintain data and applications. This technology enables businesses and consumers to use applications without installation and allows them to access their personal files at any computer with internet access. Cloud Computing allows for much more efficient computing by centralizing storage, memory, bandwidth and processing. But, in addition to its advantages, cloud storage brings various security issues. Data confidentiality appears as the biggest interest for users of a cloud storage system. Indeed, the clients' data are managed out of their governance. Meeting compliance requirements and enforcing security policy are tough enough when you deal with third parties and their known or unknown subcontractors.

In this paper we propose a method for improving data confidentiality in cloud storage systems by providing the method that encrypts the client data before sending to cloud storage using secret key and decrypts the data after receiving from cloud storage using the same secret key. These operations are done at client side making use of secret key. In this way user is assured about security of data stored in cloud and secret key never leaves the user computer.

This paper is organized as follows. Section 2 covers the general model of cloud computing that embraces services models and Cloud computing features. Then, we review some prevalent security challenges in cloud computing environment in Section 3. Section 4 deals with the general concept of Elliptic Curve Cryptography. The proposed model is discussed in section 5 and finally, Section 6 describes the conclusion and the future research works.

II. CLOUD COMPUTING MODELS

Cloud computing came into the Internet benefits as a computing resources because of the advancement of Infrastructure as Services. The features of cloud computing are as take after that are classified into four principal models [1]. Public Cloud is made accessible to the overall public or large industrial groups and it is provided by a single supplier offering some unique and requesting Cloud Services. Private Cloud is worked singularly for an association in a constrained manner with the total exclusive access of the outer individuals from the association. The Hybrid Cloud is a blend of two or more clouds. It enables data transportability through load adjusting between clouds. Supplying security in the hybrid cloud computing is much more difficult particularly for symmetric key distributions and mutual authentication. The Community Cloud Model is shared by a few organizations Agreement (SLA). A particular community shares concerns like requirements, policy, and compliance considerations. The expense of utility of the infrastructure is generally shared inside of the model organization.

There are five Cloud Characteristics as determined in [2]. On Demand Service Clouds is a large resource and service pool that the client can get service or resource at whenever he needs by paying the amount of services used. Ubiquitous Network Access is to provide services through standard terminal like Laptops, mobile phones, and Personal Digital Assistant (PDA). The Easy Use characteristic is that most cloud providers offer web based interfaces that are easier than application program interfaces which allow the clients to utilize the cloud services simpler. Cloud is a Business Model in light of the fact that it is "pay according to use" of the service or resource. The Location Independent Resource means that providers computing resources are pooled to serve numerous clients using multitenant model with diverse physical and virtual resources progressively assigned and reassigned according to demand.

III. SECURITY CHALLENGES IN CLOUD COMPUTING ENVIRONMENT

Every cloud computing based service has different sorts of security challenges. An intruder can utilize the vulnerabilities of network infrastructure to attack the services on features of cloud like on demand self-service, multi-tenancy, broad network access etc. This could make a considerable measure of vulnerabilities in the service delivered [3]. An overview conducted by [4] demonstrates that security is a major concern toward the clients staying far from the cloud. In this subsection, we analyze different sorts of security that back their heads prevalently in the applications deployed on the cloud.

A. Security issues of Network Infrastructure

With the services provided over the cloud Computing Environment, network infrastructures have caused several security issues and challenges. The attacks Distributed Denial of Services (DDOS) are realized by malicious software. They

prevent the server from providing services to its users by sending un-accessible request to the client. DDOS attack is performed on other machines when a system on the cloud is hacked and used as base. To obtain the main information about the user, attacker can analyze all packets passing through the system. But to find out the open port that can be attacked, scanning is done. Attackers use SQL injections to attack the cloud based database [5].

B. Security issues of the Web Services

The web services are vulnerable to many sorts of attacks. These vulnerabilities emerge because of the implementation mechanism and existing protocols in web services. These are described in table1.

TABLE I. VULNERABILITIES OF WEB SERVICES

Vulnerabilities	**Description**
Buffer Overflows	Xml can be forced to call itself severally thereby overflowing the memory. This could trigger error message and makes the application reveal information about itself.
Xml Injection	XML injections are used to insert a parameter into a query and let the server execute the data.
Session Hijacking	An attacker can inject a soap message and obtain the session digital identity thereby representing himself as an authenticated user to the server. Later on, he can go on to perform some serious mischief to the server.
Security Risk due to Cloud Features	Service user losses control over the data as it stores on other's servers, the user has to depend on the provider's security arrangement and its analyses.

C. Security Issues of Applications Available over the Cloud

The applications available on cloud computing can confront some sort of attacks like that are on model of client-server. To deliver their services to the client, SaaS applications depend on the web browsers and web services. The services PaaS and IaaS are hardware dependent and face more challenges emerging out of features of the cloud computing than SaaS infrastructure [4]. Security challenges emerging out of the network infrastructure and web services are described in table2.

One of the different ways that could deal with these issues is the Public key Infrastructure (PKI). There are different sorts of public key cryptographic schemes. Elliptic Curve Cryptography is one of them and it is the covering of next research in the next section.

TABLE II. SECURITY ISSUES OF CLOUD APPLICATIONS

Security Issues	**Description**
Regulatory compliance	In some cases, some cloud computing providers do not make an external audits and security certifications. In view of this, it is strongly suggested that cloud computing as a body should have a regulatory and disciplinary outfit that would consistently meet the target of the consumers.
Privilege User Access	Sensitive data processed outside the organization brings malicious data that are inherent in raising the level of risk. Cloud Providers should ensure they have adequate and strong anti-virus mechanisms in the processing of their outputs for dispensing such cloud critical systems to the consumers.
Data Location	When cloud is used, in most cases, the user does not know where the cloud is hosted. The cloud providers should give specific locations of their services if they expect trust and advantageous patronize of their services by the customers. This would also improve data recovery should the data is lost for want of recovery mechanism technology.
Investigative Support	This is a worrisome problem; investigation on cloud computing in the aftermath of fraud is a significant issue. This is more observable because laws demarcation divergence in countries of perpetration of the heinous act.

IV. ELLIPTIC CURVE CRYPTOGRAPHY

Neal Koblitz and Victor Miller independently suggested, in 1985, the use of elliptic curves in public key cryptography [6, 7]. While maintaining an equal level of security, supporters of elliptic curve cryptography (ECC) claim that ECC requires much smaller keys than those used in conventional public key cryptosystems. Therefore, the use of elliptic curves cryptography allows faster encryption and decryption.

Elliptic curve cryptography Diffie- Hellman Algorithm was described in [6,8]. If a user wants to communicate (sends/downloads data) with cloud service provider securely over an insecure network they can exchange a private key over this network in the following way:

- *P* is a particular rational base point that is published in a public domain for use with a particular elliptic curve *E(Fq)* also published in a public domain.
- User and cloud service provider pick random integers *a* and *b* respectively as private keys.
- User and cloud provider compute *a*P* and *b*P* and exchange values over an insecure network.
- Using the information exchanged, both User and cloud provider compute *(a*b)*P = a*(b*P) = b*(a*P)*. This value is then the shared secret that only User and Cloud provider possess.

The difficulty of the ECDLP (Elliptic Curve Discrete Logarithm Problem) ensures that the private keys *a* and *b* and the shared secret *(a*b)*P* are difficult to compute given *a*P* and *b*P*. Thus, cloud providers and their clients do not compromise their private keys or their shared secret in the exchange.

A. ELliptic curve cryptography Encryption/Decryption

There are different approaches using elliptic curves, to encryption/decryption, have been analyzed. This paper presents one of them. The first object is to encode the plaintext message *m* to be sent as an *x-y* point *Pm*. The point *Pm* will be encrypted as a cipher text and thereafter decrypted. This system requires a point *G* and an elliptic group *Ep(x,y)* as parameters. Each user *A* selects a private key *nA* and generates a public key *PA*.

$$PA = nA \times G \quad (1)$$

To encrypt a message *Pm* and send it to *B*, *A* chooses a random positive integer *a* and produces the cipher text *C* consisting to the pair of points [8].

$$C = \{aG, Pm + aPB\} \quad (2)$$

Note that *A* has used the public key of *B*: *PB*. To decrypt the cipher text, *B* multiplies the first point in the pair by the secret key of *B* and subtracts the result from the second point:

$$Pm + aPB - nB(aG) = Pm + a(nBG) - nB(aG) = Pm \quad (3)$$

B. Operations of ECC

In cryptography the Elliptic Curve used consists of set of points which are imposed on the curve equation. Suppose $P= (x1,y1)$ and $Q= (x2,y2)$ are two points on the elliptic curve $y^2 = x^3+ax+b$, then the two points can be added together to produce another point R on the curve such that $-P= (x3,y3)= P+Q$ as depicted in figure1.

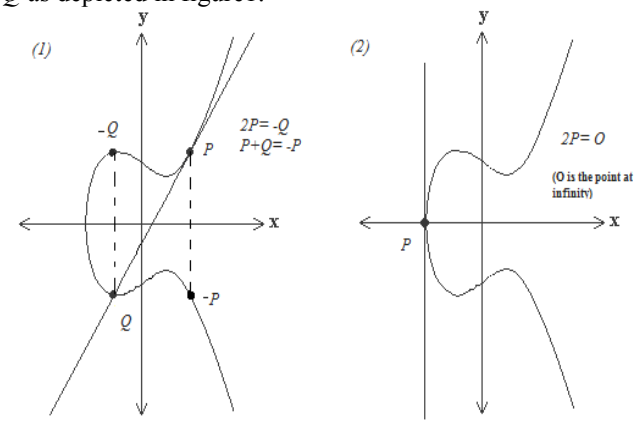

Fig. 1. Addition points *P* and *Q* in elliptic curve E/R : $y2 = x3 + ax+ b$

V. PROPOSED SOLUTION

The ECC discrete points over a finite field are used as a cyclic group. All types of schemes based in public cryptography can be implemented as analogous using the ECC. Elliptic Curve Cryptography has not gained the same popularity like the ELGamal and RSA schemes although it gives the level of security as the other public cryptographic based schemes. The ECC is based on elliptic curve discrete logarithm [9,10]. The Elliptical Curve Discrete Log Problem (ECDLP) makes it difficult to break an ECC as compared with the RSA and DSA algorithms where the problems of factorization or the discrete log problem can be solved in sub-exponential time. This signifies that in ECC smaller parameters can be used than in order competitive systems such as the DSA and RSA. This advantage greatly helps to minimize energy in processing.

We exploit the technique of elliptic curve cryptography encryption, in order to achieve secure storage and access on outsource data in the cloud. The proposed model can treats two parts in the cloud storage server, private data section and shared data section. The user use the private data section to store his private data that is accessible to particular user only, and use the shared data section to store the data that needs to be shared among trusted users. All the data stored in both section will be encrypted by using data storage model (DS-Model).

A. Authentication

Authentication Model treats the cloud security problem that is based on the critical information on transmission: authentication and non-repudiation between client and cloud.

To access the service from cloud, user must be authenticated. Username and password pair is the used security mechanism for data access. After the user provides the username and password, the authentication model (Au-Model) computes *A* = *hash* (*password*) and encrypts *A* with client's secret key then with cloud's private key to have *C* and send it to cloud service provider to verify the authenticity of the user. Then, user will be allowed to access cloud services. The architecture Au- Model is shown in figure 2.

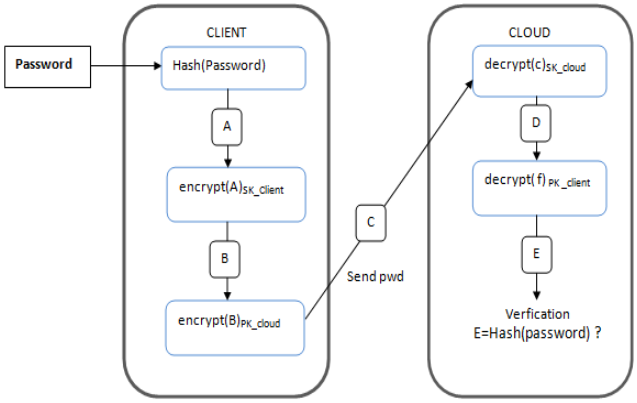

Fig. 2. Authentication-Model

B. Encryption/ Decryption

Data storage model (DS-Model) treats data security on cloud-based virtual infrastructure, which should ensure confidentiality, integrity and availability.

As this method is founded on secret key cryptography, the data stored on private data section is encrypted by ECC private key and the data stored on shared data section is encrypted by ECC public key. When a user wants to send a message he must have a key pair suitable for the elliptic curve cryptography which consists of a secret key *x* (that is a randomly selected integer) and a public key *Q* (where $Q = xG$ and *G* is the base point of primes order of the curve chosen from the elliptic curve equation). The data that has to be stored in a cloud cannot be stored in plaintext format so it must be changed into an encrypted format. Cryptographic model encrypt the user's data using the secret key of user then public key of cloud provider.

When user requests to download data stored on cloud, server send the data in encrypted format. Cryptographic model will decrypt it, and original file is available to client.

C. Signature

The data *I* received by cloud will be decrypted using client's public key then cloud's secret key to have the file *K*. Data storage model decrypts the data encrypted *G* to have the original file named *DATA* then computes *hash* (*DATA*) and compares it to the signature *K* to verify if the original file is not modified during its transmission. The architecture DS-Model is shown in figure 3.

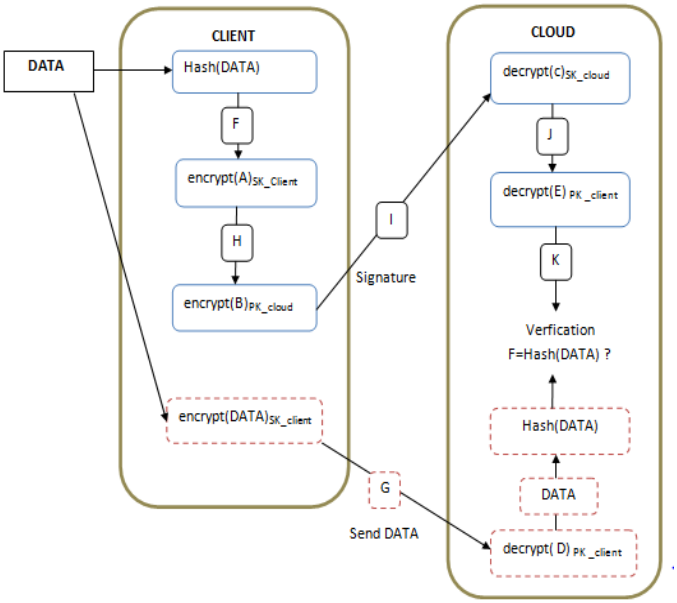

Fig. 3. Data Storage Model

The Cryptographic model defines a set of hash functions in accordance to the ECC encryption and signature schemes in use [11]. The Signature sent with data is computed as an encryption of *hash* (*DATA*): *Signature* = *encrypt* (*Hash* (*DATA*)).

40*1260The different notations used in fig.3 are listed in Table3.

TABLE III. NOTATIONS USED

Notation	Description
SK_client	Client Secret key
PK_client	Client Public key
SK_cloud	Cloud Secret key
PK_cloud	Cloud Public key

VI. CONCLUSION

The main object is to securely store and access data in cloud that is not controlled by the owner of the data. To secure storage and accessing data files in the cloud we exploit the technique of elliptic curve cryptography. The ECC algorithm used for encryption is an advantage to improve the performance during encryption and decryption process. We assume that this method of storing data have high performance and is much secure.

In this scheme just member of group can access the data stored over shared data section. The future research inclination in cloud computing models is going on to treat the problem of group sharing of data in the shared data section.

REFERENCES

[1] G. Veerraju, I. Srilakshmi, M. Satish, "Data Security in Cloud Computing with Elliptic Curve Cryptography," *International Journal of Soft Computing and Engineering (IJSCE), 2012.*

[2] J. Don , M. Alfred , V. Scott, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security, 1*(1), 36-63, 2000.

[3] P. Liu, "*The definition and Characteristics of cloud computing*." Retrieved from http://blog.sina.com.cn/blog_5f0da559010cmxw.html, 2011.

[4] T. Abhuday, Y. Parul, "Enhancing Security Cloud Computing Using Curve Cryptography." *International Journal of Computer Applications, 57*(1), 26-30, 2001.

[5] M. Dijk, J. Ari, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing." *Computing, 305*, 2001.

[6] V. Miller. "Uses of Elliptic Curves in cryptography," CRYPT'85, LNCS 218, pp.417-426, 1986.

[7] N. Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, vol. 48, pp. 203- 209, January 1987.

[8] W. Stallings. "Cryptography and Network Security: Principles and Practice." (3rd ed.). Prentice Hall, Upper Saddle River, New Jersey, 2003.

[9] H. Liao, Y. Shen, "On Elliptic Curve Digital Signature Algorithm" *Tunghai Science, 8*, 109-126, 2006.

[10] NIST, "*NISt Brief Comments on Recent Cryptanalytic Attack on SHA-1*." Retrieved from http://crsc.nist.gov/hash_standard_comments.pdf, (2005).

[11] D. Ratna, B. Rana, S. Palash. "Pairing-based cryptographic protocols : A survey." 2004.