Network and Communication Technologies; Vol. 2, No. 2; 2013
ISSN 1927-064X E-ISSN 1927-0658
Published by Canadian Center of Science and Education

Network Security in Cloud Computing with Elliptic Curve Cryptography

Victor O. Waziri[1], Ojeniyi J. Adebayo[1], Hakimi Danladi[2], Audu Isah[2], Abubakar S. Magaji[3] & Muhammad Bashir Abdullahi[4]

[1] Department of Cyber Security Science, School of ICT Federal University of Technology, Minna, Nigeria

[2] Department of Mathematics/ Statistics, School of Natural and Applied Sciences, Federal University of Technology, Minna, Nigeria

[3] Department of Mathematical Sciences, Faculty of Science, Kaduna State University, Kaduna, Nigeria

[4] Department of Computer Science, School of ICT, Federal University of Technology, Minna, Nigeria

Correspondence: Victor O. Waziri, Department of Cyber Security Science, School of ICT Federal University of Technology, Minna, Nigeria. E-mail: Victor.waziri@futminna.edu.ng

Received: February 20, 2013 Accepted: April 25, 2013 Online Published: November 27, 2013

doi:10.5539/nct.v2n2p43 URL: http://dx.doi.org/10.5539/nct.v2n2p43

Abstract

This paper researches on cloud computing based-on authentication for the security verification using Elliptic Curve Digital Signature Algorithm (ECDSA). The study structure simply focuses on the communication interaction of the Cloud providing communities and a pictured Smartphone user. The Elliptic Curve Cryptosystem is envisioned as the basic framework for data transmission security in the paper that proffers solution. We reviewed various literatures on the elliptic curves and applied the cyclic elliptic curve group based-on finite field modulo q. With the theory established, we applied the Elliptic Curve Digital Signature Algorithm as developed by ElGamal to carry out some exemplified computational sequences. The detail of the computational algorithm was done in Mathematica as given by (Jouko, 2011) with no modifications except in its translational interpretation to fit into cloud computing security environment as maybe applied by the cloud providing communities to accelerate and meeting the needs of the users on-demand as a service with embedding security consideration. Our contribution to the cloud computing environment is brought about through computational experimental activities as exemplified in this field for interactive security awareness through digital signature authenticating mechanism.

Keywords: security, cloud computing, standardization, authentication, Elliptic Curve Digital Signature Algorithm, physical security

1. Introduction

Cloud Computing is the modern paradigm that is synonymous with grid computing (which is based on the resources sharing, and making collaboration in the distribution of services between different enterprises in different geographical zones through the Internet providers). Cloud computing enhances the distribution of services for the Internet users. It is a computing mission on resource pools that include a large amount of computing resources. With cloud computing advancement as a new resource of computing on the Internet that provide assorted kinds of cloud services, also bring some security problems on the distribution of services over the Internet. At the moment, most computing systems provide digital identity for the users to access their services; these bring some inconveniences for hybrid cloud that includes multiple private and public clouds. However, the advantage of using cloud are numerous which include: i) reduced hardware and maintenance cost; ii) accessibility around the globe, iii) flexibility and the highly automated process wherein customer need not worry about software up-grading, physical hardware purchases and some basic infrastructures which tend to be a daily problem in computing environments (Robit, Ritupara, Nabendu, & Sugata, 2012; Maggini, 2009; Harold, Liu, Shivnath, Jeffrey, & Sujay, 2009). The Cloud Computing systems that provide services to the Internet users apply the asymmetric or public key and private or traditional identity based cryptography that has some identity elements that fit well in the requirement of cloud computing.

This work aims at improving cloud computing within Cloud Organizations with encryption awareness based on Elliptic Curve Cryptography. Intensive computational directions are given through illustrative Cloud Computational practical examples as in (Juokolo, 2011) with the ECC.

The rest of the paper are as follows: Section 2 deals with the general model of cloud computing that embraces services models and Cloud computing features. Section 3 overviews Some Prevalent Security Challenges in Cloud Computing Environment, Section 4, reviews the general concept of Elliptic Curve Cryptography; in section 5, we look into the Elliptic Curve Digital Signature Algorithm (ECDSA, section 6 carries out some Computational Experiments using Mathematica and finally, Section 7 adduces the conclusion and peruse over the future research works

2. Cloud Computing Features and Model of Services

Cloud Computing came into the Internet services as a computing resources due to the development of Infrastructure as Services. The features of cloud computing are as follow that are categorized into four principal models (Veeraju et al., 2012):

i. **Public Cloud:** This cloud Infrastructure is made available to the general public or large industrial groups and it is provided by a single provider selling some unique and demanding Cloud Services.

ii. **Private Cloud**: This cloud for resource infrastructural distribution, is operated solely for an organization in a limited fashion with the total exclusive access of the external members of the organization. This is achieved through the manipulation of access control devices. The advantage of this model is the security of the transaction of the cloud computing services with Compliance and Quality of Service (QoS). Some companies and Universities use the private cloud to provide cloud computing to their clients and students respectively. Private cloud is also known as Internal Network. Providing security in private cloud is easier.

iii. **Hybrid Clouds**: This cloud infrastructure is a combination of two or more clouds. It enables data portability through load balancing between clouds. Providing security in the hybrid cloud computing is much more difficult especially for symmetric key distributions and mutual authentication. Moreover, for users to access the services in a hybrid cloud computing, user digital identity is normally needed for the servers of the cloud to manage the access control. Hybrid computing consists of many different kinds of clouds and each of them has its own complex identity management. This therefore signifies that a user on the hybrid cloud that wants to access services from different clouds services environment could have multiple inconveniences in giving out different digital identities to the service providers.

iv. **Community Cloud:** This model of cloud infrastructure is shared by several organizations Agreement (SLA) otherwise known as contractual agreement. A specific community shares concerns like requirements, policy, and compliance considerations. The cost of utility of the infrastructure is commonly shared within the model organization.

Using cloud computing services, users can store their critical information (data) in servers stacked by the Cloud Service Providers (CSP) and can access their data anywhere in the parts of the world where Internet providing facilities are available and do not need to worry about their systems breakdown or disk faults. Besides, users can use one system to share their information and work; moreover, they can play games together on the same system simultaneously. Such CSPs are the Amazon, Google, IBM, Microsoft and Yahoo are the forerunners on the applications of cloud computing services in modern businesses Internet connectivity. Companies like the SalesForce, FaceBook, YouTube, MySpace etc also have begun to provide all kinds of computing services for the Internet Users.

2.1 Cloud Characteristics or Features

As derived in reference (Don, Afred, & Scott, 2001):

1) **On Demand Service Clouds:** This is a large resource and service pool that the user can get service or resource whenever she needs by paying the amount of services she uses.

2) **Ubiquitous Network Access:** Clouds provide services everywhere through standard terminal like mobile phones, Laptops and personal Digital Assistant (PDA).

3) **Easy Use:** Most cloud providers offer internet based interfaces which are simpler than application program interfaces which enable the users to use the cloud services easier.

4) **Business Model:** Cloud is a business model because it is “pay as per use” of the service or resource.

5) **Location Independent Resource:** The providers computing resources are pooled to serve multiple customers using pooling using multitenant model with different physical and virtual resources dynamically assigned and reassigned according to demand

2.1.1 Cloud Solutions

These services are categorized into five prominent sections as follows:

i. **Infrastructure as a Service (IaaS):** This provides a platform virtualization environment as a service rather than purchasing servers, software, data centres etc

ii. **Software as a Service (SaaS):** This service deploys software over the Internet which is deployed to run behind firewall in your LAN or PC.

iii. **Platform as a Service (PaaS):** This kind of cloud computing provide development environment as a service. You can use the middleman's (broker) equipment to develop your own program and deliver it to the user through the Internet and Servers.

iv. **Storage as a Service (StaaS):** This is database like services billed on utility computing services basis; e.g gigabyte per month

v. **Desktop as a Service (DaaS):** This is the provisioning of the desktop environment either within a browser or as a terminal server

2.2 Clients of Cloud Computing Services

Clients of various kind for the cloud computing abound Google, Google app Engine': http://code.google.com/aapengine and Liu Peng, http: //blog.sina.com.cn/blog_5f0da5590100cmxw.htm. These ranges from hardware clients to Software Clients. Hardware Client are also called thick client; are full featured computers. Thin client are designed for specific purposes mainly with input/output (i/o) interfaces. Mobile thin clients consist of Phones with operating system which lets the access of the cloud from anywhere. Software Clients include rich or fat client which include desktop applications connected to the internet, Web Applications/thin client run on web browsers like Google calendar. There are lots of resource sensitive clients of cloud computing like the RFID.

Mobile devices are of various kinds and structures; these include Smartphones, Notebooks, tablets etc. They all have less weights, memory and dependent on battery life. The application developers for the clouds have to keep these variations and constraints in mind. Cloud Computing provide services as saviour for many kind of networks applications as some of the computations can easily be outsourced from the cloud. This can be implemented in the cloud or developed an application which uses cloud for some specific tasks.

With the advancement of Internet speed and increase in computing power of Smartphones and tablets, a wide number of users who will access applications on the Clouds is increasing exponentially and by the day. So the Service providers for the Cloud Computing need to develop applications while keeping such facts securely embedded in their minds. Operating systems running on such clients aforementioned should be designed to conserve the battery life span with networking support built in the operating system. Since most of the service devices are mostly of small sizes and are capable of running in Internet environment of simplicity and with short life span, they need secure algorithms with small consuming energy power that are durable and portable.

3. Some Prevalent Security Challenges in Cloud Computing Environment

As noted earlier, Cloud Computing as an umbrella term involves different types of technology and services that are distributed over such computing environments as parallel as in grid computing that provides assorted computing services to the user on demand. Each of these services provide enormous opportunity for small and medium scale enterprises to grow their businesses using the service critical infrastructure provided with zero deployment.

Having said and done on the essential of the Cloud benefits such as providing lower cost service and ease of application, each cloud computing based service has various kinds of security challenges. An intruder can use the vulnerabilities of network infrastructure to attack the services on features of cloud like multi-tenancy, on demand self-service, broad network access etc. This could create a lot of vulnerabilities in the service delivered (Liu, ibid). A survey conducted by the IDC shows that security is a major concern for the users staying away from the cloud as computing services (Abhuday & Parul, 2012). In this subsection, we are analyzing various kinds of security that rear their heads predominantly in the applications deployed on the cloud. They include both traditional security challenges and recent challenges which came into prominence because of cloud computing which could be referenced in (Madhan, Sarukesi, Paul, Sai, & Revathy, 2012; Gens, 2009; Abhuday & Parul,

2012; Narpat & Sekhawat, 2011; Foster et al., 2008).

3.1 Security as a Result of Network Infrastructure

Network infrastructures have raised several security issues and challenges with the services being provided over the cloud Computing Environment. Distributed Denial of Services (DDOS) attacks are performed by malicious software to prevent the server from providing services to its clients by sending un-accessible request to the user. A system on the cloud can be hacked and used as base to perform DDOS attack on other machines. Attacker may analyze all packets passing through the system to gather important information about the user, But scanning (Dijk, Marten, & Ari, 2010) is done to find out the open port that can be attacked to get into the system., SQL injections are used to attack the cloud based database.

3.2 Security Risk Due to the Web Services

Network infrastructure web services are vulnerable to several kinds of attacks. These vulnerabilities arise due to implementation mechanism and existing protocols in web services. These are as follows:

a. **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.

b. **Xml Injection:** XML injections be used to insert a parameter into a query and let the server execute the data

c. **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

d. **Security Risk due to Cloud Features:** Security risk arises for services based on cloud due to its features. Service user losses control over the data as it stores on other's servers, the user has to depend has to depend on the provider's security arrangement and its analyses. A situation may arise where service provider might have to move to other provider or back to its server at different geographical location. In most cases, data stored in the cloud could get locked up in other server and it is difficult to move them from the provider to the user or another provider. Most of the cloud service providers support multi-tenancy services. Isolation of data from other organization's employee residing on the same server is also a challenge for the server provider. If client ceases to use the service provided by data ownership, issues could arise as some providers would refuse to release them at some later unspecified date. Also if the user fails to pay his used services, the provider could lock up the data stored and refuse to release them. Instances abound which the availability of the applications running on cloud is locked up and formed great concern for the user as cloud outages. Cloud outages have happened several times; for instance Gmail (locked up for one day in mid-October in 2008; Amazon S3/ over several hours downtime in July 20, 2008 and FlexiScale had outage for 18 hours on October, 2008. So many of these unpleasant occurrence happened in October in the year 2008.

3.3 Security Issues of Applications Available over the Cloud

Applications deployed on cloud can face some kind of attacks as that are on client-server model. SaaS based applications are vulnerable to the virus; online operating systems are available on cloud to the user for free. Viruses can spread as attachment of email, past of the software or can stay in MBR of the operating system available on the cloud. Worms residing on one system in the cloud can migrate to another system on its own. Trojan horse is software with wrong intentions. It gets divided into parts when loaded from memory. SaaS applications depend on the web services and web browsers to deliver their services to the user. They are security challenges arising out of the network infrastructure and web services in (Madhan, Sarukesi, Paul, Sai, & Revathy, 2012; Gens, 2009; Abhuday & Parul, 2012). IaaS and PaaS services are hardware dependent and face more challenges arising out of features of the cloud computing than SaaS infrastructure.

As identified in this section, Public key Infrastructure (PKI) is one of the various ways that could handle some of the issues afore-stated. There are various kinds of public key cryptographic schemes-Elliptic Curve Cryptography is one of them which is the crust of next research examinations in the next subsequent sections. ECC in its complementary application could solve the problem of Security dissemination and power optimizing in the mobile phones that communicate with the CSPs.

3.3.1 Cloud Computing from Practical Analysis

Cloud Security risks as identified through vendors are listed here under (Abhuday et al., 2012)

As we have noted above, cloud services present many challenges to an organization. As soon as Service level

Agreement (SLA) is reached between an organization and the service providers in consuming the services, especially cloud services, much of the computing system infrastructure control is always under the control of the cloud providers. This poses a lot of challenges. As a result, it is suggested that such challenges should be resolved through management initiatives which will clearly delineate the ownership and responsibility roles of both the cloud provider and the organization functioning in the role of the clients or users.

Security managers of the cloud computing on the provider and the user sides that determine what detective and preventive control exist on the cloud should be able to clearly define security posture for the both cloud environments at their individual ends.

Proper security control is expected to be implemented based on asset, threat, and vulnerability risk assessment matrices.

Cloud computing risk (Veerraju et al., 2012) assessment report mainly from vendor's point of view about security capabilities analyzed security risks faced by the cloud:

i. **Regulatory compliance:** In some cases, some cloud computing providers do refuse to 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

ii. **Privilege User Access:** Sensitive data processed outside the organization fro the cloud computing environment 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.

iii. **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.

iv. **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.

3.3.2 Proposed Solutions

In our previous section and subsections, we see that cloud computing is based on dispensing of data through transfer by virtualization process. As a result, it is imperative to have concern over the data storage. Users are anticipated apply the traditional IT security and the cloud computing security. For instance is advised that the users should know the location of the storage host; this is practically a traditional strategeous step in the right direction and best of human insight. That is users should know the exact location of their data and should also know other sources of the collectively stored with theirs if possible.

To preserve security on cloud-based virtual infrastructure, providers should ensure data confidentiality, authentication, integrity, and availability which should provided using the techniques

a. **Encryption:** All sensitive data may be required to be encrypted using some high secure cryptographic scheme on the provider OS software before sending the encrypted data on traffic over the ever busy Internet network transmission channel.

b. **Physical Security:** Keep the virtual cloud systems and the cloud management hosts safe and secure behind carded doors, and the local environment safe

c. **Authentication and Access Control:** The authentication capabilities within all virtual systems by the provider should copy the way other physical systems authenticate. One time password and biometrics should all be implemented in the same manner. Thus all encrypted data should provide authentication technique from one cloud to another cloud. To achieve this onerous and unique technique of authentication, it is advisable that digital signature should be applied in cloud data transfer.

4. Elliptic Curve Cryptography

The techniques for Jensen et al. (2009) the need of information security on the Internet had led to the evolution of Cryptography with many techniques involving. In a nutshell, cryptography is the science of keeping information secure and therefore, it is a useful tool cloud computing security. It involves encryption and decryption of messages for transmission over the Internet to the rightful recipients. The secrecy of any cryptographic scheme is the key use for the encrypting/decrypting processes of the would-be transmitted data

information. Many of the cryptographic algorithms are available publicly, though some organizations believe in having the algorithmic key a top secret through encryption.

The idea of the elliptic Curve cryptography (ECC) as a cryptographic scheme was proposed by Miller (1986) and Neil (1987) independently. It gives the same level of security as the RSA and ELGamal cryptosystems but with smaller key size. The ECC discrete points on the elliptic curve over a finite field are used as a cyclic group. All types of public cryptography based schemes can be implemented as analogous using the ECC. ECC gives the level of security as other cryptographic schemes provide but it has not gained some acceptable popularity like the ElGamal and RSA schemes. It is based on elliptic curve discrete logarithm (SEC 1 Elliptic Curve Cryptography, 2000), www.bouncecastle.org (Liao & Shen, 2006) and NIST (2005). The Elliptical Curve Discrete Log Problem (ECDP) makes it difficult to break an ECC as compared to the RSA and DSA algorithms where the problems of factorization or the discrete log problem can be solved in sub-exponential time. This means that significantly smaller parameters can be used in ECC than in other competitive systems such as the RSA and DSA. This helps significantly in minimize the energy in processing.

4.1 Arithmetic Operations of ECC

The Elliptic Curves used in cryptography consist of set of points which are imposed on the curve equation. Suppose $L = (x_1, y_1)$ *and* $J = (x_2, y_2)$ 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 $-L = (x_3, y_3) = L + J$ as depicted in Figure 1.

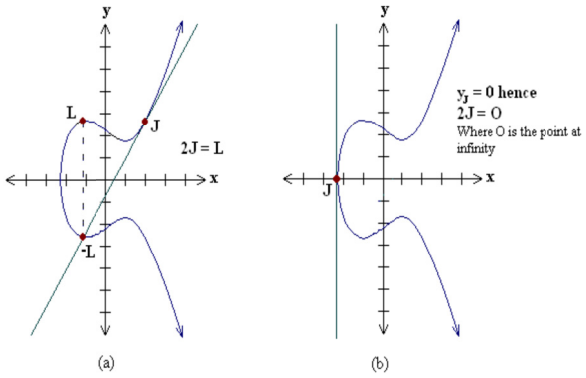

Figure 1. The elliptic curve depicting points

4.1.1 The Background of ECC

This part will provide an intuitive introduction to Elliptic Curve cryptography as we shall in section 3 for the development of encryptions and ECDSA. Let K be a field, and let $\overline{K}$ denote its algebraic closure:

Definition 4.1 (Projective Plane): The projective plane $P^2(K)$ over K is the set of one-dimensional $sub-vectorspaces\ of\ K^3$, which are in turn seen as equivalence classes of the set $K^3 \setminus (0,0,0) \bmod ulo$ scalar multiplication. The class containing the point $(X, Y, Z) \neq 0$ is denoted $(X : Y : Z)$.

Definition 4.2 (Smooth Weierstrass Equation): A Weierstrass equation is a homogeneous equation of degree 3 of the form:

$$\begin{aligned} F(X,Y,Z) &= Y^2Z + a_1XYZ + a_3YZ^2 \\ &= X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \end{aligned} \tag{1}$$

where $a_1, a_2, a_3, a_4, a_6 \in \overline{K}$.

It is said to be smooth or non-singular if the projective points

$$P = (XPY : Z) \in P^2(\overline{K}) \tag{2}$$

satisfying the equation, we have

$$\left(\frac{\partial f}{\partial X}(P), \frac{\partial f}{\partial Y}(P), \frac{\partial f}{\partial Z}(P)\right) \neq (0,0,0) \tag{3}$$

Definition 3.3 (Elliptic Curve): An elliptic curve E is the set of all solutions in $P^2(\overline{K})$ of a non-singular Weierstrass equation. There is exactly one point in E with Z-coordinate equal to O, namely (0,0). This point is called the point at infinity, and denoted O. The point at infinity is also designated the identity element of the Elliptic curve. We can write, for convenience, the Weiestrassss equation in affine (non-homogeneous) coordinates, $x = \frac{X}{Z}, y = \frac{Y}{Z}$, thus obtaining the equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4}$$

An elliptic curve E is the set of all of solutions of equation (4.4), together with the point at infinity O. If the coefficients of the equation are defined over K, we say that E is defined over K, and denote it as E/K.

Definition 4.4 (Rational Position on E): If E is defined over K and L as an extension of K, the set of L-rational points, denoted E(L), is the set of points of E with coordinates in L, together with the point at infinity O.

The set of elliptic curve comes endowed with an abelian group structure. The addition operation called group law, and point O is the zero elements in this group structure. Besides, formulas exist for sum of two points, which consists only algebraic operations on the coordinates of the points involved.

Elliptic Curves are calculated over various fields mostly: Real Field, Finite Field and over Binary fields. Narpat et al. (2011) defines elliptic curve over real as a set of points in the plane $P^2(\overline{K})$ which satisfies an algebraic equation:

$$y^2 = x^3 + bx + c \tag{5}$$

This set of equations could also be defined over the complex field.

We, in this subsection, will look into the elliptic curves based on Finite Field and Binary Field group laws under the expression Galois Field.

Multiplication Law: Let E be a given elliptic curve field over the field of real such that

$$E : y^2 = x^3 + ax + b(\mathrm{mod}\, p) \tag{6}$$

For a, b are given parameters in whatever is the appropriate set (rational numbers, complex numbers, integers mod n, etc). We also include a "point at infinity ∞" as defined earlier. Multiplication law is also known as the group law. Group Law can be categorized into three types, which include the real field, the Finite field involving real or complex fields and the Binary Field group laws. In this paper, we review the Finite Field Law and the Binary Field Law.

An elliptic Curve Galois Field GF(P) where P is a prime, can be defined as the points P(x,y) which satisfy Equation (3.6) with a further condition that $4a^3 + 27b^2 \neq 0(\mathrm{mod}\, p)$. Definition of addition and doubling of point's condition enclosed in to Equation (2.6), it enables the points so formed on the elliptic curve to form a group with addition and doubling of the points. This concept also integrates the point at infinity which is the identity element.

To achieve an efficient implementation on the elliptic curve, field Arithmetic (involving modular addition, subtraction, multiplication and inversion) must be available. These operations are used in the logarithm for addition and doubling points. Suppose we have two points on an elliptic curve E at points given as $P(x_1, y_1)$ *and* $Q(x_2, y_2)$, then the sum of P and Q given as $L(x_3, y_3)$:

$$\begin{aligned} &P(x_1, y_1) + Q(x_2, y_2) = L(x_3, y_3); \\ &where\ x_2 \neq x_3 \end{aligned} \tag{7}$$

$$\lambda = \frac{(y_2 - y_1)}{(x_2 - x_1)};$$

$$\begin{aligned} x_5 &= \lambda^2 - x_1 - x_2; \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned} \tag{8}$$

Doubling Formula for Fields of Characteristic Two:

Suppose

$$\begin{aligned} &P(x_1, y_1) \in E\ and\ Q(x_2, y_2) \in E\ with\ P = Q \\ &then\ P + Q = (x_3, y_3);\ where \end{aligned}$$

and $E \neq 0$:

$$x_3 = x_1^3 + \frac{a_6}{x_1^2} \tag{9}$$

and

$$y_3 = x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3$$

Doubling formula when $E = 0$**;** that is the elliptic curve equation is super-singular.

Let

$P(x_1, y_1) \in E$ *and* $Q(x_2, y_2) \in E$ *with*
$P = Q$ *then* $P + Q = (x_3, y_3)$; *where*

$$x_3 = \frac{x_1^4 + a_6^4}{a_3^2} \tag{10}$$

and

$$y_3 = \left(\frac{x_1^2 + a_4}{a_3}\right)(x_1 + x_3) + y_1 + a_3 \tag{11}$$

It is really advantageous to select a curve and field K so that the number of field operation involved in adding two points and doubling a point are minimized.

4.2 Simplified Weierstrass Equations Over Galois Field $GF(2^m)$

If we perform some analysis by simplification, we shall obtain the some important equations: $GF(2^m)$ such that:

$$(x, y) \to (a_1^2 x + \frac{a_5}{a_1}, a_1^2 y + \frac{a_1^2 + a_3^2}{a_1^3}) \tag{12}$$

We get other important equations:

$$y^2 + xy = x^3 + ax^2 + b \tag{13}$$

where $x, y, a, b \in GF(2^m)$.

The points in E are denoted as:

$$GF(2^m) = \{(x, y) : x, y \in GF(2^m)\} \tag{14}$$

Satisfying

$$\{y^2 + xy = x^3 + ax^2 + b\} \cup \{O\} \tag{15}$$

In some way, for the curve

$$E : y^2 + xy = x^3 + ax^2 + b \tag{16}$$

$$R = P + Q = (x_R, y_R)$$

can be determined by the following formulae

$$x_R = \lambda^2 + \lambda + ax^2 + b \tag{17}$$

$$y_R = \lambda(x_p + x_R) + x_R + y_R \tag{18}$$

where

$$\lambda = \frac{y_Q + y_p}{x_Q + x_p} \tag{19}$$

To double a point J to get L, i.e. to find L = 2J, consider a point J on an elliptic curve as shown in Figure 2.1. If y coordinate of the point J is not zero then the tangent line at J will intersect the elliptic curve at exactly one more point –L. The reflection of the point –L with respect to x-axis gives the point L, which is the result of doubling the point J. Thus L = 2J.

If y coordinate of the point J is zero then the tangent at this point intersects at a point at infinity O. Hence 2J = O when J = 0. This is shown in Figure (3.1b)

Consider a point J such that J = (x_J, y_J), where $y_J \neq 0$.

Let L = 2_J where L = (x_L, y_L), then

$x_L = s^2 - 2x_J$

$y_L = -y_J + s\,(x_J - x_L)$

s = $(3x_J + a) / (2y_J)$, where s is the tangent at point J and a, is one of the parameters chosen with the elliptic curve If $y_J = 0$ then 2J = O, where O is the point at infinity.

5. Elliptic Curve Digital Signature Algorithm (ECDSA)

This section describes the problem of security of the clouds that is based on the critical information on transmission: authentication and non-repudiation between the cloud computing organizations. Suppose that clouds C_1 *and* C_2 computing companies agree to carry out electronic business together based on ECC algorithm, then, they must carry out the following transactional mandatory agreement:

Both sides must know the following curve parameters which are used in the algorithm for the ECDSA. There are eight parameters: (p, a, b, G, n, Q). The field size is p, a and b are the two field elements that define the equation of the curve E; G is the base point of primes order of the curve chosen from the elliptic curve equation, n is the order of the points of the elliptic curve. The cloud that signs the message must have a key pair suitable for the elliptic curve cryptography which consists of a private key x (that is a randomly selected integer in the interval $[1, n-1]$ and a public key Q; (where $Q = xG$).

5.1 Generation of the ECDSA

The algorithm for the signing of the ECDSA between the two clouds should follow this pattern [18, 19, 20, 21, 22]:

1) Select an integer k from within the [1, n-1].
2) Calculate the $r = x_1 (\mathrm{mod}\, n)$ *where* $(x_1, y_1) = kG$; a scalar multiplication of k with the base point G. If $r = 0$, abort and restart from 1.
3) Compute $e = SHA-1(m)$; and covert this into an integer string H(m); this gives the message digest.
4) Calculate $s = k^{-1}(e + rx)(\mathrm{mod}\, n)$. If $s = 0$, abort and go back to step 1.
5) Cloud C_1's signature the message m is the pair (r, s).

It is imperative for the two clouds to select different k for different signatures; otherwise, the equation in step 4 can be solved for s, which is the private key.

5.1.1 ECDSA Signature Verification

To verify the signature (r, s) on, cloud C_2 obtains an authentic copy of domain parameters $(P, E_p(a,b), G, n)$ and associated key Q=xG. C_2 then does the following:

(1) Verify that r and s are the integers in the interval [1, n-1].
(2) Computes SHA-1(m) and convert the string to an integer H(m).
(3) Compute $w = s^{-1} (\mathrm{mod}\, n)$.
(4) Compute $u_1 = H(m)w (\mathrm{mod}\, n)$ and $u_2 = rw (\mathrm{mod}\, n)$.
(5) Computes $X = (x_2 y_2) = u_1 G + u_2 G$.
(6) If $X = 0$, then reject the signature. Otherwise, compute $V = x_2 (\mathrm{mod} n)$.
(7) Accept the signature.

5.1.2 Proof of the Signature Verification

If a signature (r,s) [22, 23. 24] on a message m was indeed generated by cloud C_1, then $s = k^{-1}(H(m) + xr)(\mathrm{mod}\, n)$. Rearranging gives

$$\begin{aligned} kG &= s^{-1}(H(m) + xr)G(\mathrm{mod}\, n) \\ &= s^{-1}H(m)G + s^{-1}rG(\mathrm{mod}\, n) \\ &= u_1 G + u_2 G(\mathrm{mod}\, n) \end{aligned}$$

Thus $u_1G + u_2G = (u_1 + u_2)G = kg$ and so $v = r$ as required.

6. Computational Experiments

In this experimental section, we give two types of curves: Ordinary elliptic curves and the pseudo-random curve of type P-192. The first is the normal curve while the other is the Federated approved one used for encryption with large primes, large order and cofactor $f = 1$. For each prime *p*, a pseudo-random curve

$$E: y^2 = x^3 - 3x + b(\text{mod}\, p)$$

of prime order *r* is listed. (Thus, for these curves, the cofactor is always *f* = 1.). The following parameters are given:

i. The prime modulus *p*
ii. The order *r*
iii. the 160-bit input seed *s* to SHA-1 based algorithm
iv. The output *c* of the SHA-1 based algorithm
v. The coefficient *b* (satisfying $b^2 c \equiv -27$ (*mod p*))
vi. The base point *x* coordinate G_x
vii. The base point *y* coordinate G_y

The integers *p* and *r* are given in decimal form; bit strings and field elements are given in hex. The pseudo curve P-192 has the following standardized parametric values in hexadecimal and decimal.

p = 6277101735386680763835789423207666641 60839087\ 00390324961279

r = 6277101735386680763835789423176059013767194 7\ 73182842284081

s =3045ae6f c8422f64 ed579528 d38120ea e12196d5

Ds = 3.57037640433E+24

c = 3099d2bbbfcb2538 542dcd5fb078b6ef5f3d6fe2 c745de65

Dc = 9.40077580134E+26

b =64210519e59c80e7 0fa7e9ab72243049 feb8deec c146b9b1

Db = 1.93677622648E+27

Gx =188da80eb03090f67cbf20eb43a18800f4ff0afd 82ff1012

DGx = 4.749307753E+26

Gy =07192b95ffc8da78 631011ed 6b24cdd5 73f977a1 1e794811

DGy = 1.37301502687E+26

6.1 Key Establishment between Two clouds

Suppose we have the transaction between a Cloud Providing Organization and the client (which may be viewed as a smartphone user) computing organizations which we denote as C_1 and C_2. We use this to produce an example of elliptic curve cryptosystem authentication which is based on ElGamal Cryptosystem.

Let $y^2 = x^3 + 3x + 45(\text{mod}\, 8831)$ be the elliptic curve chosen by the two clouds and a base point $G = \{4,11\}$. Cloud C_1 message that is encoded on the elliptic Curve is the point $P_m = \{5,1743\}$.

The User C_2 chooses a secret key $a_B = 3$ and it computes a new point $a_B G$ on the established curve as follows using Mathematica as a computing software:

$$In[1] = multell\{4,11\},3,3,45,8831]$$

to obtain the point

$$Out[1] = \{413,1808\}$$

Mobile C_2 publishes this point as its public key.

Cloud C_1 chooses a secret key and computes its public key using the same pattern as cloud C_2. Suppose that C_1 chooses its secret key as $k = 8$, then it will compute:

$$In[2] = multell\{4,11\},8,3,45,8831]$$

and output

$$Out[2] = \{5415,6321\}$$

In the characteristic manner of the derivation of the encryption as emphasized in section 4, cloud C_1 encodes the message $P_m = \{5,1743\}$ as a new point on the curve using the encryption algorithm $E_{key}(x_1, y_1) = \{kG,\ P_m + k\{a_B G)$. Substituting the necessary computed values above and applying them on Mathematica cloud C_1 message becomes:

$$In[3] = addell\ [\{5,1743\},$$
$$multell\ [\{413,1808\},8,3,45,8831],3,45,8831]$$

to obtain:

$$Out[3] = \{6626,3576\}$$

Cloud C_1 sends $\{5415,6321\}$ and $\{6626,3576\}$ to Smartphone C_2 who upon obtaining the message, multiplies this output with its secret key:

$$In[4] = multell[\{5415,6321\},3,3,45,8831]$$

to obtain:

$$Out[4] = \{673,146\}$$

Smartphone C_2 upon getting cloud C_1 message, subtracts the result from the last point out as in (Veerraju, Srilakshmi, & Satish, 2012) Note that the subtraction is fully in line with the subtraction of points which is achieved by adding the points with the second coordinate negated as in the elliptic curve algorithm modelled in section 3. The computational process is as follows:

$$In[5] = addell[\{6626,3576\},\{673,-146\},3,45,8831]$$

to obtain:

$$Out[5] = \{5,1743\}$$

Thus Cloud C_2, by this computational sequence receives the message sent by cloud C_1.

6.1.1 More Practical Experiment of ECSDA Using Mathematica

In this subsection as in (Aqeel, Kaldip, & Sandiap, 2010; Siham & Subramania, 2011; Jouko, 2011; Lawrence & Wade, 2002), we give detail works based on Elliptic Curve P-192 whose domain parameters are given in section 4. This experiment shows directly from (Jouko, 2011).

First let us list all the points on the Elliptic Curve $y^2 = x^3 - 3a + b(\text{mod}113)$ using Mathematica as our computing tool:

$q = 83; pts = \{\};$
$For[[x = 0, x < q, x++$

$If[Mod[y^2 - (x^3 - 3x + 10), q] = 0,\ pts = Append[pts, \{x, y\}]]]]$
$pts = pts\{0\}\ //\ S\ s\tan dardForm$

This gives the output:

{0,{0,33},{0,50},{2,26},{2,57},{3,32},{3,51},{5,28},{5,55},{7,83},{8,83},{9,31},{9,52},
{11,35},{11,48},{13,33},{13,50},{18,12},{18,71},{20,27},{20,56},{21,24},{21,59},{22,36},
{22,47},{26,24},{26,59},{28,7},{28,76},{30,32},{30,51},{31,34},{31,49},{32,35},{32,48},
{33,18},{33,65},{34,6},{34,77},{36,24},{36,59},{39,38},{39,45},{40,35},{40,48},{41,1},
{41,82},{43,17},{43,66},{44,30},{44,53},{47,5},{47,78},{48,20},{48,63},{50,32}{50,51},
{51,17},{51,66},{52,21},{52,62},{53,18},{53,65},{54,39},{54,44},{57,5},{57,78},{58,8}
{58,75},{59,6},{59,77},{60,14},{60,69},{62,5},{62,78},{63,11},{63,72},{67,19},{67,64},
{68,83},{70,33},{70,50},{71,12},{71,71},{72,17},{72,66},{73,6},{73,77},{77,12},{77,71},
{79,37},{79,46},{80,18},{80,65},{82,26},{82,57}}

Let us consider the following test on the p-192 curve based on Mathematica version 7 or newer. Consider the following domain parameters as agreed upon by the two cloud formations:

G = {6020462823 7568865675 8213480587 5261119166 9897663688 4684818 , 1740503322 936
2203140485 7552280219 4103640234 8892738665 0641};

b = 2455155546 0089438177 4029391519 7451784769 1080581611 91238065 ;

q = 6277101735 3866807638 3578942320 7666416083 9087003903 24961279;

n = 6277101735 3866807638 3578942317 6059013767 1947731828 4081;

Cloud C_1 carries out the following simulation by choosing a private key and computes its public key $Ya = kaG$:

ka = 2818646689 2849679686 0388568073 9626753757 7176687436 85369;

$Ya = Mult[ka, G, q, -3, 6]$

which yields:

Ya = {4166887439 9597854423 5935840162 6820195302 1303968539 22747090 ;
3420024909 4382013935 6288313636 6848346822 1077345149 8261724 }

Cloud C_2 chooses a private key kb and like cloud C_1, computes his public key this manner:

kb = 2101924874 3290807195 7364927874 9582309136 1968294450 0;

$Yb = Mult[kb, G, q, -3, 6]$

and yields:

Yb = {3197479727 3104411841 6665995417 6065551017 8136042108 49295029 ;
4546651453 2634953489 3230378313 7537190292 5909292275 44435757 }

The two computing structures have now computed their public keys; they now compute the same private key K in this order:

$KC_1 = Mult[kb, Ya, G, q, -3, 6]$

$KC_2 = Mult[ka, Yb, G, q, -3, 6]$

The both yield the same K:

KC_1 = {4569158537 9095858773 2989382824 9154554821 1213792385 90872510 ,
5889543201 4129985997 5026390898 2414398530 5181387950 41140383 }

KC_2 = {4569158537 9095858773 2989382824 9154554821 1213792385 90872510 ,
5889543201 4129985997 5026390898 2414398530 5181387950 41140383 }

Therefore the shared private key between clouds $C_1 \, and \, C_2$ is:

K = {4569158537 9095858773 2989382824 9154554821 1213792385 90872510 ,
5889543201 4129985997 5026390898 2414398530 5181387950 41140383 }

Texts messages are first encoded into integers before importing into the curve. Instance of this transformation is the Mathematica code:

$m01 = ToCharacte\ rCode$("$Transilvan\ ia$"};

$mo2 = ToCharacte\ rCode$("$Romania$ "

The strings are the texts to be encoded which are output as:

$mo1$ = {84,114 97, 110, 119, 97, 110, 105, 97};
$mo2$ = {82, 111,109 ,97, 105, 97}

The Clouds now insert these encoded words into an encrypted format as follows:

$(m1, m2\} = Mod$ [{$FromDigits$ [$mo1$,256],
$FromDigits$ [$m01$,256]}, q]

which produces the output:

{$m1, m2$} = {2613501847 5037405047 417185, 2320346366 7018081}

Now create a random key k and compute Ya:

$ka = Random$[$Integer$, {1, $q-1$}];

{kx, ky} = $Mult[ka, Yb, q, -3, b]$

$Ya = Mult[ka, G, q, -3, b]$

$\{kx, ky\}$ = {1491376168 3039545722 9117120423 3258426738 7251098676 91358216 ,
1214573518 8892133118 3196713283 1397062260 1125523158 25754 }

Ya = {4316361940 5243084887 3794569746 2164920394 1632731022 55552918 ,
5011586538 8192151832 3600164576 0568529066 0139556229 38010874 }

$\{c1, c2\} = Mod[\{k * m1, ky * m2\}, q]$(*ciphertext*)

$\{c1, c2\}$ = {4128091592 7955672136 4603048227 7962704855 5283313224 50992878 ,
8931547195 7531687594 8317128832 0956286990 0935206662 3304183 }

$kxinv = Power[kx, -1, 8]$;

$kyinv = Power[ky, -i, q]$;

The two simulations output the following inverses:

$\{z1, z2\}$ = {2613501847 543603704 7407185, 2320346366 7018081}

The message encoded is retrieved from the Mathematica following code:

$FormCharac\ \ terCode\ [IntegerDig\ \ its\{z1,256\}]$

$FormCharac\ \ terCode\ [IntegerDig\ \ its\{z2,256\}]$

which gives the original message:

Translvania

Romania

6.1.2 ECC Computational Experiment

To authenticate the encryption, Cloud C_1 takes the following steps as in [24]:

1) sends Cloud C_2 a random message $R = (r1, r2)$
2) C_2 encrypts it and sends response $C = (c1, c2)$
3) C_1 decrypts message with $C_2's$ public key which is obtained from certification authority. If there is a map matching, C_2 is authenticated

6.2 Elliptic Curve Digital Signature Experiment

We experiment a Mathematica implementation as in [24, 25] of the ECDSA. First let us review details of the ECDSA curve based on p-192 as done in section 4:

The Curve p-192 is a standardized curve defined as $y^2 = x^3 - 3x + b(\mathrm{mod} q)$ with a base point generator G.

The following details are performed by Cloud C_1:

(1) Computes $z = hash$ value of the message.
(2) Generates a random key k.
(3) Computes public key kG.
(4) Computes 2 numbers -1.
(5) $r = (kG)\ and\ s = k(z^{-1} + ra) \bmod n$.
(6) Sends the digital signature $DS = (r, s)$.

Cloud C_2 does the following verifications:

(1) Computes $z = hash$ value of the message'.
(2) Computes $w = s^{-1} \bmod n$.
(3) Computes $u_1 = z * w \bmod n$ and $u_2 = r * w \bmod n$.
(4) Computes point $(x_1, y_1) = u_1 G + u_2 G$ QA.

Cloud User C_2 verifies if: $r = x1 \bmod n$ then the signature is verified.

6.2.1 Computational Experimental Testing of the ECDSA on p-192 Curve

G = {6020462823 7568865675 8213480587 5261119166 9897663688 4818,
1740503322 9362203142 4857552280 2194103640 2348892738 6650641 };

b = 2455155546 0089438177 4029391519 7451784769 1080581011 91238065 ;

q = 6277101735 3866807639 9578942320 7666416083 9087003903 24941279 ;

n = 6277101735 3866807638 3578943117 6057013767 1947731828 42284081 ;

Cloud C_1's private key a and public $QA = aG$:

a = 918273645

$QA = Mult[a, G, q, -3, b]$

aG = {9964766172 0712176637 3775085331 2189
7185967729 1912391531 403, 1826671883 1
7357352264 0443946381 8706611511 42903
5326747870 55}

Message m and its ShA-hash:

m ="*Today the weather in Branov is Sunny*";

$z = Hash[m, "Sha"]$

z = {1325693890 5635126176 5017176293 5808176293 5800176203 117924031 }

C_1 creates random k and finally signature DS

$k = Random[Integer, \{1, n-1\}]$;

$r = Mod[Mult[k, G, q, -3, b][[1]], n]$;

yielding

r = 2805002020 6042585388 0106773998 4705333980 2187182641 5552405

$s = Mod[PowerMod[k, -1, n] * (z + r * a), n]$; giving

s = {6344230263 7467492751 3840555052 8894708324 5926534857 7926529 }

$DS = \{s, r\}$ = 6344230263 7467492751 3840555052 8894708324 5926534857 7926529 ,
2805002020 6042585388 0106773998 4705333980 2187182641 5552405 }

Cloud C_1 sends the digital signature DS which Cloud C_2 verifies as follows:

m ="*Today the weather in Branov is Sunny*"

$z = Has[m, "SHA"]$

z = 1325693890 5635126176 5017176293 5806176263 117924031

$w = PowerMod[s, -1, n]$

w = {7097174448 6688645107 4716979713 3369836049 2000339674 5493765 }

$u_1 = Mod[z * w, n]$

$u_2 = Mod[r * w, n]$

These respectively output the following:

u_1 = {1943471050 0416668706 6710311155 1522236113 2550672029 792224}

u_2 = 1040969572 5071744183 2503868745 8388850542 4784907826 04486423

$\{x1, y1\} = EllipticSum[q, -3, b, Mult[u_1, G, q, -3, b], Mult[u_2, G, q, -3, b]]$

This output:

$(x1, y1)$ = {1280500060 4258538890 1067739984 7053339802 1871826415 552405 ,
1225396249 6194132452 7038953790 6947698114 3855368224 73550584 }

r, $Mod[x1, n]$, pr int[" *signature is verified* "], pr int[" *Signature Failed* "]] ,

Yielding these two outputs:

1280500060 4258538890 1067739984 7053339802 1871826415 552405

2805002020604258538801067739984705333980218718264155552405

Signature is verified.

With the verification being true, User C_2 accepts the message as being authentic and that it comes from Cloud C_1.

7. Conclusion and Suggestion for Future Works

This work studies the cloud computing environment based on the transaction between the cloud provider and the Mobile User. The Cloud and the User can verify the transaction between them using the Elliptic Curve Digital Signature. Computational exposure of the work was well aligned through computational example using mathematica.

The future research inclination in cloud computing models is largely based on the interconnectivity betewween the cloud and Mobile Cloud Computing. Mobile Cloud Computing could be enhanced with the State-of-the-Art analysis in which strong support framework in Steganography and Cryptography could form the structure of the transmission of secure data over the insecure cloud. In this case, issue of privacy could be achieved maximally. We also need to work to improve on the minimization of energy consumption for these mobile devices to maximum fast computational processs and achieve efficient devices productivity.

References

Abhuday, T., & Parul, Y. (2012). Enhancing Security Cloud Computing Using Curve Cryptography. *International Journal of Computer Applications, 57*(1), 26-30.

Aqeel, K., Kaldip, S., & Sandiap, S. (2010). Implementation of Elliptic Curve Digital Signature Algorithm. *International Journal of Application, 5*(2).

Dijk, M. V., & Ari, J. (2001). On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing. *Computing, 305*, 1-8.

Don, J., Alfred, M., & Scott, V. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security, 1*(1), 36-63.

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). Cloud Computing and Grid Computing 360-Degree Compared. Grid Computing Environments Workshop, 2008. GCE '08 (pp. 1-10). http://dx.doi.org/10.1109/GCE.2008.4738445

Gens, F. (2009). New IDC IT Cloud Services Survey: Top Benefits and Challenges.

Google. (n.d.). *Google app Engine*. Retrieved from http://code.google.com/appengine

Harold, C., Lin, S. B., Jeffrey, S. C., & Sujay, S. P. (2009). Automated Control in Cloud Computing Opportunities and Challenges. *Proc. Of the First Workshop on Automated Control for data Centres and Clouds* (pp. 13-18). New York, NY, USA,

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). On Technical Security Issues in Cloud Computing. *Cloud Computing, 2009. CLOUD '09. IEEE International Conference on* (pp. 109-116). http://dx.doi.org/10.1109/CLOUD.2009.60

Jouko, T. (2011). *Cyclic Group Cryptography with Elliptic Curve*s. Finland: Ravaniemi University of Applied Sciences Rovaniemi.

Lawrence, C. W., & Wade, T. (2002). *Introduction to Cryptography with Coding Theory*. Prentice Hall, Upper Saddle River.

Lawrence, E. B. III. (2004). *The Elliptic Curve Digital Signature Algorithm Validation System (ECSDAVS)*. NIST Information Technology Laboratory Computer Security Division.

Legion of The Bouncy Castle. (2012). *Bouncycastle*. Retrieved from www.bouncecastle.org

Liao, H. Z., & Shen, Y. Y. (2006). On Elliptic Curve Digital Signature Algorithm. *Tunghai Science, 8*, 109-126.

Liu, P. (2011). *The definition and Characteristics of cloud computing*. Retrieved from http://blog.sina.com.cn/blog_5f0da5590100cmxw.html

Miller, V. S. (1986). Use of Elliptic Curves in Cryptography Advances in Cryptology. *Crypto, 85*, 417-426.

Neil, K. (1987). Ëlliptc Curve Cryptosystem. *Mathematics of Computation, 48*, 203-209. http://dx.doi.org/10.1090/S0025-5718-1987-0866109-5

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

Robit, B., Ritupara, C., Nabendu, C., & Sugata, S. (2000). *A Survey on Security Issues in Cloud Computing*. SEC

1 Elliptic Curve Cryptography: Certicom Research.

Shekhawat, N. S., & Sharma, D. P. (2011). Cloud Computing Security through Cryptography for Banking Sector. In *Proc. 2011, 5th National Conference*.

Siham, K. P., & Subramania, R. (2011). An Efficient and Secure Protocol for Ensuring Data Storag Security in Cloud Computing. *International Journal of Computer Science Issues, 8*(1).

Veerraju, G., Srilakshmi, I., & Satish, M. (2012). Data Security in Cloud Computing with Elliptic Curve Cryptography. *International Journal of Soft Computing and Engineering (IJSCE), 2*(3).