Elliptic Curve Cryptography for Securing Cloud Computing Applications

Alowolodu O.D, Alese B.K,
Adetunmbi A.O., Adewale O.S
Department of Computer Science,
Federal University of Technology, Akure, Nigeria

Ogundele O.S.
Department of Computer Science,
Federal University,Oye Ekiti, Nigeria.

ABSTRACT

Computing applications and data are growing so rapidly that increasingly larger servers and data centre are needed for fast processing within the required time. A fundamental shift in the way Information Technology (IT) and computing services are being delivered and purchased results in the development of cloud computing. The out of control cost of power in terms of electricity generation, personnel hardware and limited spaces in data centers have encouraged a significant number of enterprises to move more infrastructures into a third party provided Cloud. However, Cloud computing requires that organizations trust that a service provider's platforms are secured and provide a sufficient level of integrity for the client's data. Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. An important factor is the key strength, i.e. the difficulty in breaking the key and retrieving the plain text. In this paper, we proposed Elliptic Curve Cryptography scheme as a secure tool to model a Secured platform for the Cloud Application.

Key words: Cloud computing, Cryptography, ECC.

1. INTRODUCTION

Since the inception of Grid Computing which later developed into Cloud Computing, security issues posed great challenges to the Information Technology community. Cloud computing which was once a concept that was not really clear and understandable enough is becoming a new emerging technology that is arousing the interest of organizations industry players and even academics. The out of control cost of power in terms of electricity generation, personnel hardware and limited spaces in data centers have encouraged a significant number of enterprises to move more infrastructures into a third party provider which is the Cloud [38]. Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. It allows consumers and businesses to use applications without installation and access their personal files at any computer so far as there is internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Moving data into the cloud offers great convenience to overcome the complexities of direct hardware management. The pioneer of Cloud Computing vendors include Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) [3] offer internet-based online services by providing huge amounts of storage space and customizable computing resources. However, users are at the mercy of their cloud service providers for the availability and integrity of data [24]. It has been argued by critics of Cloud Computing that it is not secure enough and data integrity is compromised [33]. The fears tend to hold back the cloud computing market [26]. Nevertheless, the storage and computing on massive data are the driven impetus for a cloud computing infrastructures [10].

1.1 THE CLOUD ARCHITECTURE

Cloud architecture comprises of the systems architecture of the software systems involved in the delivery of cloud computing, and this involves multiple cloud components communicating with each other over application programming interfaces, usually web services. The two most significant components of cloud computing architecture are known as the front end and the back end.

In a typical cloud scenario, the user uploads the code and data to a cloud provider, which in turn runs this workload without knowledge of the code internals or configuration. Users benefit from offloading the management of their workload to the provider, while the provider gains from efficiently sharing their cloud infrastructure among workloads from multiple users. This sharing of execution environment together with the fact that the cloud user lacks control over the cloud infrastructure raises significant security concerns about the integrity and confidentiality of a user's workload.

One underlying mechanism enabling cloud computing is virtualization, be it at the hardware, middleware, or application level. While a large amount of research has focused on improving the security of virtualized environments, the ongoing work on building virtualization-aware security mechanisms for the cloud has taught that existing security techniques do not necessarily apply to the cloud because of the mismatch in security requirements and threat models.

In cloud computing, security applies to two layers in the software stack. First, users' workloads have to be run isolated from each other. Second, each user is also concerned with the security of their own workload (as in the case of a web service or Internet application). Many solutions exist for enforcing isolation between workloads which include the use of virtualization. Securing a particular workload is a much harder task and requires the knowledge of the code is part of the workload [26]. Cloud computing environments support grid computing by quickly providing physical and virtual servers on which the grid applications can run.

A representative network architecture for cloud data storage is illustrated in fig 1. The three different identifable network entities are as follows: User, Cloud Service Provider (CSP) and Third Party Auditor (TPA)

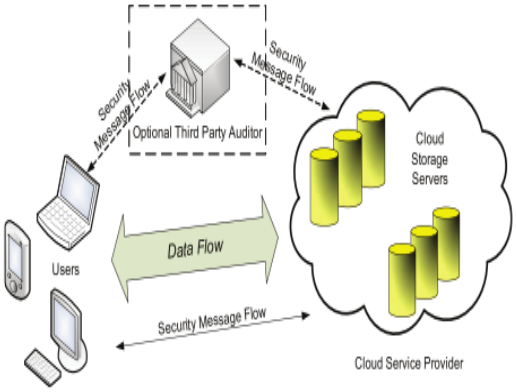

Fig. 1 Cloud data storage architecture [15].

2. MODELLING A SECURED CLOUD APPLICATION

From the perspective of data security, which is an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for a number of reasons. According to [15], traditional cryptographic primitives for the purpose of data security protection can not be directly adopted due to the users' loss of control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data by the Vendors [15]. The following are considered as platform for modeling the secured environment:

i. Creating data management scenario that releases the manipulation of data to the users by moving away from the third party which is the Cloud vendor.

ii. Providing opportunity for frequent update of stored data by the users which includes insertion, deletion, modification, appending, reordering, etc.

iii. Overcoming the limitation associated with the adaptability of correct data storage under dynamic data operations suitable for single server scenario to multiple server scenario.

iv. Overcoming data leakage which is associated with Cloud Computing attribute-Multitennancy

v. Preventing the threat posed by hackers that exploit security vulnerabilities at the user-end of the cloud computing chain.

vi. Exploring the inherent attributes in public key cryptography as far as security is concerned for modeling the secured cloud [1].

3. TRUSTED PLATFORM MODULE

Trusted Computing is a mechanism that controls the behavior of computer systems through enforcement of security policies via hardware and software controls. Deployment of trusted computing technology by Service Providers provides platform to verify the security posture in the Cloud and control the information, which achieve the economies of scale, availability, and agility that the Cloud promises. A key component of Trusted Computing is the Trusted Platform Module (TPM). The TPM is a cryptographic component that provides a root trust for building a trusted computing base. The TPM stores cryptographic keys in Platform Configuration Registers (PCRs) while the attestation process allows clients to request the PCRs of the TPM [26].

4. CRYPTOGRAPHIC TECHNIQUE

According to [17], a message in readable form is referred to in cryptographic terms as plaintext. The process of disguising a message in such a way as to hide its substance is called encryption and the resulting message is referred to as ciphertext. As shown in Figure 3, the reverse process (decryption) takes ciphertext, C as input and restores the original plaintext. P. The encryption function E operates on P to produce C:

$E(P) = C$

In the reverse process, the decryption function D operates on C to produce P:

$D(C) = P$

A cryptographic algorithm called a cipher, is a mathematical function that is used for encryption and decryption requires the cryptosystem kept secret. This method is called security by obscurity and is used only in very specific cases. All modern encryption algorithms use a key, denoted by K. The value of this key affects the encryption and decryption functions. The functions become:

E(K,P) 5C

D(K,C)5P

According to [17], the three main criteria that must be considered in cryptography are:

i. Functionality

ii. Security

iii. Performance

Other factors that influence a decision include the existence of best-practice standards developed by accredited standards organizations, the availability of commercial cryptographic products, patent coverage, and the extent of existing deployments.

According to [1], a class of Public Key Cryptography called Elliptic Curves Cryptography is equipped with inherent attributes that can be exploited for modeling the secured Cloud Application.

4.1. Elliptic Curve Cryptography

According to [34], Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications [34].

An elliptic curve E over a field K denoted by E/K is given by the Weierstraß equation

$$E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad 1$$

Where the coefficient,$a_1, a_2, a_3, a_4,$ and $a_6, \in$ K are such that for each point (x_1, y_1) with coordinates in K satisfying (Eqn.1), the partial derivatives $2y_1 + a_1 x_1 + a_3$ and $3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1$

do not vanish simultaneously. The last condition says that an elliptic curve is non singular or smooth. A point on a curve is called singular if both partial derivatives vanish. For shorter reference we group the coefficients in (Eqn.1) to the equation

$$E: y^2 + h(x) = f(x), h(x), f(x) \epsilon K[x], \deg(h) \leq 1, \deg(f) = 3 \; with \; f \; monic \quad 2$$

The smoothness condition can also be expressed more intrinsically. If

$$b_2 = a_1^2 + 4a_2, \; b_4 = a_1 a_3 + 2a_4, \quad 3$$

$$b_6 = a_3^2 4a_6, \; b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4^2 \quad 4$$

In odd characteristic, then the transformation $y \rightarrow y - (a_1 x + a_3)/2$ leads to an isomorphic curve given by

$$y^2 = x^3 + \frac{b_2}{4} x^2 + \frac{b_4}{2} x + \frac{b_6}{4} \quad 5$$

The above cubic polynomial has only simple roots over the algebraic closure K if and only if its discriminant is non zero. The equation of the discriminant is therefore useful to determine if (Eqn. 2) is an elliptic curve or not. In addition, it is relevant for characteristic2 fields as well. [25].

5. REVIEW OF SECURITY TECHNIQUES IN INFORMATION TECHNOLOGY ENVIRONMENT

Security is not a new issue and now it is recognized as one of the most complex problems. Due to an increase in the growth of network connectivity, the issue of network security is becoming increasingly demanding as far as size and implementation of new information technologies is concerned [4]; [32]. Several attempts have been made to provide security using a software agent systems approach. In these systems, the main focus was on providing a solution for specific security issues, such as authentication and authorization.

[2] ascertained the essence of network security and used Genetic Algorithm (GA) to differentiate between a normal network connection and an attack. The GA which is a programming technique that mimics biological evolution as a problem-solving strategy was used and a result of almost 95% success was achieved. One of the problems of GA was how to find a representation of the problem at hand since there are various ways by which the given problem could be represented / encoded. A good network security must be able to address the issue of availability, confidentiality, integrity accuracy, efficiency and usability. This means that a good security measure that will be on the Cloud must be able to work real time.

[9] also developed a framework using multi-agent systems for Internet security. The proposed system architecture of this approach composed of three different agent types classified on their functionalities. The first type is responsible for intrusion detection; the second type is responsible for encryption and decryption of messages, while the third type can act as the combination of the previous two types. Although this approach has provided useful security system, it does not address some other important issues such as authentication, authorization, digital signature, and verification security services. Other approaches focused on addressing the security issues for mobile agent systems. In another approach [22] have dealt with security issues in a project called DEEPSIA.(Dynamic on-line Internet Purchasing System based on Intelligent Agents) that supports companies as purchasers in electronic commerce e-procurement processes. They have focused on extending the well known KQML agent communication language to incorporate security functions and proposed a new S-KQML (Secure-Knowledge Query Manipulation Language) that includes authentication, integrity and privacy.

[29] have proposed an approach to solve some of the security problems in multi-agent systems, which utilizes delegation based trust management. However, the main focus of this approach was on authentication and authorization.

In the past decade, Grids has evolved as the infrastructure for delivering high-performance services for computer and data-intensive scientific applications [21]. To support research and development of new Grid components, policies, and middleware; several Grid simulators, such as GridSim [13], SimGrid [30], and GangSim [19] have been proposed. SimGrid is a generic framework for simulation of distributed applications on Grid platforms. Similarly, GangSim is a Grid simulation toolkit that provides support for modeling of Grid-based virtual organizations and resources. On the other hand, GridSim is an event-driven simulation toolkit for heterogeneous Grid resources. It supports modeling of grid entities, users, machines, and network, including network traffic.

[10] in their survey, gives insight into the well known cryptographic tools for providing integrity and consistency for data stored in clouds. The security solutions explored and discussed by them are keeping a local copy of the data, use of hash tree, protocols such as Proofs of Retrievability (POR), and Proofs of Data Possessions (PDP), Digital Signatures etc. These solutions still require a testing on some live data to validate their suitability and ease of use. A whitepaper by AWS (Amazon Web Services) discusses physical security, backups, and certifications in their context. Similarly, other providers such as Google, Microsoft etc. have discussed the security issues in cloud computing [26]; [39].

[12] have identified some prominent risks that customers must assess in order to utilize Cloud Computing infrastructures. In addition to these, several other major issues that must be addressed by the cloud service providers have been identified. These issues include data storage, server security, privileged user access, and data portability. They also present virtualization specific security issues in detail.

[31] has built a trust model in a distributed computing paradigm. To the best of their knowledge, none of the work so far, gives a direction to address the security challenges, specifically in cloud environments. Despite the fact that, there are solutions to address the prominent security issues, a

mechanism to measure the security risk from the perspective of a service user is strongly needed.

Data storage systems are expected to meet several rigorous requirements for maintaining users' data and information, including high availability, reliability, performance, replication and data consistency; but because of the conflicting nature of these requirements, no one system implements all requirement.

The ultimate challenge in cloud computing is data-level security, and sensitive data is the domain of the enterprise, not the Cloud Service Provider (CSP). Security will need to move to the data level so that enterprises can ensure the protection of data. With data-level security, the enterprise can specify which data is not allowed to go outside of the specific cloud server. It can also force encryption of certain types of data, and permit only specified users to access the data [28]. Cloud Data Storage System (CDSS) remains as ongoing problem for the local data center moving the data to the cloud just makes security more difficult. Many CSPs provide rudimentary security for data stored but none seem to have integrated strong authentication and encryption services that might provide true CDSS.

There are many cloud computing and CSPs, such as Google, IBM, Amazon, Sun Microsystems, HDS, Microsoft, Nirvanix, EMC, NetApp, HP, Symantec, etc. There are also more and more Cloud Data Storage (CDS) platforms, e.g., Amazon S, HDFS, Sun Network.com, CloudNAS, Data ONTAP, SkyDrive, FileStore, EMC Atoms, HP Upline, Hitachi Content Platform, GFS, KFS, Open Source Cloud Computing Environment (OSCCE) in University Putra Malaysia UPM.

A security policy is a set of rules for determining the maximum permissible access rights for a particular process to a particular segment, given the attributes of both the process and the segment. It is believed that CDSS in Cloud Computing is evolving, and many research problems are yet to be identified. The most promising one is believed to be the model in which public verifiability is enforced. Public verifiability, supported by [36] [5] [41], allows TPA to audit the CDS without demanding cloud users' time, feasibility or resources. [40], investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, Shacham Et al, proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. Erasure-correcting code in the file distribution preparation was adopted to provide redundancy parity vectors and guarantee the data dependability. By utilizing the homomorphic token with distributed verification of erasure-coded data, their scheme achieves the integration of storage correctness insurance and data error localization. Through detailed security and performance analysis, the scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks.

The computing power in a Cloud computing environments is supplied by a collection of data centers, which are typically installed with hundreds to thousands of servers [13]. The authors built architecture of a typical Cloud based data center that consist of four layers. At the lowest layers there exist massive physical resources (storage servers and application servers) that power the data centers. These servers are transparently managed by the higher level virtualization services and toolkits that allow sharing of their capacity among virtual instances of servers. These virtual instances are isolated from each other, which aid in achieving fault tolerant behavior and isolated security context [38\]. [28] described a formal "proof of retrievability" (POR) model for ensuring the remote data integrity. The scheme combines spot-cheking and error-correcting code to ensure both possession and retrievability of files on archive service systems. In a distributed servers work [37] built on this model and constructed a random linear function based homomorphic authenticator which enables unlimited number of queries and requires less communication overhead. [11] proposed an improved framework for POR protocols that generalizes both [37]; [11].

[11] proposed an improved framework for POR protocols that generalizes both [36] work. Later in their subsequent work, [11] extended POR model to distributed systems. However, all these schemes are focusing on static data. The effectiveness of these schemes rests primarily on the preprocessing steps that the user conducts before outsourcing the cloud data file. Any change to the contents, even few bits, must propagate through the error-correcting code, thus introducing significant computation and communication complexity.

In a data possession work [6] defined the "provable data possession" (PDP) model for ensuring possession of file on untrusted storages. Their scheme utilized public key based homomorphic tags for auditing the data file, thus providing public verifiability. However, their scheme requires sufficient computation overhead that can be expensive for an entire file. In their subsequent work [6] described a PDP scheme that uses only symmetric key cryptography. This method has lower-overhead than their previous scheme and allows for block updates, deletions and appends to the stored file, which has also been supported in our work. However, their scheme focuses on single server scenario and does not address small data corruptions, leaving both the distributed scenario and data error recovery issue unexplored. Our User Agent will do the same job of [6], [5].

In another data possession work [16] aimed to ensure data possession of multiple replicas across the distributed storage system. They extended the Portable Data Possession (PDP) scheme to cover multiple replicas without encoding each replica separately, providing guarantees that multiple copies of data are actually maintained. Our DER Agent will do the same job of [16].

In data integrity work [20] proposed to verify data integrity using RSA-based hash to demonstrate uncheatable data possession in peer-to peer file sharing networks. However, the proposal requires exponentiation over the entire data file, which is clearly impractical for the server whenever the file is large. In the same work [36] proposed to ensure file integrity across multiple distributed servers using erasure-coding and block-level file integrity checks. However, the scheme only considers static data files and does not explicitly studies the problem of data error localization.

[37] proposed allowing a Third Party Auditor (TPA) to keep online storage honest by first encrypting the data then sending a number of precomputed symmetric-keyed hashes over the encrypted data to the auditor. However, the scheme only works for encrypted files and auditors must maintain long-term state. [37] proposed to ensure file integrity across multiple distributed servers, using erasure-coding and block-level file integrity checks. However, this scheme only considers static data files and does not explicitly studies the problem of data error localization.

Cisco has developed the Secure Cloud Data Center Framework. This framework portrays the threat model of a cloud data center and the measures that take to mitigate security risks. Additionally, the framework shows the overarching controls, compliance, and SLA components. The key take-away in cloud data center security is that security should not be an afterthought or a building block; it should be pervasively implemented across all layers of architecture. The threat profile consists of elements such as service disruption, intrusion takeover, data leakage, data disclosure, data modification, and finally, identity theft and fraud. A cloud data center would be implemented with visibility and protection aspects across all building blocks [8].

Cryptography has always been an essential part of security. The challenge of this scheme is to apply typical cryptographic schemes to a Cloud Computing environment. Since much of Cloud Computing is based on replication, it is important to maintain the distinctiveness of encryption and decryption keys. Recently, Amazon faced a challenge with this issue on their Cloud systems. [9]. This problem has since been resolved, but lack of foresight in cryptography can lead to disastrous results. The application addresses the challenges presented by distributed cryptography, and comprise a large focus on encryption and key distribution. [9]. Ideally, this will be able to adjust and adapt existing security applications to serve as at least a basis for application. Generally, security incorporates both hardware and software aspects of Computer Science.

6. A PROPOSED CONCEPT OF PROVDING SECURED CLOUD APPLICATION

An application specific Cloud Computing model that will be based on the principle of resource sharing will be designed using SQL SERVER 2005 and JAVA application programming software. Vulnerability assessment of the resource being shared on the virtual datacenter will be carried out using the Trusted Platform Module (TPM). The TPM stores cryptographic keys that can be used to attest the operating state of the platform. The keys are used to measure the platform, which are then stored in the TPM's Platform Configuration Registers (PCRs) [27]. Data/Results obtained from the vulnerability assessment will then be analyzed in order to determine the degree of vulnerability of the Cloud application designed. To perform the assessment, a pre-measurement will first be carried out by the virtual data center architecture and a secure transfer protocol. This will tests the system security posture and allows information owners to determine the system before deployment. There is going to be a probe on the destination/target machines and identity information will be provided in the form of certificates which will be cryptographically encrypted and transferred to,;[' the virtual machine. This will now decrypts the certificate and examine the information received to determine its security. At the system environment, the probe application will receives and unseals the information from the source to know if it has been tampered with during transfer. This will be detected at the decryption phase. Methodology of Public Key Cryptosystem using Elliptic Curve mathematics as proposed by Alese formulation will be extracted and adapted in developing a formal model for the Cloud Application (Datacenter) security as follows:

A. Elliptic Curve Encryption Scheme

The encryption and decryption procedures for the elliptic curve analogy of the basic ElGamal encryption scheme adopted from [25] is presented by the underneath algorithm as analysed as follows: A plaintext m is first represented as a point M, and then encrypted by adding it to kQ where k is a randomly selected integer, and Q is the intended recipient's public key. The sender transmits the points to the recipient

$C_1 = kP$ and $C_2 = M + kQ$

The users private key is computed as

$C_1 = d(kP) = k(dP) = kQ,$

and the recovery message is computed as

$$M = C_2 - kQ.$$

An intruder will have to compute KQ in order to recover M.

According to [32a], an elliptic curve 'E' is a curve given by an equation (for a cubic or quadratic polynomial f(x)

$$E: y^2 = f(x) \quad 6$$

To ensure that the polynomial f(x) has no double roots so as to make the curve non-singular.

After a change of variables, the equation takes the simpler cubic form :

$$E: y^2 = x^3 + ax + b \quad 7$$

Extra point θ "at infinity" is added to the above equation so that E is really the set.

$$E = \{(x, y): y^2 = x^3 + ax + b\} \cup \{\theta\} \quad 8$$

Let there be a point $P_1(x_1, y_1)$ on any elliptic curve and to find $P_2(x_2, y_2)$ such that $P_2 = 2P_1$. This is known as Point Doubling and it can be done as:
Let$\lambda = x_1 + \frac{y_1}{x_1}$ then $x_2 = a + \lambda + \lambda^2$ and

$$y_2 = (x_1 + x_2)\lambda + x_2 + y_1 \quad 9$$

If there exists two points $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ on any elliptic curve and we want to find third point $P_3(x_3, y^3)$ such that $P_{3=}(P_{1+}P_2)$. This is known as Point Addition and it can be done as:

Let $\lambda = \frac{y_1 + y_2}{x_1 + x_2}$, then $x_3 = a + \lambda + \lambda^2 + x_1 + x_2$

And $y_3 = (x_2 + x_3)\lambda + x_3 + x_2 \quad 10$

B. Curve Selection

To select a Curve, one of the following are the things to put into consideration as stated by [19a]:

i. The group order has to be first chosen. Since the criteria require knowing the group order, it is easier and faster to select that parameter first and then build a curve having that attribute.

ii. Use a known curve (possibly in other fields) to build a curve with the desired properties .This approach likely limits the number and the types of possible curves that can be produced, making it an advantage for the attacker.

iii. Choose a random curve: This is the slowest method. First coefficients are generated to make a valid

elliptic curve, typically using a cryptographic random number generator. Then the number of points on the curve needs to be counted and factored. If one of the criteria is not satisfied, the values are discarded and start over. The algorithm used for counting points is Schoof's algorithm or the Schoof-Elkies-Atkin algorithm (SEA).

iv. Use a published curve: This is the easiest and fastest method. One concern is possible patent issues. Another is that the attacker may be more motivated to attack a publicly known curve since more people would use it. The chance of collision is also increased. Methods 1, 2 and maybe 4 likely produce curves with additional structure, which may be exploited by future mathematical advancements and discoveries. Although method 3 is slow, it is a better guard against future attacks on specific types of curves.

The components required for executing the task are as defined according to [34a] as follows:

• A prime number p

• A point P (with its components x and y) on a defined elliptic curve

• A scalar multiple k

• $'b'$ can be character base and it depends on the number of bits of processor. As $54xx$ is a 16-bit processor so $'b'$ in this case is 2^{16}

• Select a positive integer R which is larger than p and co-prime with p. $R = b^t >$ p may be used. t is taken as 10. So R in this case is 2^{160}

• Values of prime number p, point P and scalar multiple k used in my implementation are from the Recommended Domain Parameters document in [37a].

C Choosing the Elliptic Curve Parameters

As highlighted by [17], when choosing parameters of a public-key cryptosystem of which ECC is a class, the best parameters need to be chosen for a secure system. These are those that make brute-force key search the only method of attack and that produces a large number of keys for attackers to try. There is also the need to decide on a field and a group. The field determines how sequences of zeros and ones in the computer correspond to elements of the field and how computations are performed numerically. Consequently, the advertised strength of the cryptosystem is related to the size of the field. The group, on the other hand, affects the security of the cryptosystem. The group operation determines how elements are mapped to one another and thus shapes the encryption algorithm. The group structure helps ensure the difficulty of decryption without the correct key.

D. The Field Selection

In ECC as stated by [35], there are typically two choices of finite fields. One of them is the fields consisting of (2^m) elements (i.e. $GF(2^m)$). In this case, the way to represent elements of the fields needs to be specified because the implementation of multiplication is dependent on the field representation. Since modern computers are built using logic gates with binary states, this choice allows specifically designed hardware, or carefully implemented software, to speed up computations. The choice of the field does determine the equation used to generate points. In $GF(2^m)$, the equation used in the EC has the form

$$Y^2 = x^3 + ax + b$$ with the restriction

$$4a^3 + 27b^2 \neq 0$$

In both cases, a and b are parameters that determine the Curve. The curve to be used in this research is a non-singular curve for a secure cryptanalysis. The size of an Elliptic curve is a contributory factor to the strength of the security.

Again following [37a], Elliptic Curve Domain parameters over F_2^m must have:

$m \epsilon${113,;131,;163,;193,;233,;239,;283,;409,;571g:}

According to [35], The ECC domain parameters over F_q is defined by the septuple as given below

D = (q, FR, a, b, G, n, h), where:

q: prime power, that is q = p or q = 2^m, where p is a prime

FR: field representation of the method used for representing field elements $\in F_q$

a, b: field elements, they specify the equation of the elliptic curve E over F_q, $y^2 = x^3 + ax + b$

G: A base point represented by G= (x_g, y_g) on E (F_q)

n: Order of point G , that is n is the smallest positive integer such that nG = O

h: cofactor, and is equal to the ratio #E(F_q)/n, where #E(F_q) is the curve order.

The primary security in ECC is the parameter n which is the order of the point. This determines the strength and level of the security of the system. The model will be extended with the introduction of Secured Socket Layer (SSL) to further secure the data sharing tunnels where each users has two keys — a "public" key and a "private" key. Anything encrypted with the user's public key can only be decrypted with the private key and vice versa.

7. CONCLUSION

Although, several attempts had been made at providing a secured environment for activities in the Cloud, Elliptic Curve Cryptography (ECC) provides solutions for a secured Cloud environment with improved performance in computing power and battery resource usage. This makes it attractive for mobile applications. ECC had provided a robust and secured model for the development and deployment of secured application in the Cloud. This work would promote confidence in both large and small scale organization in Cloud investment.

8. REFERENCES

[1] Alese B.K, (2004). Design of Public Key Cryptosystem using Elliptic Curve. P.hD Thesis Submitted to the Department of Computer Science, Federal University of Technology, Akure.

[2] Alowolodu O.D, (2009). Intrusion Detection System Using Genetic Algorithm to Differentiate between Normal and Attack Traffics. M.Tech Thesis Submitted to the Department of Computer Science, Federal University of Technology, Akure.

[3] Amazon.com,"AmazonWebServices (AWS)," Online at http://aws. Amazon.com, 2008.

[4] Anderson R. (2001). In: Security engineering: a guide to building dependable distributed systems. New York: John Wiley & Sons Inc; 2001.

[5] Ateniese. G, Burns. R, Curtmola. R, Herring. J, Kissner. L, Peterson. Z, & Song. D, (2007). "Provable Data Possession at Untrusted Stores," Proc. Of CCS '07, pp. 598–609

[6] Ateniese. G, Pietro. R. D, Mancini. L. V, and Tsudik. G. (2008). "Scalable and Efficient Provable Data Possession," Proc. of SecureComm '08.

[7] Ayesh A, Bechkoum K. (2000). "Framework of multi-agents internet security system". Appl Inform (AI'2000).

[8] Bakshi,. K. (2009) "Cisco Cloud Computing - Data Center Strategy, Architecture and Solutions". Point of View White Paper for U.S. Public Sector, 1st Edition

[9] Balding, C. (2008). "Is Your Amazon Machine Image Vulnerable to SSH Spoofing Attacks?" Cloud Security. Available at: <http://cloudsecurity.org/2008/07/14/is-your-amazon-machine-image-vulnerable-to-sshspoofing-attacks/>.

[10] Bo Peng, BinCui and XiaomingLi (2009), Implementation Issues of A Cloud Computing Platform. Bulletin of the IEEE Computer Society Technical Committee on Data Engineering.

[11] Bowers. K. D, Juels. A, & Oprea. A. (2008). "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Report 2008/489, http://eprint.iacr.org/.

[12] Brodkin, J. (2008). Seven Cloud Computing Security Risks, available at: http://www.gartner.com/Display Document?id=685308. (Accessed on May 2010)

[13] Buyya R. and Murshed, M. (2002). "GridSim: A Toolkit for the Modeling and Simulation of Distributed Resource Management and Scheduling for Grid Computing", The Journal of Concurrency and Computation: Practice and Experience (CCPE), Vol 14, Issue 13-15, Wiley Press.

[14] Cachin, C., Keider, I., Shraer, A. (2009). "Trusting the Cloud". IBM Research, Zurich Research laboratory

[15] Cong Wang, Qian Wang, and Kui Ren Wenjing Lou (2009). Ensuring Data Storage Security in Cloud Computing. Department of ECE and Worcester Polytechnic Institute Illinois Institute of Technology. A journal of IEEE

[16] Curtmola. R, Khan. O, Burns. R, & Ateniese. G. (2008). "MR-PDP: Multiple- Replica Provable Data Possession," Proc. of ICDCS '08, pp. 411–420.

[17] Darrel Hankerson, Alfred Menezes, Scott Vanstone (2004). "Guide to Elliptic Curve Cryptography". Springer-Verlag New York, INC., 175 fifth avenue, New York 10010, USA.

[18] Donal O'mahony, Micheal Pierce, Hitesh Tewari (2001). "Electronic Payment Systems For E-Commerce. 2nd Edition, Published by Artech House, Boston. London.

[19] Dumitrescu C. L and Foster. I. (2005). "GangSim: a simulator for grid scheduling studies". Proceedings of the IEEE International Symposium on Cluster Computing and the Grid

[19a]Edward Yin (2005). Curve Selection in ECC. San jose University, CS 265. Prof Stamp project

[20] Filho. D. L. G, & Barreto. P. S. L. M. (2006). "Demonstrating Data Possession and Uncheatable Data Transfer," Cryptology ePrint Archive, Report 2006/150, http://eprint.iacr.org/.

[21] Foster I. and Kesselman C. (1999). "The Grid: Blueprint for a New Computing Infrastructure".

[22] Francisco M, Edson M, Joao P, Pedro S, Adolfo G.(2002). "Dealing with security within DEEPSIA Project". In the Proceedings of the WSEAS International Conference on Information Security, Hardware/Software Code sign, E-Commerce and Computer Networks 2002;2431–9.

[23] Gohring N."Amazon's S3 down for several hours," Online at http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html, 2008.

[24] Google App Engine. (2008). available at: http://appengine.google.com. (Accessed on April 2010)

[25] Henri Cohen , Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange,Kim Nguyen, and Frederik Vercauteren (2006). Handbook of Elliptic and Hyperelliptic Curve Cryptography Chapman & Hall/CRC, Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742 © 2006.

[26] John, H. (2009). "Security Guidance for Critical Areas of Focus in Cloud Computing", http://www.cloudsecurityalliance.org/guidance/ (Accessed 2 July 2010)

[27] Krautheim, J.F (2010), "Private Virtual Infrastructure for Cloud Computing" University of Maryland, Baltimore County, 1000 Hilltop Circle, Baltimore, MD 21250.

[28] Juels. A. Burton. J & Kaliski. S. (2007)."PORs: Proofs of Retrievability for Large Files," Proc. Of CCS'07, Pp. 584 – 597.

[29] Lalana K, Tim F, & Anupam J. (2002). "Developing secure agent systems using delegation based trust management". In Proceedings of Security of Mobile Multi-Agent Systems Workshop (AAMAS 2002)

[30] Legrand, A. Marchal, L. & Casanova. H. (2003). "Scheduling distributed applications: the SimGrid simulation framework". Proceedings of the 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid

[31] McClure S, Scambray J, Kurtz G. (2003). In: "Hacking exposed: network security secrets and solutions". McGraw-Hill Osborne Media; 2003.

[32] Manchala, D.W. (2000). E-Commerce Trust Matrix and Models

[32a]Micheal Rosing (1999). Implementing Elliptic Curve Cryptography.Manning Publications Co. Brucepark Avenue, Greenwhich CT 06830

[33] Microsoft Live Mesh. (2008). available at: http://www.mesh.com. (Accessed on April 2010)

[34] Mills Elinor (2009-01-27). "Cloud computing security forecast: Clear skies". News.cnet.com. http://news.cnet.com/8301-1009_3-10150569-83.html.

[34a]Muhammad Yasir Malik (2010). Efficient Implementation of Elliptic Curve Cryptography Using low-power Digital Signal Processor. ISBN 978-89-5519-146-2 ICACT 2010

[35] Randhir Kumar , Akash Anil (2011). Implementation of Elliptical Curve Cryptography. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2.

[36] Schwarz. T. S. J, & Miller. E. L. (2006). "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. of ICDCS '06, pp. 12–12.

[37] Shacham. H, & Waters. B. (2008). "Compact Proofs of Retrievability," Proc. of Asiacrypt '08.

[37a](SEC) Standards For Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, September 20, 2000. Version 1.0

[38] Smith, J. E, and Nair, R. (2005). "Virtual Machines: Versatile platforms for systems and processes". Morgan Kauffmann.

[39] Snyder bill (2010) Cloud Computing: goodbye big Data centers hello Application running in the Cloud,.

[40] Talib, A. M., Atan, R., Abdullah, R. & Murad, M. A. A. (2010). Formulate a Security Layer of Cloud Data Storage Framework Based on Multi Agent System Architecture. GSTF International Journal on Computing, ISSN: 2010-2283, Vol. 1, No. 1, 2010.

[41] Wang, C. Wang, Q. Ren, K. and Lou, W. (2009). "Ensuring data storage security in cloud computing,"

[42] Wikipedia, the free encyclopedia of Cloud Computing.