Improving Data Storage Security in Cloud Computing using Elliptic Curve
Archana Singh Parmar¹, Monika Sharma²
Assistant Professor¹, ²
Department of IT
T.I.T&S Bhiwani, Haryana, India

Abstract:
Cloud computing is one of the latest technology trend of the IT trade for business area. Cloud computing security converged into a demanding topic in the sector of information technology and computer science research programs. The cloud computing is a way to deliver IT services on demand and pay per usage, and it can stores huge amount of data. But until now many companies don’t wish to use cloud computing technology due to concerns about data secrecy and protection. So we need a method that can provide a highly secure communication, data integrity and authentication, along with the non-repudiation communication and data confidentiality. So we discussed about the Elliptical curve that works at its best to secure the cloud by applying the principles of security with Hash algo. This paper aims to provide a secure, effective, and flexible method to improve data storage security in cloud computing with help of ECC.

Keywords: Cloud Computing, Security, Elliptical, Encryption, Hash.

1. INTRODUCTION:
Cloud computing refers to Internet based development and services. Cloud is simply the trendy term for a network or remote servers that can be addressed via an internet connection store and manage information. The three main aspects of cloud computing are Software as a service (SaaS) is a model of software deployment where an application is hosted as a service provided to customers across the Internet. Oracle CRM on Demand, Salesforce.com and Net suite are some of the well known examples of SaaS SaaS is generally used to refer business software rather than consumer software, which falls under Web 2.0. By removing the need to install and run an application on a user’s computer it is seen as a way for businesses to get the same benefits as commercial software with smaller cost outlay. SaaS also make it less intense of the burden of software maintenance and support, but users relinquish control over software versions and requirements. The other terms that are used in this sphere include Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The pioneer of cloud computing vendors are Amazon Simple Storage Service (S3) and Amazon Elastic Compute cloud (EC2) are well known examples of cloud computing.

Since Cloud Computing stores the data and disseminated resources in the open environment, security has become the major issue which is hampering the deployment of Cloud environments. Even though Cloud Computing is promising and efficient, there are many challenges in data security for the Cloud user. To access a cloud based web application that will try to eliminate the concerns regarding data privacy, segregation. In this paper we certainly have discussed about the data security and cloud protection inside the cloud processing that can be attend by applying the cryptographic algorithms.

2. DATA SECURITY ISSUES IN THE CLOUD
The security issue with clouds is that the data may not have control of the data is placed. As if user wants to take advantage of the cloud, user must ensure the safe network and also utilize the resource allocation and scheduling provided by clouds. The secured data exchange is crucial for any network; so it is very important to take security and privacy into account when designing and using cloud services. Cloud Computing is enlarged way to cover security issues, concerns and challenges for Data Security in Cloud.

2.1) Cloud Privacy and Confidentiality:
Confidentiality is defined as the sensitive information is not disclosed to unauthorized persons, processes, or devices. The service provider knows where the users’ confidential data is located in the cloud computing Systems. Once the client host data to the cloud there should be some guarantee that access to
that data will only be limited to the authorized access. Inappropriate access to sensitive data by cloud personnel is another risk that can pose potential threat data in cloud computing. Assuredness should be provided to the clients for proper practices in privacy policies and procedures to assure the cloud users for the data safety. Cloud service providers should implement mechanisms to ensure data integrity. The cloud provider should make the client aware of what particular data is hosted on the cloud. it may be necessary to have exact records as to what data was placed in a public cloud, when it required, what virtual memories (VMs) and storage it resided on when it was processed, such data integrity requirements exists, that the origin and custody of data or information must be maintained in order to prevent tampering or to prevent the exposure of data beyond the agreed territories (either between different servers or different networks).

2.2. Data location and Relocation:
Cloud Computing offers a high degree of data mobility. Data mobility is at a high level then the risks and issues increase many folds especially consumers do not always know the location of their data. When an enterprise has some sensitive data that is kept on storage device in the Cloud, users want to know the location of data and also wish to specify required location. The contractual agreement, between the Cloud provider and the consumer data should stay in a particular location or reside on a given known server, cloud providers should take responsibility to ensure the security of systems and provide robust authentication to safeguard customers’ information. Data is initially stored at an appropriate location decided by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each others’ resources. For example, emails, photographs uploaded to Face book can reside anywhere in the world and Face book members are generally not concerned. They may also wish to specify a preferred location (e.g. data to be kept in the UK) then requires a contractual agreement between the Cloud service provider and the consumer.

2.1) Storage, Backup and Recovery:
When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers. Most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.

3. CRYPTOGRAPHY/ ENCRYPTION
Cryptography/ Encryption is the science or art of changing text to a coded form that makes the text unreadable for those people you don’t want to read it. The process of converting plain text to cipher text using some mechanism is called encryption. Decryption is converting the cipher text back to simple text form. In private key cryptography, the encryption and decryption both happen to be done using the same key. Examples are AES and DES. Public key cryptography is also known as asymmetric key cryptography. A key is basically a value that is used in an algorithm for cryptography to convert plain text to cipher text. That has a huge worth and is also measured in parts. The larger the key is usually in public key element cryptography, the more secure is the cryptographic mechanism.

4. TYPES OF CRYPTOGRAPHIC ALGORITHMS
There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 1):

- **Secret Key Cryptography (SKC):** Uses a single key for both encryption and decryption; also called symmetric encryption. Primarily used for privacy and confidentiality.

- **Public Key Cryptography (PKC):** Uses one key for encryption and another for decryption; also called asymmetric encryption. Primarily used for authentication, non-repudiation, and key exchange.

- **Hash Functions:** Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity.

5. PRINCIPLES OF CLOUD SECURITY
5.1) Confidentiality: Confidentiality means only the authenticated person should be able to access and retrieve the data. So in order to preserve the confidentiality of information, the information is encrypted with only the authorized person and he being able to decrypt it because of some information known only to him. There are two main threats of confidentiality those are snooping and traffic analysis. Other ways to ensure information confidentiality include enforcing file permissions and access control list to restrict access to sensitive information.

5.2) Integrity: Integrity means to protect information from being modified by unauthorized parties. Commonly used methods to protect data integrity include hashing the data you receive and comparing it with the hash of the original message. However, this means that the hash of the original data must be provided to you in a secure fashion. More convenient methods would be to use existing schemes such as GPG to digitally sign the data.

5.3) Availability: Availability is the part that guarantees the individuals which have the rights to access the information i.e. information is available to user when it is needed. There is no use of confidentiality and integrity if the approved users cannot get the information they are entitled to. It is one of the most important characteristics.

6. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)
In general, public key cryptography systems use hard-to-solve problems as the basis of the algorithm. The most predominant algorithm today for public key cryptography is RSA, based on
Signature Generation: To create a signature $S$ for message $m$, using ECC key pair $(P, K)$ over $E(k)$, the following steps followed:

1. Generate a random number $k$ such that $1 \leq k \leq (n - 1)$.
2. Compute point $kQ = (x_1, y_1)$.
3. Compute $r = x_1 \pmod{n}$. If $r = 0$, go to step 1.
4. Compute $k^{-1} \pmod{n}$.
5. Compute SHA-512($m$), and convert this to an integer $e$.
6. Compute $s = k^{-1}(e + xr) \pmod{n}$. If $s = 0$, go to step 1.
7. The signature for message $m$ is $S = (r, s)$.

6.1) Elliptic Curve Arithmetic
The main attraction of ECC is that it provides an equal level of security, but much smaller key size compared with RSA. We can defined an elliptic curve by equation all its coefficients and variables take values in the set of integers within the range from 0 to $p - 1$, which is performed calculations modulo $p$. When use an elliptic curve for cryptography, the coefficients and variables are restricted in a finite Abelian group. The group that has a finite number of elements, it's known as a finite group and the number of elements in $G$ is known as the order of $G$. ECC equation over $\mathbb{F}_2$ is:

$$y^2 = x^3 + ax + b$$

The finite fields those are commonly used over primes (FP) and binary field (F2n). The security of ECC is based on the elliptic curve discrete logarithm problem (ECDLP). This problem is defined as: Given point $X, Y$ on elliptic curve, find $z$ such that $X = zY$. The following steps describe how ECC works with SHA-512.

6.2) Hash Functions
Hash functions, also called message digests and one-way encryption, are algorithms that, in essence, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

6.3) ECC key generation: To generate a public and private key pair for use in ECC communication the steps followed are:

1. Find an elliptic curve $E(K)$, where $K$ is a finite field such as $F_p$ or $F_{2^n}$, and a find point $Q$ on $E(K)$. $n$ is the order of $Q$.
2. Select a pseudo random number $x$ whose value lies as $1 \leq x \leq (n - 1)$.
3. Compute point $P = xQ$.
4. ECC key pair is $(P, x)$, where $P$ is public key, and $x$ is private key.
7. CONCLUSION:

As ECC is based on properties of Particular type of equation created from mathematical group derived from Point where line intersects the axis. Multiplying a point on curve by a no will Produce another Point on curve ,but it is very difficult to find what no was used ,even if you know original Point and result., so we are calculating our public and private key with this method so that no one can ever know about our key . Equation based on elliptical curve have a property that is very valuable for cryptography purpose, they are relatively east to perform and extremely difficult to reserve. And with this we are using hash also for Digital signature so any unauthorized person will never be able to get access over the data. So with help of this technique with hash algorithm we can depend on cloud computing and can use cloud services without any risks or hesitation.

8. REFERENCES


