International Journal of Research
Available at
https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 05
April 2017

# Secure Big Data Storage and Sharing in Cloud using ECC Algorithm

**Tara Alimunisha**
PG Scholar
Department of CSE,
DIET, ANAKAPALLE, Visakhapatnam

**Kolli Nuka Raju** Associate
Professor, Department of CSE,
DIET, ANAKAPALLE, Visakhapatnam

**Abstract-** Users store vast amounts of data on a big data platform. Sharing data will help enterprises reduce the cost of providing users with personalized services and provide value-added data services. However, secure data sharing is problematic. This project proposes a framework for secure sensitive data sharing on a big data platform, including secure data delivery, storage, usage, and destruction on a semi-trusted big data sharing platform. At the same time, data owners retain complete control of their own data in a sound environment for modern internet information security. This paper presents an alternative approach which divides big data into sequenced parts and stores them among multiple cloud storage service providers. Instead of protecting the big data itself, the proposed scheme protects the mapping of the various data elements to each provider using ECC algorithm. Analysis, comparison and simulation prove that the proposed scheme is efficient and secure for the big data of cloud tenants. Secured data transmission using elliptic curve cryptography can be defined as transmission of data. This paper proposes a survey about secured data transmission using elliptic curve cryptography. The main problem in existing system is security issues in transmitting data between source and the destination.

This paper finds a new way to increases security consideration for transfer of data and to increment the efficiency using ECC (Elliptic Curve Cryptography). Efficiency and reliability will be increased for each transmission of data, while enclosing the proposed method by using the ECC algorithm which allow itself to encrypt and decrypt the data that is to be transferred and performs the active classification. 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.

**Keywords:** Cloud computing, big data, storage and sharing, security, secure sharing, elliptic curve cryptography algorithm.

## 1. INTRODUCTION

Cloud computing is a technology which uses internet and remote servers to store data and application. In cloud there is no need to install particular hardware, software on user machine, so user can get the required infrastructure on his machine in cheap charges/rates. Cloud computing is an infrastructure which provides useful, on demand network services to use various resources with less effort. Features of cloud computing are, huge access of data, application, resources and hardware without installation of any software, user can access the data from any machine or anywhere in the world, business can get resource in one place, that’s means cloud computing provides scalability in on demand services to the business users. Everyone kept their data in cloud, as everyone kept their data in cloud so it becomes public so security issue increases towards private data. Data usage in cloud is very large by users and businesses, so data security in cloud is very important issue to solve. Many users want to do business of his data through cloud, but users may not know the machines which actually process and host their data. While enjoying the convenience brought by this new technology, users also start worrying about losing control of their own data. Data represents an extremely important asset for any organization, and enterprise users will face serious consequences if its confidential data is disclosed to their business competitors or the public. Thus, cloud users in the first place want to make sure that their data are kept confidential to outsiders, including the cloud provider and their potential competitors. This is the first data security requirement.

In modern information technology, big data is a term applied to data sets whose size is beyond the ability of commonly used software systems to store, manage, and process within a tolerable elapsed time. Big data [1] sizes are a constantly moving target, currently ranging from a few dozen terabytes to many peat bytes of data in a data center. Elliptic curve cryptography (ECC) [7] is a public- key cryptography system which is based on discrete logarithms structure of elliptic curves over finite fields. ECC is known for smaller key sizes, faster encryption, better security and more efficient implementations for the same security level as compared to other public cryptography systems (like RSA).

ECC can be used for encryption (e.g. Megamall), secure key exchange (ECC Daffier-Hellman) and also for authentication and verification of digital signatures. The security of ECC is based on a trapdoor function where it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible. This is called Elliptic Curve Discrete Logarithm [6] Problem (ECDLP).which is considered to be computationally infeasible to solve. A data center mainly focuses on the storing and processing of big data sets, real-time data mining, and streaming media delivery etc. Data-intensive applications and research will be integral to many future scientific endeavors, but will demand specialized security mechanisms to make data centers [13] efficient and secure. In addition, the research community now has the option of accessing storage and computing resources on demand, and the IT industry is currently building multiple big data centers for social efficient scheme for tenants to access their data on the data center storage is crucial networks and applications.

Consequently, large amounts of client's private and secret data (including meta-data) will be stored in data centers, and will need protection during processing and transmission. Thus, data centers should be able to provide efficient security, access, and update mechanisms to not only huge files running into peat bytes, but also to small files that are only a few hundred bytes. In all the above cases, determining how to design a secure and efficient scheme for tenants to access their data on the data center storage is crucial. For some threats, especially the security threat of abusing private information [11] and data is fatal for the tenant. Currently, the storing of tenants data on a cloud platform is a popular practice, and this is becoming more complicated and diversified than ever.

In modern advanced information society, people have a variety of personalized requirements about their data information. Undoubtedly, privacy and security of personal data information is the most important concern for tenants when they store their confidential data on cloud storages. In order to make the confidential big data of tenants secure, this project proposes a secure cloud big data storage [12] and sharing in cloud using ECC algorithm. In the proposed scheme, divide the big data or big data set into sequential data parts according certain principles, such as same data type block or IP resembled (Internet Protocol) data packets.

## 2. LITERATURE REVIEW

### Ensure data security in cloud [4] storage

The cost of maintain a data center is increasing rapidly, especially for the medium data center. An economic choice is to use cloud computing and cloud storage instead of manage data center by itself. Small companies buy compute and storage service just like water and electronic. The difficulty is how to ensure their data safe in cloud storage. Cloud storage provider claims that they can protect the data, but no one believes them. In this project, presents a framework to ensure data security in cloud storage system. in the framework, SLA as the common standard between user and provider. And several technologies to make the data stored in cloud safe. These technologies can be divided into three parts: storage protect, transfer protect and authorize.

### Secure and privacy preserving keyword searching for cloud storage services [5]

Encrypted data search allows cloud to offer fundamental information retrieval service to its users in a privacy preserving way. In most existing schemes, search result is returned by a semi-trusted server and usually considered authentic. However, in practice, the server may malfunction or even be malicious itself. Therefore, users need a result verification mechanism to detect the potential misbehavior in this computation outsourcing model and rebuild their confidence in the whole search process. On the other hand, cloud typically hosts large outsourced data of users in its storage. The verification cost should be efficient enough for practical use, i.e., it only depends on the corresponding search operation, regardless of the file collection size. This project, first to investigate the efficient search result verification problem and propose an encrypted data search scheme [14] that enables users to conduct secure conjunctive keyword search, update the outsourced file collection and verify the authenticity of the search result efficiently. The proposed verification mechanism is efficient and flexible, which can be either delegated to a public trusted authority (TA) or be executed privately by data users. This project formally proves the universally compassable (UC) security of our scheme. Experimental result shows its practical efficiency even with a large dataset.

Mark D. Ryan proposed three types security in cloud computing viz. (I) Homomorphism encryption- it is an encryption technique that allows a part that holds cipher texts to perform certain operations on the cipher texts, which mirror the corresponding operations on the plaintexts. In the case of simple homomorphism encryption, there is just one operation on the plain text that has a corresponding operation on the cipher text.(ii) Key translation in the browser- With this approach, data is encrypted before being uploaded to the cloud, and the data owners retain the keys.

However, dissimilar parts of the data may be encrypted with unusual keys and some of the clients participating in the service may execute "key translation" in order to agree to data items to be forwarded to planned recipients.(iii)Hardware-anchored Security – to achieve confidentiality from the cloud provider is based on special hardware on the cloud side. The idea is that the cloud provider is able to decrypt the data, but is able to offer guarantees about the circumstances in which it does that. Those guarantees will promise that the data owners that the data is handled in agreement with their policy [2].

Mehmet Yilidiz et al proposed a dynamic security model for cloud security. This model is based on eight aspects and includes four layers. Network, Storage, Servers and Application layers. It includes one enterprise level principles at the highest level and a system management aspect. It also includes two kinds of dynamic security types: horizontal and vertical. The horizontal type is specific to each layer end to end. Here, horizontal dynamic security policy for storage does only cover the security objects related to storage. The vertical type is designed to cover the interfaces between layers. Some security objects between servers and storage may be partially belonging to each layer. The vertical dynamic policies ensure that any common object or exception is covered [3].

Sandeep K. Sood [15] proposed construction has been structured to make available complete protection to the data throughout the complete process of cloud computing, be it in cloud or in transfer. Consequently multiple mechanisms and accessible techniques are applied to protect the critical information from unauthorized parties. The planned frame work is separated into two phases. First phase deals with procedure of transmitting and storing data securely addicted to the cloud. Second phase deals with the recovery of data from cloud and presentation the generation of requests for data contact, double confirmation, authentication of digital signature and reliability, thereby providing approved user with data on passing all security mechanisms.

## Algorithm for Cloud Security Models

To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is using asymmetric key encryption; two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption.

### Symmetric Algorithms

**DES**: This stands for Data Encryption Standard and it was developed in 1977. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is 64 bits key size with 64 bits block size. Since that time, many attacks and methods have witnessed weaknesses of DES, which made it an in secure block cipher.

**BLOWFISH**: This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption.

**RC5**: It was developed in 1994. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The use of this algorithm shows that it is Secure. The speed of this algorithm is slow.

**3DES:** This was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods. This is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics.

**AES**: (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.

### Asymmetric Algorithms

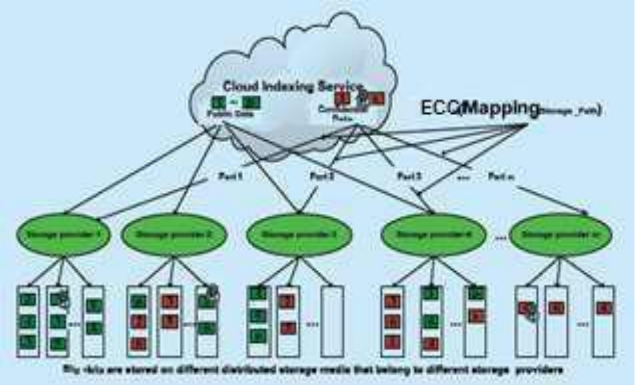
**RSA**: This is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption

**DSA**: The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013. With DSA, the entropy, secrecy, and uniqueness of the random signature value k is critical. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping k secret), using a predictable value, or leaking even a few bits of k in each of several signatures, is enough to break DSA.

**Diffie-Hellman Key Exchange (D-H):** Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using asymmetric key cipher.

**ElGamel**: In cryptography [10], the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described by Taher Elgamal in 1984. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption. ElGamal encryption can be defined over any cyclic group. Its security depends upon the difficulty of a certain problem in related to computing discrete algorithms.

## SYSTEM ARCHITECTURE


Cloud Indexing Service
Public Data
ECC(Mapping
Part 1
Part 2
Part 3
Part n
are stored on different distributed storage media that belong to different storage providers

## RELATED WORK

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller [9] (IBM) and Neil Koblitz [8] (University of Washington) as an alternative mechanism for implementing public-key cryptography. 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.

I assume that those who are going through this article will have a basic understanding of cryptography ( terms like encryption and decryption ) .

The equation of an elliptic curve is given as,

Few terms that will be used, E ->

Elliptic Curve

P -> Point on the curve

n -> Maximum limit ( This should be a prime number )

**Key Generation** :

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number ‘d’ within the range of ‘n’.

Using the following equation we can generate the public key

$Q = d * P$

d = The random number that we have selected within the range of ( 1 to n-1 ). P is the point on the curve.

‘Q’ is the public key and ‘d’ is the private key.

**Encryption**

Let ‘m’ be the message that we are sending. We have to represent this message on the curve. This have in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider ‘m’ has the point ‘M’ on the curve ‘E’. Randomly select ‘k’ from [1 – (n-1)].

Two cipher texts will be generated let it be C1 and C2.

$C1 = k*P$

$C2 = M + k*Q$

C1 and C2 will be send.

**Decryption**

We have to get back the message ‘m’ that was send to us,

$M = C2 – d * C1$

M is the original message that we have send. Proof How does we get back the message, $M = C2 – d * C1$

‘M’ can be represented as ‘$C2 – d * C1$’

$C2 – d * C1 = (M + k * Q) – d * ( k * P )$

$( C2 = M+ k * Q$ and $C1 = k * P )$

$= M + k * d * P – d * k *P$

( canceling out $k * d * P$ )

$= M$ ( Original Message )

## 3. Overview

We In order to make the confidential big data of tenants secure, we propose a secure cloud big data storage and sharing cloud using ECC algorithm, and the concept is shown in. The proposed scheme is described below. In the proposed scheme, we divide the big data or big data set into sequential data parts according certain principles, such as same data type block or IP- resembled Internet Protocol data packets.

We first introduce the trapdoor function before describing the proposed scheme. In this proposed scheme first the data is divided into the different sequential pats by using Indexing technique. after that the stored data will be encrypted by using TDES algorithm. Finally the data will be stored on different storage devices by using ECC algorithm.

### 1. Cloud computing

In cloud computing, big data storage services represent a basic function for their tenants. In the proposed scheme, firstly, tenants big data will be separated into many sequenced parts before storage, and then will be stored on different storage media owned by different cloud storage providers. When tenants access their data, the data parts in different data centers will be collected together and then be restored into original form based on the sequenced number of each data part. Generally, the tenants big data which is stored in cloud storage can be classified into public data and confidential data. There are no extra security requirements for public data, and each tenant can access these data freely, on the other hand, confidential data should always be kept secret and inaccessible to irrelevant persons or organizations.

### 2. Big Data

In order to make the confidential big data of tenants secure, we propose a secure cloud big data storage and sharing cloud using ECC algorithm. The proposed scheme is described below. In the proposed scheme, we divide the big data or big data set into sequential data parts according certain principles, such as same data type block or IP-resembled (Internet Protocol) data packets. Evidently, n is always far greater than m, these m storage providers belong to different organizations, such as Google, Amazon and Yahoo. Each data part stored on certain cloud storage providers will be allocated to some physical storage media that belongs to the storage provider, so, when big data of a tenant is stored, it will form a unique storage path for the big data given.

### 3. Storage And Sharing

In cloud computing environment, the tenants such as some companies or enterprises, when they transfer and store their big data on cloud storage center directly, it maybe arise some serious problems such as system crash or failure, however, in the proposed scheme, the big data of tenants will be divided into some smaller data blocks, these smaller data blocks will be stored in cloud storage media one by one, because these data blocks are smaller than the primitive big data ,they are very efficient for remote-distance data transmission and storage. Under the same network conditions, the transmission failure probability of the proposed scheme is lower than when the big data store and transmit directly.

### 4. Security

Now we compute the vulnerability of security of proposed scheme. Let x be an adversary who want to acquire the storage path of the big data illegally, according to the proposed scheme, the adversary can observe the whole big data only when he/she gets the storage paths of all data blocks. So, we can judge the security of storing part of big data on different cloud storages only by computing the probability that x knows the storage paths all of data blocks. some tenants are still reluctant to deploy their big data in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market a survey of the different security risks that pose a threat to the cloud is presented and the work focused on the different security issues and concerns that have emanated due to the nature of the service delivery models of a cloud computing system.

## 4. CONCLUSION

We presented a computation model for big data analytics in the cloud and surveyed several cryptographic techniques that can be used to secure these analytics in a variety of settings. While these techniques give a good starting point for secure cloud computing, further research is needed to turn them into practical solutions that can achieve secure cloud computing in the real world. Due to its enormous size, owners of big data need to consider the cost (both in terms of time and money) of encryption. Our presented solution avoids this by splitting the data among several cloud providers, and protecting by using ECC algorithm. The proposed system a content sharing scheme that is safe in the cloud computing environment, based on a conditional proxy re-encryption scheme. This system can significantly reduce burden of a client due to two characteristics. First is re-encryption process is delegated to a cloud server. A client is only involved in process of encryption and decryption of data and creation of re-encryption keys. Second, the number of re-encryption keys to be required for sharing is minimized. Secure data access when sharing in a group, Implementation and maintenance, Reliability and scalability, Guaranteed levels of services, Total cost of ownership are the main feature of this system. We analyze the efficiency and security of the proposed scheme through some theoretical proof, at the same time; we compare the proposed scheme with other related schemes and technology by simulation under two different scenarios; the simulation results coincide in the analysis very well. All the results show that the proposed scheme is effective and feasible to protect the big data for cloud tenants.

## 5. FUTURE WORK

In future work, we plan to analyze the overheads of our detection techniques such as the various distance-based methods in comparison with contemporary approaches. At present, this was developed to provide the requirements needed to provide security to data, we study and analyze big cloud storage in cloud computing. Customers put their data into single cloud which is liable to vendor lock in risk. In addition, the loss of service availability and data integrity are the major problems for the customer. This paper presented some recent advances and schemes to provide multi - cloud security and their comparison based on security issues. Distributed based approaches seems to be simple but provide less security than others. Hybrid based approaches were more realistically meeting organizational needs however they comes with private cloud costs.

## References

[1] D. Kusnetzky. What is “Big Data?” [Online]. Available: http://blogs.zdnet.com/virtualization/? p=1708.

[2] Mark D. Ryan, 2013. Cloud computing security: the Scientific Challenge and a Survey of Solutions, the Journal of System and Software, 86: 2263-2268.

[3] Mechmet Yilidiz, Jemal Abawajy, Tuncay Ercan and Andrew Bernoth, 2009. A Layered Security Approach for Cloud Computing Infrastructure, Proceedings of 10 International Symposium on Pervasive Systems, Algorithms and Networks (IEEE), pp: 763-768

[4] X. Zhang, H. tao Du, J. quan Chen, Y. Lin, and L.jie Zeng, “Ensure data security in cloud storage,” in Network Computing and Information Security (NCIS), 2011 International Conference on, vol. 1, may 2011, pp. 284 – 287.

[5] Liu Q, Wang G, Wu J. Secure and privacy preserving keyword searching for cloud storage services [J]. Journal of network and computer applications, 2012, 35(3): 927-933.

[6] Gaudry, P.: Some remarks on the elliptic curve discrete logarithm (2003),http://www.loria.fr/~gaudry/publis/liftDL.ps.gz

[7] Hankerson, D., Menezes, A., Vanstone, S.: Guide to Elliptic Curve Cryptography, Springer Professional Computing (2004).

[8] Koblitz, N.: Elliptic curve cryptosystems. Math. Comp. 48,203–20 (1987)MATHCrossRefMathSciNetGoogle Scholar.

[9] Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986).

*[10]* Landau, Susan *(2004)*. " Explanation Of Cryptography by A. J. Menezes, P. C. Oorschot, and S. A. Vanstone and 9 other books by various authors" *(PDF)*. *Bull. Amer. Math. Soc. (N.S.). 41 (3): 357–367*. doi:10.1090/s0273-0979-04-01011-0.

[11] Singla J S. the security threat of abusing private information and data is fatal Global Journal of Computer Science and Technology, 2013, 13(3).

[12] Spoorthy V, Mamatha M, Kumar B S. A secure cloud big Data Storage and sharing scheme. International Journal of Advanced Research in Computer Engineering & Technology, [J]. 2013.

[13] Inbarani W S, Moorthy G S, Paul C K C. specialized security mechanisms to make data centers efficient and secure .An Approach for Security in Cloud Computing-A Survey[J]. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2013, 2(1): pp: 174-179.

[14] Popa R A, Stark E, Helfer J, et al. an encrypted data search scheme building web applications on top of encrypted data using Mylar[C]//USENIX Symposium of Networked Systems Design and Implementation. 2014.

[15] Sood Sandeep, K., 2012. A combined Approach to ensure data security in cloud computing, journal of Network and Computer Applications, 35: 1831-1838.

## AUTHORS

**Tara Alimunisha**
PG Scholar
Department of CSE,
DIET, ANAKAPALLE,
Visakhapatnam

**Kolli Nuka Raju**
Associate Professor,
Department of CSE,
DIET, ANAKAPALLE,
Visakhapatnam

,