EasyChair Preprint

№ 10126

# Secure Data Storage on Cloud Using Hybrid Cryptography Methods

R Sabitha, Shaik John Sydulu, S Karthik and M S Kavitha

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

May 12, 2023

# Secure Data Storage on Cloud using hybrid cryptography Methods

Sabitha R [1]
Professor,
Department of Computer-Science and Engineering,
SNS College of Technology,
Coimbatore,India,
Dr.r.sabitha@gmail.com

Sk.John Sydulu[2]
Research scholar,
Department of Computer-Science and Engineering,
SNS College of Technology,
Coimbatore,India,
johny.ciet@gmail.com

KarthikS[3]
Professor and Dean,
Department of Computer-Science and Engineering,
SNS College of Technology,
Coimbatore,India,
profskarthik@gmail.com

Kavitha M S[4]
Associate Professor,
Department of Computer-Science and Engineering,
SNS College of Technology,
Coimbatore,India,
drmskavitha@yahoo.com

*Abstract*— **The protection of information stored in cloud-based databases is a multifaceted and intricate matter that demands attention, given the existence of malevolent attacks, data violations, and unguarded entryways. Historically, numerous scholars have posited security mechanisms, such as access control, detection and avoidance of intrusion methods, storage methods like cryptography, and some schemes for key management. Security of data kept in cloud databases is compromised by attackers who exploit the privileges obtained from multiple roles, thereby undermining the role-based control mechanisms for access that were designed to safeguard sensitive information. Hence, The examination of the correlation among various attributes is crucial in proposing more efficient mechanisms for protecting sensitive information through attribute-based encryption. In order to address security concerns associated with the management of vast quantities of cloud-based data, we have suggested the utilisation of Elliptic Curve Cryptography (ECC) for the encryption of data, as well as for secure connection establishment we implement the Diffie-Hellman Key Exchange (DHKE) method. The proposed encryption system utilises a hybrid methodology that integrates parametric and elliptical cryptography techniques. The system is composed of three discrete security checkpoints, specifically authorization, generating keys, and data encryption. The utilisation of Elliptic Curve cryptography is known to reduce computational power requirements due to its small key size, thereby resulting in lower energy consumption. The present study demonstrates that the implementation of elliptic curve cryptography in a cloud computing setting results in expedited data protection and heightened efficiency, as it mitigates computational demands.**

*Keywords*— **Elliptic Curve Cryptography, Diffle Hellman Key Exchange, Encryption, Decryption, Key generation**

## I. INTRODUCTION

The Information Technologies community has faced significant security challenges since the emergence of Grid Computing, which subsequently evolved into Cloud Computing. The concept of cloud computing, previously ambiguous and challenging to comprehend has evolved into a burgeoning technology that has captured the attention of organizations, industry stakeholders, and scholars alike. The escalating expenses associated with electricity generation, personnel hardware, and spatial constraints in data centres have prompted a considerable number of enterprises to migrate a greater portion of their infrastructure to a third-party provider, namely the Cloud.

CC is a technological paradigm that leverages the internet and centralised remote servers to facilitate the storage and management of data and applications. Cloud computing enables both individuals and organisations to utilise software applications without the need for installation, and to retrieve their personal data from any computer, provided that an internet connection is available. The centralization of storage, memory, processing, and bandwidth through this technology results in significantly enhanced computing efficiency. The migration of data to cloud-based systems provides significant advantages in terms of simplifying the challenges associated with direct hardware administration. Amazon Simple Storage Service (S3) and Elastic Compute Cloud (EC2) are considered to be among the first Cloud Computing vendors. These vendors provide internet-based online services that offer significant storage capacity and customizable computing resources. Nonetheless, the accessibility and reliability of data are contingent upon cloud service providers, leaving users vulnerable to their discretion. The public of CC have posited that the security measures employed are inadequate, resulting in compromised data integrity. Apprehensions often impede the growth of the cloud computing industry. The impetus for cloud computing infrastructures is primarily driven by the need to store and process large amounts of data.

Almost all cryptosystems rely on elaborate mathematical procedures. While symmetric encryption relies on a secret key and elementary mathematical processes like substitution and permutation, asymmetric encryption relies on more complex procedures like factoring big prime numbers or solving Discrete Logirathimic problems (DLP). A holomorphic cryptosystem is another name for the public key encryption technique. In public-key encryption, the size of the key is crucial. Asymmetric encryption is computationally intensive because of the huge key size. Asymmetric encryption is used for key exchange in modern cryptosystems, while symmetric encryption is used for data encryption. The issue of excessively long keys has been addressed by elliptic curve encryption. Small key sizes are used in ECC, which allows it to be implemented on the cloud, on wireless sensor networks, and on smart devices with minimal computational overhead. Many users in cloud computing share a massive amount of data. Security, anonymity, safety, reliability, and authentication all pertain to data, and thus, various problems arise. Data is typically stored in plaintext format by cloud service providers, therefore users must encrypt their data using the provider's encryption technique. Before the information can be used, it must be decrypted.

## II. Literature Survey

Many academics have proposed various methods using the ECC algorithm to improve cloud security; these methods vary with respect to the methodology used for managing keys, both encryption and decryption, digital signature generation, and authentication.

Dheepak [18] suggested a method for solving optimisation problems that takes into account the dynamics of both humans and genetics. In order to enhance the cloud storage security several genetic algorithms are used to produce the key, ECC used for both encryption and decryption and also digital signature based has function.

Initialization, user registration, registration of vehicles, authorization, and biometric password are the five tiers of the technique outlined by Kumar et al. [19] that affect the User and Vehicular Cloud. All of our data transfers to and from the cloud are encrypted and decrypted using a set of keys called public and private key, both of which are generated randomly using ECC.

Since the e-healthcare system is the primary focus of the hybrid approach developed by A. Kumari et al. [20], this approach is broken down into four stages: hospital and patient data uploading, treatment, and checkups. The ECC random number generator is used to generate keys, then the technique moves on to encrypting and decrypting data and verifying digital signatures via a hash function. The main concern here is not that security is improved, but rather the increased processing and communication overhead.

When compared to other, more basic security methods, the multilayer approach presented by Tallapally et al. [21] is far superior. First, keys are generated using ECC and Hessian Algorithms, then encrypted and decrypted using ECC and TDES. This method improves authentication and privacy by restricting cloud data access to only those who have been granted access to it in advance.

Four distinct algorithms namely Meerkat, SHA512, multiple levels lempel-ziv, and a data transfer algorithm called CP-ABE using elliptic curve cryptography are hydride and their performances are detailed in Vengala et al. [6] method. The programme starts by gathering information about the user's data and the cloud itself. The algorithm developed by the meerkat-inspired Hybrid Meerkat clan determined which cloud was most attentive to each feature. After receiving data from the user, SHA512 performs a repetition of all or a portion of a word. After data redundancy check, the reduced file is reduced in size and encrypted with a multi-level lempel- ziv algorithm and a newly introduced CP-ABE-ECC method. The encoded file is then transferred to the cloud storage.

In their study, B. Prabhu Kavin and colleagues (2012) proposed a hybrid approach that utilises a secure ECC algorithm for key generation. Elliptic curve authorization based on identity is another approach to consider. The ultimate generation of digital signatures involves the utilisation of ECC's Diffie-Hellman algorithm for the encryption and decryption processes, which are executed in two distinct phases. On the other hand, the Lightweight Digital Signature Algorithm is responsible for carrying out the verification process. This guarantees the protection of data integrity and retrieval then storing in cloud.

The major application of the suggested technique by Khan et al. [7] lies in the domain of mobile cloud security. This methodology involves the generation of a key through the utilisation of Elliptic Curve Cryptography (ECC), followed by the implementation of both the Substitution-Ceaser cypher algorithm and an enhanced version of ECC for encryption and decryption. The latter involves the generation of an additional key to bolster security measures. The authorization system that was presented includes the integration of biometric applications. In their study, Hema and colleagues (2015) introduced a novel methodology that involves the utilisation of a third-party cloud for all operations, excluding the user and the primary cloud. The proposed methodology utilises the SHA algorithm and hash function to generate keys, employs ECC for encryption and decryption, and utilises the hash-based message authentication code (HMAC) signature to generate and verify digital signatures. The responsibility of ensuring the privacy of information and integrity, along with implementing various security measures, is crucial for facilitating the secured distribution of medical records.

The hybrid approach was introduced by Bommala et al. (2017), ECC is proposed to generate the keys and AES algorithm is performed for both encryption and decryption. The implementation of a security measure that effectively restricts unauthorized access to private Clouds involves the monitoring and complete blocking of Internet Protocol Addresses and Media Access Control addresses assigned to individual machines. Research indicates that this technique surpasses all linear algorithms in terms of security. Hosam et al [5]. In the Galois field, keys are generated through random number generation and subsequently encoded using AES and ECC algorithms via homomorphic and hybrid approaches. Ultimately, the key that has been encrypted using ECC will be embedded within the user's photograph through the utilisation of the Least Significant Bit (LSB) steganography technique. This methodology has the potential to furnish robust safeguarding measures, alongside proficient generation and management of cryptographic keys, catering to a diverse range of users. Thangapandiyan and colleagues (2019) proposed a novel technique that eliminates the need for transferring both private key and public key. As an alternative, a distinct key is generated for each user and administrator following identity authentication. This method effectively mitigates all potential risks associated with key management. The researchers further suggest utilising customised elliptic curve cryptography to encrypt and decrypt data. The homomorphic approach proposed by Gupta et al. (2010) involves performing operations on encrypted messages in a manner that yields an appropriate encoding of predetermined computations on the plain text. The authors Jana et al. (2013) presented a multilayered methodology that involves the utilisation of ECC algorithm to generate random numbers for generating keys. AES algorithm is used for both encryption and decryption, followed by ECC for further processing, and hash function for digital signature manufacturing and verification. The implementation of this approach results in a significant enhancement of the authentication process.

In the hybrid method proposed by Gajra et al. (2014), key management is initially addressed through the use of the ECC method, followed by the Elliptic Curve Diffie-Hellman algorithm. Encryption and decryption processes are subsequently executed through the Advanced Encryption Standard (AES) and Blowfish algorithms, respectively. Finally, signature creation and confirmation are carried out through the Elliptic Curve electronic signature method. This approach can offer a robust defence due to its heightened levels of confidentiality and genuineness. The proposed methodology by Tirthani et al. [16] comprises of four sequential steps, namely connection establishment, account creation, authentication, and data sharing. The Diffie-Hellman key exchange technique is employed for key generation, while ECC is utilised for encryption and decryption purposes.

## III. PROBLEM STATEMENT

The primary responsibility of the cloud provider is to ensure the security of their client information. Sequentially to ensure effective data protection, it is needded to implement a mechanism that offers robust data encryption and reliable safeguards against unauthorised data access. The aforementioned literature has primarily concentrated on matters pertaining to security in cloud computing. Various mechanisms have been implemented to ensure data security in cloud environments. Numerous studies have emphasised the need for users to securely access substantial amounts of data from the cloud. However, the significance of the cryptographic algorithm's complexity has not been adequately emphasised. The algorithm's level of complexity has a direct impact on the efficiency of data retrieval. An algorithm that enables efficient and secure data access is required.

## IV. ELLIPTIC CURVE CRYPTOGRAPHY

The cryptographic scheme known as Elliptic Curve Cryptography (ECC) is introduced by Koblitz and Miller during the 1980s [8]. The ECC is a cryptographic scheme that utilises public key cryptography. Elliptic Curves are utilised in the development of cryptographic algorithms. The security of ECC relies on the computational complexity of resolving the Elliptic Curve Discrete Logarithm Problem (ECDLP). The definition of Elliptic Curve Cryptography involves the utilisation of the following parameters:

$$b = (p, FR, x, y, B, n, m) \qquad (1)$$

The prime number, denoted as 2m, serves as the defining factor for the form of the curve. The FR is for Field Representation. The variables x and y represent the coefficients of the curve. The base point is denoted as (Bx, By). The variable "n" refers to the order of the group G. The number in question must be a prime number of significant magnitude. The terms "cofactor" and "coefficient" are commonly used in mathematical contexts.

Public-key protocol implementation frequently makes use of elliptic curves (EC) over finite fields. The Elliptic curve may be formulated over a prime field BF (p) or a binary field BF (2n). As a result of the enhanced computational efficiency in the latter domain, we have chosen to execute our tasks in BF, with a complexity of (2n). The definition of EC E is established through the utilisation of simplified projected coordinates in the following manner:

$$y2z + xyz = x3 + ax2z + bz3 \qquad (2)$$

The utilisation of public key cryptographic scheme is developed over two separate fields, specifically the prime Galois Field, BF (p), and the binary diversification Galois Field, BF (2m). The mathematical expression representing an Elliptic Curve in the finite field of prime order p, denoted as BF(p), can be expressed as follows:

$$y2mod\ p = x3 + ax + b\ mod\ p \qquad (3)$$

$$4a3 + 27b2\ mod\, p \neq 0 \qquad (4)$$

The parts of BF (p) are represented as integers within the range of 0 to p-1, as indicated in reference [7]. The equation of the Elliptic Curve in BF (2m) is provided by a mathematical expression:

$$Y^2 + xy = x^2 + ax2 + b \quad (5)$$

In the field of Galois over a binary extension of degree m, it is possible to implement regulations for the addition and doubling of points, provided that b is not equal to zero.

The Elliptic Curve Cryptography (ECC) algorithm offers superior security compared to the RSA algorithm, despite having a smaller 256-bit public key size as opposed to RSA's 3072-bit public key size. The ECC algorithm executes an encryption procedure that involves the utilisation of an EC and a finite field, and is formally described as follows,

$$Y^2 = X^3 + aX + b \quad (6)$$

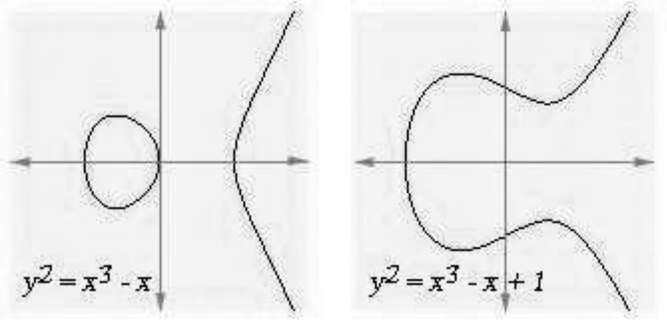

Figure 1: Elliptic Curves for two equations

## V. Diffie-Hellmann Key Exchange (DHKE)

The Diffie-Hellman protocol is widely acknowledged as the pioneering public key cryptography scheme. The proposition was put forth by Witfield Diffie and Martin Hellman in the year 1976. The system employs a set of keys, namely a confidential key and a distinct private key. In order for the sender to establish communication with the receiver, it is necessary for the former to encrypt the message using their private and the public key of the recipient. Upon reception, the recipient decrypts the transmitted message utilising their private key in conjunction with the public key of the sender. The aforementioned scheme is founded upon the computational complexity of logarithmic functions with prime exponents. The mathematical concept being referred to is commonly referred to as the Discrete Logarithm Problem (DLP).

## IV. Proposed Hybrid Architecture for Cloud

The objective of this study is to mitigate security risks associated with cloud architecture through the application of hybrid encryption methods, specifically, the Diffie Hellmann Key Exchange and Elliptic Curve Cryptography. A novel model has been proposed to facilitate the implementation of two methods for enhancing security and reliability in cloud systems. This architecture is designed to ensure data integrity from the user's perspective. The methodology employed in our system comprises a series of sequential steps:

Step 1: Connection Establishment: Upon the first instance of accessing the system, the user is presented with a prompt to establish an account. The initiation of the primary linkage is expedited by the utilisation of Hyper Text Transfer Protocol and Secure Socket Layer protocols.

Step 2: Account Creation: Upon the initial establishment of a secure connection, the user is prompted to provide the necessary account information for the creation of an account within our cloud-based system. The aforementioned particulars are transmitted via the web to our server. An account has been successfully created within the system. Moreover, the establishment of the connection is facilitated through the utilisation of the Diffie Hellmann Key Exchange protocol. The server is responsible for generating a unique user identifier, which serves as a means of distinguishing individual users. Additionally, it generates a Diffie Hellman equivalent stream, as well as the necessary private and public keys for ECC encryption. The user identification is transmitted to the user via a secure channel. The user is instructed to maintain confidentiality of the provided identification information, as it serves as a means of authentication for accessing the system during subsequent logins.

Step 3: Authentication: Upon accessing the homepage of the cloud server, the SSL connection is promptly established. Upon creating an account, the user is prompted to authenticate themselves by providing requisite personal information and the confidential user identification previously issued to them. The authentication process on the cloud server involves the retrieval of the Diffie Hellman equivalent of the user identifier from the server repository to verify the user's authenticity. Following the successful verification of the key, the protocol commences the process of establishing a connection, thereby granting the user access to log in to the server. The private key of the user is transmitted to the back end for encryption, in conjunction with the Elliptic Curve Cryptography (ECC) algorithm.

Step 4: Data Exchange

The process of data exchange in this context comprises two distinct stages:

A. At client side: The user desires to retrieve message from server storage. To accomplish this, their query is transformed into a file format and subsequently encrypted utilising their public key. The aforementioned encrypted data is subsequently transmitted to the client for the purpose of dealing.

B. At server side: The encrypted data is received by the server. The private key is utilised to decrypt the data, after which the user query is processed. The outcome of the aforementioned process is subsequently subjected to encryption and subsequently transmitted to the client.

### 6.1.1 Key for ECC

The public key is represented as an idea on the curve. The private key is a randomly generated numerical value. The generation of a public key involves the multiplication of a private key with a generator point G. The present discourse delves into the topic of point generation and various other related factors.

A. Curve’s point Calculation: The ECC algorithm is capable of calculating a novel curve point based on the multiplication of points. The point is encrypted as a means of exchanging information between end users.

B. Choice of Field : Polynomial time algorithms are utilised to evaluate computations with smaller computations, whereas exponential time algorithms are employed to evaluate complex computations, as stated in reference [9]. The equation representing an elliptic curve is provided as follows:

$$Y^2 = X^3 + aX + b \qquad (9)$$

C. Integer Factorization: The process of finding the prime factors of a given integer is commonly referred to as integer factorization. The equation is obtained when considering an integer n that is the result of multiplying two large prime numbers i and j. (9)

The computation of n, given i and j, is a straightforward task. For large values of n, the determination of i and j is considered computationally infeasible. The security of the system is contingent upon the level of complexity involved in factoring the sizable prime numbers. The approach employed for resolving the Integer Factoring problem is the The number Field Sieve, which is an algorithm that exhibits sub-exponential behavior.

D. Key Generation

The process of generating keys holds significant importance. It is imperative that an algorithm be designed to generate both a public and private key. The message data will be encrypted by the sender using the public key of the receiver, and subsequently decrypted by the receiver utilising its private key. Choose an integer, n, such that n belongs to the range of m. The public key is generated through the utilisation of the subsequent equation,

$$Publick_{key} = n * p \qquad (10)$$

The variable n is a randomly generated number within a specified range. (1 to m-1). Point P lies on the curve.

E. Encryption

Let 'M' denote the message that is intended to be transmitted. Let 'M' be a point on the curve 'C' and let 'N' be a point on 'C' such that 'N' is coincident with 'M'. Select a value 'i' from the range of [1 - (m-1)] in a random manner. Two cypher texts, denoted as C1 and C2, will be produced.

$$C1 = i * Publick_{key} \qquad (11)$$

$$C2 = N + (i * Publick_{key}) \qquad (12)$$

F. Decryption

Utilize the provided formula to derive the initial communication that was transmitted.

$$M = C2 - n * C \qquad (13)$$

### 6.1.2 Diffle Hellman for Key Exchange

This particular protocol is considered to be a trailblazer in the emergence of public key cryptography. The process comprises the subsequent stages:

Step 1: let X be an abelian group

i € X, p is prime multiplicative order

Step 2: generated secrete key $S_{key}$

Step 3: A random $decrypt_A$ € {2,……M-1}is generated at sender side and compute $encrypt_A$=$i^d{}_A$

Step 4: Sender transmits $encrypt_A$ to the receiver

Step 5: A random $decrypt_B$ € {2,……M-1}is generated by receiver and compute $encrypt_B$= $i^d{}_B$

Step 6: Receiver sends $encrypt_B$ to receiver.

Step 7: Sender calculates $S_{key}$=$(encrypt_B)_A{}^d$ = $i^d$ $A^d$B

Step 8: Receiver calculates $S_{key}$= $(encrypt)_B{}^A$= $i^d$ $A^d$B

## VII. Conclusion and Future Scope

This paper presents an analysis of the security challenges encountered by private user data in cloud systems, highlighting the pressing need for a viable solution to address the issue. The use of linear algorithms for cryptography can effectively ensure data security. However, the vast amount of data present in cloud computing poses a challenge to this approach. The present study introduces an architectural framework that can be deployed in a cloud-based setting, leveraging the benefits of linear cryptography to establish a reliable connection and increasing cryptography to encrypt data. The present study employs two cryptographic algorithms, namely Diffie Hellman Key Exchange and Elliptical Curve Cryptography. By utilising the aforementioned algorithms, we present a four-step methodology for verifying the legitimacy of a user. The initial stage involves establishing a connection, followed by the creation of an account, authentication, and ultimately, data exchange. The ECC method was selected due to its relatively low computational cost and faster processing speed in comparison to existing linear algorithms. An additional benefit is that its time complexity is sub-exponential, rendering it challenging to decipher. The Diffie-Hellman protocol was utilised due to its superior ability to establish connections.

In future, our focus lies on the execution of the suggested framework, accompanied by various comparisons to demonstrate the efficacy of our proposed architecture.

## References

1. Dheepak, T. "Enhancing the Cloud Security with ECC based Key Generation Technique." Annals of the Romanian Society for Cell Biology (2021): 3874-3891.

2. Kumar, Vinod, et al. "SEBAP: a secure and efficient biometric-assisted authentication protocol using ECC for vehicular cloud computing." International Journal of Communication Systems 34.2 (2021): e4103.

3. Kumari, Adesh, Vinod Kumar, and M. Yahya Abbasi. "EAAF: ECC-based anonymous authentication framework for cloud-medical system." International Journal of Computers and Applications (2020): 1-10.

4. Tallapally, Sampath Kumar, and B. Manjula. "Competent multi-level encryption methods for implementing cloud security." IOP Conference Series: Materials Science and Engineering. Vol. 981. No. 2. IOP Publishing, 2020.

5. Vengala, Dilip Venkata Kumar, D. Kavitha, and AP Siva Kumar. "Secure data transmission on a distributed cloud server with the help of HMCA and data encryption using optimized CP-ABE-ECC." Cluster Computing 23.3 (2020): 1683-1696.

6. KHAN, MOHAMMAD AYOUB, et al. “A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data.” IEEE Access, 2020

7. Hema, V. Sri Vigna, and Ramesh Kesavan. “ECC Based Secure Sharing of Healthcare Data in the Health Cloud Environment.” Springer Science+Business Media, LLC, part of Springer Nature, 2019.

8. Bommala, Harikrishna, et al. "Performance of Evaluation for AES with ECC in Cloud Environment." International Journal of Advanced Networking and Applications 10.5 (2019): 4019-4025.

9. Hosam, Osama, and Muhammad Hammad Ahmad. "Hybrid design for cloud data security using combination of AES, ECC and LSB steganography." International Journal of Computational Science and Engineering 19, no. 2 (2019): 153-161.

10. N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, Vol. 48 (1987) pp. 203–209.

11. Thangapandiyan et al. )Thangapandiyan, M., PM Rubesh Anand, and K. Sakthidasan Sankaran. "Enhanced cloud security implementation using modified ECC algorithm." 2018 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2018.

12. Gupta, Daya Sagar, and G. P. Biswas. "A secure cloud storage using ECC-based homomorphic encryption." International Journal of Information Security and Privacy (IJISP) 11, no. 3 (2017): 54-62

13. Jana, Bappaditya, et al. “A Multilevel Encryption Technique in Cloud Security.” 7th International Conference on Communication Systems and Network Technologies, 2017

14. Gajra, Nikhil, et al. “Private Cloud Security : Secured User Authentication by using Enhanced Hybrid Algorithm.” International Conference on Advances in Communication and Computing Technologies, 2014

15. Tirthani, Neha, and R. Ganesan. "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography." IACR Cryptol. ePrint Arch. 2014 (2014): 49.