**IMPLEMENTATION**

**PROPOSED SECURITY SOLUTION**

To secure data, most systems use a combination of techniques

Encryption, which means they use a complex algorithm to encode information. To decode the encrypted files, a user needs an encryption key. While it’s possible to crack encrypted information, most hackers don’t have access to the amount of computer processing power they would need to decrypt information.

1. Authentication processes, which require creating a user name and password.
2. Authorization practices -- the client lists the people who are authorized to access information stored on the cloud system.

Data Uploading:

The uploading of data in the cloud is effectively performed in two distinct sets. The data which is very susceptible is authorized to encrypt before entering the cloud scenarios which is known as the Private data. The private data is encrypted by means of the ECC technique in which the key produced is shared for the purpose of downloading the data. The ECC technique smartly brings in superior-level safety, in a very effective and cost-conscious way. The public data is uploaded as such in the identical version without any variation.

ECC:

Ecc Based Encryption: An Elliptic Curve Cryptography (ECC) is exploited for the file encryption by creating a personal and public key of encryption in our suggested file. The personal and public keys are produced by the ECC method makes the updated input file more safe as well the produced keys are vigorous. The key generation and formation are explained beneath.

Key Generation:

Key generation is an important part where an algorithm should 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, select a number, d within the range of n. Generate the public key using the following equation,

Q = d \* P

Where d = the random number selected within the range of (1to n-1). P is the point on the curve, Q is the public key and d is the private key.

Encryption:

Encryption Let ‘m’ be the message that has to be sent. 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 \* P) E.

Decryption:

Use the following equation to get back the original message ‘m’ that was sent.

M = C2 - d \* C1

M is the original message that was sent.

**3.1Elliptic Curve Cryptography (ECC) domain parameters**

The public key cryptographic systems involve arithmetic operations on Elliptic curve over finite fields which are determined by elliptic curve domain parameters.

The ECC domain parameters over Fq 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 = 2m, where p is a prime

• **FR:** field representation of the method used for representing field elements ∈ Fq

• **a, b:** field elements, they specify the equation of the elliptic curve E over Fq,

y2 = x3 + ax + b

• **G:** A base point represented by G= (xg, yg) on E (Fq)

• **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(Fq)/n, where #E(Fq) is the curve order

The primary security in ECC is the parameter n; therefore the length of ECC key is the bit length of n. For comparative length, the security of ECC keys is much more than that of other cryptosystems. That is for equivalent security, the key length of ECC key is much lesser than other cryptosystems.

Data Download:

The owner of the data is the only person who is expected to download the data uploaded in the private mode. Each and every access to the data is effectively reported by the TPA. The access record encompasses the data being shared or depends on the cloud scenarios. The private data download consists of easy steps as on data upload. The encrypted data is decrypted by means of the key produced while uploading the content. In accordance with the ECC encryption logic, the pair of the key has created the key left for decrypt is for the download [10]. The corresponding decrypt on the data authenticates the veracity of the original data, which goes a long way in authenticating the data safety.