**CHAPTER 4**

**PROBLEM OUTLINE**

(Cloud computing 2022)Despite a number of benefits of CC, it has specified amelioration to a variety of challenges and difficulties. One of the greatest hurdles is Security that hinders among users to the acceptance of CC [1], [6]. Client’s sensitive information and software are placed on the premises of cloud provider’s. Data security issues increase because of this and it is the most important concern that must be taking into consideration [7]. For data transmissions and operations, if appropriate security measures are not provided then they will be at excessive vulnerability [8]. Thus, data, applications and from internal and external threats cloud infrastructure must be protected by cloud service providers (CSPs). The security of cloud information depends on the countermeasures, suitable information security implementation measures and a difficult operation of making the management and creation of a reliable and safe cloud environment. Unreliable servers and protecting user sensitive data against malicious attacks are essential.

The user data that have to be secured are as follows [3]:

1. custom data: data congregated from computers;
2. private data: such as health and bank account information;
3. personally distinguishable data: the data that might be used to describe an individual; and
4. Unique device identifiers: data that can be tracked uniquely, such as IP addresses.

To prevent unwanted access encryption is one of the safest methods. Encryption is used to prevent data from online theft. In CC environments, to protect cloud information and user data there are various types of encryption techniques have been used, which have contributed to downgrading hacking to some amount. To enhance data security the data can be converted into cipher text. On the other hand, this procedure may lead to the loss of various characteristics. By using two widespread techniques encrypted text can be achieved. Based on the safety index the first technique is, which generates a safeguard cipher text keyword index by checking the existence of keywords, and the another technique is based on scanning cipher text, which evaluates each word to guarantee that the keywords are in the cipher text [3].

Symmetric cryptographic encryption technique same key use for both encryption (from sender sides) and decryption (from receiver side’s) so key must be shared between two parties (sender and receiver). Now its vulnerable by the attackers and if third party know this key so they modify the content in middle.

At the present time data security is a crucial concern that may be maltreated by both external and internal parties. To encrypt the Information there may be a number of ways and then encrypted information sent over the Internet. In spite of this, also these methods have the shortcoming of requiring a great deal of resources, such as a lot of computing power and memory, to safety measure the data. Corresponding AES encryption, after an input file is uploaded a key is generated quickly. To encrypt and decode data, AES make use of a technique known as symmetric key encryption, which have need of the use of a single key. If a third party has knowledge of the single key, they may decrypt the input data file and encrypt it again deprived of the user ever knowing that the file was read so it’s vulnerable to attack. Although AES is one of the safeguard algorithms, but by knowing the single key its safety can be compromised. On the other hand, one of the most protected algorithms is Asymmetric key encryption. ECC uses asymmetric key encryption because it requires two keys, the public key and the private key respectively. This indicates that it has an advance level of protection since to decrypt both keys at the same time it is challenging for hackers. The foremost advantage of ECC is its smaller key size. Contrasting other algorithms, with a smaller key size it can be responsible for the security of the same level. In Symmetric key cryptosystem, the same key is used for encryption and decryption. Key establishment and Trust Issue are the two main challenges in symmetric key cryptosystem. There is a requirement to develop a system which provides a smaller amount of computational charge and the security of the data over the cloud with a smaller amount time for the encryption/decryption procedure. We combine the properties of three encryption techniques that are symmetric, asymmetric and hashing .we utilize them in our proposed architecture.

So we proposed an architecture in which we use ECC algorithm for key generation diffie hellman for reliable key exchange over communication channel along with digital signature during login. Developing a system that provides data security through the cloud with lower computational costs and faster encryption / decryption process is essential. To leverage the strengths of both, we combine them in our proposed model.

Currently, the security of data is a major issue which can be compromised in different ways using either external or internal means. To protect the transmission of data over the Internet, different encryption techniques are used. The problem with these techniques is that they need large key size, large memory size, and require a lot of computation power to protect the data. As in AES encryption, a key is generated soon after the input file is uploaded, and we know AES uses symmetric key encryption method in which a single key is used for encryption as well as decryption. Hence, if the single key is known by the third party, then the input file will easily be decrypted and again encrypted so that the user does not know that the input file has been read by someone else. Although AES is one of the secure algorithms, its security can be compromised by knowing the single key. ECC uses asymmetric key encryption in which there are two keys for encryption and decryption, public and private key, respectively. This is the reason that its security level is higher, and it is not easy for hackers to crack both keys at once. ECC is also mainly known for its smaller key size. ECC can provide the same security level as compared to other algorithms in a smaller key size.

(AES + Modified ECC 2023 )

Data security is now a key concern that may be abused by both internal and external parties. Information sent over the Internet may be encrypted in a number of ways. However, these methods have the drawback of requiring a lot of resources, such as a lot of memory and computing power, to safeguard the data. Like AES encryption, a key is created quickly after an input file is submitted. To encrypt and decode data, AES employs a technique known as symmetric key encryption, which requires the use of a single key. If a third party has knowledge of the single key, they may decrypt the input file and encrypt it again without the user ever knowing that the file was read. Asymmetric key encryption is one of the most secure algorithms. MECC uses asymmetric key encryption because it requires two keys, the public key and the private key. This means that it has a higher level of protection since it is difficult for hackers to decrypt both keys at the same time. MECC’s main advantage is its smaller key size. Unlike other algorithms, it can provide the same level of security with a smaller key size. Developing a system that provides data security through the cloud with lower computational costs and faster encryption / decryption process is essential. To leverage the strengths of both, we combine them in our proposed model.

Numerous researchers have focused on finding various answers to the CC data security issue [9]. Further research is needed to understand the cloud’s associated security and privacy problems. This Research provided a robust hybrid encryption algorithm by using both symmetric and asymmetric techniques that can be used to provide greater cloud security.