**SYSTEM ANALYSIS**

**EXISTING SYSTEM:**

The stored information of integrity is conserved for data integrity in the cloud system. The unauthorized users should not be accessed misappropriate or vary of data. Data integrity and reliability of data are faithful to preserve by the cloud computing provider. Data confidentiality is also a crucial way from a user’s point of perspective therefore they store their private or confidential data in the cloud. Data confidentiality is taken to assure access control policies and authentication. The faith of cloud computing could be forward by rising cloud authenticate and data confidentiality. So the keep data on the cloud should be security, integrity, privacy, and confidentiality of crucial demands from the user perspective.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Security challenge that desires an autonomous auditing scheme to analyze the data integrity on the cloud server. In this approach, the random oracle model has been used to prove the security of cryptography. In the model maintain can the data integrity but cannot maintain the data confidentiality.
* Merkle hash tree in this approach, confidentiality is not maintained and batch auditing is supported.
* According to Meenakshi MHT the data confidentiality not available.

**PROPOSED SYSTEM:**

In the proposed system uses AES256, RSA-15360, and SHA512 algorithm. AES- 256 is a standard and most acceptable algorithm for encryption and decryption processes. It works on the input block size of 128 bits having a key size of 256 bits. Therefore, it has 2256 possible a key combination which is 78 digits number. It exponentially generates the number of astronomically in the observable universe. It is considered a strong algorithm among all. If a computer breaks 1 trillion decryption/seconds then it has taken 257year to break the AES-256. It is more secure than RSA and ECC.

**ADVANTAGES OF PROPOSED SYSTEM:**

* SHA-512 algorithm was developed by NIST. It is a member of SHA-2 which is the latest version of the secure hash algorithm based on the Merkle-Damgard scheme.
* The SHA224, SHA256, SHA384, and, SHA512 are made by NIST of as the new standard hash function.
* The reliability of SHA512 is achieved by the ability to generate 512 bits hash value, This long hash value makes the SHA-512 more resistant to attack.