**CONCLUSION**

Data and privacy protection are the primary problems that need to be solved in cloud computing. Data Security and privacy issues exist in all levels in cloud service. The above mentioned model is fruitful in getting the user to trust the cloud computing so that the user can able to store confidential data over the cloud computing. The Encryption Algorithm applicability provides the flexibility in range and sequence to the user's choice because of the various Methods a user can apply all or omit any in any order. Even if the user does not select any encryption technique, then random number algorithm will be implemented by default thus providing atleast a single level security. The opted sequence will also be stored in the database so that the decryption may be possible. The negative effect of this scheme is that it creates an overhead on the query performance due to multilevel of encryption and decryption but for the sake of security the performance issue can be over looked as we are concerned with only a small amount of data like that of passwords and not the large files. In this way we can conclude that security vendor enhances security with the help of multilevel hybrid encryption.