**6. CONCLUSION AND FUTURE WORK**

**6.1 CONCLUSION**

The Project simulates a model that is already quite common for consumer apps like email and photo sharing, and for certain business applications. But in this project, we present a way to secure the data using different security techniques and efficient encryption algorithms to secure the file along with its location from the users that stores and retrieves it. As with the Internet, on-demand applications have grown so ubiquitous that almost every business user interacts with at least one, whether it's an email service, a Web conferencing application, or a file hosting system.

The data is stored at multiple places over the information space (over the Internet). It sounds similar to file hosting websites which stores the data that is being uploaded by different users and can be retrieved using proper authentication. The only difference is that the system for which project is targeted is an application based system like which will run on the client’s own system. This application will allow users to upload file of different formats with security features including Encryption, secure OTP verification, uploading and downloading over the cloud securely.

This prototype works using a mixture of elliptical curve cryptography and symmetric key algorithm. ECC is used to achieve the process of user's verification and to keep the private data secure. AES algorithm is used to allow the user to store and access their data securely to the cloud by encrypting the data in the client side and decrypting the data after downloading from the cloud. Since the private key is owned only by the user of the data, no one can decrypt the data, even though the hacker can get the data through some approaches.

The uploaded files can be accessed from anywhere using the application which is provided. We believe this system serves as a foundation for future work in integrating and securing information sources across the World Wide Web.

34

**6.2 SCOPE FOR FUTURE WORK**

The development of this project surely prompts many new areas of investigation. We have successfully completed all the phase of the development and did our research prior to the development about the various encryption techniques along with their strengths and weaknesses. After in depth comparisons and review we decided to use ECDH and AES Algorithms to implement the whole idea of this model. We referred multiple research papers whose links can be found in the references. Lastly, we implemented the model using Java Servlets & JSPs, Apache Tomcat server and MySQL for storage. We will be using cloud hosting services for the actual deployment of the project. For the GUI, we have used HTML and CSS 3.

In the last semester, we completed database modelling, new user registration module, secure key generation, exchange module along with introduction, user interface of the application and we managed to develop approximately 50% of the whole project. In current semester, we have worked on modules like, file encryption-decryption, secure file download and upload using user ID and another OTP, Secure AES Key generation for the file handling features, testing of the whole application, load balancing, checking the border cases to make sure that all the modules are completed and running.

Keeping all the deadlines in mind and the project development life-cycle of our project, we have been able to complete all the phases of the development cycle on time with minimum possible errors. Talking about scope of future work, we believe that it is possible to minimize the processing time taken in all the encryption-decryption processes by using professional hosting services and even better implementation of the security model. Also, some advanced hybrid cryptography algorithms and system can be incorporated to ensure cutting edge security and protection.

35