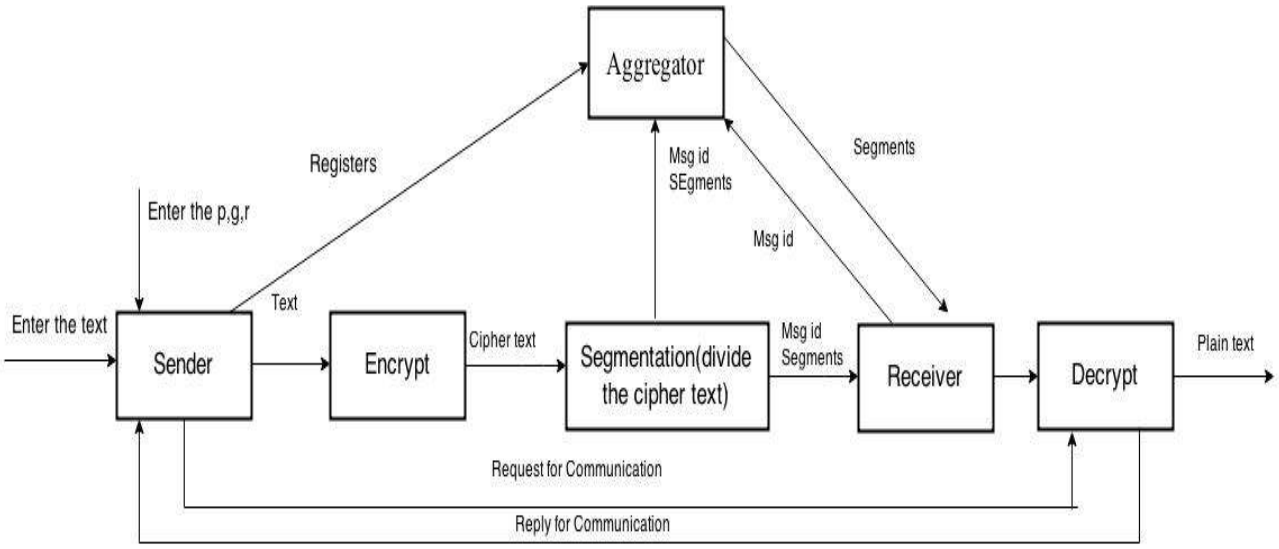

Figure 1: Block Diagram for EVPPP

The protocol aims to establish an intruder free communication between the sender and receiver. The objective of this project is to encrypt the text and decrypt the text using aggregator. In this project users encrypt the text using the Efficient Verifiable Privacy Preserving Protocol (EVPPP) algorithm. The EVPPP algorithm divides the cipher into segments and then passes these segments to the aggregator and receiver using sockets. The socket is the endpoint communication between the two computers in networks. The sender and receiver register itself with the aggregator. The receivers decrypt the cipher text by comparing with the IP address, id and segments.

This project uses EVPPP algorithm which reduces the time required for encryption and decryption. It is observed that EVPPP is nearly 80% more efficient than existing algorithms.

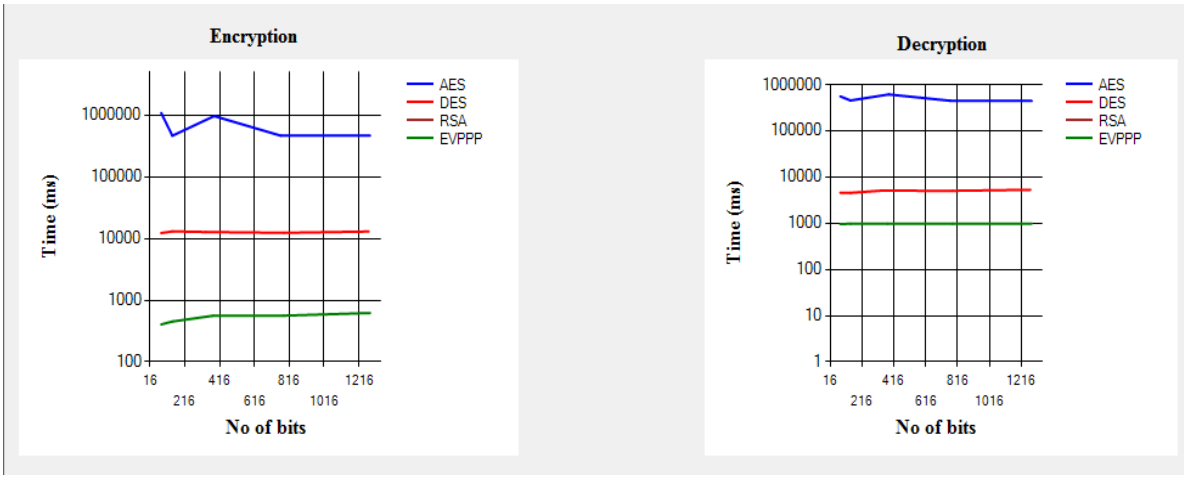

Figure 2: Comparison of encryption and decryption

Aggregator is the trusted party consisting of all the information about sender and receiver. The real time application is Military application, Mobile data Communication, Social Networks. The efficiency can be increased by sending the segments to multiple intermediate receivers, and then in turn to the final recipient.