**ABSTRACT**

Outsourcing data and computation to cloud server provides a cost-effective way to support large scale data storage and query processing. However, due to security and privacy concerns, sensitive data (e.g., medical records) need to be protected from the cloud server and other unauthorized users. One approach is to outsource encrypted data to the cloud server and have the cloud server perform query processing on the encrypted data only. It remains a challenging task to support various queries over encrypted data in a secure and efficient way such that the cloud server does not gain any knowledge about the data, query, and query result. In this paper, we study the problem of secure skyline queries over encrypted data. The skyline query is particularly important for multi-criteria decision making but also presents significant challenges due to its complex computations. We propose a fully secure skyline query protocol on data encrypted using semantically-secure encryption. As a key subroutine, we present a new secure dominance protocol, which can be also used as a building block for other queries. Furthermore, we demonstrate two optimizations, data partitioning and lazy merging, to further reduce the computation load. Finally, we provide both serial and parallelized implementations and empirically study the protocols in terms of efficiency and scalability under different parameter settings, verifying the feasibility of our proposed solutions.**LIST OF FIGURES**

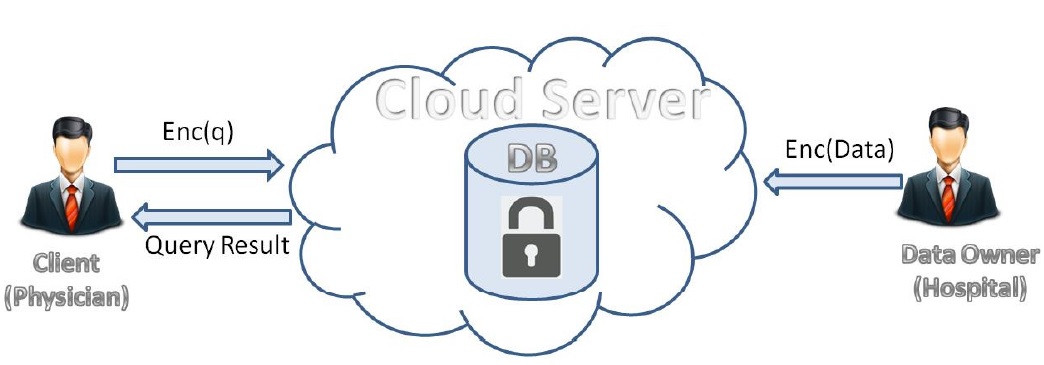
****

Figure1:overall architecture

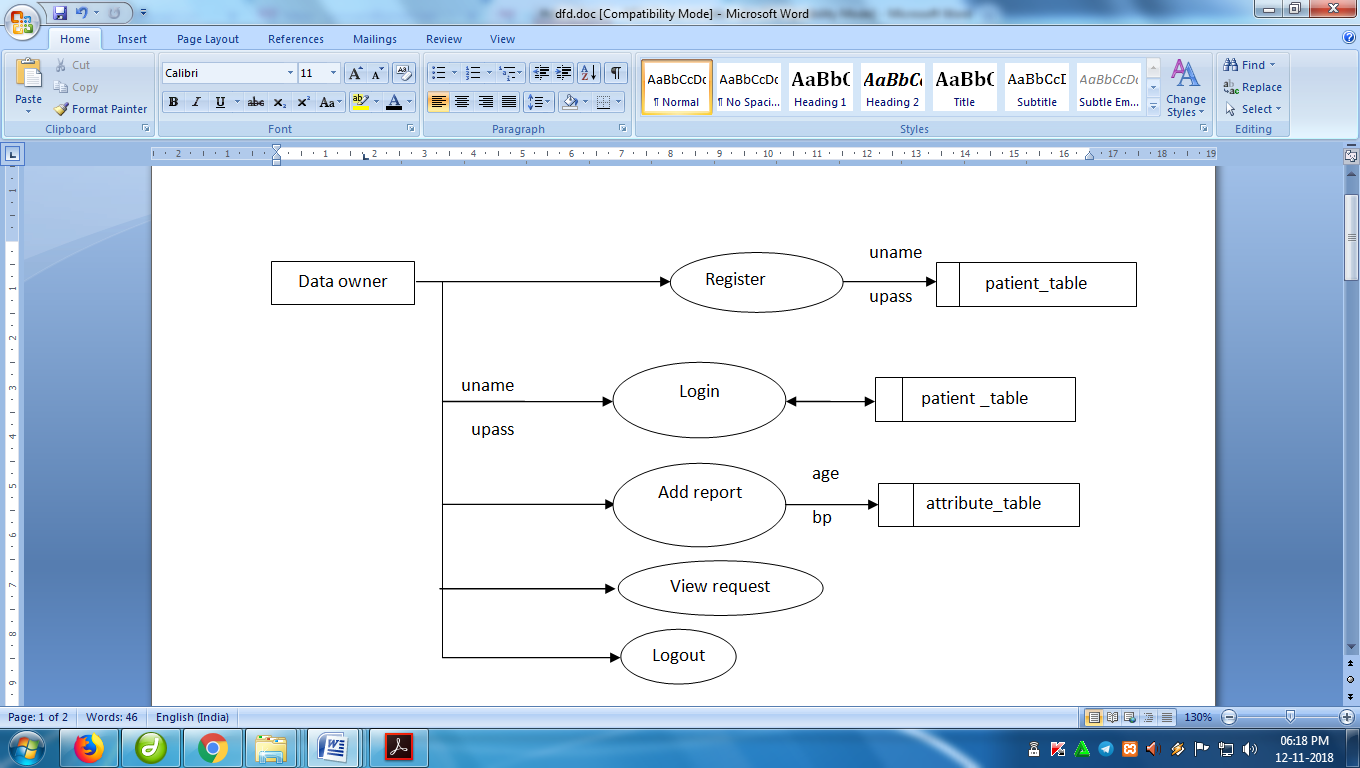
****

Figure2: Dataowner module

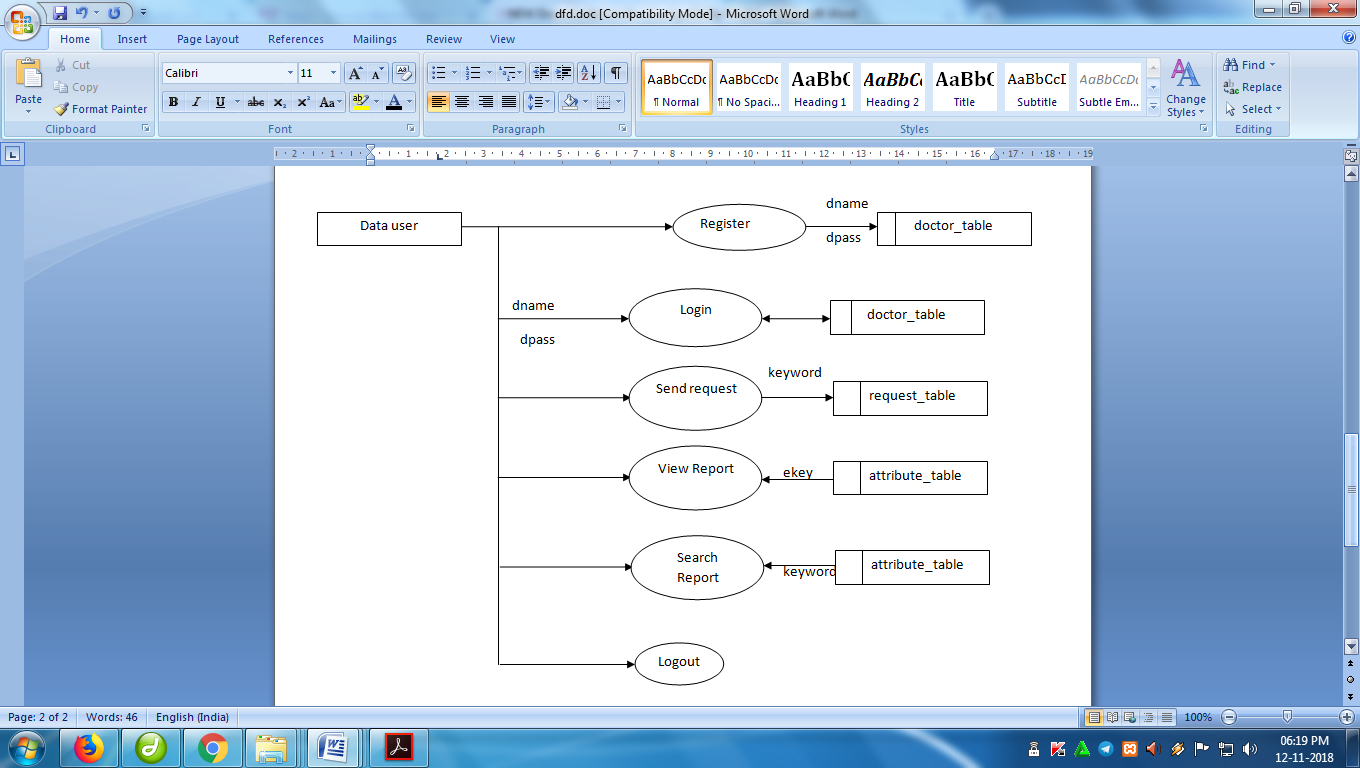
****

Figure2: Datauser module

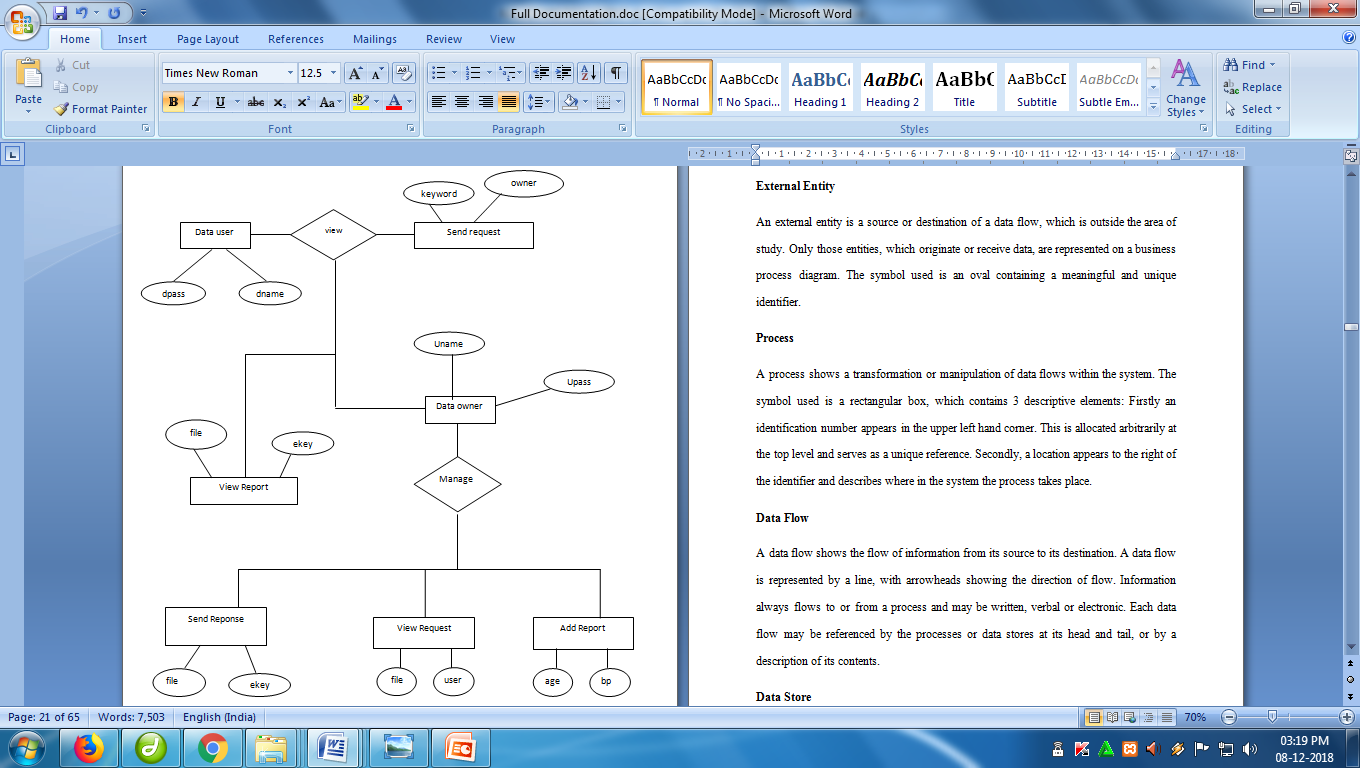


Figure4: Data user-Data owner Interaction

**LIST OF ABBRVIATIONS**

|  |  |
| --- | --- |
| SGX - | Software Guard Extensions |
| SMC - | Secure Multi-party Computation |
| SLESS - | Secure Less |
| SMIN - | Secure Minimum |
| kNN - | k-Nearest Neighbour |