**EAFS: AN EFFICIENT, ACCURATE, AND FORWARD SECURE SEARCHABLE ENCRYPTION SCHEME SUPPORTING RANGE SEARCH**

**CHAPTER-1**

**ABSTRACT**

Forward privacy in existing searchable symmetric encryption approaches generally supports only keyword searches, rather than range searches. In addition, existing approaches that support range search over encrypted datasets have limitations associated with efficiency, accuracy, and security. Seeking to address these limitations, we formally propose the definition of the forward privacy for secure range searches. Also, we demonstrate how three widely used cryptographic tools— order-preserving encryption (OPE), pseudorandom function, and one-time pad–can be leveraged to design an efficient, accurate, and forward secure (EAFS) searchable encryption scheme supporting range search in encrypted numerical databases. In the proposed EAFS scheme, a trapdoor only matches the last data record that satisfies the search range, and the other results are found iteratively using the previous result. The chain-like search and the embedded ciphertexts of OPE simultaneously guarantee its efficiency, forward privacy, and accuracy. We also use the simulation-based method to demonstrate that our scheme is secure. Then, we implement EAFS in Microsoft Azure and evaluate its performance. The evaluation findings demonstrate that our proposed scheme supports secure range search practically and efficiently.