Abstract

Odata cu dezvoltarea cloud-ului si incercarea portarii aplicatiilor in acest mediu, nevoia de securitate a crescut considerabil, deoarece a devenit mult mai usor ca bazele de date ale aplicatiilor sa fie atacate sau observate de catre adversari malitiosi. Din aceasta cauza a aparut necesitatea criptarii permanente a bazelor de date in moduri din ce in ce mai complexe. Acest lucru aduce in mod natural cu sine timpi de decriptare mai mari, chiar si pentru utilizatori autorizati care nu ataca sistemul. Acest fapt nu face din decriptarea unei baze de date pentru fiecare query un lucru dezirabil. Un mecanism bun si eficient in efectuarea de query-uri asupra bazelor de date criptate este OPE (order-preserving encryption/encoding). Acest tip de criptare lasa criptotextele in aceiasi ordine ca plaintextele aferente fara a dezvalui si alte proprieteti ale plaintextelor.

In lucrarea de fata vom studia scheme OPE existente, avantajele si dezavantajele lor si vom propune o noua schema OPE cu aplicatii in baze de date relative stabile (cu rata de insertie sufficient de mica, dar cu rata de cautare mare). Mai specific, aceasta schema va avea timpi excelenti de cautare pentru datele care au mai fost cautate anterior (relative recent), insa va scrifica din timpul de inserare pentru noi date (similar pentru stergere). Vom realiza acest lucru printr-o combinatie de encoding minimal, structure de date bine alese si probabilitati. Rezultatul va fi o schema de encoding care are putine interactiuni intre client si server si care nu dezvaluie decat ordinea criptotextelor.