Soluții inovative folosind mecanisme criptografice pentru a asigura securitatea datelor în cloud

Progresul tehnologic recent și varietatea de servicii oferite de către entități terțe a produs atât o schimbare de paradigmă în zona securității cât și noi oportunități privind monetizarea datelor. Diferitele stadii în care se află informația au propriile provocări, unele adresate iar altele fiind încă o problemă deschisă, precum protejarea datelor în momentul utilizării. Adresarea incompletă a problemei permite ca la granița dintre etape să se formeze zone puternic expuse incidentelor cibernetice.

Scopul acestei teze este acela de a prezenta tehnologiile emergente și soluțiile necesare pentru asigurarea securității în timpul execuției, indiferent unde are loc aceasta. Pentru început, sunt adresate schemele de criptare homomorfică împreună cu o serie de contribuții la nivel teoretic și practic, acoperind subiecte de optimizare a circuitelor, scheme noi de criptare, accelerări folosind platforme hardware precum și aplicații concrete. Ulterior, sunt abordate computațiile sigure multi-participant unde regăsim propus un sistem de autentificare complet descentralizat folosind o tehnologie conexă numită blockchain și protocoalele de SMPC pentru semnarea digitală distribuită. Un alt domeniu al contribuțiilor aduse este acela al mediilor sigure de execuție unde se realizează un modul software de securitate capabil să emuleze un HSM, prin utilizarea setului de instrucțiuni Intel SGX. În finalul tezei sunt prezentate și o serie de tehnologii similare, capabile să ofere protecție în timpul procesării.

Pe baza rezultatelor obținute acestei cercetări, se poate ajunge la concluzia că există instrumentele necesare protecției informațiilor pe toată durata de viața a lor, iar segmentul emergent abordat lasă loc inovării și îmbunătățirii soluțiilor actuale.