REZUMATUL TEZEI DE DOCTORAT
„MACHINE LEARNING ÎN CYBERSECURITY”

Autor: **Constantin-Ilie NILĂ**
E-mail: constantin.nila@mta.ro, tel.: +40751 375 077
Conducător de doctorat: Prof.emer.dr.ing. **Victor-Valeriu PATRICIU**

În contextul dezvoltării tehnologiilor de inteligență artificială, al integrării acesteia în domenii din ce în ce mai variate, accesibile publicului larg, și al demonstrațiilor inovative, trebuie să luăm în considerare și necesitatea de adaptare a sistemelor de securitate. Soluțiile de securitate au devenit uzuale, fiind de neconceput configurarea unei arhitecturi de informatică și comunicații fără ca acestea să joace un rol principal. Variind de la sistemele de detectare a intruziunilor și clasificare a programelor malware până la metodele de detectare a phishingului și de autentificare sigură, toate aceste sisteme pot beneficia de capacitatea modelelor de învățare automată.

Această lucrare explorează integrarea învățării automate în securitatea cibernetică, subliniind trecerea de la abordările tradiționale de securitate la strategii mai dinamice și adaptive. Abordările propuse dezvăluie provocările cu care se confruntă modelele predictive actuale în detectarea amenințărilor în timp real, evidențiind importanța datelor de antrenare relevante și de înaltă calitate. Un aspect cheie definit în cadrul lucrării este aplicarea diversă a tehnicilor de învățare automată în procesul de dezvoltare al soluțiilor de securitate cibernetică. Această abordare proactivă este crucială într-un peisaj în care strategiile reactive sunt adesea insuficiente împotriva amenințărilor avansate și persistente.

Totodată este analizată perspectiva în care însăși sistemele de securitate sunt expuse la riscul atacurilor cibernetice, iar implementarea cu succes a algoritmilor de protecție a datelor cu caracter personal poate aduce o contribuție semnificativă la sistemele viitoare de inteligență artificială și la alte sisteme de gestionare a datelor. Echilibrarea sensibilității și specificității modelelor se extinde dincolo de considerentele de securitate, atingând aspecte etice și de confidențialitate în implementarea soluțiilor de securitate cibernetică bazate pe învățarea automată. Deoarece aceste sisteme procesează și analizează adesea datele personale și organizaționale sensibile, asigurarea confidențialității datelor și respectarea conformității cu reglementările actuale devin primordiale. În cadrul lucrării sunt susținute diferite abordări ce descriu aceste preocupări, inclusiv protecția diferențială a datelor și criptarea homomorfă, care permit prelucrarea datelor într-o formă criptată.

Lucrarea abordează, suplimentar față de aspectele tehnice, importanța colaborării interdisciplinare în acest domeniu. Aplicarea eficientă a învățării automate în securitatea cibernetică necesită un amestec de experiență în informatică, știința datelor, securitate cibernetică și cunoștințe specifice domeniului. Această abordare interdisciplinară asigură alinierea la realitățile practice și nevoile viitoare de securitate cibernetică.