

Mărginean Radu

EXPERIENȚĂ PROFESIONALĂ

IMOGEN — Cercetător Junior

Iulie 2018 - Prezent (Cluj-Napoca, România)

Fac parte din proiectul imATFIB, ce urmărește dezvoltarea de unelte imagistice pentru diagnosticarea fibrozei atriale. Responsabilitățile principale includ dezvoltarea și analiza de algoritmi de segmentare a imaginilor medicale folosind automate celulare.

Accesa — Analist de Date Stagiari

Decembrie 2017 - Iunie 2018 (Cluj-Napoca, România)

Am făcut parte dintr-o echipă ce dezvoltă platforme de monitorizare și control a apei. Am analizat înregistrările generate de aceste sisteme, implementate în aplicații variate. Munca mea a fost în principal experimentală - am explorat moduri prin care datele au putut fi folosite pentru a adăuga valoare companiei. Munca mea a implicat procesare de date, analiză de serii de timp și regresie, precum și instruire automată.

University of Maryland — Cercetător Stagiari

August 2017 - Noiembrie 2017 (College Park, MD, S.U.A.)

Am făcut parte din Centrul de Securitate Cibernetică a Universității din Maryland, unde am lucrat în cadrul unui proiect de cercetare în domeniul instruirii automate adversariale, concentrat pe atacuri de tip *targeted poisoning* împotriva rețelelor neuronale artificiale.

Responsabilitățile mele au inclus analiza rezultatelor, proiectarea experimentelor, analiza și dezvoltarea algoritmilor de atac și a proprietăților acestora. Stagiul a fost încheiat cu publicarea unui articol într-o conferință de rang înalt.

National Instruments — Inginer Software Stagiari

Mai 2015 - Februarie 2017 (Cluj-Napoca, România)

Am făcut parte din echipa LabVIEW FPGA Fabric, unde am fost implicat în dezvoltare, proiectare și validare de funcționalități software ce gestionează, compilează și interfațează resurse FPGA (FIFO, Registre, Memorii).

EDUCAȚIE

Universitatea Babeș-Bolyai — M.Sc. Inteligență Computațională

Octombrie 2017 - Iulie 2019 (Cluj-Napoca, România)

Studiez concepte, modele și metode în Inteligența Computațională, precum și aplicațiile acestora în științele naturale și sociale.

Universitatea Tehnică din Cluj-Napoca — B.Sc. Calculatoare

Octombrie 2013 - Iulie 2017 (Cluj-Napoca, România)

Am studiat concepte fundamentale în știința și ingineria calculatoarelor. Am terminat cu o medie ponderată a notelor de 9.45. Teza de licență a constat în dezvoltarea și analiza unei metode de predicție a comportamentului șoferilor. Aceasta folosește semnale provenite de la mașină, care sunt transformate în unități discrete, ce sunt mai departe modelate folosind un model lingvistic abstract. Predicția comportamentului se bazează pe inferență în modelul de limbaj. Metoda se bazează pe metode statistice neparametrice Bayesiene, precum procese Dirichlet și Pitman-Yor ierarhice. Teza fost notată cu 10.

COMUNICARE

Aptitudini de comunicare și muncă în echipa dezvoltate în contextul unui proiect mare (LabVIEW), precum și în contextul unui grup de cercetare mic și concentrat (Universitatea din Maryland).

APTITUDINI DE CERCETARE

Abilitați de analiză și vizualizare a datelor, precum și de raportare, tehnoredactare și elaborare de lucrări academice dezvoltate prin muncă de cercetare (UMD), teme din cadrul universității și proiecte personale.

Aptitudini de prezentare, raportare și sumarizare a literaturii de specialitate și a rezultatelor propriilor experimente, dezvoltate în proiecte de cercetare (UMD) și în elaborarea tezei de licență.

CUNOȘTINȚE TEORETICE

Familiaritate cu metode și tehnici din Instruirea Automată, precum și înțelegere a conceptelor de Calcul Diferențial/Integral, Algebră Liniară, Probabilități și Statistică utilizate în Instruirea Automată/Inteligența Artificială.

PROGRAMARE

Aptitudini bune de programare, dezvoltate atât pe latura de sisteme (cursul de Proiectarea Sistemelor de Operare) cât și pe latura aplicațiilor (algoritmi de Inteligență Artificială, procesare de date, manipularea imaginilor). Iscusit în python, C#, Java, C/C++, VHDL

PUBLICAȚII

Suciu, O., Mărginean, R., Kaya, Y., Daumé, H. III, Dumitraș, T. (2018) **When Does Machine Learning FAIL? Generalized Transferability for Evasion and Poisoning Attacks**. USENIX Security 2018

Suciu, O., Kaya, Y., Mărginean, R., Dumitraș, T. (2018) **Too Big to FAIL: What You Need to Know Before Attacking a Machine Learning System**. Security Protocols Workshop 2018.