UNIVERSITETI I PRISHTINËS
FAKULTETI I SHKENCAVE MATEMATIKE - NATYRORE
DEPARTAMENTI I MATEMATIKËS
PROGRAMI: Shkencë Kompjuterike

TEZA MASTER

Një shqyrtim sistematik i literaturës për metodat e mësimit automatik dhe të mësimit të thellë për sigurinë e internetit të gjërave

Mentori:
Prof. Ass. Dr. Eliot Bytyçi

Studenti:
Arditë Morina

Shkurt 2025, Prishtinë

Abstrakti i zgjeruar

Ky punim paraqet një analizë gjithëpërfshirëse të metodave të mësimit automatik (ang. machine learning - ML) dhe mësimit të thellë (ang. deep learning - DL) në kontekstin e sigurisë së Internetit të Gjërave (ang. Internet of Things - IoT). Qëllimi kryesor i punimit është të identifikojë, analizojë dhe vlerësojë teknikat më efektive për përmirësimin e sigurisë dhe integritetit të të dhënave në sistemet IoT, duke theksuar sfidat dhe mundësitë që shoqërojnë zbatimin e këtyre teknologjive në praktikat aktuale.

Në këtë punim shqyrtohen mënyrat se si ML dhe DL ndihmojnë në identifikimin dhe parandalimin e kërcënimeve, detektimin në kohë reale të sulmeve, ruajtjen e integritetit të të dhënave dhe zhvillimin e sistemeve mbrojtëse të avancuara. Gjithashtu, trajtohen kufizimet kryesore, përfshirë mungesën e dataset-eve cilësore për trajnimin e modeleve, sfidat e implementimit në pajisje me burime të kufizuara dhe vështirësitë e integrimit në infrastrukturat ekzistuese.

Punimi përfshin një analizë të aplikimeve praktike të IoT në sektorë të ndryshëm si shëndetësi, industri, qytete inteligjente dhe shtëpi inteligjente, duke vlerësuar kërkesat dhe sfidat specifike të sigurisë për secilin sektor. Në qytetet inteligjente, IoT përdoret për të menaxhuar trafikun, ku ML lejon analizën e modeleve dhe parashikimin e rreziqeve të mundshme, si identifikimi i sjelljeve anormale në rrjetet e transportit për të parandaluar aksidentet ose bllokimet. Në sektorin industrial, detektimi i anomalive përmes ML ndihmon në mbrojtjen e sistemeve të automatizuara, duke reduktuar rreziqet nga sulmet kibernetike dhe dëmtimet e mundshme të pajisjeve.

Në punim, paraqiten rekomandime konkrete për përmirësimin e sigurisë në IoT, me fokus në zhvillimin e qasjeve të personalizuara, përshtatjen e algoritmeve për burime të kufizuara dhe krijimin e mekanizmave më efikasë për detektimin dhe përgjigjen ndaj kërcënimeve.

Mungesa e dataset-eve cilësore për trajnimin e modeleve ML dhe DL, është një sfidë, pasi të dhënat IoT janë shpesh të shpërndara dhe përmbajnë informacione të ndjeshme, duke ngritur

shqetësime për privatësinë. Gjithashtu, implementimi i këtyre metodave në pajisje me burime të kufizuara mbetet sfidë, pasi fuqia përpunuese dhe kapaciteti i ruajtjes janë të limituara. Një tjetër sfidë është ndjeshmëria e modeleve të inteligjencës artificiale ndaj sulmeve kundërshtare, ku aktorët keqdashës mund të manipulojnë të dhënat për të mashtruar sistemet e sigurisë.

Një aspekt kyç i këtij punimi është eksplorimi i teknikave për të përmirësuar mbrojtjen e modeleve ML dhe DL në mjediset IoT. Një qasje premtuese është mësimi i federuar (ang. federated learning), i cili mundëson trajnimin e modeleve pa ndarë të dhënat e ndjeshme, duke ruajtur kështu privatësinë e përdoruesve. Për më tepër, zhvillimi i protokolleve të unifikuara të sigurisë për IoT mund të krijojë një standard të qëndrueshëm që siguron një nivel të lartë mbrojtjeje për pajisjet e ndërlidhura, duke reduktuar fragmentimin aktual të qasjeve të sigurisë në këtë fushë.

Rezultatet e këtij punimi sugjerojnë se zhvillimi i metodave më efikase dhe të optimizuara për zbatimin e ML dhe DL në IoT është një hap thelbësor drejt krijimit të një ekosistemi të sigurt dhe të qëndrueshëm. Pavarësisht sfidave, avancimet në këtë drejtim mund të sjellin mekanizma më të fuqishëm të sigurisë, të domosdoshëm për mbrojtjen e një infrastrukture gjithnjë në zgjerim siç është IoT.

Ky punim synon të kontribuojë në përmirësimin e qasjeve aktuale për sigurinë e IoT, duke siguruar jo vetëm mbrojtjen ndaj kërcënimeve, por edhe ruajtjen e integritetit të të dhënave, për të ndërtuar një mjedis më të sigurt dhe të besueshëm në epokën e lidhjes globale.

Fjalët kyçe: Internet of Things security, Machine learning, Deep learning, Data integrity