RIINVEST

Departamenti Shkenca e të dhënave dhe Analiza e Biznesit

PËRDORIMI I INTELIGJENCËS ARTIFICALE NË SIGURI KIBERNETIKE

Niveli Master

Engjëll Gashi

Shtator / 2023
Prishtinë

Departamenti Shkenca e të dhënave dhe Analiza e Biznesit

Punim Diplome

2022 - 2023

Engjëll Gashi

PËRDORIMI I INTELIGJENCËS ARTIFICALE NË SIGURI KIBERNETIKE

Dr. Fatbardh Veseli

Shtator, 2023

Ky punim është përpiluar dhe dorëzuar në përmbushjen e kërkesave të pjesshme për Shkallën Master

ABSTRAKT

Në vitet e fundit Inteligjenca Artificiale dhe Siguria Kibernetike kanë arritur që të përjetojnë zhvillime të mëdha. Pasi teknologjia ka shkuar gjithmonë duke përparuar, atëherë edhe këto dy degë të ndryshme të teknologjisë, kanë filluar të ndërthuren shumë afër me njëra tjetrën duke krijuar një lloj "varshmërie" nga njëra tjetra. Teknologjitë e reja gjithmonë sfidohen me avancim të sigurisë kibernetike por pa humbur efikasitetin e tyre dhe gjithmonë duke automatizuar proceset the detyrat e ndryshme. Këto sfida mund të adresohen përmes inteligjences artificiale, ku shumë nga funksionet e saj përdoren në teknologjitë që ne përdorim përmes Të Nxënit të Makinës (ML). Por, çdo e mirë vjen me barrat e saj, në rastin tonë, nuk është vetëm siguria kibernetike ajo e cila gëzon të mirat e inteligjencës, pasi që edhe pse inteligjenca artificiale në fushën e sigurisë kibernetike shpreh një thikë me dy tehe, ku në njërën anë ajo ndihmon sigurinë kibernetike që të ketë një efikasitet më të madh duke ndihmuar në mbrojtjen aktive në kohë reale ndaj sulmeve kibernetike dhe menaxhimin e mbrojtjes, njëkohësisht ndihmon edhe akterët kërcënues që të automatizojnë dhe zhvillojnë sulmet e tyre kibernetike.. Inteligjenca Artificiale mund të duket si një mjet i mjaftueshëm për ndalimin e sulmuesve por duhet të mirret në konsideratë se akterët kërcënues gjithmonë arrijnë që të bëhen më kreativë me metodat e tyre të sulmeve duke depërtuar përtej masave të mbrojtjes të inteligjencës artificiale. Në konkluzion, ky hulumtim ka për qëllim që të gjejë mundësitë e përdorimit të inteligjencës artificiale në siguri kibernetike dhe cilat janë disa nga praktikat më të mira. Inteligjenca Artificiale vjen me dobitë poashtu dhe me rreziqet e saj. Nëse duam që të kemi një mbrojtje efektive ndaj sulmeve dhe kërcënimeve kibernetike në një kohë ku teknologjia po zhvillohet në mënyrë të shpejtë, është kritike të kuptohet se cili është potenciali dhe poashtu cilat janë limitimet dhe sfidat e inteligjencës artificiale.

DEKLARATË E ORIGJINALITETIT

Unë, Engjëll Gashi deklaroj se: (1) Ky punim masteri përfaqëson punën time origjinale, përveç rasteve të citimeve dhe referencave dhe (2) Ky punim nuk është përdorur më parë si punim apo projekt në këtë kolegj apo në universitete/kolegje/institucione të tjera.

FALËNDERIME

Gjithmonë falënderues ndaj njerëzve të cilëve u takojnë meritat më të mëdha që unë sot përfundoj me sukses këtë kapitull. Falënderimi më i veçantë shkon për familjen time, të cilët më kanë dhënë përkrahjen më të madhe qe nga fillimi i rrugëtimit tim profesional duke më shtyrë që gjithmonë të arrija edhe ato qëllime që shumë herë mendova që do ishin te paarritshme me këshillat dhe afërsinë e tyre. Po ashtu një falënderim tjetër i veçantë shkon për mentorin Prof.Fatbardh Veseli, ku përkrahja dhe përkushtimi i tij ka qenë një ndihmë shumë e madhe për mua. Gjithashtu, falënderoj shoqërinë dhe kolegët e mi të cilët e përcjellën rrugëtimin tim!

PËRMBAJTJA

LISTA E TABELAVE

LISTA E FIGURAVE

1. HYRJE

Siguria kibernetike dhe inteligjenca artificiale janë dy ndër temat më të përfolura kohës së fundit. Të dyja kanë pësuar një evolucion të madh pasi me avancimin e teknologjisë dhe krijimin e sistemeve të reja teknologjike, këto dyja kanë qenë të ndërvarura me teknologjinë. Çdo sistem i ri është ballafaquar me sfidën bazë të rritjes së sigurisë kibernetike dhe mbrojtjen e të dhënave, por, duke pasur çdo herë e më shumë anëtarë të rinj në komunitetin e teknologjisë, është shfaqur nevoja për automatizimim e proceseve. Në këtë të fundit hyn dhe inteligjenca artificiale, ku përmes saj dhe të nxënit të makinës janë arritur që funksione të ndryshme të inteligjencës artificiale në teknologji të ndryshme që ne përdorim sot.

Potenciali i të dy degëve ende nuk ka arritur maksimumin por avancimi i të dyjave ka arritur të ndodhë në një kohë shumë të shpejtë. Krahas avancimit të sigurisë kibernetike, është rritur edhe numri i sulmuesve dhe metodave që ata përdorin për të arritur qëllimet e tyre keqdashëse. Siguria kibernetike filloi që të përballej me sfida të papërballueshme dhe ishte e paevitueshme që të mos ndërlidhej me inteligjencën artificiale. Inteligjenca artificiale ka ndihmuar shumë sigurinë kibernetike që të automatizojë procese të ndryshme vitale të sigurisë kibernetike duke e bërë atë më efikase duke ndihmuar në arritjen e menaxhimit dhe izolimit të sulmeve që ndodhin në kohë reale duke përdorur algoritmet e të nxënit të makinës ku këto modele duke u trajnuar me të dhëna paraprake mund të arrijnë të parashikojnë, detektojnë dhe si rezultat të parandalojnë një sulm potencial i cili mund të ndodhë në të ardhmen. Kjo është një lloj thike me dy tehe, pasi në të njëjtën mënyrë që inteligjenca artificiale përdoret për rritjen e sigurisë kibernetike, inteligjenca artificiale mund të përdoret edhe për kryerjen e sulmeve kibernetike. Ndërkohë, shumë kompani kanë arritur të zhvillojnë programe të ndryshme të cilat detektojnë dhe parandalojnë në kohë reale sulmet që vijne, por numri i akterëve keqdashës po rritet gjithnjë e më shumë dhe nevoja për inxhinierë të sigurisë kibernetike po bëhet më e madhe.

Në shikim të parë, mund të thuhet se zhvillimet në fushën e shkencës kompjuterike me softuerë mbrojtës (Tenable, Splunk, IBMQRadar etj.), kanë ulur vendet e punës për inxhinierët e sigurisë, por përkundrazi, nevoja për ta vazhdon e rritet çdo ditë e më shumë (Ballard, 2020). Inteligjenca Artificiale mund të parandalojë sulme të ndryshme, por, duke pasur parasysh që akterët kërcënues trajtë bazë e kanë mendimin jashtë kutisë ne asnjëherë nuk mund të themi se një sistem është

njëqind për qind i sigurt. Ndër problemet më të mëdha që egzistojnë sot në këtë sferë janë vetëdijësimi i organizatave dhe kompanive dhe kuptimi i rrezikut që mund t'i ballafaqojë në të ardhmen. Ka shumë mënyra të ndryshme që secili entitet, varësisht nga madhësia mund t'i implementojë në vete duke ulur dukshëm rrezikun e një sulmi të suksesshëm kibernetik.

1.1. Organizimi i punimit

Ky dokument është i organizuar si vijon: Kapitulli 1 ofron një hyrje për temën ku flitet për inteligjencën artificiale dhe sigurinë kibernetike. Në kapitullin 2 do shtjellojmë Sigurinë Kibernetike, llojet e ndryshme të Sulmeve Kibernetike dhe evolucionin e Sigurisë Kibernetike. Poashtu do shtjellojmë Inteligjencën Artificiale, aplikimet e saj dhe dallimet mes Machine Learning dhe AI. Në pjesën e fundit të kapitullit do shtjellojmë të nxënit e makinës, si përdoren ato në sigurinë kibernetike, algoritmet e të nxënit me dhe pa mbikëqyrje në siguri kibernetike. Në kapitullin 3 do shtjellojmë se si përdoret AI në siguri kibernetike ku do përmendim sistemet e zbulimit dhe reagimit të ndërhyrjeve, ndikimin e AI në sulmet kibernetike dhe se cilat janë disa nga softuerët e sigurisë kibernetike që përdorin AI. Në kapitullin 4 do shohim se si përdoret AI për sulmet kibernetike. Në kapitullin 5 do shikojmë kufizimet e AI në siguri kibernetike. Në kapitullin e 6 do shtjellojmë të ardhmen e AI në sigurinë kibernetike. Në kapitullin e 7 do e përmbyllim punimin me një konkluzion.

2. SHQYRTIMI I LITERATURËS

Në këtë kapitull do shtjellojmë disa nga elementet esenciale për Sigurinë Kibernetike, Inteligjencën Artificiale dhe Të nxënit e makinës.

2.1. Siguria Kibernetike

Ndër trendet më të përmendura gjatë viteve të fundit, siguria kibernetike ka arritur të bëhet pika kyqe e qdo entiteti qe ka bazë teknologjinë e informacionit, qoftë ajo biznes, organizate, korporate apo edhe organ qeveritar. Nëse duam ta definojmë, mund të themi se siguria kibernetike është aktiviteti ku pjesa harduerike, softuerike e një entiteti mbrohet nga kërcënimet kibernetike. Pasi që të dhënat e një entiteti dhe privatësia janë gjithmonë të ndjeshme, atëherë kanë filluar që të parashihen forma të ndryshme të parandalimit dhe mbrojtjes ndaj sulmeve të ndryshme kibernetike. Rritja e vetëdijësimit dhe forcimi i mbrojtjes së infrastrukturës automatikisht ka ndikuar qe siguria kibernetike të fillojë të lulëzojë. Më poshtë do shohim se cilat janë disa nga llojet e sulmeve të sigurisë kibernetike dhe evolucionin e sigurisë kibernetike.

2.1.2. Llojet e sulmeve të sigurisë kibernetike

Sulmet kibernetike janë të shumta në numër dhe po rriten qdo ditë e më shumë. Nëse mundohemi ta definojmë se çfarë është një sulm kibernetik, mund të themi se një sulm kibernetik është një tentativë e paautorizuar dhe ilegale nga një akter kërcënues apo disa akterë kërcënues që të marrë qasje të paautorizuar, të vjedhë, fshijë apo edhe të ndryshojë të dhëna (A. IBM, n.d.). Nëse i shikojmë në mënyrë të detajuara sulmet kibernetike, atëherë do mbetemi me një shumëllojshmëri të sulmeve, por, do të përmendim vetëm sulmet më të zakonshme kibernetike sipas CrowdStrike, një kompani globale lidere në tregun e sigurisë kibernetike (Baker, 2023). Sipas CrowdStrike, këto janë dhjetë sulmet më të shpeshta kibernetike:

1.**Malware** (Përndryshe softuerët me qëllim të keq, janë programe apo pjesë kodi të cilat e kanë një qëllim të caktuar që të dëmtojnë apo marrin qasje te paautorizuar në një sistem kompjuterik,

qoftë ai një pajisje kompjuterike apo edhe një rrjet i tërë. Ky term përmendet më së shumti tek pjesa e viruseve kompjuterike, pasi ky term enkapsulon sulme të ndryshme si ransomware, virusët worm, trojanët, spyware, virusët e thjeshtë etj.)

2.**DOS Sulmet** (Ky sulm është ndër sulmet më të rrezikshme "komerciale" pasi qëllimi i këtij sulmi është të ndërprejë qasshmërinë e shënjestrës së tij. Vetë fjala DOS (Denial Of Service) do të thotë mohim i shërbimit duke na bërë të nënkuptojmë se përmes këtij sulmi arrihet që të ndalohen proceset vitale digjitale të ndonjë kompanie pasi që sulmuesi arrin që ta mbushë të tërë rrjetin me kërkesa falco duke ndërprerë të gjitha proceset e punes (A. Cloudflare). Shpesh termin DOS mund ta shohim se shoqërohet edhe me termin tjeter DDOS. Dallimi mes këtyre dy të fundit është pika fillestare e sulmit. Përderisa në një sulm DOS, burimi i sulmit është vetëm një pajisje, atëherë ne DDOS (Mohim i Shërbimit i shpërndarë), lansohen një numër i madh i sulmeve DOS nga pajisje të ndryshme me shënjestrën e njëjtë.)

3. **Inxhinieria Sociale** – Një metode sulmi ku sulmuesit kryesisht shfrytëzojnë dhe manipulojnë faktorin human duke e mashtruar që të ndërmarrë aksione që sulmuesi të marrë qasje të paautorizuar (A. Enisa, n.d.). Disa nga llojet e sulmit të Inxhinierisë Sociale janë:

a) **Phishing i thjesht**ë - Është një metodë sulmi ku sulmuesi dërgon një mesazh, sms apo përdor teknika të ndryshme të inxhinierisë shoqërore, në mënyrë që ta bindë viktimën të ofrojë kredencialet dhe të dhënat e ndjeshme ose të instalojë një program me qëllim të keq në mënyrë që të marrë qasje të paautorizuar tek viktima.

b) **Spear Phishing** – Një sulm phishing i cili është i kostumizuar për një person të caktuar dhe ka një qellim ekzakt.

c) **Whaling** – Një lloj tjeter i phishing ku shënjestër kryesore janë punëtorët e kompanive me pozita të larta dhe me privilegje më të larta, në mënyrë që sulmuesi të zgjerojë hapësirën e qasjeve të tij.

d) **SMiShing** – një sulm tejet efektiv i phishing ku sulmuesi dërgon SMS ose edhe tekst mesazhe duke u maskuar si një entitet legjitim në mënyrë që të marrë të dhëna të ndjeshme dhe konfidenciale të shënjestrës së tij.

e) **Vishing** – Është ndër format e phishing ku sulmuesi bën kontakt direkt me shënjestrën duke e thirrur direct në telefon apo duke dërguar mesazhe me zë që të tingëllojë më i besueshëm dhe të arrijë të bindë viktimën që të ofrojë të dhënat e tij/saj konfidenciale.

Pra, mund të kuptojmë se edhe pse në konceptin e procesit dhe punës llojet e phishing mund të duken ndryshe, në thelb qëllimi i qdo lloj sulmi phishing është i njëjtë.

4.**Spoofing -** Një teknikë në të cilën akterët kërcënues arrijnë që të fshehin veten dhe të imitojnë një burim të besueshëm për viktimën. Në këtë mënyrë, sulmuesi arrin të marrë qasje në sistemet kompjuterike të viktimës. Ka poashtu disa lloje të spoofing si psh:

a) **Domain Spoofing** – Ku sulmuesi ekzekuton sulmin phishing më një domain falso që është i përafërt me domain-in e vërtetë duke bërë viktimën të mendojë se ka vizituar uebfaqen e vërtetë.

b) **Email Spoofing** – Ku sulmuesi bën të njëjtin hap por kësaj here me një email ku në email i kërkon viktimës të ofrojë të dhëna konfidenciale apo të shkarkojë një program të caktuar.

c) **ARP Spoofing** – Përndryshe quhet ARP Helmim dhe kjo është një lloj spoofing sulm ku sulmuesi mashtron një pajisje dhe bën atë të dërgojë të dhëna tek ai në vend se të dhënat të shkojnë tek shënjestra iniciale. Me ARP Spoofing, sulmuesit arrijnë që të marrin të dhëna të ndjeshme në mënyrë të paautorizuar.

Pra, edhe spoofing është njëra ndër teknikat më efektive të sulmit kibernetik pasi ajo mashtron viktimën duke u maskuar si një burim i besueshëm.

5.**Sulmet e bazuara në identitet** – Janë sulmet në të cilat sulmuesi vetëm se ka marrë qasje në të dhënat e viktimës dhe arrin që të bëjë dëme të mëtutjeshme duke u sillur si viktima. Disa nga sulmes e bazuara në identitet janë:

Kerberoasting, **Sulmi i biletës së argjendtë**, **Sulmi Kalo Hashin**, **MITM** (Njeriu në Mes) **Sulmi**, **Brute Force Sulmet** etj.

6.**Sulmet me injektim të kodit -** Janë ndër sulmet më të rrezikshme pasi sulmuesit fusin kod me qëllim të keq në pajisjet kompjuterike që kanë ndonjë dobësi. Disa lloje të këtij sulmi janë: SQL Injection, XSS dhe Malvertising.

7.**Sulmet e zinxhirit të furnizimit** - Këto janë sulme kibernetike që kanë për cak sulmi parti të treta të besueshme që ofrojnë shërbime të caktuara softuerike që një kompani duhet ti posedojë. Si shembull i partive të treta mund të jetë kompania Adobe, programet e së cilës përdoren nga shumë kompani nëpër botë. Sulmet e zinxhirit të furnizimit shënjestrojnë këto kompani dhe injektojnë kod me qëllim të keq në softuerët e tyre dhe si pasojë, të gjitha pajisjet të cilat kanë këtë lloj kodi do afektohen nga ky sulm.

8.**Sulmet e brendshme** - Janë sulme të cilat në shumicën e rasteve ekzekutohen nga ish-punëtorë apo edhe punëtorë aktual të kompanisë pasi që ata kanë shumë informacion për procedura të brendshme të kompanisë dhe mund të kenë edhe qasjë direkte në pajisjet e ndryshme brenda rrjetit të kompanisë. Ka raste kur kërcënimet e brendshme nuk lidhen fare me qëllimet e akterëve brenda kompanisë, por një akter mund të llogaritet kërcënim nëse ai/ajo është neglizhent në punë apo nuk ka dijeni të mjaftueshme për punën dhe pjesën e rrjetit dhe si pasojë një sulm mund të rezultojë i suksesshëm shkaku i neglizhencës së punëtorit.

9. **DNS Tunneling** - Një sulm poashtu i rrezikshëm ku përdoren pyetje dhe përgjigjje (response and queries) në mënyrë që të transmetohet kod dhe të dhëna në rrjet me qëllim që të infektohet rrjeti dhe që akteri kërcënues të arrijë të realizojë qëllimet e tij në rrjet.

10.**Sulmet e bazuara n**ë **IoT** - Këto sulme si shënjestër kanë pajisjet e ndryshme IoT pasi që nëse sulmuesi merr qasje në mjaftueshëm pajisje, atëherë ai arrin që të ekzekutojë sulme më të mëdha DOS apo DDOS me një fushëveprim masiv. Pajisjet IoT janë të gjitha pajisjet që arrijnë të transmetojnë të dhëna në rrjet (Baker, 2023).

2.1.3. Evolucioni i Sigurisë Kibernetike

Siguria kibernetike është një temë shumë e ndjeshme e cila kaplon të gjitha sferat e botës së tashme digjitale. Në fillet e teknologjisë kompjuterike, fjala apo edhe koncepti siguri kibernetike nuk ka ekzistuar pasi që kompjuterët e parë kanë qenë kompjuterë me madhësi gjigande dhe e vetmja mënyrë që një sulm kibernetik të ndodhte do ishte nëse sulmuesi do merrte qasje fizike, e cila në atë kohë ka hyrë tek koncepti i sigurisë fizike. Më vonë, kur teknologjia filloi të lulëzonte, filluan të krijohen mundësi të ndryshme për të pasur qasje në pajisjet kompjuterike. Kjo ishte një

dukuri të cilën hakerët filluan ta shfrytëzonin që të merrnin informacione në mënyrë të paautorizuar. Për të kuptuar se si Siguria Kibernetike ka evoluar kemi marrë një hulumtim nga Furstenau, Sott, Homrich & Kipper ku sipas një hulumtimi që ata kishin bërë, kuptohet se gjatë viteve 1999-2011 (Figure 1), ka ekzistuar një numër shumë i vogël i publikimeve sa i përket sigurisë kibernetike, kurse nga viti 2011 ka pasur një rritje shumë më të madhe, ku viti 2018 shënon 630 publikime dhe viti 2019 shënon 617 publikime. Kjo tregon një trend në rritje dhe do të thotë se tema "Siguria Kibernetike" ka filluar të jetë njëra ndër temat më të rëndësishme në sferën e teknologjisë pasi është një ndër pilaret e revolucionit të katërt industrial (Kagermann, Wahlster, & Helbif, 2013) (Furstenau, Sott, Homrich, & Kipper, 2020).

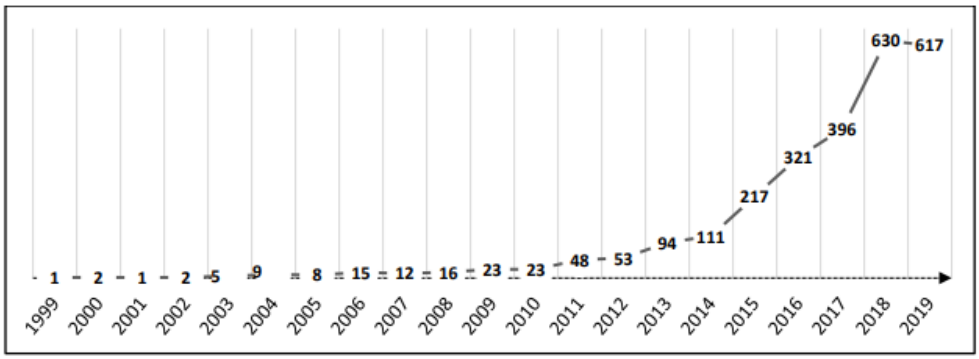

Figura 1.Numri i publikimeve shkencore ne lidhje me "Cyber Security" pergjate viteve 1999-2019, (Furstenau, Sott, Homrich, & Kipper, 2020)

Kjo na bën të kuptojmë se sulmet kibernetike kanë pasur një rritje dhe mund të themi që nevoja për inxhinierë të sigurisë gjithmonë ka shkuar duke u rritur. Një raport nga Lightcast tregon se gjatë vitit 2021 deri ne Prill të vitit 2022 ka pasur rreth 714,458 pozita të lira pune në Shtetet e Bashkuara Te Amerikës. (Tim Hatton, 2022) Ky trend na tregon se nevoja për inxhinierë të duhur të sigurisë kibernetike nuk po arrin të përmbushet dhe se kërkesa për ta është gjithmonë në rritje.

Pra, po kuptojmë se siguria kibernetike ka qenë një term i cili pothuajse nuk ka ekzistuar në vitet e 90-ta kurse gjatë 4 viteve të fundit, është ende një temë për të cilën interesimi shkon e rritet.

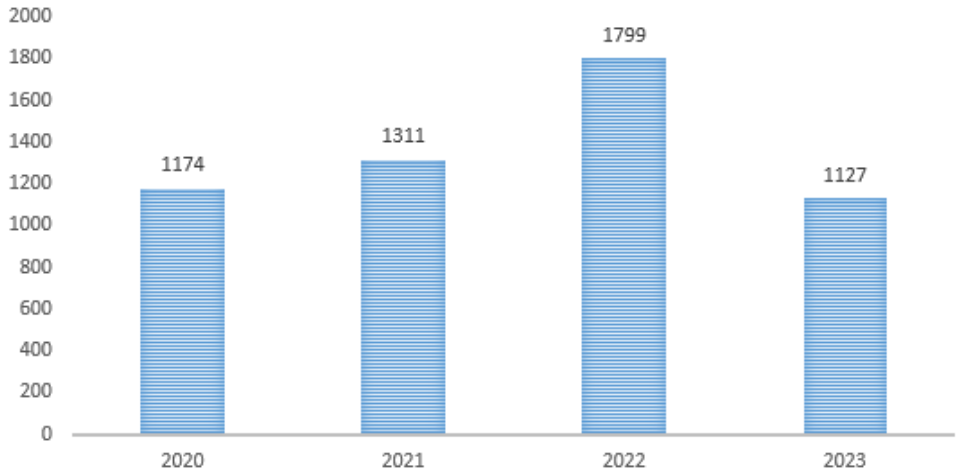

Figura 2. Numri i publikimeve në fushën e "Cyber Security" gjatë viteve 2020-2023 në Platformën IEEE Xplore, diagram vetanak

Duke ndjekur hapat e hulumtuesve të mëparshëm, kemi hulumtuar në burimin e njëjtë për të shikuar se a është rritur numri i hulumtimeve të cilat janë të ndërlidhura më sigurinë kibernetike nga viti 2019. Në vitin 2020, shohim se ka një kërcim të madh nga viti paraprak pasi si shkak mund ta lëmë pandeminë që ndodhi në atë vit dhe të arsyetojmë se sulmet kibernetike janë rritur më shumë pasi që njerëzit kanë filluar të shpenzojnë më shumë kohë në internet duke rezultuar në interesim më të madh në siguri kibernetike. Por, përsëri shohim se interesimi për siguri kibernetike nuk ka ndaluar dhe në vitin 2022 ka pasur një rritje të madhe të publikimeve duke arritur 1799 publikime vetëm në atë vit. Ne momentalisht nuk kemi përfunduar as gjysmën e vitit dhe shohim se numri i publikimeve për këtë vit ka tejkaluar 1000 publikime, dhe nëse kjo dukuri vazhdon, numri i publikimeve deri në fund të vitit mund të shkojë deri në 2000, një nivel më i madh i interesimit të sigurisë kibernetike.

2.2. Inteligjenca Artificiale (AI)

Inteligjenca Artificiale i referohet sistemeve të cilat shfaqin sjellje inteligjente duke analizuar një mjedis të caktuar dhe duke kryer detyra dhe duke arritur një shkallë të caktuar autonomie. (Boucher, 2020)

Që nga zhvillimet e hershme të kompjuterëve, është demonstruar se kompjuterët mund të arrijnë të përfundojnë detyra inteligjente me aftësi të lartë. Mund edhe të themi se qëllimi i AI është që ta mësojë një kompjuter se si të operojë në mënyrë vetanake që të kryeje detyra gjithnjë e më komplekse dhe të arrijë të vendosë në mënyrë të saktë, trajtë kjo e cila ngjason me inteligjencën e qenieve njerëzore.

AI kryesisht përbëhet nga disa komponente kryesore (adservio, 2022):

1. Të nxënit – Ku qëllimi i të nxënit është që sistemi të mësojë nga të dhënat të cilat i ofrohen dhe të arrijë që të dale në konkluzione në mënyrë vetanake apo edhe që të parashikojë përfundime të ndryshme.
2. Arsyetimi – Ku sistemi me AI arrin që të ofrojë një informacion nga informacioni i dhënë duke përdorur rregulla apo logjikë ekzistuese. Qëllimi i kësaj pjese është që sistemi të arrijë që të ofrojë një arsyetim të ngjashëm me arsyetimet njerëzore.
3. Zgjidhja e problemeve – Ku ai tenton që të zgjidhë probleme të ndryshme në mënyrën që zgjidhin njerëzit, ku mund të marrim si shembull parashikimet në blerjet online ku AI arrin që ti prezantojë vizitorit vetëm produktet të cilat i nevojiten atij/asaj.
4. Perceptimi – Ku mund të marrim shembullin e makinave autonome. Sistemi AI përmes senzorëve të ndryshëm dhe perceptimeve që merr nga ambienti i jashtëm, duke marrë informacion për mjedisin, dritat e trafikut, vijat në rruge apo të dhëna të tjera.
5. Procesimi i gjuhës – Kjo pjesë e AI ndihmon duke mundësuar skanimin e teksteve të mëdha, kuptimin e tyre dhe arrin që të gjejë gabime drejtshkrimore apo gjuhësore.

Të gjitha këto komponente krijojnë një sistem të AI por nuk janë domosdosmërisht të ndërlidhura me njëra tjetrën. Mund të themi se AI mund të cilësohen sistemet që kanë trajtat e përmendura më lartë.

AI ka filluar të transformojë botën në mënyrë të shpejtë. Rasti më i fundit ku AI ka bërë një revolucion ka qenë me shfaqjen e AI gjeneruese ku e gjithë bota morri qasje në një sistem të AI e cila arrinte të ofronte përgjigjje shumë të sakta për shumicën e kërkesave të rëndomta por arrinte të gjente zgjidhje edhe për kërkesat më komplekse, e veqanërisht kërkesat për pjesën e zhvillimit të softuerit pasi që modeli i ChatGPT ishte një model i trajnuar për shumë vite me rradhë (Carpentier, 2023). Por kjo nuk është i vetmi vend ku AI gjen aplikim. AI poashtu kontribon edhe në fushën e mjekësisë ku po zhvillohet një dorë robotike e cila mund të kontrollohet me tru dhe mund ta bëjë një person të paralizuar të arrijë të ndjejë dorën përsëri (NIST, N/A). Më poshtë do shohim se cilat janë aplikimet e AI dhe dallimet mes Machine Learning dhe AI.

2.2.1. Aplikimet e AI

AI arrin të gjejë aplikim poashtu tek robotët që merren me shërbimin e konsumatorit në mënyrë që të kthejnë përgijgjje më të sakta dhe të ndihmojnë me eksperiencën e konsumatorit përmes automatizimeve të ndryshme, në sektorin e financave ku bëhen tregtitë e valutave përmes AI, në siguri kibernetike, në industrinë e makinave autonome dhe poashtu në industritë komerciale si në industrinë e filmave ku mund të marrim një kompani gjigante si Netflix në të cilën AI rekomandon filmat apo serialet e përshtatshme për klientin e poashtu në industrinë e videolojërave ku AI implementohet në videolojëra në mënyrë që eksperienca e lojtarëve të ngjasojë me jetën reale.

Shumë herë ngritet tema se si AI do krijojë robotë shumë të mençur dhe se ata do e marrin botën në dorë, por ky nuk është qëllimi i AI, përkundrazi, AI ka për qëllim që të ndihmojë dhe zhvillojë kualitetin e jetës së racës humane (Kumar, Priya, & Kumari, 2019).

Në mënyrë që këto kërcënime potenciale të mënjanohen në të ardhmen, atëherë duhet të krijohen rregullore dhe standarde se si AI mund të përdoret dhe ku mund të aplikohet. Në vitin 2021 është hartuar një plan për rregullimin e AI nga Lucilla Sioli (SIOLI, 2021) ku klasifikohen katër nivele rreziku ku niveli kritik është i ndaluar dhe nëse sistemet që kanë AI kanë rrezik të lartë atëherë duhet të përshtaten me rregullat që vendosen paraprakisht. Sistemet me rrezik minimal apo pa rrezik nuk do ketë kërkesa të obliguara por sistemet të cilat potencialisht prezantojnë rrezik të vogël janë të obliguar që të njoftojnë përdoruesit që AI është në përdorim, duke rritur transparencën dhe besimin në AI (SIOLI, 2021).

AI ka zhvilluar cilësinë e jetesës duke arritur që të automatizojë procese të ndryshme, disa nga to që përmendëm më herët si krijimi i makinave që vozisin veten, asistentët virtualë, kuptimin e gjuhëve të ndryshme, ndihmesën në orarizimin e tasqeve, parashikimin e rezultateve në mjekësi, shkencë të të dhënave etj. Të gjitha këto janë pjesë të shoqërisë të cilat shohin përfitim të madh tani dhe do shohin edhe më shumë në të ardhmen kur AI do arrijë në nivele më të larta të mësimit dhe avancimit.

2.2.2. Ndikimi i AI në sulmet kibernetike

Deri në këtë pikë, diskutimi është përqëndruar tek AI dhe si ajo përdoret. Tani do dalim tek pjesa se si AI ndihmon që sulmet kibernetike të jenë shumë më efektive sesa sulmet tradicionale duke krijuar telashe të shumta për inxhinierët e sigurisë kibernetike. Nëse sistemet e avancuara të AI bien në duart e gabuara, atëherë sulmuesit mund të rrisin madhësinë e sulmeve të tyre, zgjerojnë fushëveprimin e tyre dhe poashtu automatizimin dhe rritjen e shpejtësisë të sulmeve.

Sipas një studimi të vitit 2022, teknikat tradicionale të sigurisë kibernetike nuk mund të detektojnë dhe ndalojnë sulmet kibernetike të fuqizuara nga AI pasi që nuk mund të jenë të reagojnë shpejt aq sa duhet dhe se këto lloje sulmesh kanë sjellje të shumëfishta dhe një logjikë komplekse të vendimeve. (Blessing Guembe, 2022) Në mënyrë që inxhinierët e sigurisë të arrijnë në një hap me sulmet e fuqizuara nga AI, duhet që të krijohen sisteme shumë më të sofistikuara të mbrojtjes sesa ato që janë tani dhe të ketë shumëllojshmëri datasetesh të avancuara.

2.2.3. Machine Learning vs. AI

Ndodh shumë herë që këto dy koncepte shoqërohen me njëra tjetrën pasi duken të njëjta në thelb. Duhet të kuptohet që në thelb këto dyja kanë një dallim të cekur me njëra tjetrën. Në mënyrë më të shkurtër, mund të themi se AI është vetë dukuria dhe procesi ku një sistem kompjuterik mundohet që të imitojë sjelljen humane të njeriut. Në anën tjetër, të nxënit e makinës është pjesë e AI e cila përdor metoda metoda statistikore dhe algoritme të ndryshme në mënyrë që të krijohet një model dhe të trajnohet sa më shumë duke shkuar e duke u bërë më i "mençur" (A. K21Academy

, 2022). Ky lloj i procesit arrin që ta krijojë një model mësues që ka trajtat e inteligjencës së njeriut. Si rezultat kësaj, mund të themi se kemi arritur që ta rrisim inteligjencën artificiale të një sistemi.

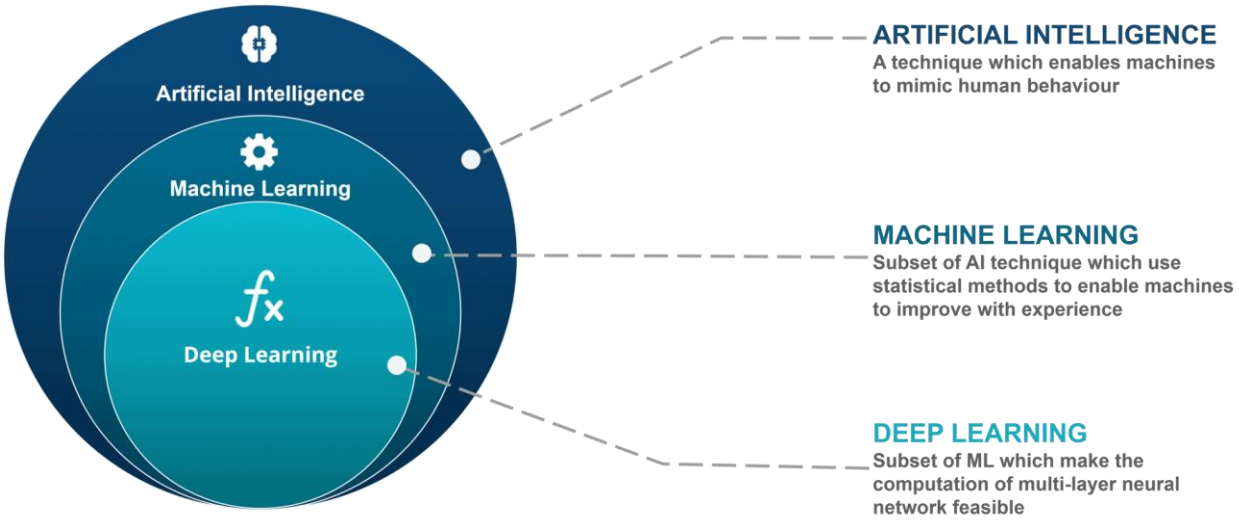

Figura 3. Struktura e AI dhe nëndegët e saj, (A. K21Academy , 2022).

Pra, mund të kuptojmë se AI dhe ML janë shumë të afërta me njëra tjetrën por nuk janë të njëjta. ML është një metodë për trajnimin e kompjuterit për të mësuar nga inputet e tij por pa programim eksplicit për secilin rast, pra, ML ndihmon kompjuterin që të arrijë AI (B.J.Copeland, artificial intelligence, n.d.).

Që të arrijmë në një përfundim më të saktë se cili është dallimi kryesor mes të dyjave, mund të themi se ML arrin që të zhvillojë algoritme dhe modele të cilat kryesisht mësojnë nga të dhënat paraprake dhe arrijnë të mësojnë dhe të marrin vendime vetanake duke u bazuar nga të nxënit e kaluar. Kurse, në anën tjetër, AI përfshin një spektër më të gjerë të teknikave dhe sistemeve me qëllimin e krijimit të sistemeve inteligjente të cilat përvec se marrin vendime, arrijnë edhe të përfundojnë detyra me inteligjencë „më humane“.

2.3. Të nxënit e makinës (ML)

Të nxënit e makinës është një nëndegë e AI dhe është aftësia e sistemeve që të mësojnë nga të dhënat e trajnimit në mënyrë që të krijojnë një model që të zgjedhin detyra të caktuara (A. IBM, 2023). ML përdor algoritme dhe të dhëna që të imitojë mënyrën se si humanët mësojnë, gjithmonë duke përparuar dhe duke rritur saktësinë (A. IBM, 2023). Gjatë dekadave të fundit, kemi pasur disa produkte shumë innovative të bazuara në ML siç është motori i rekomandimit i Netflix, makinat që vozisin veten, prodhimi i mençur, parashikimi i trafikut, administrimi i përmbajtjes së rrjeteve sociale etj. Nga kjo mund të shohim se aplikimet e ML luajnë një rol shumë të madh në jetën e përditshme pasi që ne përdorim shumë nga ato aplikime çdo ditë pa ditur se po përdorim ML. Më poshtë do shtjellojmë se qka janë Algoritmet e të nxënit të makinës në sigurinë kibernetike dhe do shikojmë se cilat janë algoritmet e të nxënit me dhe pa mbikëqyrje në sigurinë kibernetike.

2.3.1. Algoritmet e të nxënit të makinës në sigurinë kibernetike

Më lartë përmendëm se ML është një nëndegë e AI e cila gjithmonë shkon duke u avancuar sado detyra të reja që trajton. Rrjedhimisht ne mund të kuptojmë se ML ka një aplikim shumë të nevojshëm në siguri kibernetike ku mund të përdoret për parashikimin e kërcënimeve kibernetike dhe poashtu parandalimin e tyre nëse modeli trajnohet mire. ML poashtu mund të automatizojë detyrat manuale dhe të sintetizojë të dhëna të mëdha në mënyrë të shpejtë dhe të saktë. Kemi dy lloje të algoritmeve të të nxënit të makinës në sigurinë kibernetike, algoritmet e të nxënit me mbikëqyrje dhe pa mbikëqyrje dhe të dy llojet arrijnë që të kenë rolin e tyre në ndikimin pozitiv në siguri kibernetike.

2.3.2. Algoritmet e të nxënit me mbikëqyrje në sigurinë kibernetike

Që të kuptojmë se si Algoritmet e të nxënit me mbikëqyrje ndikojnë në siguri kibernetike së pari duhet të kuptojmë se si ato funksionojnë. Të nxënit me mbikëqyrje ndodh kur një model trajnohet në inputet e etiketuara dhe kemi një rezultat të cilin duam ta arrijmë. Atëherë modeli trajnohet dhe

arrin që të përfundojë tasqët kur merr të dhëna të reja duke bërë parashikimin e mësuar përmes fazës së trajnimit (A. CROWDSTRIKE, 2022). Pra, një ndër aplikimet e këtyre algoritmeve do ishte për të parashikuar një kërcënim të caktuar apo edhe rreziqe të ndryshme si skanimet në rrjetë. Disa nga algoritmet e të nxënit me mbikëqyrje janë Naïve Bayes, SVM, Pema e vendimmarrjes, Regresioni logjistik etj.

Disa hulumtues (Panda & Patra, 2007) kanë përdorur Naïve Bayes për parashikim të sulmeve duke mbledhur të dhëna nga katër lloje sulmi. Përmes këtij algoritmi klasifikues, ata arritën në një saktësi testuese prej 96%, 99%, 90% dhe 90%. Kjo na bën të kuptojmë se parashikimet me algoritmet me mbikëqyrje gjejnë vend aplikimi tek pjesa e sigurisë kibernetike duke pasur sukses në detektimin dhe parandalimin e sulmeve kibernetike përmes AI.

2.3.3. Algoritmet e të nxënit pa mbikëqyrje në sigurinë kibernetike

Algoritmet e të nxënit pa mbikëqyrje funksionojnë në një mënyrë krejtësisht tjetër, pasi ato funksionojnë duke marrë të dhëna të cilat nuk kanë etiketim dhe ideja e algoritmeve pa mbikëqyrje është që të arrijnë të gjejnë mostra dhe anomali të ndryshme që ndodhin në atë „set të të dhënave“ (Yagcioglu, 2020). Nëse përdorimin e tyre e shohim nga aspekti i sigurisë kibernetike, atëherë lehtësisht mund të kuptojmë aplikimin e tyre. Secili sulm kibernetik ka paternën e tij të caktuar dhe ka tregues apo indikatorë ku këto algoritme e caktojnë se a është sulm apo jo. Duke përdorur algoritmet e të nxënit pa mbikëqyrje, ne mund të arrijmë të zbulojmë anomalitë dhe shkeljet e ndryshme dhe poashtu të minimizojmë ndodhinë e lajmeve falso pozitive. Disa nga algoritmet pa mbikëqyrje që përdoren mund të jenë teknikat e grumbullimit (*clustering*) siq janë K-means (Kumar V.) apo K-medoids (Safwab, 2020).

Të dy këto algoritme bëjnë grumbullimin e të dhënave rreth një K-Grumbullimi ku në duhet të ofrojmë numrin e grumbullimeve që duam të analizojmë. Me anë të këtyre grumbullimeve ne mund të arrijmë të gjejmë mostrat apo anomalitë të cilat po i kërkojmë pasi që të dhënat vizualizohen në grupe të ndryshme.

3. DEFINIMI I PROBLEMIT

Siguria kibernetike dhe inteligjenca artificiale ndërlidhen në dy mënyra të cilat janë aq fitimprurëse për sigurinë kibernetike po aq të dëmshme për të. Në këtë punim do trajtojmë mënyra të ndryshme të përdorimit të inteligjencës artificiale për të kuptuar se si ajo rrit mbrojtjen dhe të gjejmë mënyrat më optimale për përdorimin e kësaj teknologjie që të kemi një mbrojtje sa më të sigurt. Ky punim do të arrijë t'i përgjigjet pyetjes së mëposhtme hulumtuese:

1. Si mund ta përdorim dhe implementojmë Inteligjencën Artificiale në Siguri Kibernetike?

4. METODOLOGJIA

Ne aspektin metodik, ky punim përdor analizën e literaturës dhe dy raste studimi. Analiza e literaturës përdor të dhëna nga raporte, artikuj shkencorë dhe hulumtime tjera qe janë relevante për temën të cilën po e trajtojmë. Në këtë punim përdoren të dhëna sekondare. Objektivi primar i punimit do jetë ti përgjigjjet pyetjes së hulumtimit të shtruar në pjesën 3.Pyetjet e Hulumtimit. Përtej objektivës primare, tema do mundohet që të shtjellojë se cilat janë disa nga softuerët që përdorin AI për të ngritur sigurinë kibernetike dhe se cila është e ardhmja e AI në fushën e sigurisë kibernetike. Për të nxjerrur informacionet e duhura kemi kërkuar katër (4) platforma kryesore të cilat na ndihmojnë të gjejmë literaturën që kërkojmë dhe i shfaqim tek Tabela 1. Burimet kanë qenë Google Scholar, Google Search, Research Gate dhe IEEE Xplore. Për të arritur në rezultate më korrekte, kemi përdorur disa fjalë kyçe si fjalë stringje të cilat i kemi përfshirë në queryt e kërkimit.

Tabela 1.Platformat dhe fjalët kyçe të përdorura në hulumtim.

Burimi	**Fjalët Kyçe**
Google Search Google Scholar Research Gate	(“Artificial Intelligence” AND “Cyber Security” OR “Artificial Intelligence” AND “Machine Learning” OR “Machine Learning” AND “Cyber Security” OR “Artificial Intelligence” OR “AI” OR “Machine Learning” OR “Cyber Attack” OR “Machine Learning Algorithms” AND “Cyber Security” OR “ML”)
IEEE Xplore	“Cyber Security”

Në total kemi arritur të nxjerrim rreth 200 artikuj ose hulumtime të ndryshme të cilat i kemi filtruar si më poshtë me kushtet e vendosura tek Tabela 2 dhe kemi vendosur kushte për përfshirje apo përjashtim.

Tabela 2. Kushtet e filtrimit të artikujve të gjetur.

Kushtet përfshirëse	**Kushtet përjashtuese**
Gjuha e punimeve të jetë anglisht	Nuk shkruhet në anglisht
Studimet duhet të lidhen direkt me kapitujt e temës	Studimet pa fokus në AI, Siguri Kibernetike ose ML
Studimet apo artikujt që kemi menduar se janë direkt relevante me temën.	Artikujt Duplikatë

Njëri ndër burimet e të dhënave që përmendëm është edhe platforma IEEE Xplore. Në këtë platformë kemi kërkuar për të gjitha publikimet që kanë të bëjnë me Siguri Kibernetike gjatë viteve 2020-2023. Fjala kyçe ka qenë „Cyber Security“ dhe kemi filtruar variablat („Journals“, „Books“, „Magazines“, „Early Access Articles“, „Standards“, „Courses“).

5.Rezultatet/Diskutimi Kritik

5.1. PËRDORIMI KONKRET I AI PËR SIGURINË KIBERNETIKE

AI arrin që në teknologjitë të cilat integrohet, të ndihmojë në rritjen e sigurisë kibernetike. Më poshtë do paraqesim disa nga mënyrat se si AI përdoret që të detektojë dhe reagojë ndaj ndërhyrjeve, si ndikon në mbrojtjen e sigurisë duke forcuar sulmet dhe poashtu se cilat janë disa nga softuerët të cilët përdorin AI për rritjen e sigurisë kibernetike.

5.1.1. Sistemi i zbulimit dhe reagimit të ndërhyrjeve

Inteligjenca Artificiale gjen një përdorim të madh në siguri kibernetike. Njëra ndër mënyrat e aplikimit të AI në siguri kibernetike është edhe sistemi i zbulimit të ndërhyrjeve. Me anë të AI dhe ML sistemi i cili përmban këto teknologji arrin që të detektojë dhe parandalojë një sulm potencial i cili i është drejtuar rrjetit tonë. Mënyrat e detektimit mund të jenë të ndryshme. Sistemi mund të detektojë kërcënimin duke kontrolluar për ndonjë sjellje të dyshimtë, nëse vjen nga një burim i panjohur dhe ka vetëm një numër të caktuar të lidhjeve që vijnë drejt nesh apo edhe mund të krahasojë "nënshkrimin" (signature) e softuerit duke e krahasuar atë me nënshkrimet tjera të cilat i ruan në databazën e kërcënimeve të njohura. Janë dy kategori kryesore për sistemet e zbulimit të ndërhyrjeve: Detektimi i Anomalive dhe Detektimi i Keqpërdorimit.

Detektimi i anomalive analizon të dhënat e marra dhe i krahason ato me të dhënat standarde që ajo ka sa i përket sjelljes normale në një sistem, dhe kështu mëson se si mund të detektojë sulmet të cilat nuk njihen kurse detektimi i keqpërdorimit bazohet në nënshkrimet e sulmeve që i njeh, pra, nuk mund të detektojë sulmet që nuk i njeh (Mrutyunjaya Panda, 2007). Por, duhet të ceket se nëse një model është i trajnuar dhe avancuar shumë mirë, atëherë modeli mund të arrijë të parashikojë dhe të ndalojë një sulm potencial edhe nëse sulmi është Sulmi Zero Ditë për të cilin nuk ka njohuri pasi që sulmet e këtilla mund të kenë një sjellje jo të njohur e cila potencialisht mund të cilësohet sikur anomali.

Ndër mënyrat se si AI mund të përdoret hulumtuesit Panda dhe Mrutyunjaya (Panda & Patra, 2007) arrijnë që të përdorin algoritmin Naïve Bayes që të demonstrojnë se si ky algoritëm mund të përdoret në sistemin e zbulimit të ndërhyrjeve.

Naïve Bayes është një algoritëm ML me mbikëqyrje i cili përdoret për tasqe të klasifikimit si klasifikimi i tekstit. Ndryshon nga klasifikuesit diskriminativë pasi që nuk mëson se cilat tipare janë më të rëndësishme të diferencohen mes klasave (A. IBM).

Ata propozojnë një model i cili do marrë trafik nga rrjeti, pastron të dhënat përmes para-procesimit dhe krijohet një dataset. Dataseti ishte nga DARPA i cili ishte dataseti me i pasur për atë kohë, pra gjatë vitit 2007. Kornizat e sistemit të ndërtuar do krijojnë mostra të shërbimeve të rrjetit përmes dataseteve të etiketuara nga shërbimet ku sistemi detekton sulmet duke përdorur algoritmin Naïve Bayes. Naïve Bayes arrin që të detektojë më shumë sulme se Rrjetet Neurale në këtë rast për një kohë më të shkurtër por arrin që poashtu të ketë më shumë falso pozitive. Në tabelën më poshtë shihen rezultatet e arritura janë detektim i sulmeve prej 95% të rasteve me një përqindje të gabimit prej 5%. Kjo u bë në krahasim me rezultatet e KDD, ky i fundit proces për identifikimin e shenjuesve validë në datasete të mëdha (Sharma, 2020).

Tabela 3.Rezultatet e përdorimit të Algoritmit Naive Bayes për zbulimin e ndërhyrjeve të paautorizuara (Panda & Patra, 2007)

Experiments	**Overall Error Rate**	**Kosto**	**Koha në sekonda**
Best KDD Result	7.29%	0.2331	Not Provided
Panda, Patra Res.	5.1%	0.16	1.89

Pra, pasi Naïve Bayes po ofron falso pozitive kuptojmë që një problem qëndron tek saktësia dhe tek vendimet e modelit por kjo mund të rregullohet nëse datasetet janë më të mbushura me të dhëna dhe modeli trajnohet siç duhet.

Kur sistemet e mbrojtjes kibernetike me AI arrijnë që të detektojnë një sulm në ardhje atëherë sulmi arrin që të ndalohet me sukses në kohë reale. Sulmi mund të neutralizohet duke u bllokuar automatikisht duke mos i dhënë hapësirë që të depërtojë. Poashtu burimi i sulmit mund të vendoset në lista të zeza në mënyrë që komunikimet me atë burim të mos lidhen asnjëherë në të ardhmen. Pra, mund të izolohet sistemi i prekur, të bllokohet trafiku me qëllim të keq, karantinimi i elementeve me qëllim të keq apo të startohet ndonjë procedurë tjetër e vënë në aksion nga inxhinierët e sigurisë.

Nga ajo kohë mund të themi se këto lloj sistemesh kanë përparuar shumë pasi që një studim i publikuar në vitin 2023 prezanton një sistem të ri për zbulimin e ndërhyrjeve dhe rritjen e sigurisë (S. Sivamohan, 2023). Sistemi përdor algoritme të avancuara, përkatësisht algoritmin e optimizimit të tufës krill (KHO - është një algoritëm i frymëzuar nga biologjia që përdor sjelljen e tufave krill për të gjetur zgjidhje optimale në një sërë fushash). (Amir Hossein Gandomi, 2012)) për zgjedhjen e veçorive përkatëse dhe kornizën BiLSTM-XAI, kjo kornizë e cila kombinon fuqinë e modeleve të kujtesës afatshkurtër dydrejtimshe (BiLSTM) me inteligjencën artificiale të spjegueshme (XAI) (S. Sivamohan, 2023). Ai mundëson klasifikim të saktë të bazuar në sekuencë duke ofruar shpjegime transparente dhe të interpretueshme për procesin e vendimmarrjes së modelit për klasifikim të saktë. Krahasuar me metodat ekzistuese, qasja e propozuar arrin saktësi më të lartë, me shkallë zbulimi prej 97.2% dhe 95.8% në datsetin Honeypot dhe datasetin NSL-KDD. Studimi gjithashtu sugjeron drejtime kërkimore të ardhshme për të identifikuar në mënyrë efektive sulmet e panjohura kundërshtare.

Si përmbledhje, sistemet e zbulimit dhe reagimit të ndërhyrjeve duhet të marrin të dhëna dhe t'i paraprocesojnë ato, të trajnojnë modelet me algoritme të caktuara të të nxënit të makinës, të nxjerrin tipare të veqanta dhe paterna të rasteve paraprake, të detektojnë kërcënimet në kohë reale, gjenerojnë njoftime dhe të marrin masa të automatizuara nga të nxënit e mëhershëm apo nga rregullat e vendosura nga krijuesi. E mira e këtyre sistemeve është që ato gjithmonë shkojnë duke përmirësuar shpejtësinë, saktësinë dhe efikasitetin e tyre sado më shumë që mësojnë.

5.1.2 Softuerët e sigurisë kibernetike që përdorin Inteligjencë Artificiale

Përveq automatizimit të proceseve apo ndihmës me menaxhim të detyrave, AI ka gjetur aplikimin edhe tek pjesa e sigurisë kibernetike në Cloud. Përmes integrimit në Cloud, nuk do ketë nevojë aq të madhe për intervenim human, të dhënat e mëdha mund të procesohet më lehtë, mund të parashikohen sulmet para se të ndodhin dhe mund që sistemet Cloud të testohen me siguri duke ofruar një kosto më të lirë (Brathwaite, 2022).

Më poshtë do shohim në një tabelë se cilat janë disa nga sistemet e detektimit dhe parandalimit me AI të cilat ofrojnë zgjidhje për siguri kibernetike në cloud dhe se cilat janë mundësitë e tyre. Kemi zgjedhur katër tipare për këto sisteme:

1. **Zbulimi në kohë reale** (kur kërcënimet detektohen në momentin e ekzekutimit)
2. **Zbulimi i kërcënimeve të avancuara** (kërcënimet që kanë metoda të shmangjes, ndërrojnë formë apo janë shumë të fshehta)
3. **Zbulimi i bazuar në mashtrim** (ku sistemi vendos kurthe të ndryshme për sulmuesit dhe detekton ato në momentin që sulmuesi afrohet)
4. **Kompatibiliteti në Cloud** (A janë këto programe të përshtatshme për mjedise në cloud)

Tabela 4.Sistemet IDPS që përdorin AI, Diagram Vetanak

Emri I softuerit	Zbulimi në kohë reale	Zbulimi i kërcënimeve të avancuara	Zbulimi i bazuar në mashtrim	Kompatibiliteti në Cloud
Darktrace	Po	Po	Jo	Po
Vectra AI	Jo	Po	Jo	Po
EDR/Cynet	Jo	Po	Jo	Po

Të gjitha këto sisteme janë sisteme të mbrojtjes kibernetike me AI dhe mund të integrohen edhe në Cloud. Ajo që mund të shohim është se për të arritur në një pikë ku AI do arrijë të zëvendësojë njeriun duhet të kalojmë një rrugë të gjatë të trajnimit të modeleve. Më poshtë do shohim se si këto programe funksionojnë dhe cilat janë teknikat që ato përdorin për të siguruar një sistem kompjuterik.

5.2.1. DarkTrace

DarkTrace është i bazuar në sistemin Bayesian i cili arrin që të integrojë indikatorë të dobët të sjelljes jo normale të një rrjeti në mënyrë që të ketë dijeni sipërfaqësore se sa ekziston mundësia që një sistem të kompromitohet (A. DarkTrace). Kjo qasje matematikore probabilistike është pike kyçe e DarkTrace pasi kjo mundëson që të kuptohet informacioni i rëndësishëm në një sistem edhe nëse softueri nuk e din se për çfarë po kërkon (A. DarkTrace). Tiparet e DarkTrace janë se përdorin algoritme ML pa mbikëqyrje duke arritur që modeli të mësojë në kohë reale pa dijeni paraprake të sulmeve të caktuara, mund të përshtatet me bizneset diverse modern dhe përditëson veten pa nevojë të inputit. Kjo teknologji arrin që të ndalojë sulmet e mëposhtme: Sulmet e brendshme në një rrjet, Sulmet Zero Ditë, Dobësitë Latente (dobësitë për të cilat ka kohë që dihet që ekzistojnë

dhe janë si pasojë e ripërdorimit të kodit me dobësi (Beng Heng Ng, 2010)) , sulmet e automatizuara dhe mutante, Sulmet në Cloud dhe SaaS, sulmet e fshehta dhe sulmet e avancuara Spear-Phishing (Author Darktrace). Metodat të cilat Darktrace i përdor janë metodat grupuese të të dhënave (clustering methods) në mënyrë që të identifikojë grupacionet të cilat nuk mund të zbulohen manualisht. Në implementimin e saj në rrjeta të një rrjeti lokal apo të gjerë, arrin që të monitorojë paketat në rrjet duke aplikuar teknikat L1-Rregullative (teknikë që ndihmon në përzgjedhjen e veçorive duke i shtyrë disa nga peshat e veçorive të bëhen saktësisht zero (Singh, 2023)). Në mënyrë që të gjitha këto aktivitete digjitale të kombinohen Darktrace e përdor fuqinë e vlerësimit rekurziv baesian (VRB), metodë e cila arrin që përditëson dhe korrigjon modelin duke u adaptuar me informacione të reja që vijnë në sistem (Techslang, n.d.). Në përfundim, Darktrace përdor rrjetet neurale të thella dhe një kombinim teknikash të të nxënit të makinës me dhe pa mbikëqyrje për të rritur detektimin dhe ndalimin e anomalive dhe rreziqeve. Duke përdorur rrjetet neurale të shtresuara, Darktrace gjurmon dhe vendos pikëvlerësime të të dhënave të DNS, grupon pajisjet me algoritme të grupimit (clustering) dhe zbulon sjellje të çuditshme dhe paterna jonormale. Kjo qasje mundëson identifikim më të shpejtë të mjediseve të reja ku program integrohet dhe përmirëson përgjithësisht mundësinë e zbulimit të rreziqeve.

5.2.2. Vectra AI

Vectra përdor Inteligjencën Artificiale (AI) për korrelacionin e kërcënimit, duke shkuar përtej metodave individuale të sulmuesit për të identifikuar, kategorizuar dhe dhënë përparësi sulmeve të avancuara. Inteligjenca artificiale e tyre analizon sjelljet në të gjithë llogaritë, hostet, rrjetet dhe cloud, duke ia atribuar ato ankorave të qëndrueshme si llogaritë ose makinat pritëse (A. Vectra , 2022). Inteligjenca artificiale e Vectra mund të zbulojë kanalet e komandës dhe kontrollit të përdorura nga sulmuesit, pavarësisht nga teknikat e kriptimit ose evazionit. Duke u fokusuar në formën e trafikut të rrjetit me kalimin e kohës, ata identifikojnë tregues të qartë të metodave komanduese dhe kontrolluese. Kjo qasje e drejtuar nga AI mundëson zbulimin dhe prioritizimin efektiv të kërcënimeve (A. Vectra , 2022).

Nga informacionet e raportit nga Vectra, mund të kuptojmë se Vectra kombinon teknikat të bazuara në rrjet dhe poashtu në ‘host’ dhe poashtu përdor algoritme të ML me dhe pa mbikëqyrje,

analizë të sjelljes, nxjerrje të tipareve dhe Deep Learning. Kjo na bën të kuptojmë se Vectra është një ndër softuerët më të mirë për mbrojtje në siguri kibernetike.

5.2.3. EDR/Cynet

Cynet është një kompani e cila poashtu ofron zgjidhje për siguri kibernetike. Njëra ndër pikat e forta të Cynet është se këta të fundit kanë arritur që të implementojnë një sistem punues ku ekspertët e sigurisë punojnë në mënyrë të harmonizuar me produktet e kësaj kompanie (A. Cynet). Produkti i tyre për siguri kibernetike EDR (Detektimi i zgjeruar i sulmeve) i Cynet ka tiparet e mëposhtme:

1.SSDEEP Scan (Ku përdoret një algoritëm kompresimi që kërkon për "malwares" të njohur me taktikën tradicionale të bazuar në nënshkrim.)

2.Mostrat e memories (Ku analizohet memoria e një pajisjes dhe kërkohet për anomaly apo paterna të sjelljes të dyshimta, të dhëna me stringje të dyshimta etj.)

3.Teknologji e avancuar e zbulimit (Ku detektohen aktivitetet me qëllim të keq në proceset legjitime si PowerShell apo Cmd.)

4.Driver Mode | Kernel (Ku arrihet të gjehen kërcënimet e nivelit Kernel. Kjo u ndalon sulmuesve që të ndalin të gjitha proceseve mbrojtëse të Cynet.) (A. Cynet)

Pra, kuptojmë se me një kombinim të ML me mbikëqyrje dhe disa prej teknikave tradicionale të mbrojtjes si mbrojtja e bazuar në nënshkrim, Cynet arrin që të neutralizojë dhe zbutë kërcënimet që i dalin në rrugë.

5.2. NJË KORNIZË PËR MBROJTJE NGA SULMET KIBERNETIKE ME AI

Në këtë pjesë të punimit do paraqesim një kornizë për zbatimin e një strategjie të sigurisë kibernetike e cila bazohet në AI duke shfrytëzuar poashtu potencialin e programeve që përmendëm

më herët si “Vectra AI”, “Darktrace” apo “EDR/CYNET” duke u fokusuar në zbatimin praktik të teknologjisë AI. Kornizën e kemi ndarë në disa pika por në dy faza kryesore: Faza e përgaditjes dhe Faza Operative. Duhet të kuptohet se kjo kornizë është një kornizë më gjenerale dhe varësisht nga arkitektura e rrjetës apo madhësia e kompanisë, kërkesat mund të ndryshojnë. Nëse fazat që përmendim më poshtë ekzekutohen me rradhë dhe në mënyrë të duhur, atëherë mund të arrihet një implementim i AI në rrjet që rrit sigurinë kibernetike në një masë shumë të madhe. Në figurën më poshtë do shohim se si kjo kornizë funksionon dhe hapat e saj duke filluar nga faza përgaditore, faza operative, permirësimi dhe përshtatja e modelit AI dhe pjesa e rregulloreve për mbrojtjen e të dhënave.

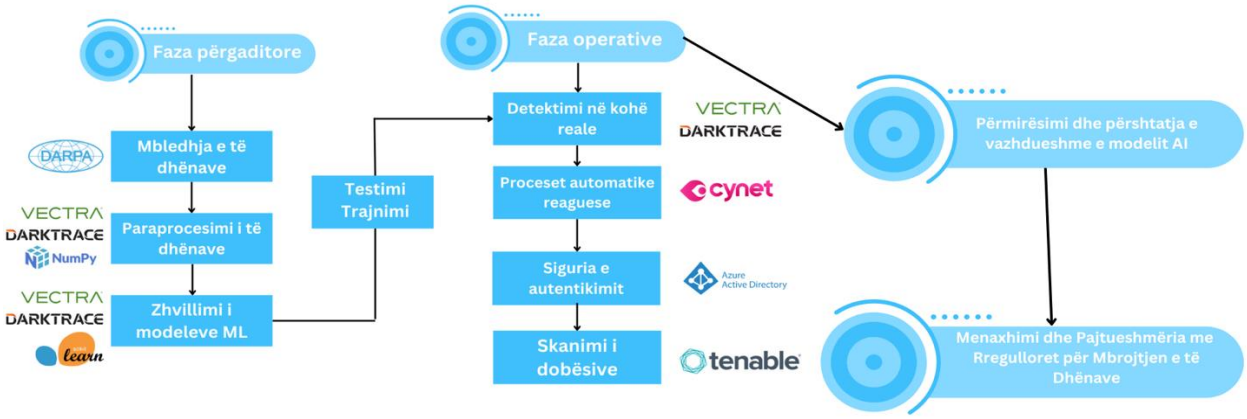

Figura 4. Korniza për mbrojtje kibernetike e bazuar në AI

5.2.1. Faza e përgatitjes

Në këtë fazë do kuptojmë që për një përgatitje të mirë të një kornize të mbrojtjes duhet që të mbledhim një sasi të konsiderueshme të të dhënave nga datasete të ndryshme, ti pastrojmë dhe përpunojmë të dhënat në mënyrë që ato të jenë të kuptueshme në pjesën e zhvillimit të modeleve ML të cilat duam ti implementojmë në sistem. Pas zhvillimit, modeli duhet të trajnohet dhe përgatitet për mbrojtje të sistemit, varësisht nga qëllimi i tij.

5.2.1.1. Mbledhja e të dhënave

Ideja është që të mblidhen të dhëna relevante me sigurinë që nevojitet duke mbledhur të dhëna të ndryshme si trafiku i rrjetit, logjet e rrjetit dhe të pajisjeve të ndryshme në mënyrë që të krijojmë një pamje sipërfaqësore të rrjetit. Përmes AI do kemi mundësi që të trajtojmë këto të dhëna në mënyrë që të jenë gati për paraprocesim dhe analizë. Disa nga datasetet të cilat mund të përdoren janë datasetet si „ADFA intrusion dataset“, „ISOT CID Dataset“, „DARPA dataset“ etj (Choudhury, n.d.). Datasete të pasura si këto arrijnë që të ofrojnë një ndihmë të madhe në krijimin e modeleve të avancuara të sigurisë. Poashtu dhe "Vectra AI" mund të shfrytëzojë burime të ndryshme të të dhënave për detektim, duke përfshirë metadatat dhe kokat e paketave, duke mundësuar zbulimin e avancuar të kërcënimit.

5.2.1.2. Përpunimi fillestar i të dhënave

Në këtë hap do marrim të gjitha të dhënat e mbledhura dhe do i pastrojmë dhe paraprocesojmë në mënyrë që të heqim të dhënat e panevojshme të cilat mund të na shfaqin falso pozitive në të ardhmen (A. L. Buczak). Poashtu për paraprocesim të të dhënave mund të përdoren sistemet që kemi përmendur më herët si Vectra AI Pandas.

Mund edhe të përdoren kodifikuesit automatikë variacional (VAE) për gjenerimin e të dhënave sintetike për të adresuar çështjet e mosbalancimit të të dhënave dhe për të shtuar grupet e të dhënave të trajnimit (Samar Mouti, n.d.).

5.2.1.3. Zhvillimi dhe përdorimi i modeleve ML për zbulimin e anomalive

Ku trajnojmë modele me algoritmet me dhe pa mbikëqyrje në mënyrë që të detektohen anomalitë apo edhe të kuptohen mostrat e ndryshme (A. L. Buczak). Vectra AI dhe DarkTrace veqse i kanë modelet dhe algoritmet e tyre të cilat i përdorin për detektimin e anomalive por ato nuk janë publike për përdoruesit e platformës. Nëse do duhej të zhvillohej modeli në mënyrë vetanake atëherë mund të përdoret libraria e Python „scikit-learn“. Mund të përdoret poashtu të mësuarit aktiv me

optimizimin Bayesian për përzgjedhje efikase të mostrave dhe trajnimin e modelit të AI-së (Frazier, 2018).

5.2.1.4. Trajnimi dhe "përgatitja" e modelit

Të përdoret Transferimi i Mësimit (Barak, 2023) nga modele të para-trajnuara si GPT-3 për analizën e "logs", kuptimin e gjuhës natyrore dhe detektimin e kërcënimeve. Mund edhe të përdoren programe si RapidMiner ku mund të trajnojmë modelin.

5.2.2. Faza operative

Në këtë fazë, do diskutohet për fazën operative të mbrojtjes ku hyjnë pjesa e inteligjencës monitorimit dhe analizës së kërcënimeve. Do diskutohet edhe për sigurinë e autentifikimit të drejtuar nga AI dhe mekanizmat për kontrollin e qasjes, skanimet e sistemit me AI dhe për reagimet e automatizuar të kërcënimeve.

5.2.2.1. Inteligjenca, Monitorimi dhe Analiza e Kërcënimeve

Mund të përdoren mjete si Esper ose Apache Flink me Përpunimin e Kohës së Ngjarjeve, duke lehtësuar monitorimin e vazhdueshëm dhe zbulimin e shpejtë të kërcënimit (Moreno, Bertoa, Burgueno, & Vallecillo, 2019).

Mund të përdoren aftësitë e "Darktrace" si një Sistem i detektimit të ndërhyrjeve i drejtuar nga AI duke përdorur algoritmet e të nxënit pambikëqyrje për identifikimin dhe përgjigjen e kërcënimeve në kohë reale.

5.2.2.2. Autentifikimi i drejtuar nga AI dhe mekanizmat e kontrollit të qasjes

Të implementohet sistem AI për autentikim dhe për mekanizmat e kontrollit të qasjes për të parandaluar qasjet jo të autorizuara. Mund të implementohen AI për njohje të fytyrës apo metoda

tjera biometrike për autentikim. Një softuer që mund të përdoret është edhe Microsoft Azure Active Directory (Azure AD) i cili ka tipare inteligjente të autentifikimit si zbulimi i paternave të përdoruesve, qasjet me kushte duke ditur informacione të detajuara për përdoruesin, çkyçja e mençur ku nëse zbulohet një anomali në sjelljen e përdoruesit atëherë sistemi çkyç përdoruesin (SailPoint, 2020). Duhet edhe të zbatohet Kriptimi Biometrik për ruajtjen e sigurt të të dhënave biometrike, duke përdorur Enkriptimin Homomorfik për të siguruar privatësinë gjatë vërtetimit (Xun Yi, n.d.).

5.2.2.3. Skanimi i sistemit të bazuar në AI dhe vlerësimi i sigurisë

Të implementohen sisteme AI të cilat në mënyrë aktive skanojnë sistemin për siguri dhe vlerësojnë sigurinë e sistemit. Në këtë pjesë mund të përdoret Tenable.io i cili është një platformë për menaxhim të dobësive që bën prioritizim të rreziqeve duke u bazuar në AI (Tenable, n.d.).

5.2.2.4. Reagimi i automatizuar i kërcënimit

Këto procese mund të ofrohen nga EDR/Cynet i cili arrin që të reagojë në mënyrë automatike ndaj kërcënimeve (A. Cynet). Qëllimi i kësaj pike është që me kohë modeli të arrijë të parashikojë dhe të reagojë sa më shpejt edhe ndaj një sulmi të panjohur.

5.2.2.5. Mbajtja, Zhdukja dhe rikuperimi

Duke u bazuar në kornizën e NIST (Instituti Kombëtar i standardeve dhe teknologjisë), disa ndër pjesët e rëndësishme të fazës operative janë mbajtja, zhdukja dhe rikuperimi i kërcënimit ku mbajtja tregon se si kërcënimi duhet të ndalet para se sulmi të bëjë ndonjë dëm të madh ku poashtu duhet të identifikohet kërcënuesi dhe të arrihet t'i ndalohet lidhja. Pas mbajtjes nën kontroll, me zhdukjen dhe rikuperimin fshijmë të gjitha elementet kërcënuese dhe rikuperojmë sistemin në një gjendje të sigurt dhe shëndoshë (Cynet A.).

5.2.3. Zbatimi teknik i AI në Rrjet

Në këtë pjesë do diskutohet se në cilat pika kryesore do zbatohet sistemi AI i zhvilluar me AI. Pikat kryesore që do cekim janë: Perimetri i rrjetit, Siguria e emailit, “Firewalls” të Ueb Aplikacioneve dhe pikat fundore të rrjetit.

5.2.3.1. Perimetri i rrjetit

Këtu luan rol "Darktrace" si një Sistem i zbulimit të ndërhyrjeve i drejtuar nga AI në perimetrin e rrjetit, duke shfrytëzuar aftësitë e tij të ML pa mbikëqyrje të pajisjeve për zbulimin e kërcënimeve në kohë reale. Qëllimi është që sulmi të ndalohet para se të hyjë në rrjetin e brendshëm.

5.2.3.2. Siguria e emailit

Mund të përdoren rrjetet gjenerative për gjenerimin e emaileve sintetike të phishing, duke shtuar të dhënat e trajnimit për të përmirësuar mbrojtjen kundër teknikave të ndryshme të phishing (Sharif Amit Kamran, 2022). Qëllimi është që AI të ndalojë dhe filtrojë e-mails të dyshimta phishing apo e-mails që përmbajnë programe të këqia. Mund të bëhet dhe integrimi softuerëve të specializuar të sigurisë së e-mail si "Mimecast" për të rritur masat e sigurisë së e-mailit.

5.2.3.3. “Firewall” të aplikacionit në ueb

Të zbatohen modelet “Multi-Modal AI” që kombinojnë analizën e imazhit, gjuhës natyrale procesuese dhe modelimin e sjelljes së përdoruesit për zbulimin general të sulmeve të aplikacioneve në ueb (Gavrilova & Monwar, 2013). Mund të implementohen sisteme si Imperva apo Fortinet FortiWeb.

5.2.3.4 Mbrojtja e pikave fundore

Këtu hyn në punë softueri "EDR/CYNET" si një zgjidhje për detektimin dhe reagimin e pikave fundore për zbulimin e kërcënimeve në kohë reale, analizën e sjelljes së përdoruesve dhe rrjetit dhe poashtu reagimin e automatizuar (A. Cynet).

Në këtë pikë "EDR/CYNET" plotëson aftësitë e "Vectra AI" dhe "Darktrace" në mbrojtjen e pikave fundore nga kërcënimet e avancuara.

5.2.4. Përmirësimi dhe përshtatja e vazhdueshme e modelit AI

Modeli i AI duhet të ketë një proces ciklik të ritrajnimit duke përdorur teknikat ML për t'iu përshtatur modeleve të reja të kërcënimeve apo edhe përditësimit të metodave të reja të reagimit. Përsëri të përdoren sistemet Bayesiane për përditësime të vazhdueshme të modelit bazuar në të dhënat më të fundit të kërcënimit dhe sjelljeve të rrjetit.

5.2.5. Menaxhimi dhe Pajtueshmëria me Rregulloret për Mbrojtjen e të Dhënave

Duhet mbrojtur privatësinë e të dhënave individuale gjatë trajnimit dhe vendosjes së modelit të AI, duke mos shkelur të drejtat e individëve dhe të arrihet që të proceset e trajnimit të jenë në përputhje me rregulloret e mbrojtjes së të dhënave si GDPR.

Duhet të implementohet dhe të mësuarit të federuar për të trajnuar modelet e AI mbi burimet e decentralizuara të të dhënave pa ndarjen e të dhënave të papërpunuara.

5.3. RAST STUDIMI: DEEP LOCKER - PËRDORIMI I AI PËR SULME KIBERNETIKE

5.3.1. Background

Deeplocker është një koncept i një programi me qëllim të keq (malware) i cili u zhvillua nga IBM Research që përdor teknologjinë e inteligjencës artificiale për të shënjestruar individë apo entitete të caktuara për t’i sulmuar dhe gjatë të tërë procesit ky sulm qëndron i pazbuluar (Kumar M. ,

2018). Ky program i zhvilluar nga hulumtuesit e IBM arrin që të identifikojë shënjestrat e tij përmes treguesve si njohja e fytyrës, gjeolokacioni apo edhe njohja e zërit.

5.3.2. Zhvillimi dhe motivimi mbrapa DeepLocker

Në mënyrë që inxhinierët e sigurisë kibernetike të jenë disa hapa përpara akterëve kërcënues, është e nevojshme të kuptohet se këta të fundit arrijnë që të përdorin teknika të avancuara të AI për të lëshuar sulmet e tyre. Në këtë rast, praktika e marrë është të luftohet zjarri me zjarr ku hulumtuesit e IBM kanë arritur të krijojnë një sulm i cili është në gjëndjë të shënjestrojë entitete apo individë të caktuar duke arritur që ti shmanget të gjitha masave mbrojtëse duke qëndruar i pazbuluar (Kumar M. , 2018).

5.3.3. Funksionaliteti i DeepLocker

Deeplocker arrin që të fshehet dhe mos aktivizohet deri sa të gjejë shënjestrën e tij dhe të aktivizohet në kohën e duhur. Thuhet se ky sulm mund të arrijë që të infektojë miliona pajisje pa u zbuluar, prandaj cilësohet si një sulm kibernetik shumë i rrezikshëm i fuqizuar nga AI (Kumar M. , 2018). Mënyra se si DeepLocker funksionon është shumë e veçantë. Vetë modeli AI i tij është i trajnuar që të sillet në mënyrë normale deri në momentin që plotësohet kushti i duhur që ky sulm të aktivizohet. Vetë çelësi i cili e lëshon sulmin prodhohet nga AI, më saktësisht rrjeti neural brenda sistemit. Disa nga kushtet që mund ta aktivizojnë sulmin janë audio, pamjet, gjeolokacioni por edhe tiparet humane si fytyra apo zëri i një njeriu. Kjo e bën këtë sulm që të mos arrijë të bëhet një “reverse engineering” në këtë softuer me qëllim të keq. Në figurën 1 kemi 3 mbulime të cilat e bëjnë këtë malware të mos kuptohet se çfarë qëllimi ka (Jiyong Jang, 2018).

Figura 5. DeepLocker - Mbulimi nga AI, (Jiyong Jang,2018)

Demonstrimi që u bë në konferencën ku ky softuer u zbulua, vazhdoi duke përdorur një "ransomware" të cilin e futën në një aplikacion për videokonferenca dhe që sulmi të aktivizohej, shkrehëza ishte fytyra e njërit prej pjesëmarrësve (Jiyong Jang, 2018).

Tani po shohim se sulmet kibernetike mund të arrijnë nivele të reja të avancimit dhe se modele të shumta të AI mund të përdoren për të shënjestruar një individ në veçanti, gjë që e bën një sulm me AI më të rrezikshëm se kurrë.

5.4. KUFIZIMET E AI NË SIGURINË KIBERNETIKE

Përveç të mirave të integrimit të AI në shoqërinë tone duhet të kuptojmë se kjo teknologji vjen me kufizimet dhe të metat e saj. Duke mbledhur informata nga burime të ndryshme (SIOLI, 2021) (Segal) (Zenonos, 2022), dhe eksperienca vetanake më poshtë do shikojmë disa nga sfidat e AI të cilat janë:

1. Mbështetja e tepërt në AI
2. Qasja në të dhëna
3. Mbrojtja e të dhënave

5.4.1. Mbështetja e tepërt në AI

Siguria kibernetike është njëra ndër aspektet që luan më së shumti rol në një kompani, organizatë apo entitet i cili ka të dhëna të ndjeshme. Ndër gabimet më të mëdha që mund të bëhet, është mbështetja e tepërt në AI sepse AI nuk mund të ketë asnjëherë një saktësi prej 100% pasi që anomali të ndryshme mund të ndodhin në rrjet të cilat asesi nuk mund të kalkulohen nga AI. Poashtu duhet ta kemi parasysh se shpesh ndodhin dhe falsot pozitive duke na dhënë informacion të gabuar. Edhe sulmuesit poashtu mund të përdorin AI në mënyrë që të ekzekutojnë sulme edhe më të sofistikuara prandaj nëse mbështetja qëndron tërësisht në AI pa pasur ndërhyrje humane atëherë mundësia për ndërhyrje të paligjshme dhe sulme të ekzekutuara me sukses rritet në mënyrë drastike. Pra, duhet që të krijohet një balanc mes pjesës digjitale dhe humane të infrastrukturës së sigurisë të një entiteti. Duke marrë për bazë aktin Europian të vitit 2021 ku u propozua një strategji për rregullimin e AI (SIOLI, 2021), vlen të ceket se e njëjta duhet të vlejë në implementimin e një teknologjie të tillë në mënyrë që siguria kibernetike të rritet dhe që të ulen rreziqet e AI në këtë fushë.

5.4.2. Qasja në të dhëna për trajnimin e modeleve

Ndër limitimet tjera më të mëdha është edhe qasja në të dhëna pasi që mësuam se në mënyrë që algoritmet e ML dhe një softuer i AI të funksionojnë siç duhet, atëherë modeli duhet që të trajnohet me të dhëna të shumta në mënyrë që të krijojë modele parashikimi dhe poashtu të ketë një saktësi të madhe. Saktësia e modelit luan rolin më të madh pasi siguria kibernetike e një kompanie apo organizate është ndër pikat më të ndjeshme dhe nuk ka hapësirë për gabim. Pra, edhe nëse kompania ka qasje në të dhëna dhe resurse përsëri nuk ekziston krijimi i një strukture perfekte të mbrojtjes pasi që inxhinierët e sigurisë duhet të kenë qasje në datasete të shumta dhe të avancuara. Procesi i trajnimit të modeleve është një process që merr shumë kohë dhe poashtu kushton financiarisht. Kjo na bën të kuptojmë se qasja në resurse është shumë e vështirë edhe për kompanitë që kanë financa stabile dhe përsëri nuk mund të krijohet ndonjë model ideal i mbrojtjes kurse kjo

qasje është edhe më joreale për kompanitë e vogla të cilat nuk kanë resurse, financa apo edhe kohë të marrin të gjithë datasetet ekzistuese dhe ti trajtojnë ato (Segal).

5.4.3. Mbrojtja e të dhënave

Njëra ndër kufizimet tjera të AI është poashtu sfida për mbrojtjen e të dhënave. Të dy këto fusha mund të themi se ndërthuren mjaft mirë me njëra tjetrën. Teknologjitë me AI gjithmonë shkojnë dhe rriten dhe si pasojë mund të ndodhë që mbrojtja e të dhënave nuk qëndron në nivelin e duhur. Duhet të konsiderohet me shumë seriozitet qështja e transparencës mes AI dhe të dhënave të përdoruesve, pasi që përdoruesit duhet ta dijnë saktë se si të dhënat po përdoren, procesohen dhe duhet që t'u ofrohet mundësia përdoruesve që ta kenë zgjedhjen se a duan ata që të mirren të dhënat e tyre apo jo (Zenonos, 2022). Kompanitë që mbajnë të dhëna duhet të sigurohen që të krijojnë një shtresë sigurie të sigurt dhe jo ti mbrojnë ato vetëm që të kalojnë testet e rregullacioneve. Duhet të merren parasysh edhe partitë apo programet e treta që përdoren në kompani mund të jenë shkaku i rrjedhjes së të dhënave duke rezultuar në humbje të mëdha. Të dhënat janë burimi më i vlefshëm i secilit individ dhe kjo na bën të kuptojmë se organet ndërkombëtare rregullative duhet që të bëhen së bashku dhe të krijojnë rregullacione shumë strikte duke e bërë prioritet mbrojtjen e të dhënave.

5.5. E ARDHMJA E AI NË SIGURINË KIBERNETIKE

Më poshtë do shohim se cila është e ardhmja e AI në Siguri Kibernetike. Do shikojmë të gjitha kategoritë më të zhvilluara të AI në kohët e fundit, ku qëndron integrimi i AI në sigurinë kibernetike cilat janë rreziqet që AI mund t'i ngrisë në të ardhmen.

5.5.1. Kategoritë më të zhvilluara të AI në kohët e fundit

AI ka pasur përparime të mëdha gjatë vitit 2023. Disa nga to janë lansimi i ChatGPT, një model i trajnuar i cili gjen përgjigjje pothuajse për çdo gjë, Adobe Firefly, MidJourney etj. Trendet më të fundit në AI janë:

1. **AI i spjegueshëm (XAI) -** Është një trend që krijon AI sisteme që spjegojnë se si arrijnë në vendime apo rekomandime të caktuara. Kjo ndihmon në transparencën dhe besimin në AI. XAI do ndihmojë shumë industritë si sistemet autonome, financat, inxhineria etj. (Deepak STATANALYTICA, 2023)
2. **Të nxënit federativ** – Arrin që të ndihmojë pajisje të ndryshme të mësojnë nga një model i përbashkët pa shpërndarë të dhëna me njëra tjetrën. Kjo arrin që të ulë shqetësimet mesa i përket privatësisë që zakonisht i përkasin mësimit të centralizuar. Me mësim të federuar mund të kemi avancime në industrinë e mjekësisë dhe financave. (Deepak STATANALYTICA, 2023)
3. **Sistemet Autonome** – Kanë qenë dhe ende janë një trend në botën e AI. Makinat Autonome kanë arritur që të ngrisin saktësinë e tyre dhe shumë kompani të prodhimit të makinave kanë filluar implementimin e kësaj teknologjie në makinat e tyre si Mercedes, BMW etj. Momentalisht Tesla është njëra ndër kompanitë që po e qon përpara më së shumti AI të sistemeve autonome pasi që AI i saj ka arritur të mbledhë të dhëna për shumë vite me rradhë dhe mund të themi se ka modelin më të avancuar të sistemit autonom. (Deepak STATANALYTICA, 2023)
4. **Generative AI** (AI gjenerues) – ku kemi rastin e modelit gjuhësor Chat-GPT që përdor AI gjenerues dhe version i tij më i fundit pritet që të ketë një performancë shumë më të madhe kundrejt versioneve paraprake dhe do arrijë të revolucionalizojë industritë e ndryshme, ndër to edhe krijimin e përmbajtjes në rrjete sociale edhe poashtu edukimin (Deepak STATANALYTICA, 2023). Dhe ky lloj i AI (ky model) arrin që të kthejë përgjigjje shumë të shpejta dhe të sakta ose poashtu të krijojë përmbajtje të gjera me saktësi shumë të madhe.

5.5.2. Integrimi i AI në Sigurinë Kibernetike dhe Cloud

AI po rritet shpejt. Duke shikuar aftësitë e saj pritet të rritet edhe aftësia e integrimit të saj në siguri kibernetike. AI do arrijë që të jetë gjithmonë e më e saktë duke ndihmuar në automatizimin e shumë detyrave dhe proceseve të sigurisë kibernetike. Njëra ndër pjesët ku AI mund të ndihmojë me automatizim mund të jetë menaxhimi i identitetit dhe qasjes ku AI mund të monitorojë dhe analizojë aktivitetin e përdoruesve dhe të shikojë për ndonjë anomali në mënyrë që ta ndalojë një kërcënim potencial apo person të paautorizuar që ka marrur qasje në një sistem. Poashtu mund të ndihmojë edhe në krijimin e llogarive dhe në proceset e kyçjes në mënyrë të sigurt. Duke

monitoruar këto aktivitete arrin të diferencojë ngjarjet e dyshimta dhe mund të anulojë ato sesione (Hunt, 2021).

AI poashtu mund të rrisë edhe sigurinë e rrjeteve Cloud pasi që ne veçse po shohim se shumë kompani kanë filluar të lëvizin të dhënat dhe proceset e tyre në Cloud. Implementimi i AI në Cloud pritet të jetë një ndër kërkesat më të mëdha pasi që menaxhimi dhe implementimi do jetë më i lehtë në sisteme të reja. Mund të themi se jemi duke shkuar drejt një pike ku mbrotja kibernetike me AI do implementohet në çdo rrjetë dhe në çdo pajisje pasi që kërkesa për një botë digjitale të sigurt është shumë e madhe dhe poashtu mungesa e sistemeve mbrojtëse me AI po dëmton kompanitë çdo ditë e më shumë, pra, është vetëm një çështje kohë për t'u zhvilluar sisteme të reja mbrojtëse që janë të lehta për t'u implementuar, përdorur dhe janë të përballueshme me çmim.

5.5.3. Rreziqet e AI

Deri tani arritëm të kuptojmë të mirat e AI, limitimet dhe sfidat me të cilat përballet zhvillimi i saj. Por, me teknologji të nivelit kaq të lartë, vijnë edhe rreziqet së bashku me të. Gjatë vitit 2023, Drejtorë ekzekutiv nga kompani lidere në AI kanë kërkuar që zhvillimi i AI të ndalet për 6 muaj por nuk kanë arritur ta arrijnë qëllimin. Disa nga figurat që janë pajtuar me këtë vendim janë figura botërore si Elon Musk (Tesla), Sam Altman (OpenAI), Demis Hassabis (DeepMind) dhe poashtu Geoffrey Hinton i cili ka lënë pozitën e tij në kompaninë gjigante në Google dhe ka lajmëruar për rreziqet që AI posedon (Perrigo, 2023).

Por, cilat janë këto rreziqe që AI mund ti sjellë?

Së pari, nëse një AI e zhvilluar bie në duart e gabuara, një akter kërcënues mund të arrijë ta përdorë atë për të krijuar një super armë kibernetike që të lëshojë sulme masive kibernetike. Tjetër rrezik mund të jetë çështja e privatësisë pasi momentalisht nuk ka ndonjë regullacion i cili trajton çështjet me AI. Në vitin 2021 është propozuar një regulacion por vetëm drafti i parë ka kaluar (Goldman, 2023).

Tjera rreziqe që posedon AI janë (Thomas):

a) **Zëvendësimi i vendeve të punës nga automatizimi i AI** – pasi ka shumë vende punë ku nëse teknologjia AI arrin të implementohet në mënyrë të duhur atëherë proceset e punës mund të

automatizohen dhe shumë njerëz mund të humbasin vendet e tyre të punës. Njëra ndër degët që potencialisht mund të preket është poashtu siguria kibernetike ku inxhinierët e sigurisë kibernetike mund të zëvendësohen me një algoritëm AI.

b) **Manipulimi i rrjeteve sociale me AI** – Kemi rastet më të fundit ku në rrjete sociale përdorues të ndryshëm krijojnë video me deepfake, ku kjo teknologji AI arrin që ta ndryshojë fytyrën e personit në video duke e bërë atë të ngjasojë me një figurë të famshmë publike, dhe kjo mund të rezultojë në mashtrim masiv nëse një akter me qëllime të këqia e merr në dorë këtë teknologji dhe imiton një figurë publike.

c) **Mbikëqyrja me teknologji AI** – Ku shembull primar mund të mirret përdorimi i teknologjisë së njohjes të fytyrës në Kinë në shkolla, zyre dhe vende tjera pa miratimin e popullit. Kjo dukuri është një shkelje masive e privatësisë dhe e të drejtave të njeriut.

d) **Sulmet Kibernetike t**ë **Automatizuara me AI** – Ku sulmet kibernetike avancohen dhe automatizohen në një gamë aq të gjerë saqë mbrojtjet tradicionale dhe inxhinierët pa përvojë të sigurisë nuk do munden ti bëjnë ballë këtyre sulmeve.

Në kohët e fundit është shfaqur dhe një rrezik i ri i cili është i fuqizuar nga AI. Bëhet fjalë për një sulm ku një sistem AI arrin që të mësojë fjalëkalimin e një përdoruesi vetëm duke dëgjuar dhe analizuar tingujt e tasteve të cilat shtypen (Joshua Harrison, 2023). Një sulm i tillë rezulton të ketë një saktësi prej 95%, gjë që e bën këtë sulm shumë të rrezikshëm nëse ekzekutohet.

6. KONKLUZIONE DHE REKOMANDIME

Teknologjia çdo ditë shkon dhe zhvillohet më shumë duke avancuar të gjitha fushat që ajo prek. Duke analizuar këtë hulumtim ku fokuse kryesore kemi sigurinë kibernetike dhe inteligjencën artificiale, mund të kuptojmë se AI mund të arrijë që të revolucionalizojë sigurinë kibernetike duke forcuar detektimin e kërcënimeve, reagimet ndaj incidenteve dhe aspektet tjera digjitale gjenerale të sigurisë kibernetike. Integrimi i AI në sigurinë kibernetike mund të ndihmojë shumë në mbrojtje efiçiente dhe efektive ndaj sulmeve kibernetike.

Zhvillimet e fundme në fushën e inteligjencës artificiale si AI i spjegueshëm (XAI), të nxënit e federuar, sistemet autonome dhe poashtu njëri ndër më të fundmit GPT-4 modeli, tregojnë progresin që ka ndodhur në zhvillimin e teknologjive të AI në aplikimet e përditshme. XAI i mundëson sistemet AI që të ofrojnë spjegime se si ato kanë arritur deri tek një vendim i caktuar apo tek rekomandimet e ndryshme, dhe kjo ka një efekt pozitiv në shoqëri pasi rrit besimin dhe transparencën tek AI. Të nxënit e federuar lejon pajisje të shumta që të mësojnë në mënyrë të përbashkët pa shpërndarë të dhënat e ndjeshme duke arritur të krijojë përfitim për fushat e shëndetësisë apo edhe financave. Sistemet autonome që janë zhvilluar nga kompani të ndryshme si Tesla, arrijnë që të evoluojnë industrinë e makinave duke rritur saktësinë dhe mundësitë e tyre për zhvillim.

Kur dalim tek integrimi dhe aplikimi i AI në siguri kibernetike, kemi shumë dobi si automatizimi i detyrave të ndryshme siç janë menaxhimi i identiteteve apo edhe kontrolli i qasjes. AI mund të analizojë dhe monitorojë aktivitetin e përdoruesit në kohë reale, duke njoftuar dhe neutralizuar kërcënimet të cilat mund të ndodhin duke i parashikuar apo detektuar ato. Mund të arrijë që poashtu të ndihmojë në proceset e ndryshme digjitale siç është krijimi i një llogarie në mënyrë të sigurt, proceset e authentikimit duke ndaluar tentimet e ndryshme të paautorizuara duke krijuar një siguri efiçiente apo edhe qasjet e kontrolluara. Poashtu, AI mund të ndihmojë në mbrotjen e rrjeteve në cloud, pasi që vitet e fundit shumë kompani kanë filluar të dalin në cloud. Në rrjete të tilla, AI mund të ndihmojë në detektimin dhe ndaljen e kërcënimeve dhe mbrojtjen e informacionit. Përveq të gjitha këtyre përfitimeve, është shumë e rëndësishme që të kuptohen edhe rreziqet të cilat AI paraqet në siguri kibernetike. Kërcënime të sigurisë kibernetike mund të jenë qështjet e privatësisë, regulloret joadekuate, humbjet e vendeve të punës si shkak i automatizimit nga AI, manipulimi i

masave me përmbajtje si “deepfakes”, automatizimi dhe rritja e sulmeve kibernetike të avancuara dhe poashtu keqpërdorimi i Teknologjive të përgjimit me AI. Në mënyrë që këto rreziqe te zvogëlohen, atëherë duhet të vendosen rregulla të forta dhe korniza etike të cilat drejtojnë zhvillimin dhe vendosjen e AI në siguri kibernetike. Nëse liderët e “Big Tech” si Apple apo Google, krijuesit e politikave dhe ekspertët e sigurisë kibernetike dhe privatësisë arrijnë të bashkëpunojnë, atëherë mund të sigurohet se teknologjitë e AI do përdoren në mënyrë të sigurt duke mbrojtur shoqërinë, privatësinë, sigurinë digjitale dhe poashtu ruajtjen e vendeve të punës. AI arrin që të implementohet pothuajse në qdo cep të rrjetit të një kompanie duke ofruar siguri të pikave fundore, siguri të autentikimit dhe një mbrojtje active e cila ndalon kërcënimet në kohë reale, qofshin ato të njohura apo të panjohura për sistemin.

E kjo mund të arrihet me hulumtime, bashkëpunime të vazhdueshme dhe me një angazhim të përbashkët për të formuar një të ardhme të sigurt të një jete digjitale harmonike.

REFERENCAT

A. Cloudflare. (n.d.). *What is a denial-of-service (DoS) attack?* Retrieved from cloudflare : https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

A. CROWDSTRIKE. (2022, September 14). *MACHINE LEARNING (ML) & CYBERSECURITY*. Retrieved from crowdstrike: https://www.crowdstrike.com/cybersecurity-101/machine-learning-cybersecurity/

A. Cynet . (n.d.). *Cynet 360 AutoXDR.* Retrieved from cynet web site: https://go.cynet.com/hubfs/NEW/Cynet-Detailed-Solution-Brief.pdf

A. DarkTrace . (n.d.). Machine Learning: A Higher Level Of Automation.

A. Enisa. (n.d.). *What is "Social Engineering"?* Retrieved from enisa.europa.eu Web Site: https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

A. FORTINET. (n.d.). *What is a Zero Day Attack?* Retrieved from fortinet: https://www.fortinet.com/resources/cyberglossary/zero-day-attack

A. IBM. (2023). *What is machine learning?* Retrieved from ibm: https://www.ibm.com/topics/machine-learning

A. IBM. (n.d.). *What are Naive Bayes classifiers?* Retrieved May 2023, from IBM Web Site: https://www.ibm.com/topics/naive-bayes#:~:text=The%20Na%C3%AFve%20Bayes%20classifier%20is,a%20given%20class%20or%20category.

A. IBM. (n.d.). *What is a cyberattack?* Retrieved from IBM: https://www.ibm.com/topics/cyber-attack

A. Juniper. (2020, November 10). *QRadar Pulse Dashboard Components and Workspaces*. Retrieved from juniper: https://www.juniper.net/documentation/en_US/jsa7.4.1/jsa-pulse-app-guide/topics/task/operational/t_Qapps_PulseDashboard_import_export.html

A. K21Academy . (2022, June 25). *Deep Learning Vs Machine Learning*. Retrieved from k21academy Web Site: https://k21academy.com/datascience-blog/deep-learning/dl-vs-ml/

A. L. Buczak, E. G. (n.d.). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection.

A. TABLEAU. (n.d.). *AI Is as Risky as Pandemics and Nuclear War, Top CEOs Say, Urging Global Cooperation.* Retrieved from TABLEAU: https://www.tableau.com/data-insights/ai/risks#real-life

A. Vectra . (2022). *The AI behind Vectra AI.* Retrieved from Vectra : https://content.vectra.ai/hubfs/downloadable-assets/WhitePaper_2022_ai_behind_vectra_ai.pdf

adservio, A. (2022, October 6). *what are the components of AI?* Retrieved from adservio: https://www.adservio.fr/post/what-are-the-components-of-ai

Amir Hossein Gandomi, A. H. (2012, May 6). Krill herd: A new bio-inspired optimization algorithm. USA.

Author Darktrace. (n.d.). *Darktrace AI: Combining Unsupervised and Supervised Machine Learning.* Retrieved from https://assets-global.website-files.com/626ff4d25aca2edf4325ff97/62a292c20b7371fb41311930_wp-machine-learning.pdf

B.J.Copeland. (1998, July 20). *artificial intelligence*. (T. E. Britannica, Editor) Retrieved April 2023, from britannica: https://www.britannica.com/technology/artificial-intelligence

B.J.Copeland. (n.d.). *artificial intelligence*. Retrieved June 22, 2023, from Britannica Web Site: https://www.britannica.com/technology/artificial-intelligence

Baker, K. (2023, February 13). *10 MOST COMMON TYPES OF CYBER ATTACKS*. Retrieved from CROWDSTRIKE: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

Ballard, B. (2020, December 10). *AI could replace humans in cybersecurity by 2030.* Retrieved from Tech Radar Web Site: https://www.techradar.com/news/ai-could-replace-humans-in-cybersecurity-by-2030

Barak. (2023, January 6). *Learning Transfer Learning*. Retrieved from towardsdatascience: https://towardsdatascience.com/learning-transfer-learning-31b4b05f5a1a

Beng Heng Ng, X. H. (2010, December). *A Study on Latent Vulnerabilities*. Retrieved from Research Gate: https://www.researchgate.net/publication/224189979_A_Study_on_Latent_Vulnerabilities

Blessing Guembe, A. A.-S. (2022, March 4). The Emerging Threat of Ai-driven Cyber Attacks: A Review.

Boucher, P. (2020, June). Artificial intelligence: How does it work, why does it matter, and what can we do about it? Europe.

Brathwaite, S. (2022, August 19). *The State of AI in Cloud Security*. Retrieved from Software Secured Website: https://www.softwaresecured.com/the-state-of-ai-in-cloud-security/

Carpentier, A. (2023, January 25). *GPT Chat: the AI revolution in web content writing, a real competitor to Google?* Retrieved from botnation: https://botnation.ai/site/en/chat-gpt-revolution/

Choudhury, A. (n.d.). *Top 8 Cybersecurity Datasets For Your Next Machine Learning Project*.

Cisco, A. (n.d.). *What is Cyber Security?* Retrieved from Cisco.

Cynet A. (n.d.). *NIST Incident Response Plan: Building Your Own IR Process Based on NIST Framework.* Retrieved from Cynet website: https://www.cynet.com/incident-response/nist-incident-response/#the-nist-incident-response-life-cycle

Deepak STATANALYTICA. (2023, March 20). *What Are The Latest Trends In AI For 2023?* Retrieved from statanalytica: https://statanalytica.com/blog/latest-trends-in-ai-for-2023/#:~:text=Latest%20Trends%20In%20AI%20For%202023%201%20%E2%97%8F,...%205%20%E2%97%8F%20Generative%20Pre-trained%20Transformer%204%20%28GPT-4%29

Everson, S. (2015, December 7). *Executive Summary Dashboard*. Retrieved from tenable: https://www.tenable.com/sc-dashboards/executive-summary-dashboard

Frazier, P. I. (2018, 10 19). *Bayesian Optimization*. Retrieved from informs: https://pubsonline.informs.org/doi/abs/10.1287/educ.2018.0188

Furstenau, L. B., Sott, M. K., Homrich, A. J., & Kipper, L. M. (2020). *20 Years of Scientific Evolution of Cyber Security: a Science Mapping.* Dubai: IEOM Society International.

Gavrilova, M., & Monwar, M. (2013). *Multimodal biometrics and intelligent image processing for security systems*. Retrieved from Scholar: https://books.google.com/books?hl=en&lr=&id=af1yQ9mKYZ4C&oi=fnd&pg=PR1&dq=multimodal+ai+security&ots=dmC0rBuYc6&sig=euejf7DSsEBqUoRpWxoSz2B2jP4#v=onepage&q=multimodal%20ai%20security&f=false

Goldman, S. (2023, April 27). *EU lawmakers pass draft of AI Act, includes copyright rules for generative AI.* Retrieved from venturebeat: https://venturebeat.com/ai/eu-lawmakers-pass-draft-of-ai-act-includes-last-minute-change-on-generative-ai-models/

Hairab, B. I., Aslan, H. K., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023, January 23). Anomaly Detection of Zero-Day Attacks Based on CNN and Regularization Techniques. Cairo, Egypt, Egypt.

Hunt, S. (2021, September 27). *Trends in Artificial Intelligence (AI) in Cybersecurity*. Retrieved from Datamation: https://www.datamation.com/security/artificial-intelligence-ai-in-cybersecurity-trends/#:~:text=Trends%20in%20Artificial%20Intelligence%20%28AI%29%20in%20Cybersecurity%201,5%205.%20AI%20will%20improve%20cloud%20network%20security

Jiyong Jang, D. K. (2018, August 8). *DeepLocker: How AI Can Power a Stealthy New Breed of Malware.* Retrieved from securityintelligence: https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/

Joshua Harrison, E. T. (2023, August 3). *A Practical Deep Learning-Based Acoustic Side.*

Kagermann, H., Wahlster, W., & Helbif, J. (2013). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0 Final report of the industrie 4.0 Working Group.* Frankfurt.

Kumar, A., Priya, R., & Kumari, S. (2019). *Research Paper on Artificial Intelligence.* Greater Noida: Galgotias University.

Kumar, M. (2018, August 09). *Researchers Developed Artificial Intelligence-Powered Stealthy Malware.* Retrieved from thehackernews: https://thehackernews.com/2018/08/artificial-intelligence-malware.html

Kumar, V. (n.d.). *k-means.* Retrieved from towards machine learning: https://towardsmachinelearning.org/k-means/

Kun Zhang, L. C. (2007, April). *An Improvement of Matrix-based Clustering Method for Grouping Learners in E-Learning*. Retrieved from IEEE: https://ieeexplore.ieee.org/document/4281577

Li, L. (2021, June 9). *Dashboard Studio: Dashboard Customization Made Easy*. Retrieved from splunk: https://www.splunk.com/en_us/blog/platform/dashboard-studio-dashboard-customization-made-easy.html

Mimecast, A. (n.d.). *email security* . Retrieved from mimecast.com: https://www.mimecast.com/products/email-security/

Moreno, N., Bertoa, M. F., Burgueno, L., & Vallecillo, A. (2019). *Managing measurement and occurrence uncertainty in complex event processing systems*. Retrieved from IEEE Access: https://ieeexplore.ieee.org/abstract/document/8740975/

Morgan, K. (2023, April 12). Role of AI in Threat Detection and Zero-day Attacks. Virginia, USA: Old Dominion University.

Mrutyunjaya Panda, M. R. (2007). *Network intrusion detection using naive bayes.* Research Gate.

NIST. (N/A). *ARTIFICIAL INTELLIGENCE*. Retrieved from NIST.

Panda, M., & Patra, M. R. (2007). *NETWORK INTRUSION DETECTION USING NAIVE BAYES.* Berhampur: Department of Computer Science, Berhampur University,.

Patlolla, C. R. (2018, December 10). *Understanding the concept of Hierarchical clustering Technique*. Retrieved from https://towardsdatascience.com/: https://towardsdatascience.com/understanding-the-concept-of-hierarchical-clustering-technique-c6e8243758ec

Perrigo, B. (2023). AI Is as Risky as Pandemics and Nuclear War, Top CEOs Say, Urging Global Cooperation. *TIME*, 1-1.

Petronaci, M. (2020, April 14). *Dashboards & Business Intelligence - Feature Spotlight*. Retrieved from sentinelone: https://www.sentinelone.com/blog/dashboards-business-intelligence-feature-spotlight/

S. Sivamohan, S. S. (2023, March 10). An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework.

Safwab, H. (2020, September 20). *What is K Medoid Clustering: Why and How?* Retrieved from medium: https://medium.com/analytics-vidhya/what-is-k-medoid-clustering-why-and-how-b4e518c49e10

SailPoint, A. (2020, September 8). *Enhance Security and Compliance for Microsoft Azure Active Directory with AI-driven Identity*. Retrieved from Sail Point: sailpoint.com/identity-library/enhance-security-and-compliance-for-microsoft-azure-active-directory-with-ai-driven-identity/

Samar Mouti, S. K. (n.d.). *Cyber Security Risk management with attack detection frameworks using multi connect variational auto-encoder with probabilistic Bayesian networks*. Retrieved from Science Direct: https://www.sciencedirect.com/science/article/abs/pii/S0045790622005328

Segal, E. (n.d.). The impact of AI on Cybersecurity.

Sharif Amit Kamran, S. S. (2022, November 16). *Semi-supervised Conditional GAN for Simultaneous Generation and Detection of Phishing URLs: A Game theoretic Perspective*. Retrieved from arvix: https://arxiv.org/abs/2108.01852

Sharma, R. (2020, November 23). *KDD Process in Data Mining: What You Need To Know?* Retrieved from upGrad: https://www.upgrad.com/blog/kdd-process-data-mining/

Singh, J. (2023, February 27). *Difference between L1 and L2 regularization?* Retrieved from Tutorials Point: https://www.tutorialspoint.com/difference-between-l1-and-l2-regularization#:~:text=What%20is%20L1%20regularization%3F,values%20of%20the%20model's%20parameters.

SIOLI, L. (2021, April 23). A European Strategy for Artificial Intelligence. Europe.

Techslang, A. (n.d.). *What is Recursive Bayesian Estimation?* Retrieved from https://www.techslang.com/definition/what-is-recursive-bayesian-estimation/#:~:text=Recursive%20Bayesian%20estimation%20is%20an,a%20task%20that%20requires%20estimation.

Tenable, A. (n.d.). *https://www.tenable.com/products/tenable-io*. Retrieved from Tenable: https://www.tenable.com/products/tenable-io

Thomas, M. (n.d.). *8 Risks and Dangers of Artificial Intelligence to Know.* Retrieved from builtin Web Site: https://builtin.com/artificial-intelligence/risks-of-artificial-intelligence

Tim Hatton, C. E. (2022, June 7). *Cybersecurity Jobs Surging.* Retrieved from lightcast: https://lightcast.io/resources/blog/cybersecurity-jobs-surging

Xun Yi, R. P. (n.d.). *Homomorphic Encryption*. Retrieved from https://link.springer.com/chapter/10.1007/978-3-319-12229-8_2

Yagcioglu, S. (2020, May 18). *Classical Examples of Supervised vs. Unsupervised Learning in Machine Learning.* Retrieved from springboard: https://www.springboard.com/blog/data-science/lp-machine-learning-unsupervised-learning-supervised-learning/#:~:text=One%20practical%20example%20of%20supervised,houses%2C%20i.e.%20the%20corresponding%20labels.

Yıldırım, S. (2020, April 22). *DBSCAN Clustering — Explained*. Retrieved from towardsdatascience: https://towardsdatascience.com/dbscan-clustering-explained-97556a2ad556

Zenonos, A. (2022, December 13). *Artificial Intelligence and Data Protection*. Retrieved from Towards Data Science Web Site: https://towardsdatascience.com/artificial-intelligence-and-data-protection-62b333180a27