Werkplan Masterproef

Titel	Federated Learning for Intrusion Detection in Distributed Systems: Privacy and Security Challenges
Naam Student	Ilkay Yuksel
Email	Ilkay.yuksel@ugent.be; ilkay.yuksel.27@live.be
Bedrijf/ Onderzoeksgroep	IDLab, Vakgroep informatietechnologie (INTEC), Faculteit Ingenieurswetenschappen en Architectuur (FEA), Universiteit Gent
Promotoren	prof. dr. Bruno Volckaert prof. dr. ir. Filip De Turck
Begeleiders	Miel Verkerken Laurens D'hooge dr. ir. Tim Wauters

Opsplitsing per semester:

	Semester 1	**Semester 2**
# studiepunten vakken	24	18 (incl. 6SP bedrijfsstage)
# studiepunten masterproef	6	12

Bestaande situatie en probleemstelling

In de huidige wereld van cybersecurity zijn intrusiedetectie- en preventiesystemen (IDS/IPS) essentiële hulpmiddelen die worden gebruikt om informatiesystemen te beschermen tegen kwaadaardige activiteiten. Deze systemen spelen een cruciale rol bij het identificeren en reageren op potentiële bedreigingen, en zorgen voor de beveiliging en integriteit van digitale middelen.

Traditionele IDS/IPS-oplossingen maken doorgaans gebruik van een op misbruik gebaseerde aanpak, die afhankelijk is van vooraf gedefinieerde regels en handtekeningen om bekende aanvalspatronen te detecteren. Hoewel deze systemen effectief zijn geweest bij het bestrijden van bekende bedreigingen, hebben ze vaak moeite om zich aan te passen aan nieuwe en evoluerende aanvalstechnieken. Deze beperking is te wijten aan hun statische aard, aangezien ze afhankelijk zijn van een database met bekende aanvalspatronen, waardoor ze minder effectief zijn tegen zero-day-aanvallen en andere nieuwe beveiligingsbedreigingen.
Bovendien zijn de conventionele IDS/IPS-oplossingen voornamelijk gecentraliseerd van opzet. Ze opereren vanuit één locatie, waar ze gegevens verzamelen en analyseren vanuit verschillende bronnen binnen het netwerk. Deze gecentraliseerde aanpak heeft enkele inherente nadelen, met name in de context van gedistribueerde systemen. Deze problemen omvatten:

1. **Schaalbaarheid**: In gedistribueerde systemen kan de hoeveelheid gegenereerde gegevens enorm zijn, waardoor het uitdagend is om alle gegevens centraal en in realtime te verwerken.
2. **Vertraging**: De vertraging bij het verzenden van gegevens van verschillende bronnen naar een centrale locatie kan leiden tot verhoogde latentie, wat de responsiviteit van het systeem op bedreigingen kan beïnvloeden.
3. **Privacyzorgen**: Gecentraliseerde systemen vereisen vaak het verzamelen van gegevens vanuit verschillende bronnen, wat privacyzorgen en het risico van blootstelling van gevoelige informatie met zich meebrengt. Dit wordt nog kritischer nu gegevensprivacyregelgeving, zoals de GDPR, strenger is geworden.
4. **Eén Punt van Uitval**: Een gecentraliseerd IDS/IPS vertegenwoordigt een enkel punt van uitval in het netwerk. Als het centrale systeem wordt gecompromitteerd, kan dit catastrofale gevolgen hebben voor de algehele netwerkbeveiliging.

Het onderzoeksprobleem in deze context is dat bestaande IDS/IPS-systemen, met name in gedistribueerde omgevingen, moeten evolueren om deze uitdagingen het hoofd te bieden. Met de verschuiving van de focus naar anomalie-gebaseerde detectie zijn machine learning-technieken naar voren gekomen als een veelbelovende oplossing. Traditionele machine learning-benaderingen staan echter ook voor uitdagingen in gedistribueerde systemen vanwege privacyzorgen en de noodzaak van gecentraliseerde gegevensaggregatie.

Om deze kwesties aan te pakken, beoogt het onderzoek de toepassing van federated learning te onderzoeken als een innovatieve aanpak voor intrusiedetectie in gedistribueerde systemen. Federated learning is een machine learning-techniek die modeltraining op gedistribueerde apparaten mogelijk maakt zonder de gegevens te centraliseren. Het pakt de privacyzorgen aan die gepaard gaan met gecentraliseerde gegevensverzameling, terwijl het mogelijk effectievere en aanpasbare intrusiedetectiemogelijkheden biedt. Het doel is om een federated learning-systeem te ontwerpen en ontwikkelen dat is afgestemd op de specifieke behoeften van intrusiedetectie, met de nadruk op effectiviteit, privacy en beveiliging.

Het onderzoek zal ook het benchmarken van dit op federated learning gebaseerde systeem voor intrusiedetectie tegen traditionele gecentraliseerde benaderingen omvatten om de

generalisatiekracht en mogelijke voordelen ervan te beoordelen. Hiermee beoogt dit onderzoek waardevolle inzichten te bieden in de toekomst van intrusiedetectie en -preventie in de context van gedistribueerde systemen, met speciale nadruk op privacy en beveiliging.

Doelstelling van de masterproef

Hieronder wordt in een notendop uitgelegd wat de doelstelling is van mijn masterthesis. Momenteel heb ik paar onderzoeksvragen kunnen uitpikken, maar dit zal naarmate de bevordering van mijn literatuurstudie nog veranderen en concreter worden. Ook mijn planning en mijlpalen zullen veranderen. Deze zullen pas definitief worden eens ik klaar ben met mijn literatuurstudie en dus mijn onderzoeksvraag heb vastgelegd.

Deze masterproef heeft tot doel de privacy- en beveiligingsaspecten van federated learning (FL) in het kader van intrusiedetectie te onderzoeken en aan te pakken. FL is een veelbelovende techniek die modeltraining mogelijk maakt over gedistribueerde apparaten zonder gegevens te centraliseren. Het wordt steeds relevanter gezien de privacygevoelige aard van de gegevens die worden gebruikt voor intrusiedetectie. Het onderzoek zal zich richten op twee belangrijke gebieden: het hercreëren van datasets op basis van doorgegeven modelparameters en federated poisoning attacks.

Onderzoeksvragen

1. **Privacy van Federated Learning**: Hoe kunnen externe partijen gevoelige gegevens hercreëren door de parameters die worden doorgegeven aan het centrale model? Welke methoden kunnen worden gebruikt om deze privacyrisico's te verminderen of te voorkomen, bijvoorbeeld via blockchain-technologie?
2. **Federated Poisoning Attacks in IDS**: Hoe kunnen federated poisoning attacks de integriteit van FL-gebaseerde intrusiedetectiesystemen beïnvloeden? Hoe kunnen deze aanvallen worden gedetecteerd en voorkomen?

Onderzoeksopzet

1. **Privacy van Federated Learning**:
    - Verdieping in de technische aspecten van federated learning en de gegevensuitwisseling tussen deelnemende modellen en het centrale model.
    - Identificatie van potentiële kwetsbaarheden en privacyrisico's in FL-gebaseerde intrusiedetectie, met een focus op het hercreëren van datasets.
    - Onderzoek naar mogelijke oplossingen om deze privacyrisico's te verminderen of te elimineren, zoals het gebruik van blockchain, differentiële privacy, of versleutelingstechnieken.
    - Experimenten om de effectiviteit van de voorgestelde oplossingen te meten met betrekking tot privacybehoud.
2. **Federated Poisoning Attacks in IDS**:
    - Diepgaand begrip van federated poisoning attacks en hun potentiële impact op FL-gebaseerde intrusiedetectie.
    - Ontwikkeling van strategieën om federated poisoning attacks te detecteren en te mitigeren, inclusief het gebruik van machine learning-algoritmen voor het identificeren van kwaadaardige deelnemers.
    - Evaluatie van de effectiviteit van de voorgestelde aanpak in realistische FL-gebaseerde intrusiedetectiescenario's.

Verwachte Resultaten

Dit onderzoek zal naar verwachting leiden tot:

- Een diepgaand begrip van de privacy- en beveiligingsuitdagingen binnen FL voor intrusiedetectie.
- Een reeks aanbevelingen en oplossingen voor het behoud van privacy in FL-gebaseerde IDS.

- Een strategie voor het detecteren en voorkomen van federated poisoning attacks in FL-gebaseerde IDS.

Methodologie
Dit onderzoek zal een combinatie van literatuuronderzoek, theoretische analyse en praktische experimenten omvatten. De experimenten zullen worden uitgevoerd op real-world of gesimuleerde datasets en FL-gebaseerde intrusiedetectiesystemen. De analyse van de resultaten zal de effectiviteit van de voorgestelde oplossingen aantonen en mogelijkheden bieden voor verdere verbeteringen.

Conclusie
Dit onderzoeksvoorstel heeft tot doel bij te dragen aan de ontwikkeling van privacy- en beveiligingsmaatregelen in federated learning voor intrusiedetectie. Het zal waardevolle inzichten verschaffen in het omgaan met privacy-uitdagingen en het voorkomen van federated poisoning attacks in een gedistribueerde omgeving. Deze masterproef is van groot belang, gezien de voortdurende relevantie van cybersecurity en privacybescherming in moderne informatiesystemen.

Planning en mijlpalen

Taak 1	2 weken	*Deadline:* 8 oktober 2023	**Infosessie masterthesis, eerste meeting met begeleider, informatie verzamelen**
Inhoud Infosessie over masterthesis gehad, gesprek gehad met begeleider over de aanpak ervan, verder ook nog de website https://masterproef.tiwi.ugent.be verkent (verplichte taken opgeschreven, templates gedownload, logboek bijhouden etc.), mail met literatuurlijst grondig bekeken.			
Belangrijkste resultaten, deliverables of inzichten na deze fase: Een goed overzicht van het verloop van mijn literatuurstudie.			

Taak 2	1,5 weken	*Deadline:* 20 oktober 2023	**Eerste literatuurstudie en technologieverkenning (~10 papers)**
Inhoud Wetenschappelijke artikelen opzoeken en samenvatten over het onderwerp machine learning x intrusion detection systems, cursus van Jeremy Howard volgen, meeting met begeleider gehad (meer uitleg over intrusion detection en algemeen info over papers gekregen)			
Belangrijkste resultaten, deliverables of inzichten na deze fase: Eerste versie van de literatuurstudie, opsomming van de belangrijkste bestaande technieken, weten hoe een paper gelezen moet worden.			

Taak 3	1 week	*Deadline:* 20 oktober 2023	**Werkplan opstellen en indienen**
Inhoud Een grondig werkplan opstellen, wat gediend zal worden als een houvast, maar kan in de loop van de tijd zeker nog veranderen waarschijnlijk.			
Belangrijkste resultaten, deliverables of inzichten na deze fase: Administratief in orde zijn, deadline respecteren			

Taak 4	4 weken	*Deadline:* 19 november 2023	**literatuurstudie en technologieverkenning (~30 papers)**

Inhoud

Allerlei papers lezen over het onderwerp Federated Learning x Intrusion Detection Systems, weten wat al onderzocht is en wat niet, weten welke methodes bestaan om aanvallen te detecteren bijvoorbeeld, onderzoeksvragen opstellen, papers met elkaar linken en op die manier een verhaal maken, cursus van Jeremy Howard volgen.
Meeting met begeleider om vragen te stellen over mijn literatuurstudie en onderzoeksvraag.

Belangrijkste resultaten, deliverables of inzichten na deze fase:

Interessante onderzoeksvragen worden opgesteld en besproken met de begeleider, eigen onderzoeksvraag kiezen, kennis over Federated Learning uitbreiden

Taak 5	4 weken	*Deadline:* 10 december 2023	**Implementatie van basis zaken en laatste papers lezen**

Inhoud

Grondige studie naar beschermingstechnieken die relevant zijn voor federated learning in het kader van intrusion detection, In deze taak wordt een grondige studie uitgevoerd naar privacybeschermingstechnieken die relevant zijn voor federated learning binnen het domein van intrusion detection. Het begint met de identificatie en evaluatie van verschillende privacybeschermingstechnieken, zoals differentiële privacy, federated learning met beveiligde aggregatie en homomorfe encryptie.

Alle interessante papers zijn ondertussen gelezen, cursus van Jeremy Howard afwerken, tutorials over Federated Learning bekijken (vooral implementatie daarvan), datasets analyseren, op basis van literatuurstudie en gekozen onderzoeksvraag basis zaken realiseren zoals framework opstellen, trainen, parameters doorgeven, aanvallen voorzien, trap weights, schalen,

Belangrijkste resultaten, deliverables of inzichten na deze fase:

Een basis notebook met paar experimenten, framework opgesteld, resultaten geanalyseerd

Taak 6	1 week	*Deadline:* 17 december 2023	**Tussentijds presentatie**

Inhoud

Grondige voorbereiding van presentatie over literatuurstudie, implementatie, methodes, voorlopige analyses
Meeting met begeleider om vragen te stellen over deze presentatie en over mijn notebook

Belangrijkste resultaten, deliverables of inzichten na deze fase:

Feedback over mijn werk, analyses gemaakt over technieken en technologieën

Taak 7	8 weken	*Deadline:* 31 maart 2024	**Eerste 25 bladzijden van scriptie**

Inhoud

Schrijven van een introductie en het volledige afwerken van de literatuurstudie. Een eerste deel van de scriptie wordt afgegeven aan de begeleiders en promotoren.

Belangrijkste resultaten, deliverables of inzichten na deze fase:

Introductie en bespreking van mijn literatuurstudie

Taak 8	6 weken	*Deadline:* 15 maart 2024	**Uitvoeren van experimenten met Privacybescherming**

Inhoud

Na een zorgvuldige selectie van de meest geschikte privacybeschermingstechnieken, zal de implementatie in het federated learning-model worden uitgevoerd. Experimenten worden uitgevoerd om de effectiviteit van deze technieken in het beschermen van de privacy van de gegevens te beoordelen. Deze taak omvat praktische experimenten waarbij privacybeschermingstechnieken worden toegepast op het federated learning-model. Het begint met de implementatie van geselecteerde privacybeschermingstechnieken in het model. Ook zullen deze getest worden Geschikte datasets met gevoelige informatie worden geselecteerd en gebruikt voor experimenten. Vervolgens worden een reeks experimenten uitgevoerd om de impact van de toegepaste technieken op de gegevensprivacy en de prestaties van het model te beoordelen.

Belangrijkste resultaten, deliverables of inzichten na deze fase:

Het doel is om te begrijpen hoe deze technieken werken en welke voordelen ze bieden in termen van gegevensprivacy, hiervan wordt een analyse gemaakt.

Taak 9	3 weken	*Deadline:* 24 maart 2024	**Analyseren van de resultaten**

Inhoud

- Het analyseren van de resultaten van de experimenten waarbij privacybeschermingstechnieken zijn toegepast op het federated learning-model.
- Evaluatie van de effectiviteit van deze technieken in het beschermen van de privacy van de gegevens.
- Beoordeling van de impact van de toegepaste technieken op zowel gegevensprivacy als de prestaties van het model.

Belangrijkste resultaten, deliverables of inzichten na deze fase:

- Inzicht in hoe effectief de privacybeschermingstechnieken zijn in het beveiligen van gevoelige informatie binnen het federated learning-model.
- Het beoordelen van eventuele prestatie-impact van de toegepaste technieken.
- Mogelijke aanpassingen aan de technieken om de balans tussen privacybescherming en modelprestaties te optimaliseren.
- Rapporten en documentatie die de bevindingen en resultaten van de privacybeschermingsexperimenten samenvatten.

Taak 10	3 weken	*Deadline:* 10 mei 2024	**Visualisatie van de experimenten en resultaten**

Inhoud

- Creëren van visuele representaties van de experimenten en hun resultaten.
- Grafische weergave van gegevensprivacy-maatregelen en prestatie-indicatoren na toepassing van de privacybeschermingstechnieken.

Belangrijkste resultaten, deliverables of inzichten na deze fase:

- Grafieken, diagrammen of andere visuele hulpmiddelen die de impact van de privacybeschermingstechnieken op gegevensprivacy en modelprestaties illustreren.
- Deze visualisaties kunnen helpen bij het communiceren van de resultaten aan belanghebbenden, zoals teamleden, management en stakeholders.
- Het vergemakkelijkt de interpretatie van complexe gegevens en benadrukt eventuele patronen of trends die zijn waargenomen tijdens de experimenten.

Taak 11	4 weken	*Deadline:* 30 april 2024	**Scriptie 55% voltooid**

Inhoud

Extende abstract, abstract, introductie, literatuurstudie, methodologie volledig af

Belangrijkste resultaten, deliverables of inzichten na deze fase:

Gevorderde scriptie

Taak 12	4 weken	*Deadline:* 25 mei 2024	**Scriptie 95% voltooid**

Inhoud

Script bijna afgewerkt, enkel aan bijzaken werken, onderzoeksvraag zo goed als beantwoord. Resultaten, discussie, conclusie volledig af.
Scriptie 1e versie (95%) voorleggen aan promotoren/begeleiders

Belangrijkste resultaten, deliverables of inzichten na deze fase:

Gevorderde scriptie, Onderzoeksvraag wetenschappelijk zo goed als beantwoord.

Taak 13	2 weken	*Deadline:* 6 juni 2024	**Scriptie indienen**

Inhoud

Scriptie volledig afgewerkt, voldaan aan alle voorwaarde kwa layout, regels etc.

Belangrijkste resultaten, deliverables of inzichten na deze fase:

Onderzoeksvraag wetenschappelijk beantwoord.

Taak 14	3 weken	*Deadline:* 28 juni 2024	**Openbare verdediging**
Inhoud Op Plato volgende documenten indienen: • logboek/e-mailrapportering • presentatie Grondig voorbereiden, meeting begeleider over hoe dit in elkaar zit			
Belangrijkste resultaten, deliverables of inzichten na deze fase: Verdedigingsvaardigheden, afgestudeerd, feedback en discussie, eindbeoordeling			

Contactmomenten

In het eerste semester zal de tweewekelijkse tussentijdse communicatie plaatsvinden via e-mail of Teams, waarbij de student vragen kan stellen en ook kan rapporteren over zijn of haar voortgang in die twee weken.

In het tweede semester zal de student voornamelijk in de IGent Tower werken, waar begeleiders fysiek aanwezig zullen zijn voor vragen. Daarnaast zal de communicatie, zoals in het eerste semester, plaatsvinden via Teams.

Gantt chart:

Taken =>	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Week 1	X													
Week 2	X													
Week 3		X												
Week 4		X	X											
Week 5				X										
Week 6				X										
Week 7				X										
Week 8				X										
Week 9					X									
Week 10					X									
Week 11					X									
Week 12						X								
Week 13														
Kerstvakantie														
Examenperiode januari														
Week 1							X	X						
Week 2							X	X						
Week 3							X	X						
Week 4							X	X			X			
Week 5							X	X	X		X			
Week 6							X		X		X			
Week 7							X		X	X	X			
Week 8							X			X		X		
Week 9										X		X		
Week 10												X		
Week 11												X		
Week 12													X	
Week 13													X	
Week 14														X
Week 15														X
Week 16														X