РЕЦЕНЗИЯ

от проф. Радослав Даков Йошинов
Институт по Математика и информатика при БАН
член на Научното жури, назначена от Ректора на Варненския свободен университет „Черноризец Храбър“ със заповед № 892 от 28 ноември 2025 г.

относно дисертация на ALI MOHAMAD SABRA
на тема “Deep Learning Approach for Modeling DDoS Attacks in Cybersecurity”
представена за придобивана на образователна и научна степен „Доктор“ по докторска програма “Информационни системи и технологии, компютърни науки и компютърни науки”, професионално направление 4.6. “Информатика и компютърни науки”

На първото заседание на научното жури, проведено на 5 декември 2025 г., бях избран да изготвя рецензия по процедурата. Като член на научното жури съм получил:

1. Дисертация за присъждане на образователната и научна степен “доктор”;
2. Автореферат на дисертацията;
3. Копия на статиите, включени в дисертационния труд;
4. Справка за изпълнение на минималните изисквания на ВСУ „Черноризац Храбър“ за придобиване на образователната и научна степен “доктор”.
5. Други съпътстващи процедурата документи.

Определящи при оценка на дисертацията, са условията на Закона за развитие на академичния състав в Република България (ЗРАСРБ),

Правилника за прилагането му и Правилника за специфичните условия във Варненски свободен университет „Черноризец Храбър“.

Съгласно Правилника за прилагане на ЗРАСРБ:

Чл. 27. (1) (Нов – ДВ, бр. 19 от 2011 г., в сила от 08.03.2011 г.) Дисертацията трябва да съдържа научни или научно-приложни резултати, които представляват оригинален принос към науката. Дисертацията трябва да показва, че кандидатът притежава задълбочени теоретични познания по съответната специалност и способности за самостоятелни научни изследвания.

(2) (Предишен текст на чл. 27 – ДВ, бр. 19 от 2011 г., в сила от 08.03.2011 г.) Дисертацията трябва да бъде представена във форма и обем, съответстващи на специфичните изисквания на основната дисциплина. Дисертацията трябва да съдържа: заглавна страница; съдържание, въведение; изложение; заключение – обобщение на получените резултати с декларация за оригиналност; библиография.

АКТУАЛНОСТ

DDoS атака, или разпределена атака за отказ от услуга, е злонамерен опит за нарушаване на нормалното функциониране на целеви сървър, услуга или мрежа чрез претоварване с поток от интернет трафик. Моделирането на такива атаки е критична практика в киберсигурността. Атака с DDoS включва множество компрометирани компютърни системи, които се използват за изпращане на огромен обем заявки към целта. Този прилив на трафик може да претовари ресурсите на целта, правейки я неспособна да отговаря на легитимни заявки. По същество, това е като задръстване, което блокира магистрала, предотвратявайки нормалния трафик да достигне до своята дестинация. DDoS моделирането помага на екипите по сигурността да анализират вектори на атака (обемни, протоколни, на ниво приложение), модели на трафик и аномалии, координация на нападателите и поведение на ботнет мрежите. DDoS моделите също така помагат за оценка на

максималното натоварване на трафика, точките на изчерпване на ресурсите и праговете на влошаване на услугите. Това позволява по-добро мащабиране на инфраструктурата, планиране на резервирането и гаранции за наличност на услугите. Съвременните DDoS атаки се адаптират динамично. Моделирането предоставя етикетирани набори от данни за обучение на ML модели, реалистични модели на трафик за тестване и враждебни сценарии за AI срещу AI защитни системи. Извършването на DDoS моделиране позволява откриване въз основа на поведение на системата, , идентифициране на аномалии, подкрепя проактивна, а не реактивна защита. То подпомага за изграждането на интелигентни защитни системи, придава киберустойчивост на тези системи и ги поставя в съответствие с регулаторните изисквания, . Описаното по-горе доказва актуалността на дисертационното изследване.

ПОЗНАВАНЕ НА ИЗСЛЕДОВАТЕЛСКИЯ ПРОБЛЕМ

За това съдя по направения обзор и по публикационната дейност на докторанта отразена в публикуваните по дисертацията материали. Докторантът убедително представя постигнатите резултати, с много добра и задълбочена аргументация, както и използва професионално графично оформление на материалите. Като допълнително доказателство за това могат да се използват представените приложения, документиращи подробности за имплементацията на LSTM-базиран модел с Conv1D, нормализиране на партиди, планиране на скоростта на обучение и ранно спиране, използвани за откриване на DDoS атаки на приложно ниво от лог файлове за достъп до уеб сървър.

Считам, че докторантът се е справил успешно, като не поставям под съмнение личното и участие в разработването на дисертационния материал.

АНАЛИТИЧНИ ХАРАКТЕРИСТИКА

Дисертационният труд на Ali Mohamad Sabra се състои от 118 страници, 23 фигури, 5 таблици, както и 77 литературни източника, цитирани в материала. Трудът е структуриран, както следва: благодарности, резюме, три

глави, заключение, обобщение на резултатите, бъдещи насоки, списък с публикации, библиография и 4 приложения. Основната цел на дисертацията е формулирана както следва „Да се разработи и оцени интелигентна система за откриване на DDoS атаки на приложно ниво, използвайки модели за машинно обучение и дълбоко обучение, обучени върху реални регистрационни файлове за достъп до уеб сървъри". За постигане на тази цел докторантът е формулирал пет задачи, както следва:

1. Да се създаде реалистичен набор от данни, комбиниращ доброкачествен и злонамерен уеб трафик, генериран от различни DDoS инструменти.

2. Да се извърши предварителна обработка и да се създадат релевантни характеристики от сървърните логове за обучение на модела.

3. Да се обучат и сравнят ML и DL алгоритми за прецизно откриване на DDoS атаки, като се минимизират фалшивите положителни резултати.

4. Да се тестват обучените модели върху други видове атаки (например SQL Injection, XSS), за да се оцени тяхната генерализация.

5. Да се оцени интерпретируемостта на модела чрез SHAP анализ и да се предложи рамка за реална интеграция. Структурата на дисертацията е твърде фрагментирана, с раздели, които предимно увеличават обема, но без да добавят научна стойност.

Предвид актуалността на изследвания проблем, са налични голям брой публикации, много от които авторът не цитира. Освен това, представената библиография не следва единен стандарт.

АВТОРЕФЕРАТ И АВТОРСКА СПРАВКА

Представеният проект за автореферат е в съответствие с правилника за изготвяне на авторефератите по дисертационните трудове във Варненския свободен университет „Черноризец Храбър". Авторефератът е съобразен с изискванията на Закона за развитие на академичния състав в Република България (ЗРАСРБ) и Правилника за неговото прилагане. Авторефератът отразява същността и постигнатите резултати, както и приносите на автора.

Графично е оформен много добре и включва необходимата информация, описваща в резюме дисертационния труд. Докладът от проверката в платформата Strikeplagiarism.com показа, че коефициентът на сходство 1 е 2,02%, а коефициентът на сходство 2 е 0,00%, което потвърждава оригиналността на резултатите от проведеното изследване.

ОЦЕНКА НА СЪОТВЕТСТВИЕТО С МИНИМАЛНИТЕ НАЦИОНАЛНИ ИЗИСКВАНИЯ И С ДОПЪЛНИТЕЛНИТЕ ИЗИСКВАНИЯ НА ПРАВИЛНИКА ЗА ПРИЛАГАНЕ НА ЗРАСРБ

По дисертационния труд са представени 6 публикации, 5 от които са публикувани, а една е приета за публикуване. Три от публикациите са индексирани в Световната база данни за научна информация Scopus. Всички публикации са в съавторство, като следва да се отбележи, че на две от публикациите докторантът е първи автор. Съгласно Правилника за прилагане на LDASPB, тези публикации носят на докторанта 54 точки, което надвишава, както минималните национални изисквания, така и специфичните изисквания на ВСУ „Черноризец Храбър“, който е, както следва 30 точки за образователната и научна степен „Доктор“.

КРИТИЧНИ КОМЕНТАРИ И ПРЕПОРЪКИ

Нямам критични забележки към дисертационния материал. Разработката предполага достатъчно задълбочени знания, възможност за интерпретация и подобряване на разграничаването между доброкачествен и злонамерен трафик на приложенията, както и формулиране на стратегии за ефективно развитие на областта. Използването на изкуствен интелект чрез SHAP-базирана интегрпруемост, е пример за това. Съдържателно и графично материалът е разработен много добре. Този материал представлява интерес за широк кръг читатели и ако след преработка се публикува ще има мултипликативен ефект.

Препоръчам на докторанта да има по-активната публикационна дейност в научни списания с импакт фактор.

Препоръчвам по-кратка вербализация от докторанта на неговите постижения - да се научи ясно и стегнато да излага своите постижения.

Някои не съществени забележки съм отразил върху копието, което ми бе предоставено.

ПРИНОСИ

По-съществените резултати, получени в дисертационната работа, са обобщени в авторски претенции за три научно-приложни и приложни приноса:

Предложен е емпиричен методологичен подход, който комбинира усъвършенствани техники за машинно обучение (ML) и дълбоко обучение (DL) за откриване на DDoS атаки на приложното ниво (OSI model),

Така предложеният модел е адаптиран за уеб трафик.

Разработена е методология базирана на фрейм (рамка) „Междуиндустриален стандартен процес за извличане на данни“.

В рамките на тази методологията се отчитат приоритетно протичащите процеси, следвано от отчитане на използваните данни във фазите на тяхната подготовка, моделиране, оценка и внедряване.

Приемам така формулираните приноси от докторанта,.

ВЪПРОСИ ПО ДИСЕРТАЦИЯТА

1. В какво се изразява същността на предложения подход за се отчитат приоритетно протичащите процеси, последвано от отчитане на използваните данни
2. Как предложеният модел е адаптиран за уеб трафик.

ВЪЗМОЖНОСТИ ЗА ИЗПОЛЗВАНЕ НА ПОЛУЧЕНИТЕ РЕЗУЛТАТИ

В цялостното развитие на дигиталното общество през последните години се проявява дигиталната трансформация на индустрията – резултат от на

растващото проникване на Интернет на нещата (IoT), роботиката, процеси и данни, облачните решения и когнитивните технологии, базирани на изкуств ен интелект.

ЗАКЛЮЧИТЕЛНА КОМПЛЕКСНА ОЦЕНКА

Съдържанието и приносите на дисертационния труд на магистър ALI MOHAMAD SABRA, напълно покрива изискванията на Закона за развитие на академичния състав на Република България, на Правилника за неговото приложение и на Правилника за условията и реда за придобиване на научни степени във ВСУ "Черноризец Храбър". Извършена е значителна по обем и съдържание изследователска работа. Има достатъчен брой научно-приложни и приложни приноси. Представени са достатъчен брой публикации по дисертацията публикувани на престижни научни форуми. Покрит е образователният докторантски минимум, заложен в индивидуалния план. Безспорно е личното участие на докторанта в разработката и получените приноси. Получените резултати по темата на дисертационното изследване ми дават достатъчно основание да дам положителна оценка на представената дисертация. Това ми дава основание убедено да препоръчам на Уважаемото Научно жури да присъди на ALI MOHAMAD SABRA образователната и научна степен „доктор" в докторската програма „Информационни системи и технологии, компютърни науки и компютърни науки", професионално направление 4.6. „Информатика и компютърни науки".

15.01.2025 Рецензент:

/проф. Радослав Йошинов/