Варненски свободен университет „Черноризец Храбър“

Факултет "Социални, стопански и компютърни науки"

Катедра "Компютърни науки"

СТАНОВИЩЕ

от проф., д-р, инж. Юлиян Иванов Цонев
за дисертационен труд на тема: “Deep Learning Approach for Modelling DDoS Attacks in Cybersecurity” („Дълбоко учене при моделирането на DDOS атаки в киберсигурността“)
Автор: Али Мохамад Сабра
Професионално направление: 4.6. „Информатика и компютърни науки“
Докторска програма: „Информационни системи и технологии, информатика и компютърни науки“
Научен ръководител: доц. д-р Златогор Борисов Минчев

1. Актуалност на проблема.

На сегашния етап осигуряването на киберзащитеността на различни информационни и комуникационни системи е от първостепенно значение предвид нарастващия брой и сложност на провеждани кибератаки. Едни от трудните за откриване, анализ и противодействие са атаките от типа DDoS, които са обект на изследване в дисертационния труд.

Безспорно използването на machine learning (ML) and deep learning (DL) models би спомогнало за бързото и прецизно откриване на DDoS атаки и последващо противодействие. В тази връзка считам, че изследването на възможностите за използване и създаване на подходи за използване на machine learning (ML) and deep learning (DL) models за анализ и откриване на DDoS атаки е актуално и дисертабилно.

2. Обща оценка на съдържанието на дисертационния труд.

Предоставеният ми дисертационен труд е в общ обем от 118 страници. В началото са дадени списъци на използваните съкращения, фигури и таблици в дисертационния труд. В края на дисертационния труд са представени списък с направени публикации по темата, списък на използваната литература, приложения и декларация за оригиналност.

Основната част от дисертационния труд е организирана в последователна и логична поредица от четири глави, всяка от които постепенно развива и представя интелигентна система за откриване на DDoS атаки на приложно ниво, използвайки техники за машинно обучение и дълбоко обучение. Подредбата на главите логично преминава от основите на изследването до крайните резултати и заключението. Предложени са насоки за бъдещи изследвания и работа в областта.

В първа глава се обосновава актуалността на темата и необходимостта от детайлно анализиране на DDoS атаки. Параграф 1.3 уточнява целта и задачите на изследването в дисертацията. Според мен те са правилно формулирани и отговарят на темата на дисертационния труд. В параграф 1.5 е дефинирана коректно основната хипотеза в работата, която е конкретизирана с уточняващи 2 подхипотези. Доказването на хипотезата би потвърдило, че използването на усъвършенствани техники за обучение с автентични източници на данни ще подобри способностите за откриване на DDoS атаки и ще позволи на моделите да откриват различни уеб-базирани заплахи.

Във втора глава са представени съществуващите научни изследвания за DDoS атаките и използването на изкуствен интелект за тяхното откриване. Съществуващите подходи са критично оценени като са посочени пропуските в изследванията, свързани с липсата на реални данни и прекалената обобщеност на познатите модели.

В трета глава подробно е представен начина за получаване на експерименталните данни чрез комбинирането на легитимен нормален трафик и атаки от осем различни софтуера за DDOS атаки. Анализирани са протоколните файлове от Apache web сървър. Представени са структурата на различни модели за машинно обучение и дълбоко обучение като Random Forest, Support Vector Machine, Artificial Neural Networks, and Long Short-Term Memory networks.

В четвърта глава са обобщени получените резултати, посочени са научно-приложните и приложните приноси и са предложени бъдещи направления на изследване и продължаване на работата.

В обобщение бих посочил, че дисертационният труд е добре оформен и структуриран и логически издържан от идентифицирането на проблема до получаването на приложни резултати.

3. Научни и научно-приложни приноси на дисертационния труд.

В четвърта глава докторантът е формулирал авторовите си претенции за приноси. Същите приемам във вида:

Приноси с научно-приложен характер:

- създаден е подход за откриване на DDoS атаки на приложно ниво с използване на дълбоко обучение чрез данни от реални сървърни логове, пригоден за анализ на уеб трафик;

- анализирана е ефективността на ML и DL моделите за откриване на DDoS атаки на приложно ниво въз основа на реални данни от сървърни протоколни файлове;

- базиран на SHAP анализ е създаден AI слой, чрез който се постигат по прецизни резултати при откриването на DDoS атаки. Същият може да се използва и за откриване и на други видове атаки като SQL Injection, Cross-Site Scripting).

Приноси с приложен характер:

- разработена е система за откриване на DDoS атаки, която може да бъде интегрирана в реални среди за мониторинг и противодействие, отличаваща се с нисък процент на фалшиви положителни сработвания;

- създаден е реалистичен набор от данни чрез различни софтуери за атаки, позволяващ бъдещи изследвания и обучение;

- представена е среда за обучение и валидиране на модели за кибер-сигурност въз основа на реалистични набори от данни.

Считам, че една част от приносите на дисертационния труд са от тип обогатяване и потвърждаване на съществуващи знания, а друга част са от тип приложение на научни постижения в практиката.

4. Оценка на публикациите по дисертацията.

Посочени са 6 публикации, които са публикувани в различни специализирани издания. Считам, че същите са по темата на дисертационния труд. С тези 6 публикации се покриват изискванията на Правилник за прилагане

на Закона за развитие на академичния състав в Република България за изискуемия минимален брой от 30 точки по група критерии „Г“ за присъждане на ОНС „доктор“ в професионално направление 4.6 „Информатика и компютърни науки“.

5. Становище относно наличието на плагиатство

В края на работата е приложена „Declaration of Originality“ от автора на дисертационния труд Ali Sabra. На тази база, както и на факта, че не са получавани сигнали за плагиатство, считам, че в настоящата работа няма плагиатство и нямам съмнения за наличие на неетични авторски практики.

6. Критични бележки и препоръки.

Направените от мен критични бележки по време на предварителната защита са отстранени.

Препоръчвам продължаване на изследванията и периодично обновяване на набора от експериментални данни за обучение с използването на новоразработени софтуери за атаки. В допълнение, осигуряването на възможността за атакуване на web сървъра от лабораторната среда в параграф 3.2.2 не само от виртуалната среда, но и от публични IP адреси, би направило набора от данни напълно реалистичен.

8. Заключение

Считам, че представеният ми дисертационен труд е на добро академично ниво. Изложението е методично и логическо обосновано. Постигнати са конкретни резултати. Докторантът умее да анализира и обобщава постигнатите резултати и има необходимата научно теоретична и специална подготовка. Това ми дават основание да дам положителна оценка на представения дисертационен труд и да предложа на Научното жури да присъди на Али Мохамад Сабра образователната и научна степен „доктор“ по професионално направление 4.6 „Информатика и компютърни науки“, докторска програма „Информационни системи и технологии, информатика и компютърни науки “.

18.01.2026 г. Изготвил становището:

проф. д-р инж. /Ю.Цонев/

Digitally signed by : YULIYAN IVANOV TSONEV
Date : 26/01/19 00:19:09+0200
Compliant with eIDAS.