دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

اطلاعیه دفاع

نام دانشجو: علی کلاته عربی		**نام استاد راهنما: دکتر مجتبی وحیدی اصل**
مقطع: کارشناسی ارشد	**رشته: مهندسی کامپیوتر**	**گرایش: نرم افزار**
نوع دفاع: • **دفاع پروپوزال** □ • **دفاع پایان نامه** ■ • **دفاع رساله دکترا** □		**تاریخ: ۱۴۰۲/۷/۲۷** **ساعت: ۴ عصر** **مکان: کلاس ۱۱۷**
عنوان شناسایی بدافزار ترکیبی به وسیله تحلیل ایستا و پویا و روش های یادگیری ماشین		
داوران خارجی: دکتر سلیمان فلاح		**داوران داخلی: دکتر شاملی**

چکیده:

بدافزار یا همان نرم افزارهای مخرب، به هدف نقص عملکرد، دزدی اطلاعات و یا باج گیری و جاسوسی از سامانه های شخصی و شرکتی توسعه داده می شوند. مقابله با این نرم افزارهای مخرب و تضمین امنیت سامانه ها از مهم ترین زمینه های تحقیقات نرم افزاری می باشد. در این پژوهش سامانه تشخیص بدافزار با ترکیب روش های ایستای مبتنی بر بردار پاراگراف بدست آمده از درخت نحوی انتزاعی و پویای مبتنی بر جانمایی و طبقه کننده های هوش مصنوعی بر روی کدهای جاوااسکریپت توسعه داده شده است. هدف این سامانه مقابله با روش های پیشرفته مبهم سازی و فرار از تشخیص است که روند تشخیص بدافزار را بسیار سخت کرده اند. در سال های اخیر و با توجه به حساسیت و اهمیت روز افزون داده ها، امر تشخیص این قبیل بدافزارهای پیچیده و همچنین بدافزارهای جدیدی که الگو و ساختار دقیق آنها بدست نیامده، به جز حیاتی تحقیقات حوزه امنیت تبدیل شده است. تحقیق حاضر با ترکیب ویژگی های معنایی و ساختاری کدها در نظر دارد تا فراتر از ساختار و الگوهای ظاهری و مشخص رفته و ماهیت هر کد را مورد بررسی قرار دهد. ارزیابی های انجام شده خود نشان از موفقیت تحقیق حاضر دارند. در نظر گرفتن بردار بدست آمده از ترکیب برداری روش های ایستا و پویا نیز به ایجاد امضایی منعطف منجر شد که میتواند با سرعتی بالا بدافزارهای شناخته شده حتی در صورت ایجاد ظاهری جدید، کشف کند. در نهایت روش جنگل تصادفی توانست با ارائه دقت و صحتی در حدود ۹۹ درصد و نرخ مثبت کاذب ۰.۱ درصد، روش درخت تصمیم با دقت و صحت حدود ۹۵ درصد و نرخ مثبت کاذب ۱ درصد، که بر روی مجموعه داده ای جامع و متشکل از انواع مختلف بدافزار و فایل سالم بدست آمده است، نشان دهد روش حاضر توانایی بسیار خوبی برای مقابله با بدافزارها در هر نوع خانواده و با هر .نوعی از مبهم سازی را دارد