

اطلاعیه دفاع

نام دانشجو: ابراهیم فرجام فرد		نام استاد راهنما: دکتر علیرضا شاملی سندی	
مقطع: کارشناسی ارشد		رشته: مهندسی کامپیوتر	
نوع دفاع: <input type="checkbox"/> دفاع پروپوزال <input checked="" type="checkbox"/> دفاع پایان نامه <input type="checkbox"/> دفاع رساله دکترا		تاریخ: ۱۴۰۳/۷/۳۰	
		ساعت: ۰۹:۳۰ - ۰۷:۳۰	
		مکان: اتاق ۱۱۷ دانشکده برق و مهندسی کامپیوتر	
عنوان			
تشخیص ناهنجاری مبتنی بر گزارش‌های سیستمی با استفاده از شبکه‌های مولد رقابتی شرطی و ترنسفورمر			
داوران خارجی: دکتر سعید شکرالهی		داوران داخلی: دکتر مقصود عباسپور	
<p>چکیده:</p> <p>در دنیای امروز، سیستم‌های کامپیوتری با چالش‌های متعددی مواجه‌اند که از جمله آن‌ها می‌توان به تشخیص ناهنجاری‌ها اشاره کرد. ناهنجاری‌ها تغییرات غیرمنتظره و غیرعادی در رفتار سیستم‌ها هستند که ممکن است نشان‌دهنده وجود مشکلاتی چون خطاهای نرم‌افزاری، حملات سایبری، یا خرابی‌های سخت‌افزاری باشند. تشخیص به موقع این ناهنجاری‌ها می‌تواند از بروز خسارات جدی جلوگیری کند و عملکرد سیستم‌ها را بهینه سازد. هدف این پژوهش، ارائه روشی نوین برای تشخیص ناهنجاری‌ها با استفاده از گزارش‌های سیستمی و بهره‌گیری از شبکه‌های رقابتی مولد (GAN) است. روش‌های سنتی تشخیص ناهنجاری به دلیل وابستگی به الگوریتم‌های مبتنی بر امضا و ناتوانی در پردازش حجم بالای داده‌ها، کارایی محدودی دارند. این پژوهش با ارائه یک مدل مبتنی بر GAN، تلاش می‌کند تا این محدودیت‌ها را برطرف کند. در این مدل، از چارچوب Log2Vec برای تبدیل گزارش‌های سیستمی به بردارهای معنایی استفاده شده است که قادر به استخراج دقیق ویژگی‌های مربوط به ناهنجاری‌هاست. سپس، با استفاده از شبکه رقابتی مولد آموزش‌دیده، به بازسازی داده‌های ورودی پرداخته و در نهایت از توانایی مدل در بازسازی داده ورودی به عنوان شاخصی برای تشخیص ناهنجاری‌ها استفاده می‌کنیم.</p> <p>یکی از جنبه‌های نوآورانه این پژوهش، استفاده از GAN برای آموزش مدل بر روی داده‌های هنجار است که به دلیل قابلیت تولید داده‌های مشابه، می‌تواند به بهبود دقت و کاهش هشدارهای کاذب کمک کند. همچنین، مدل پیشنهادی با تمرکز بر کاهش پیچیدگی محاسباتی و افزایش سرعت پردازش، به طور موثری بر محدودیت‌های روش‌های قبلی غلبه کرده است.</p> <p>نتایج ارزیابی‌های انجام شده نشان می‌دهد که مدل پیشنهادی نه تنها نرخ دقت و یادآوری بالاتری در تشخیص ناهنجاری‌ها دارد، بلکه در کاهش هشدارهای کاذب نیز بهبود قابل توجهی را نسبت به روش‌های سنتی نشان می‌دهد. در مجموعه داده OpenStack، این مدل با دستیابی به نرخ دقت ۹۷٪ و یادآوری ۹۴٪، در مقایسه با مدل‌های شناخته‌شده‌ای مانند Deeplog، PCA و PRPCA-CS عملکرد بهتری نشان می‌دهد. همچنین در مجموعه داده HDFS نیز مدل ما به امتیاز F1 معادل ۹۲٪ دست یافته است که نسبت به هر دو مدل Trine و LogGAN بیشینه بوده و به واسطه معماری بهینه خود، از نظر زمان اجرا نسبت به مدل DeepLog برتری دارد.</p> <p>واژگان کلیدی: تشخیص ناهنجاری، یادگیری عمیق، تعبیه کلمات، شبکه‌های مولد رقابتی</p>			