دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

اطلاعیه دفاع

نام دانشجو: مریم‌السادات طبائی‌فرد		**نام استاد راهنما:** دکتر علی جهانیان
مقطع: کارشناسی ارشد	**رشته:** مهندسی کامپیوتر	**گرایش:** معماری سیستم‌های کامپیوتری
نوع دفاع: • **دفاع پروپوزال** □ • **دفاع پایان نامه** ☑ • **دفاع رساله دکترا** □		**تاریخ:** ۱۴۰۲/۰۴/۲۴ **ساعت:** ۱۲:۰۰ - ۱۴:۰۰ **مکان:** دانشکده مهندسی و علوم کامپیوتر
عنوان: حمله الگو به پردازنده قربانی با یادگیری با نظارت روی پردازنده مشابه		
داوران خارجی: دکتر مرتضی صاحب‌الزمانی		**داوران داخلی:** دکتر راضیه سالاری‌فرد

چکیده:

در دنیای ارتباطات امروز، حفاظت از داده‌های مهم بسیار حائز اهمیت است و دسترسی مهاجمان به این داده‌ها می‌تواند بسیار مخرب و حساس باشد. برای ارتقاء هرچه بیشتر امنیت داده‌های حیاتی، شناسایی قوی‌ترین حملات امری ضروری است. حملات کانال جانبی روشی مؤثر برای استخراج کلید رمزنگاری دستگاه است و با ورود روش‌های یادگیری عمیق به این حوزه حملات بسیار قوی‌تری بر روی دستگاه‌های قربانی انجام شده است ولی استفاده از یادگیری عمیق در حمله کانال‌های جانبی در صورت یکسان نبودن دستگاه نمایه و دستگاه مورد حمله با چالش‌هایی روبه‌رو است. در این نوع حمله، مرحله ایجاد نمایه روی دستگاهی که در اختیار مهاجم است انجام می‌شود و از مدل‌ها و وزن‌های به دست آمده از شبکه عصبی عمیق، به دستگاه دیگری که مشابه با دستگاه نمایه است حمله می‌شود که حتی در صورت مشابه بودن دستگاه‌ها، به دلیل وجود اختلاف بین فرایندهای آن‌ها، حمله با مشکل مواجه می‌شود .

در این پژوهش، روش جدیدی برای بهبود حملات کانال جانبی با استفاده از یادگیری عمیق در دستگاه¬های مشابه ارائه شده است. در این روش با بهره‌گیری از ترکیب پیش‌پردازش با فیلتر پایین¬گذر گاوسی و رمزگذار خودکار مبتنی بر یادگیری عمیق، داده‌ها پیش‌پردازش می‌شوند تا حمله با قدرت بیشتری انجام شود. نتایج حمله صورت‌گرفته روی ردیابی‌های ۶ دستگاه مشابه نشان می‌دهد که استفاده از روش پیش‌پردازش رمزگذار خودکار مبتنی بر یادگیری عمیق همراه با انتخاب لایه‌ها و پارامترهای مناسب، دقت حمله را تا میانگین ۷۰٪ افزایش می‌دهد و در راستای بهبود بیشتر دقت، استفاده از فیلتر پایین‌گذر گاوسی پیش از اعمال رمزگذار خودکار مبتنی بر یادگیری عمیق، منجر به افزایش این دقت تا میانگین ۸۲٪ و موفقیت در حمله با حداکثر ۳۰۰ ردیابی از دستگاه قربانی می‌گردد.

واژگان کلیدی: امنیت سخت‌افزار، حملات کانال جانبی، حملات یادگیری عمیق، حملات کانال جانبی بین دستگاهی