

## ارائه راه حلی جهت بهبود امنیت موبایل با استفاده از سیم کارت

معصومه فهیدصابر

کارشناسی ارشد رایانش امن دانشگاه شاهد-تهران

محمدعلی دوستاری

استادیار دانشگاه شاهد-تهران

### چکیده

با توجه به افزایش استفاده‌ی افراد از موبایل برای کاربردهای مختلف روزمره و به ویژه در زمینه‌های مربوط به تبادل داده‌های حساس، (مانند: ذخیره‌سازی و پردازش اطلاعات شخصی، برنامه‌های بانکی، پرداخت و سلامت الکترونیکی) برقراری امنیت در این وسیله به یک نیاز حیاتی در جهان تبدیل شده است. بیش از دو دهه است که در رایانه‌های شخصی و سرویس‌دهنده‌ها از فناوری محاسبات مورد اعتماد و فناوری‌های تأمین‌کننده‌ی آن مانند ماژول TPM برای حفظ یکپارچگی دستگاه در برابر حملات نرم افزاری استفاده می‌شود. با این وجود، پیاده‌سازی کارکرد TPM در دستگاه‌های موبایل به دلیل کمبود فضا، کمبود قدرت پردازشی و مصرف زیاد توان با چالش‌های از لحاظ کارایی و امنیتی مواجه است. در این پژوهش، ماژول سیم‌کارت و فضای ابری اپراتورهای دستگاه موبایل، به عنوان راه حلی برای پیاده‌سازی سخت‌افزاری کارکرد TPM در دستگاه‌های موبایل مورد بررسی قرار گرفته است. در این مقاله ابتدا مروری بر مفاهیم محاسبات مورد اعتماد و تلاش‌های صورت گرفته توسط برخی شرکت‌ها جهت پیاده‌سازی این فناوری در موبایل صورت پذیرفته است. در ادامه راه حل پیشنهادی مبتنی بر سیم‌کارت و ابر مورد اعتماد اپراتور موبایل بیان شده و پروتکل‌های امنیتی پیشنهادی (جهت ارتباط اولیه و احراز هویت بین موجودیت‌ها) با استفاده از زبان رسمی Proverif شبیه‌سازی شده است. در آخر، راه‌حل پیشنهادی با راه‌حل‌های مشابه در این زمینه، از لحاظ جنبه‌های برتری و نکات ضعف مورد مقایسه قرار گرفته است.

**واژگان کلیدی:** امنیت سخت‌افزاری موبایل، امنیت موبایل، سیم‌کارت، محاسبات ابری موبایل، برنامه‌های امن موبایل.