به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

معرفی مفهوم محاسبات وارسی پذیر

An introduction to verifiable computations

سمیه دولت نژاد

زمان: شنبه ۱۶ بهمن ۱۳۹۵ ساعت ۹:۱۵

مکان: دانشگاه صنعتی شریف، دانشکده مهندسی کامپیوتر، طبقه چهار، سالن خوارزمی

امروزه استفاده از ابر عمومی برای برون‌سپاری محاسبات و داده، به شدت موردتوجه قرارگرفته است. در محاسبات برون‌سپاری‌شده، نحوه‌ی انجام محاسبات از دید کارخواه کاملا پنهان است و کارخواه هیچ کنترلی بر آن ندارد. لذا این سوال و نگرانی برای استفاده‌کنندگان از سرویس‌های محاسباتی ابر همواره مطرح است که چگونه می‌توان به این سرویس اعتماد کرد. به عنوان مثال، فراهم‌کننده سرویس برای کاهش استفاده از منابع خود، می‌تواند محاسبات یا بخشی از آن را انجام ندهد و به شکل کاملا ساده‌ای یک خروجی تصادفی را در اختیار کارخواه قرار دهد. همچنین ممکن است گره‌های انجام دهنده‌ی محاسبه در محیط ابری، آلوده به بدافزار باشند و مهاجم نتایج یا داده‌های استفاده‌شده در حین محاسبه را تغییر دهد؛ بنابراین نیاز است کارخواه از صحت انجام محاسبات اطمینان یابد.

محاسبات وارسی‌پذیر مفهوم جدیدی است که سعی دارد با کمترین سربار پردازشی، تضمینی را در رابطه با صحت نتایج حاصل از محاسبات برون‌سپاری‌شده فراهم کند. در این نوع از محاسبات، سرویس‌دهنده در کنار نتایج حاصل از انجام محاسبه، اثباتی را نیز در اختیار کارخواه قرار می‌دهد و کارخواه با استفاده از اثبات، درستی انجام محاسبه را بررسی می‌کند. در این ارائه مفهوم محاسبات وارسی‌پذیر معرفی و دید سطح بالایی در رابطه با سیستم‌های اثباتی موجود در این حوزه، ارائه خواهد شد.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.