دانشکده مهندسی برق

۲۶۹

جلسه دفاعیه از پایان نامه کارشناسی ارشد

ایجاد قابلیت پاسخگویی وحفظ حریم خصوصی در سیستم مدیریت هویت دیجیتال مبتنی بر بلاکچین با استفاده از دانش صفر تقویت‌شده

فقدان حریم خصوصی در بلاکچین‌های نسل اول مانند بیت کوین و اتریوم، همچنان یک موضوع اساسی و شناخته‌شده است. برای غلبه بر این مشکل، سیستم‌های بلاکچین مانند مونرو، زیروکش و بلاکچین‌های لایه دوم اتریوم، برای تضمین حریم خصوصی کاربران، تراکنش‌ها را بصورت ناشناس منتشر می‌کنند. با این حال، گمنامی کاربران غالبا با قوانین ضدپولشویی و احراز هویت بانک‌ها و موسسات در تضاد است و سبب تسهیل فعالیت‌های غیرقانونی خواهد شد. از سوی دیگر، در ساختارهایی که قابلیت ابطال گمنامی کاربران مخرب وجود دارد، اساسا تبانی نهادهای درگیر در سیستم، می‌تواند به حریم خصوصی کاربران آسیب بزند.

در این پایان نامه، یک سیستم مدیریت هویت دیجیتال معرفی خواهد شد که مشکلات بالا را برطرف می‌کند. بدین صورت که از حریم خصوصی کاربران، در یک سطح بالا محافظت خواهد کرد، در عین حال با داشتن قابلیت پاسخگویی، توانایی ردیابی و افشای هویت کاربران مخرب وجود دارد. بصورت رسمی‌تر، با تکیه برکارهای پیشین، نوآوری‌های زیر را ارائه خواهد شد:

- یک پروتکل دانش صفر غیرتعاملی ساخته می‌شود و اثبات خواهد شد که در مدل اوراکل تصادفی ROM، این کلاس از پروتکل‌ها، در برابر حملات مرد میانی همزمان، مقاوم هستند.
- مفهوم امضای کور قابل ویرایش مطرح شده و یک ساختار پیشنهادی برای آن ارائه می‌گردد. همچنین امنیت سیستم درمدل گروه عمومی (GGM) نشان داده خواهد شد.
- یک سیستم مدیریت هویت دیجیتال ایمن، ارائه خواهد شد. برای اثبات امنیت سیستم، یک حمله‌گر فعال، بصورت مرد-میانی-همزمان درنظر گرفته می‌شود، به گونه‌ای که طیف وسیعی از حملات رایج در چنین سیستم‌هایی را پوشش دهد؛ سپس با استفاده از مدل اوراکل تصافی (ROM) و مدل گروه عمومی(GGM) ، امنیت سیستم پیشنهادی، نشان داده می‌شود.

دانشجو: **شادمان محمدی**

استاد راهنما: **دکتر ابوالفضل فلاحتی**

هیات داوری: **دکتر فرزان حدادی ؛ دکتر شهرام خزایی**

تاریخ دفاع: **سه شنبه ۱۴۰۳/۷/۲۴** ساعت: **۱۵**

محل: **سالن خوارزمی**