باسمه‌تعالی

جلسه دفاع از پایان‌نامه کارشناسی ارشد

مهندسی کامپیوتر گرایش رایانش امن

# ارائه یک طرح مقاوم نسبت به حمله سرقت پایگاه‌داده برای احراز هویت گمنام و بدون جفت‌سازی دوخطی در کاربردهای اینترنت اشیاء


**دانشگاه اصفهان**

**دانشکده مهندسی کامپیوتر**

**گروه مهندسی فناوری اطلاعات**

استاد راهنما:

دکتر مائده عاشوری تلوکی

استاد داور داخل:

دکتر حمید ملا

استاد داور خارج:

دکتر مجتبی خلیلی

پژوهشگر:

مهدی ذهبی


تاریخ برگزاری:

۱۴۰۵/۰۴/۲۳

ساعت

۱۰:۰۰

مکان برگزاری:

تالار دکتر براآنی


با گسترش روزافزون اینترنت اشیاء در زندگی روزمره، چالش‌های مربوط به امنیت و کارایی در این حوزه اهمیت دوچندانی یافته است. تجهیزات در محیط اینترنت اشیاء معمولاً دارای محدودیت‌هایی از نظر توان پردازشی، ظرفیت حافظه و منابع انرژی هستند و همین مسئله، طراحی پروتکل‌های احراز هویت و توافق کلید (AKA) سبک‌وزن و در عین حال امن را به یک چالش اساسی در این حوزه تبدیل کرده است. یکی از مهم‌ترین الزامات امنیتی در سامانه‌های اینترنت اشیاء، فراهم‌سازی ساز و کارهای احراز هویت و توافق کلید میان موجودیت‌های مختلف شبکه است. این ساز و کارها باید تضمین کنند که تنها موجودیت‌های مجاز قادر به برقراری ارتباط و تبادل اطلاعات باشند و از دسترسی غیرمجاز، جعل هویت و حملات مختلف جلوگیری شود. در سال‌های اخیر، طرح‌های متعددی برای احراز هویت و توافق کلید در محیط‌های اینترنت اشیاء و زیرساخت‌های مرتبط با آن ارائه شده است. با این حال، بسیاری از پروتکل‌های موجود به دلیل اتکا بر عملیات سنگین جفت‌سازی دوخطی یا عدم در نظر گرفتن برخی تهدیدات امنیتی پیشرفته، با محدودیت‌هایی از نظر کارایی یا امنیت مواجه هستند. در این پژوهش پس از بررسی و تحلیل طرح‌های احراز هویت موجود در حوزه اینترنت اشیاء، طرح ارائه شده توسط وو و همکاران در سال ۲۰۲۰ مورد ارزیابی کامل قرار گرفت. اگرچه طرح وو و همکاران با هدف مقابله با حمله سرقت پایگاه داده ارائه شده بود، اما تحلیل‌ها نشان داد که طرح آن‌ها شکست خورده و همچنان دارای نقاط ضعف امنیتی و کارایی است. این طرح در تامین ویژگی‌هایی مانند گمنامی و امنیت رو به جلو کامل، ناتوان است. علاوه بر این، از منظر کارایی، اتکای آن بر عملگر محاسباتی جفت‌سازی دوخطی، باعث سنگین شدن قابل توجه طرح شده و افت شدید کارایی را به همراه داشته است. از این رو، به منظور رفع چالش‌ها و بهبود کارایی، یک طرح احراز هویت و توافق کلید گمنام و بدون استفاده از جفت‌سازی دوخطی پیشنهاد شده است. امنیت طرح پیشنهادی به صورت شهودی بررسی شده و نتایج نشان می‌دهد که این طرح علاوه بر مقاومت در برابر حملاتی نظیر سرقت پایگاه‌داده، جعل هویت، حمله فردی در میانه و حمله تکرار، ویژگی‌هایی همچون گمنامی، عدم قابلیت ردیابی و امنیت رو به جلو کامل را فراهم می‌کند. به علاوه، مقایسه‌های انجام شده تأیید می‌کند که راهکار پیشنهادی در مقایسه با پروتکل‌های پیشین، امنیت بالاتر و هزینه محاسباتی و ارتباطی کمتری را ارائه می‌دهد و می‌تواند به عنوان یک راهکار قابل اعتماد برای احراز هویت و توافق کلید در سامانه‌های مبتنی بر اینترنت اشیاء مورد استفاده قرار گیرد.