ارائه طرحی برای احراز هویت متقابل گمنام و توافق کلید بین دستگاه ها در اینترنت اشیا

شذی حیدر محمد علی الحکیم[۱] ، مرتضی نیکوقدم[۲]

۱- دانشجوی کارشناسی ارشد گروه کامپیوتر دانشگاه بین المللی امام رضا(ع)

۲- استادیار گروه کامپیوتر دانشگاه بین المللی امام رضا(ع)

خلاصه

با پیشرفت‌هایی که در حوزه علوم کامپیوتر، فناوری اطلاعات و اینترنت به وجود آمده است هر روز شاهد خدماتی در بستر اینترنت مانند پزشکی از راه دور، پرداخت‌های الکترونیکی و تلفن‌های اینترنتی هستیم. به دلیل اینکه ارتباط بین خدمات‌دهندگان و خدمات‌گیرندگان مبتنی بر بستر اینترنت که محیطی ناامن است انجام می‌شود بحث احرازهویت و توافق کلید اهمیت ویژه‌ای برای اینترنت اشیاء دارد. در این مقاله در ابتدا به بررسی طرح احرازهویت رستم‌پور و همکاران خواهیم پرداخت و اثبات خواهیم کرد که طرح آن‌ها به درستی کار نمی‌کند و نمی‌تواند طرح مناسبی برای حوزه اینترنت اشیاء باشد و سپس پروتکلی بهبود یافته برای احرازهویت و توافق کلید برای دستگاه‌های اینترنت اشیاء ارائه خواهیم داد. در ادامه اثبات خواهیم کرد که طرح پیشنهادی در برابر تمامی حملات مقاوم بوده و نیازهای امنیتی مختلف را تامین می‌کند. در نهایت امنیت طرح بهبودیافته با ابزار رسمی scyther ارزیابی شده است.

کلمات کلیدی: احرازهویت دوطرفه، اینترنت اشیاء، پروتکل، توافق کلید، محرمانگی،scyther

[۲]**Corresponding author:** مرتضی نیکوقدم استادیار گروه کامپیوتر دانشگاه بین المللی دانشگاه امام رضا(ع)
Email: m.nikooghadam@imamreza.ac.ir