

عنوان مقاله:

یک طرح احرازصالت جدید با ویژگی حفظ حریم خصوصی کاربر در اینترنت اشیا

محل انتشار:

چهاردهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1396)

تعداد صفحات اصل مقاله: 8

نویسندگان:

محمد بهشتی آتشگاه - مجتمع دانشگاهی فناوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران- شرکت صنایع امنیت فضای تبادل اطلاعات صا ایران

مجید بیات - گروه مهندسی کامپیوتر، دانشگاه شاهد، تهران

محمدرضا عارف - دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران

مرتضی براری - مجتمع دانشگاهی فناوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران

خلاصه مقاله:

اینترنت اشیا (IoT) مفهومی است که در آن، هرشیء و چیزی در زیرساخت اینترنت به یک شبکه وسیع پویای جهانی متصل می شود. به منظور رسیدن به هدف نهایی اینترنت اشیا، IoT از مزایای دیگر فناوری ها همانند RFID ها، شبکه های حسگر بی سیم (WSN)، ارتباطات ماشین به ماشین (M2M)، داده بزرگ و رایانش ابری بهره می برد. شبکه های حسگر بی سیم (WSN) یکی از اجزای اصلی و مهم در مفهوم IoT به شمار می رود که تقریباً در تمامی حوزه های کاربردی IoT قابل استفاده است. به دلیل اهمیت امنیت شبکه های حسگر بی سیم، محققین تاکنون بر روی تکنیک های، طرح ها و پروتکل های جدید و کارآمد حوزه های مختلف امنیتی آن از جمله طرح های احرازصالت کار کرده اند. در سال گذشته، Wu و همکارش یک طرح احرازصالت جدید برای اینترنت اشیا و مبتنی بر شبکه های حسگر بی سیم ارائه نمودند. آن ها در مقاله خود، رویکرد جدیدی را مطرح نمودند که در آن، یک کاربر IoT می تواند از طریق یک دروازه با یک گره مشخص در شبکه WSN احرازصالت بشود. علاوه بر آن، طرح آن ها ویژگی محافظت از حریم خصوصی را برآورده نموده و همچنین اثبات امنیتی دارد. به هر حال، در این مقاله نشان داده می شود که طرح Wu و همکارش در برابر برخی حملات دچار آسیب پذیری می باشد. در این مقاله قصد بر آن است تا با برطرف نمودن ضعف های طرح Wu همکارش، یک طرح جدید و بهبودیافته ارائه گردد. همچنین امنیت طرح جدید ارائه شده با استفاده از اثبات امنیتی احتمالاتی و همچنین ابزار رسمی ProVerif اثبات شده و نهایتاً با دیگر طرح های مطرح مقایسه می شود.

کلمات کلیدی:

اینترنت اشیا، شبکه حسگر بی سیم، طرح احرازصالت کاربر، اثبات امنیتی، محافظت از حریم خصوصی، کارت هوشمند

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/781747>

