عنوان مقاله:
ارائه یک مکانیزم امن احراز هویت جهت حفظ حریم خصوصی کاربران مبتنی بر الگوریتمAES در خانه های هوشمند

محل انتشار:
نخستین کنفرانس ملی اینترنت اشیا (سال: 1402)

تعداد صفحات اصل مقاله: 20

نویسندگان:
نرگس خلیقی - *دانشجوی ارشد مهندسی کامپیوتر گروه آموزشی مهندسی کامپیوتر واحد اهواز دانشگاه آزاد اسلامی اهواز ایران*

محمدرضا نوری مهر - *اسلامی اهواز ایران استادیار دانشگاه آزاد اسلامی اهواز گروه آموزشی مهندسی کامپیوتر واحد اهواز دانشگاه آزاد*

خلاصه مقاله:
خانه های هوشمند از محبوب ترین فناوریهای زمانه ما محسوب میشوند که تحولی عظیم را در نحوه زندگی آسایش و آرامش ساکنان آن خانه فراهم می آورند یکی از عوامل مهم عدم استفاده از این فناوری نگرانی های امنیتی لو رفتن روابط و اطلاعات محرمانه و خصوصی اهالی خانه است؛ که در صورت برطرف شدن این مشکل رشد چشمگیری در استفاده از این فناوری توسط صاحب خانه ها در پی خواهد داشت. در این پژوهش با تاکید بر روی امنیت داده های تبادل شده یک روش احراز هویت دو طرفه کارا مبتنی بر الگوریتم AES پیشنهاد شده است. طرح پیشنهادی شامل دو مرحله می باشد. مرحله اول ثبت نام موجودیتها در سرور و مرحله دوم احراز هویت متقابل موجودیتها و در انتها تبادل کلید نشست میباشد. به گونه ای که کلید نشست را فقط کاربر و دستگاه هوشمند در اختیار دارند و هیچ موجودیت و یا دستگاه دیگری از کلید نشست خبر ندارد بنابراین تبادل پیام ها بین این دو موجودیت به صورت End to End رمزنگاری و رمزگشایی میشوند. از طرف دیگر گمنامی کاربر دروازه و دستگاههای هوشمند و به دنبال آن عدم ردیابی این سه موجودیت در روش پیشنهادی گنجانده شده است. در تحلیلهای امنیتی و کارایی طرح مذکور ضمن داشتن کارایی بالا در برابر انواع حملات رمزنگاری مانند حمله تکرار حمله ،تغییر حمله داخلی حمله حدس کلید جلسه و دیگر حملات مقاوم است. همچنین این روش گمنامی کاربر دروازه و دستگاههای هوشمند و به تبع آن عدم ردیابی این سه موجودیت را فراهم می آورد.

کلمات کلیدی:
احراز هویت گمنامی، حریم خصوصی، خانه های هوشمند ،AES