عنوان مقاله:
الگوریتم رمزنگاری اطلاعات با استفاده از یک روش جدید رمزنگاری در راستای بهبود امنیت اینترنت اشیا

محل انتشار:
نوزدهمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات (سال: 1402)

تعداد صفحات اصل مقاله: 15

نویسندگان:
علیرضا یلالی - *دانشجوی کارشناسی ارشدگروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، موسسه آموزش عالی کارون، اهواز، ایران*

محمدرضا محمدرضایی - *استادیار گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، موسسه آموزش عالی کارون، اهواز، ایران*

خلاصه مقاله:
اینترنت اشیاء، شبکه بزرگی است که دستگاه های هوشمند مانند حسگرها و محرکها را به هم متصل می نماید. طیف دامنه های کاربردهای اینترنت اشیاء بسیار وسیع است و از خانه های هوشمند، شهرهای هوشمند، مراقبتهای بهداشتی هوشمند و غیره تشکیل شده است. این دستگاه ها دارای قابلیتهای هوشمندی برای جمع آوری، تحلیل و تصمیم گیری بدون تعامل انسان دارند. در این شرایط، امنیت یک نیازمندی بسیار مهم است و به ویژه، احراز هویت نیز اهمیت بسیار ویژه ای دارد، زیرا دستگاه غیرمجاز مخرب میتواند آسیبهای جبران ناپذیری به سیستم اینترنت اشیاء وارد کند. در این پژوهش، از الگوریتم PRESENT در راستای رمزگذاری فایل متنی استفاده شده است. روش انجام کار به این صورت است که در ابتدا فایل ایجاد شده توسط الگوریتم Present رمزگذاری میشود و کلید نیز در اختیار کاربر گیرنده قرار میگیرد که برای رمزگشایی استفاده میشود. شبیه سازی روش پیشنهادی با استفاده از نرم افزار MATLAB انجام شده است. معیارهای مورد ارزیابی زمان اجرا و امنیت هستند که طبق نتایج به دست آمده، روش پیشنهادی توانسته است مدتزمان کمتری امنیت بهتری را جهت شبکه های اینترنت اشیا ارائه دهد.

کلمات کلیدی:
رمزنگاری فایل متنی، اینترنت اشیا، الگوریتم Present، پیچیدگی زمانی