عنوان مقاله:

پیاده سازی سخت افزار از طرح های رمزنگاری سبک و ایمن برای کاربردهای اینترنت اشیا (مورد مطالعه:معماری سیستم های سخت افزاری اداره فن آوری اطلاعات سازمان بازرسی شهرداری تهران که پروژه های IOT بر روی آنها اجرا شده)

محل انتشار:

اولین کنفرانس برق، مکانیک ، هوافضا، کامپیوتر و علوم مهندسی (سال: 1401)

تعداد صفحات اصل مقاله: 10

نویسندگان:

علیرضا سبزیان - *کارشناسی مهندسی فن آوری عمران -ساختمان*

جواد سلمانیان - *دانشجوی دکتری تخصصی مهندسی کامپوتر-نرم افزار*

خلاصه مقاله:

الگوریتم رمزگذاری کوچک (TEA) یک الگوریتم رمزنگاری سبک وزن مناسب است که در سیستم های امنیتی متوسط مانند سیستم های RFID استفاده می شود . TEA یک ساختار آهنی است که برای جبران سردرگمی و خواص انتشار برای پنهان کردن مشخصات آماری متن ساده استفاده می شود. با این حال،TEA نقاط ضعف کمی دارد ، به ویژه از کلیدهای معادل و حملات مربوط به کلید. بنابراین ، یک الگوریتم اصلاح شده (MTEA TEA) پیشنهاد شده است که با استفاده از Linear Feedback Shift Register (LFSR)) ضعف امنیتی الگوریتم TEA را در برابر حملات برطرف می کند. در این j اجرای الگوریتم MTEA ارائه شده و با توجه به مساحت و میزان مصرف برق با الگوریتم استاندارد TEA محک زده می شود.همچنین به عنوان نمونه موردی پروژه های اینترنت اشیا (IOT) سازمان بازرسی که توسط اداره آی تی این سازمان بر روی سخت افزارهای سازمان قرار است اجرا گردد می باشد.

کلمات کلیدی:

سازمان بازرسی ، اینترنت اشیاء ، رمز نگاری ، سخت افزار ، IOT

لینک ثابت مقاله در پایگاه سیویلیکا: