سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:
ارتقاء امنیت در کاربردهای اینترنت اشیا از طریق رمزنگاری سبک وزن منحنی بیضوی

محل انتشار:
فصلنامه فناوری اطلاعات و ارتباطات انتظامی, دوره 2, شماره 6 (سال: 1400)

تعداد صفحات اصل مقاله: 14

نویسندگان:
محمدرضا حسینی - *گروه الکترونیک، واحد شهر قدس، دانشگاه آزاد اسلامی، تهران، ایران*

مژده مهدوی - *گروه الکترونیک، واحد شهر قدس، دانشگاه آزاد اسلامی، تهران، ایران*

محسن معدنی - *گروه الکترونیک، واحد شهر قدس، دانشگاه آزاد اسلامی، تهران، ایران*

خلاصه مقاله:
در بستر اینترنت اشیا بخصوص در کاربردهای نظامی، کانالی امن برای تبادل اطلاعات محرمانه وجود ندارد. تنها راه حل، رمزکردن اطلاعات و انتقال آن از طریق کانال ناامن است. یکی از اساسی ترین مسائل در رمزنگاری، چگونگی ایجاد یا تبادل کلید مشترک برای رمز کردن اطلاعات می باشد. رمزنگاری منحنی بیضوی به علت ویژگی های حائز اهمیت آن نظیر حجم محاسباتی کمتر، طول کلید کمتر، نیاز به حافظه کمتر و در عین حال امنیت بسیار بالای آن، جایگزین مناسبی برای سایر الگوریتم های کلید عمومی می تواند باشد و این روش، رمزنگاری را برای استفاده در کاربردهایی مختلف بخصوص نظامی، مناسب می نماید. هدف از این مقاله، ارائه ساختاری به منظور ایجاد یک پروتکل توزیع از طریق رمزگذاری سبک وزن بر پایه رمزنگاری منحنی بیضوی در اینترنت اشیا می باشد، به طوری که اطلاعات شنودگر احتمالی به حداقل مقدار ممکن برسد. نتایج حاصل از این پژوهش با میزان رگرسیون کلی بدست آمده ناشی از همگرایی داده ها در مرحله تست برابر با ۰.۹۹۶۳۷ بیانگر آن است که این روش در ارتقا امنیت در برابر انواع حمله ها، ساز وکار بهتری را در مقایسه با روش های دیگر ارائه می دهد.

کلمات کلیدی:
اینترنت اشیا, رمزنگاری سبک وزن, الگوریتم منحنی بیضوی, افزایش امنیت

لینک ثابت مقاله در پایگاه سیویلیکا:
https://civilica.com/doc/1487802