عنوان مقاله:
چارچوب رمزنگاری در شبکه اینترنت اشیاء با استفاده از مدل های ترکیبی و توزیع شده

محل انتشار:
بیست و هفتمین کنفرانس بین المللی کامپیوتر انجمن کامپیوتر ایران (سال: 1400)

تعداد صفحات اصل مقاله: 8

نویسندگان:
محسن بختیاری - *کارشناسی ارشد مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد تهران شمال*

زهره مافی - *عضو هیات علمی گروه مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد تهران شمال*

خلاصه مقاله:
امنیت داده ها و تبادل امن اطلاعات یکی از مقوله های مهم در اینترنت اشیاء میباشد. با توجه به قدرت محاسباتی اندک و همچنین ظرفیت کوچک ذخیره سازی در گره های شبکه اینترنت اشیاء، در بسیاری از موارد امکان رمزنگاری اطلاعات وجود ندارد و یا نیاز به صرف زمان زیادی است. چالش دیگر نگهداری کلید مشترک رمزنگاری در جای امن است. در چارچوب پیشنهادی بار پردازش رمزنگاری محدود به گره حاوی فایل یا اطلاعات نسبتا بزرگ نیست. بلکه با تقسیم فایل به قطعات کوچکتر از مشارکت دیگر گره های شبکه استفاده میگردد. بدین منظور سه نوع گره خاص منظوره هماهنگ کننده، ادغام کننده و مشارکت کننده تعریف شده است تا با مشارکت یکدیگر در یک معماری توزیع شده پردازش صورت پذیرد. برای تبادل کلید از روش ECDH استفاده شده است تا دو طرف بتوانند یک کلید امن مشترک را از طریق یک کانال ناامن ایجاد کنند. این چارچوب با فایلی با حجم ۵۶۰ کیلوبایت روی دو گره واقعی ESP۸۲۶۶ و ESP۳۲ در کنار سایر گره های شبیه سازی شده مورد آزمون قرار گرفته شده است. و زمان رمزنگاری در دو حالت استفاده از گره های با توان های یکسان و متفاوت محاسبه شده که کاهش زمان تا ۴ برابر را نشان می دهد.

کلمات کلیدی:
اینترنت اشیاء، رمز نگاری متقارن، تبادل کلید نا متقارن، رمزنگاری ترکیبی، کلید امن مشترک