وزارت ارتباطات و فناوری اطلاعات
پژوهشگاه ارتباطات و فناوری اطلاعات

# کاربرد رمزنگاری مبتنی بر ویژگی در اینترنت اشیاء

تهیه‌کنندگان: مهدی مهدوی علیائی، محمد حسام تدین

عنوان گزارش: کاربرد رمزنگاری مبتنی بر ویژگی در اینترنت اشیاء

تهیه کنندگان: مهدی مهدوی علیائی، محمد حسام تدین

گروه پژوهشی: پژوهشکده امنیت فاوا

تاریخ نشر: ۱۴۰۲

## مقدمه

اینترنت اشیا[۱] روند رو به رشدی است که جهان را با میلیاردها دستگاه متصل به‌هم پر کرده است. این دستگاه‌ها به «اشیاء» فیزیکی، از حسگرها گرفته تا گوشی‌ها و خودروهای هوشمند مربوط می‌شوند. متأسفانه، اگرچه اینترنت اشیاء(IoT) پتانسیل ایجاد خدمات نوآورانه را دارد، اما با این حال افزایش شدید تعداد دستگاه‌های متصل، خطرات و چالش‌های امنیتی و حریم خصوصی جدیدی را برای سیستم‌های IoT به همراه دارد. از آنجایی که دستگاه‌های اینترنت اشیاء به طور گسترده توزیع می‌شوند، اعمال کنترل‌های امنیتی دقیق آنقدر دشوار است که آنها را در برابر حملات مختلف آسیب‌پذیر می‌کند. محافظت از دستگاه‌های اینترنت اشیاء در برابر دسترسی غیرمجاز ضروری است، زیرا این دستگاه‌ها اغلب حاوی داده‌های بسیار ارزشمند و حساس هستند.

شبکه IoT، علاوه بر امنیت و مسائل مربوط به حریم خصوصی، که با رمزنگاری تأمین می‌شود، مشمول چالش‌های دیگری نیز می‌باشد. مثلاً شاید لازم باشد داده‌های ارسال شده فقط برای برخی از طرف‌های منتخب فاش شود. این چالش‌ها نیاز به احراز هویت کارآمد و مکانیزم‌های کنترل دسترسی دقیق را می‌طلبد که نیازمند روش‌های رمزنگاری پیشرفته است. علاوه بر این، یکی از جنبه‌های مهم IoT، مدیریت کلید انعطاف‌پذیر است. چالش‌های مذکور در اینترنت اشیاء را می‌توان با استفاده از رمزنگاری مبتنی بر ویژگی[۲] پاسخ داد. بنابراین شناخت رمزنگاری مبتنی بر ویژگی(ABE) و نحوه استفاده از آن در اینترنت اشیاء از اهمیت بالایی برخوردار است. استفاده از ABE در IoT خالی از چالش نیست. یکی از مهم‌ترین آنها بار محاسباتی بالایی است که به سیستم تحمیل می‌کند.

## ۱. معرفی رمزنگاری مبتنی بر ویژگی

اگر کاربری بخواهد پیامی را به چند نفر از اعضای شبکه ارسال کند باید با استفاده از کلیدهای عمومی افراد مورد نظر، پیام را جداگانه رمز کرده و به آنها بفرستند. یعنی به تعداد افراد مورد نظر عملیات رمزگذاری لازم است که بار مخابراتی و محاسباتی را افزایش می‌دهد. مشکل دیگر ناتوانی فرستنده در شناسایی همه گیرنده‌های مورد نظر است. این مشکل در شبکه‌های بزرگ مانند اینترنت اشیاء که تعداد کاربران شبکه بسیار زیاد است، بیشتر مورد توجه قرار

---

[۱] Internet of Things(IoT)

[۲] Attribute Based Encryption(ABE)

می‌گیرد. فرض کنید، فرستنده می‌خواهد پیام خود را به تمام دانشجویان دکتری در شهر تهران که در رشته‌های مربوط به امنیت مشغول به تحصیل هستند، بفرستد که شناسایی همه این افراد دشوار است. رمزنگاری مبتنی بر ویژگی به دنبال تحقق این ایده است که پیام بر این اساس رمزگذاری شود که توسط هر کاربری که واجد تعداد مشخصی ویژگی است، قابل رمزگشایی باشد. در همان مثال مذکور، فرستنده می‌تواند یک پیام را طبق ویژگی‌های مطلوب موردنظر (دانشجوی دکتری، مقیم تهران و رشته امنیت)، رمز کرده و تنها گیرنده‌هایی که این ویژگی‌ها را دارند بتوانند آن را رمزگشایی کنند. در صورت اجرای چنین طرحی اولاً نیازی نیست که فرستنده تک تک گیرنده های واجد این شرایط را شناسایی کند و ثانیاً نیازی نیست که برای هر گیرنده بطور مجزا عملیات رمزنگاری را انجام دهد. رمزنگاری مبتنی بر ویژگی همچنین این قابلیت را ایجاد می‌کند که بتوان یک ساختار دسترسی طبق ویژگی‌های تعریف شده در سیستم تعریف کرده و رمزنگاری با استفاده از این ساختار دسترسی صورت گیرد. ساختار دسترسی می‌تواند یک تابع بولی از ویژگی‌ها باشد. با اعمال ساختار دسترسی می‌توان به یک کنترل دسترسی روی پیام‌های ارسالی در شبکه دست یافت.

## ۲. دلایل استفاده از رمزنگاری مبتنی بر ویژگی در اینترنت اشیاء

با توجه به اینکه اینترنت اشیاء یک شبکه بزرگ با تعداد زیادی کاربر و دستگاه متصل به هم است. بنابراین مدیریت کلید و نیز شناسایی همه کاربران شبکه برای ارسال پیام رمزشده با مشکلاتی همراه است. رمزنگاری مبتنی بر ویژگی(ABE) مشکل شناسایی همه کاربران برای ارسال پیام را حل می‌کند. همچنین امکان بهبود مدیریت کلید، سربار مخابراتی و کنترل دسترسی را فراهم می‌کند. برای مثال وقتی که تعداد کاربران گیرنده خیلی زیاد باشد، اگر پیام جداگانه رمز کرده و ارسال شود سربار مخابراتی بسیار بالایی را به شبکه تحمیل خواهد کرد. همچنین اگر برای هر کاربری زوج‌کلید عمومی و خصوصی جداگانه تولید شود، تعداد کلید به‌شدت افزایش یافته و مدیریت آنها در شبکه ساده نخواهد بود. در مورد سربار مخابراتی، به سادگی می‌توان دید که در رمزنگاری مبتنی بر ویژگی برای هر پیام تنها یک متن رمزشده تولید شده و در شبکه ارسال خواهد شد و مستقل از تعداد کاربران گیرنده است. در مورد مدیریت کلید نیز، با تعریف چند ویژگی می‌توان کلیدهای تولید شده را ثابت نگه داشت و کاربران با توجه به ویژگی‌هایی که دارند، کلیدهای مطلوب را دریافت خواهند کرد. برای مثال با تعریف تنها ۱۰ ویژگی، می‌توان برای

تعداد ۱۰۲۴ (و بیشتر) از کاربران در شبکه کلید تولید کرد، بدون آنکه تعداد کلید عمومی (که همان تعداد ویژگی-هاست) افزایش یابند. این درحالی است که اگر از ABE استفاده نشود، برای تعداد کاربران ۱۰۲۴، باید دقیقاً ۱۰۲۴ زوج کلید تولید شود که باعث دشواری در مدیریت کلید خواهد شد. اتحادیه اروپا و مؤسسات پیشرو در فناوری‌های جدید، با توجه به اهمیت موضوع پروژه‌هایی را تعریف و اجرا کرده‌اند که در ادامه به تعدادی از آنها می‌پردازیم.

## ۳. پروژه‌های موجود در زمینه رمزنگاری مبتنی بر ویژگی

پروژه‌های مختلفی در سراسر دنیا وجود دارد که از رمزنگاری مبتنی بر ویژگی به عنوان یک ابزار موثر در کاربردهای مختلف از جمله اینترنت اشیاء استفاده شده است. با توجه به این پروژه‌ها می‌توان به اهمیت استفاده از ABE در کاربردهای مختلف به خصوص در IoT پی برد. بنابراین تعریف یک پروژه برای استفاده از رمزنگاری مبتنی بر ویژگی در اینترنت اشیاء کاملاً توجیه‌پذیر است. در ادامه به بررسی چند نمونه از این پروژه‌ها، پرداخته می‌شود.

- ASCLEPIOS

این پروژه با نام پلتفرم رمزگذاری شده ابر ایمن پیشرفته برای راه حل‌های هماهنگ بین المللی در مراقبت‌های بهداشتی[۱] (ASCLEPIOS) در اواخر سال ۲۰۱۸ توسط اتحادیه اروپا شروع شد و تا ۲۰۲۲ نیز ادامه دارد. خروجی این پروژه، ارائه حریم خصوصی در سلامت الکترونیک خواهد بود. یکی از مهمترین اهداف پروژه، ترکیب رمزگذاری جستجوپذیر[۲] و رمزگذاری مبتنی بر ویژگی برای کنترل دسترسی کارآمد کاربران است. این پروژه با همکاری دانشگاه‌ها و مؤسسات علمی از سراسر اروپا و جهان اجرا شده است. اطلاعات بیشتر درباره این پروژه در وبسایت پروژه[۳] قابل دسترسی است.

---

[۱] Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare

[۲] Searchable Encryption

[۳] https://www.asclepios-project.eu/

- **اینترنت اشیاء سبز**

پروژه‌ای تحت عنوان «اینترنت اشیاء سبز[۱]» در اواخر سال ۲۰۱۵ توسط دانشگاه شهر اوپسالا[۲] در سوئد در تلاش برای تبدیل این شهر به یک شهر هوشمند، شروع شد. اصطلاح شهر هوشمند برای توصیف توسعه شهری با استفاده از فناوری اطلاعات و ارتباطات(ICT) به‌کار می‌رود. در این پروژه سنسورهایی در شهر برای جمع‌آوری اطلاعات آلودگی هوا مستقر شدند. داده‌های جمع‌آوری شده توسط حسگرها می‌تواند برای نتیجه‌گیری در مورد وضعیت محیط و چگونگی تأثیر آن بر سلامت شهروندان استفاده شود. جمع‌آوری داده‌ها و نظارت بر محیط توسط حسگرهای کوچکی انجام می‌شود که می‌توانند در ساختمان‌ها، اتومبیل‌ها یا اشیاء دیگر نصب شوند. این حسگرها بخشی از اینترنت اشیا(IoT) هستند. دستگاه‌های موجود در اینترنت اشیا معمولاً به دلایل عملی مانند کاهش هزینه و محدود کردن مصرف انرژی برای افزایش طول عمر باتری، محدودیت منابع دارند. برای داشتن یک اشتراک‌گذاری کارآمد و امن در سراسر شبکه از رمزنگاری مبتنی بر ویژگی در شبکه داده‌محور[۳] (ICN) استفاده کرده‌اند. در این پروژه دانشگاه‌ها و مؤسسات مختلفی از سراسر دنیا مشارکت داشتند. از اهداف مهم این پروژه می‌توان به استفاده از زیرساخت داده‌محور در اینترنت اشیاء و تأمین امنیت توأم با کنترل دسترسی با استفاده از ABE اشاره کرد. برای اطلاعات بیشتر به وبسایت پروژه[۴] مراجعه کنید.

- **AU۲EU**

پروژه احراز هویت و مجوز برای اتحادیه‌های مورد اعتماد[۵] (AU۲EU) توسط اتحادیه اروپا با همکاری چندین دانشگاه و مؤسسه از سال ۲۰۱۳ شروع و تا اواخر ۲۰۱۵ ادامه یافت. این پروژه در راستای ارائه چارچوب احراز هویت و مجوز الکترونیکی یکپارچه در محیط واقعی تعریف شد. در این پروژه، طرح‌های پیشرفته رمزگذاری مانند رمزگذاری مبتنی بر ویژگی(ABE) مورد استفاده و بررسی قرار گرفته است. همچنین نحوه استفاده از ABE برای به‌روزرسانی

---

[۱] Green IoT

[۲] Uppsala

[۳] Information Centric Network

[۴] https://user.it.uu.se/~eding۸۱۰/GreenIoT/

[۵] Authentication and Authorisation for Entrusted Unions

ساختار دسترسی و ابطال کلید مطالعه گردید. از اهداف مهم این پروژه می‌توان به طراحی چارچوب احراز هویت در شبکه سلامت الکترونیکی اشاره کرد. برای اطلاعات بیشتر به وبسایت پروژه[۱] مراجعه فرمایید.

## ۴. نتیجه‌گیری

باتوجوه به اینکه امروزه فعالیت های بسیاری با تمرکز بر پیاده‌سازی و استفاده از رمزنگاری مبتنی بر ویژگی در پروژه‌های مختلف توسعه اینترنت اشیا در حال انجام است، بررسی طرح‌های مربوطه و شناسایی چالش های آن بسیار کاربردی و مورد نیاز است. البته هدف اصلی در ادامه این پژوهش علاوه بر شناسایی روش های موجود، ارائه تکنیک ها و طرح های اجرایی به منظور حل چالش های استفاده از رمزنگاری مبتنی بر ویژگی می باشد که بصورت مستقیم بر حل مسائل امنیتی کاربردهای اینترنت اشیا و توسعه فناوری تاثیرگذار است.

[۱] https://www.sps.tue.nl/ictlab/project/au۲eu/ و https://cordis.europa.eu/project/id/۶۱۱۶۵۹

**نشانی:** تهران، انتهای کارگر شمالی، پژوهشگاه ارتباطات و فناوری اطلاعات، معاونت پژوهش و توسعه ارتباطات علمی

**تلفن:** ۰۲۱-۸۸۶۳۰۳۵۵

**نمابر:** ۰۲۱-۸۸۶۳۰۳۵۶