نهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
مشهد- ۱۳ آذر- ۱۳۹۳
کمیسیون دوم: همایش ملی علوم و مهندسی کامپیوتر
بامحوریت
امنیت ملی و توسعه پایدار
9th SASTech Symposium on Advances in & Science Technology (2014)
برگزارکننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

# اشتراک اطلاعات در گروه‌های همکاری پویا

**علی زاغیان، سیدمحمدجعفرهاشمی گرم دره، فرشید بلدی**

**۱- عضو هیئت علمی دانشکده ریاضی کاربردی و رمز، دانشگاه صنعتی مالک اشتر**

**۲- محقق دانشکده ریاضی کاربردی و رمز، دانشگاه صنعتی مالک اشتر**

**۳- دانشجوی کارشناسی ارشد رمز، دانشگاه صنعتی مالک اشتر**

عکس
ارائه‌دهنده

f.baladi@chmail.ir
فرشید بلدی

**خلاصه**

در این مقاله به بررسی اشتراک اطلاعات در یک گروه همکاری پویا، با استفاده از دستگاه های موبایل مانند گوشی‌های هوشمند و تبلت پرداخته می‌شود و پروتکل اشتراک اطلاعات مبتنی بر گروه قابل اعتماد (TGIS) معرفی می‌شود که از این پروتکل در دستگاه‌های موبایل برای برقراری یک ارتباط مطمئن به منظور اشتراک اطلاعات در گروه استفاده می‌شود. در این طرح با بهره گرفتن از هویت سلسله مراتبی کاربران و استفاده از رمزنگاری مبتنی بر هویت سلسله مراتبی(HIBE)، اطمینان بین اعضای گروه برقرار می‌شود. به منظور کنترل دسترسی امن اطلاعاتی که در یک گروه یا گروه‌های مختلف به اشتراک گذاشته می‌شود، از رمزنگاری مبتنی بر مشخصه (ABE) استفاده می‌شود و کلیدهای خصوصی اعضای گروه، از طریق رابطه‌ای مطمئن با استفاده از رمزنگاری مبتنی برهویت سلسله مراتبی توزیع می‌شوند.

**کلمات کلیدی:** گروه همکاری پویا، اشتراک اطلاعات، رمزنگاری مبتنی برهویت سلسله مراتبی (HIBE)، رمزنگاری مبتنی بر مشخصه (ABE).

## ۱. مقدمه

در دهه گذشته توجه زیادی روی طراحی محاسبات سیار انجام شده است و انواع مختلفی از دستگاه‌های موبایل (مانند گوشی‌های هوشمند) و پروتکل‌های ارتباطی (۳G/۴G و Wi-Fi) در دسترس است. اگر چه در سال‌های اخیر از دستگاه‌های موبایل برای سرگرمی و کاربردهای اجتماعی استفاده می‌شود اما کاربردهای مهم تری نیز وجود دارد: برای مثال ارتش استفاده از گوشی‌های هوشمند را برای ارتباطات و همکاری‌ها در میدان جنگ شروع کرد. در اینجا به بررسی استفاده از دستگاه‌های موبایل برای ارتباطات در یک گروه پویا پرداخته می‌شود. چندین نیاز امنیتی برای ارتباطات گروه پویا و اشتراک اطلاعات با دستگاه‌های موبایل لازم است. برای مثال دستگاه‌ها باید قادر باشند که به طور امن ارتباط برقرار کنند و در یک گروه با یکدیگر همکاری کنند. اطلاعاتی که در یک گروه به اشتراک گذاشته می‌شود می‌تواند تنها برای اعضای گروه قابل دسترس باشد، این کار به وسیله‌ی رهبر گروه و مشخصه‌هایی که تعیین کرده امکان پذیر است. از این گذشته حتی در یک گروه، اطلاعات می‌تواند برای همه اعضای گروه به اشتراک گذاشته نشود و به دلیل سطوح دستیابی مختلف، تخصص و وظیفه‌ای که اعضای گروه به عهده دارند اطلاعات تنها برای بخشی از اعضای یک گروه به اشتراک گذاشته شود. برای مثال فرض کنید یک سرباز از یکی از یگان‌های ارتش بخواهد با سربازی از یگان دیگر (یگان شناسایی) همکاری کند و بعضی از اسلحه‌های دشمن را شناسایی کند در حالیکه نخواهد هیچ سرباز دیگری از این اطلاعات باخبر شود. بنابراین در گروه‌های ارتباطی پویا لازم است که ابتدا بین اعضای گروه اعتماد برقرار شود و سپس از ساختار کنترل دسترسی استفاده شود که به کاربران اجازه دهد اطلاعات خود را تنها با افراد مورد نظر خود در گروه به اشتراک گذارد. در این مقاله یک پروتکل اشتراک اطلاعات مبتنی بر گروه قابل اعتماد (TGIS)، معرفی می‌شود که با استفاده از رمزنگاری مبتنی برهویت سلسله مراتبی (HIBE) [۱] اعتماد را بین سازمان‌های مستقل که قصد همکاری باهم دارند، ایجاد می‌کند، و با