مروری بر کنترل دسترسی مبتنی بر ویژگی در محیط‌های ابری

سعید رضایی[1*]، محمد علی دوستاری[2] و مجید بیات[3]

[1]دانش‌آموخته کارشناسی ارشد مهندسی فناوری اطلاعات، دانشگاه شاهد، تهران، ایران
s.rezaei@shahed.ac.ir
[2]استادیار گروه مهندسی کامپیوتر دانشگاه شاهد، تهران، ایران
doostari@shahed.ac.ir
[3] استادیار گروه مهندسی کامپیوتر دانشگاه شاهد، تهران، ایران
mbayat@shahed.ac.ir

چکیده

محیط‌های‌ابری در دهه اخیر به‌عنوان یک انقلاب در صنعت IT شناخته شده و سازمان‌های زیادی به‌منظور پردازش و ذخیره اطلاعات خود از این سرویس استفاده می‌کنند. با وجود رشد سریع و مزایای فراوان این سرویس، هنوز برخی از سازمان‌ها به‌دلیل مشکلات امنیتی و حریم‌خصوصی مرتبط با ذخیره داده‌های حساس بر روی سرورهای غیرقابل اعتماد ابری، از این سرویس استفاده نمی‌کنند. مدیریت کنترل دسترسی کاربران با استفاده از تکنیک‌های رمزنگاری یکی از روش‌های پرکاربرد و مؤثر برای مقابله با این مشکلات است. رمزنگاری مبتنی بر ویژگی، شیوه‌ای جدید از رمزنگاری است که از ویژگی‌های توصیفی و ساختار دسترسی برای اعمال کنترل دسترسی استفاده می‌کند. در این مقاله جدیدترین روش‌های کنترل دسترسی در محیط‌های ابری که از رمزنگاری مبتنی بر ویژگی استفاده کرده‌اند، بررسی شده است. ما این پروتکل‌ها را بر اساس ویژگی‌های امنیتی و کارایی دسته‌بندی کرده‌ایم. در انتها نیز نقاط ضعف و قوت مقالات بررسی شده، آورده شده است و مقایسه امنیتی و عملکردی کاملی ارائه شده است.

واژگان کلیدی: رایانش ابری، رمزنگاری مبتنی بر ویژگی، کنترل دسترسی، حریم‌خصوصی، برون‌سپاری داده.

۱- مقدّمه

رایانش ابری[1] یک طرح محاسباتی جدید است که بخاطر مزایای فراوانی که ارائه می‌دهد، هم در حوزهٔ دانشگاهی و هم در حوزهٔ صنعت توجه زیادی را به خود جلب کرده است. این واژه برای نخستین بار در سال ۱۹۹۷ توسط Chellappa تعریف شد [۱]؛ و شامل سه مدل اصلی ارائه خدمت است: ۱)نرم‌افزار به‌عنوان خدمت[2]، ۲) بستر به‌عنوان خدمت[3] و ۳) زیرساخت به‌عنوان خدمت[4]. البته در سال‌های اخیر مدل‌های دیگری از این فناوری مانند امنیت به‌عنوان خدمت[5]، پایگاه داده به‌عنوان سرویس[6]، شبکه به‌عنوان سرویس، نظارت به‌عنوان سرویس[7] و... نیز ارائه شده است. این فناوری[8] به‌دلیل فراهم‌کردن فواید بسیار، مانند مقیاس‌پذیری[9] بالا، هزینه پایین، توسعه سریع، فراهم‌کردن خدمات ذخیره‌سازی و محاسباتی، دسترس‌پذیری فراگیر به شبکه[10]، انعطاف[11] بالا، پرداخت به‌ازای استفاده و... چه در کشورهای در حال پیشرفت و چه در کشورهای توسعه‌یافته فرصت‌های زیادی را برای شرکت‌ها و سازمان‌ها ایجاد کرده

[1] Cloud Computing
[2] Software as a service
[3] Platform as a service
[4] Infrastructure as a service
[5] Security as a service
[6] storage as a service
[7] monitoring as a service
[8] Technology
[9] Scalability
[10] Broad network access
[11] Flexibility

[*] نویسندهٔ عهده‌دار مکاتبات

است. البته این فرصت‌ها با موانعی مانند امنیت[1] و حریم‌خصوصی[2] روبه‌رو هستند که از مهمترین‌های چالش‌های موجود در رایانش‌ابری محسوب می‌شوند [۵-۲]، برخلاف مدل‌های سنتی که کاربران کنترل کامل بر روی داده‌های ذخیره‌شده دارند، در رایانش ابری مشتری هیچ‌گونه کنترل فیزیکی بر روی داده‌ها و محاسبات ندارد و اطلاعات مشتریان در آن‌سوی مرزهای سازمان نگه‌داری می‌شود؛ بنابراین با توجه به این عدم کنترل فیزیکی، ممکن است محرمانگی[3] و صحت[4] داده‌های ذخیره‌شده به خطر بیفتد. به‌همین دلیل بیش‌تر سازمان‌ها و شرکت‌ها با توجه به خطرات مرتبط با امنیت و حریم خصوصی مشتاق به استفاده از خدمات ابری نیستند و خطرات امنیتی را به‌عنوان مهم‌ترین مانع در حرکت به‌سوی خدمات ابری معرفی می‌کنند. بنابراین اگر مهیاکنندگان سرویس‌های ابری بتوانند موانع موجود را از بین ببرند و یا به کمینه برسانند، رایانش ابری به یک عامل مهم در حوزه فناوری اطلاعات تبدیل و اعتماد و استفاده از این فناوری برای شرکت‌ها و عموم راحت‌تر می‌شود. برای تضمین محرمانگی داده‌ها و مقابله با تهدیدها[5] و خطرات[6] امنیتی موجود نظیر دزدی و افشای اطلاعات، نقض جامعیت داده و ...، راه‌حل‌های امنیتی بسیاری توسط پژوهش‌گران پیشنهاد شده است [۶-۱۰]. یکی از ابزارهای مهم برای بالابردن سطح امنیت داده‌های ذخیره‌شده کاربران استفاده از روش‌های کنترل دسترسی[7] است [۱۱]،[۱۲]؛ در سال‌های اخیر بهترین راه برای اعمال کنترل دسترسی استفاده از تکنیک رمزنگاری مبتنی بر ویژگی[8] (ABE) بوده است. یکی از کاربردهای رمزنگاری مبتنی بر ویژگی، مدیریت کنترل دسترسی بر روی داده‌های رمزشدهٔ ذخیره‌شده در سرورهای ابری است که این کار را با استفاده از یک سیاست دسترسی و ویژگی‌های مرتبط با کلید خصوصی و متن رمز شده انجام می‌دهد. در این روش مالک داده باید قبل از برون‌سپاری، داده‌های خود را با استفاده از یک سیاست دسترسی[9] رمز کند و فقط کسانی می‌توانند داده‌ها را رمزگشایی کنند که با کلیدشان بتوانند سیاست دسترسی را برآورده سازند[10].

در این مقاله قصد داریم تا پس از معرفی انواع روش‌های کنترل دسترسی مورد استفاده در محیط‌های ابری، روش‌های مختلفی که برای ذخیرهٔ امن داده‌ها در محیط‌های ابری از الگوریتم رمزنگاری مبتنی بر ویژگی استفاده کرده‌اند مورد بررسی قرار داده و سپس آنها را از دیدگاه‌های متفاوت مقایسه خواهیم کرد.

ساختار مقاله به این صورت است که در بخش ۲ کنترل دسترسی و روش‌های مخلف آن را بررسی کرده و یک دسته‌بندی از آنها را ارائه می‌دهیم. در بخش ۳ روش‌های مختلف کنترل دسترسی را که از رمزنگاری مبتنی بر ویژگی استفاده کرده‌اند بررسی می‌کنیم. در فصل ۴ روش‌های گفته‌شده در فصل ۳ را بر اساس معیارهای امنیتی، اجرایی و فنی مقایسه می‌کنیم و نقاط ضعف و قوت هر کدام را ارائه می‌دهیم و درنهایت در فصل ۵ نتیجه‌گیری و کارهای آینده آورده شده است.

۲- کنترل دسترسی

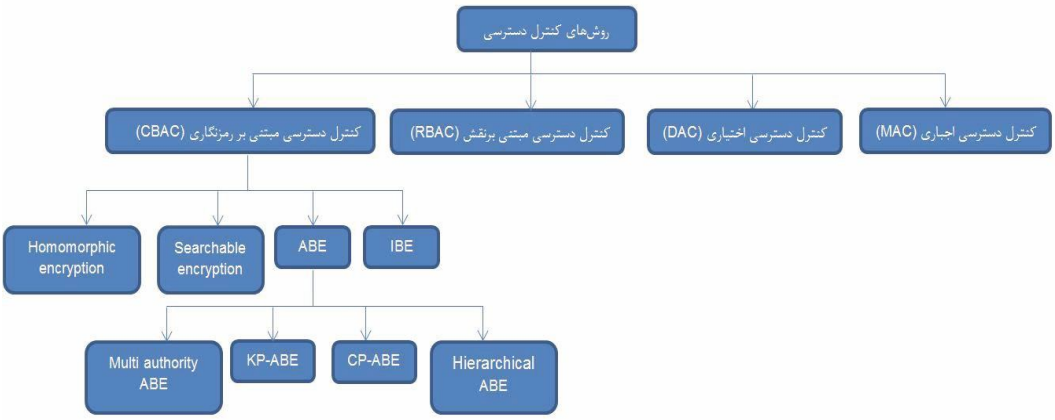
کنترل دسترسی یک تکنیک امنیتی است که به‌وسیلهٔ آن حق دسترسی به منابع اطلاعاتی یا انجام یک عملیات خاص به کاربران اعطا یا از آنها لغو می‌شود. امروزه به‌طور گسترده از روش‌های مختلف کنترل دسترسی برای محدودکردن دسترسی کاربران به داده‌های ذخیره‌شده در محیط‌های ابری استفاده می‌شود. مدل‌های کنترل دسترسی کنونی را می‌توان به چهار دسته تقسیم‌بندی کرد، ۱- کنترل دسترسی اختیاری[11] (DAC) [۱۳]، ۲- کنترل دسترسی اجباری[12] (MAC)[۱۴]، ۳- کنترل دسترسی مبتنی بر نقش[13] (RBAC) [۱۵] و ۴- کنترل دسترسی مبتنی بر رمزنگاری[14] (CBAC). این دسته‌بندی در (شکل نشان داده شده است. در ادامه به بررسی هر کدام از این روش‌ها می‌پردازیم.

- ✓ کنترل دسترسی اختیاری (DAC): در DAC، مالکان داده بر اساس هویت افراد سطح دسترسی آنها را تنظیم می‌کنند و فقط کاربرانی که توسط مالک داده مشخص

[1] Security
[2] Privacy
[3] Confidentiality
[4] Integrity
[5] threat
[6] Risk
[7] Access control
[8] Attribute based encryption
[9] Access Policy
[10] Satisfy
[11] Discretionary Access Control
[12] Mandatory Access Control
[13] Role Based Access Control
[14] Cryptography Based Access Control

شده‌اند می‌توانند یک فایل را بخوانند، بر روی آن بنویسند و یا آن را اجرا کنند. سیستم عامل یونیکس یک مثال خوب است که از کنترل دسترسی DAC برای دادن اجازه به کاربرانش استفاده می‌کند. این روش کنترل دسترسی دارای دو عیب عمدهٔ زیر است که مانع از استفاده آنها در محیط‌های ابری شده است: ۱- استفاده از این روش در سیستم‌های توزیع‌شده که داده‌ها بین چندین سرور تقسیم شده‌اند، یا زمانی که اندازه شبکه و تعداد کاربران سیستم در حال گسترش است، مناسب نیست. ۲- DAC در برابر حملات اسب تروجان آسیب‌پذیر است [۱۶].

- ✓ کنترل دسترسی اجباری (MAC): در MAC، سطوح دسترسی توسط مدیر سامانه یا یک مرجع مرکزی مشخص، اعمال می‌شود و مالکان نمی‌توانند سطوح دسترسی مشخص‌شده به‌وسیله برچسب‌های امنیتی را تغییر دهند. برچسب‌های امنیتی می‌توانند شامل یکی از دسته‌های طبقه‌بندی‌نشده، طبقه‌بندی‌شده، مخفی و خیلی مخفی باشند. روش‌های کنترل دسترسی DAC و MAC دارای چندین محدودیت از جمله عدم مقیاس‌پذیری و سازگاری پویا به تغییر سیاست‌های امنیتی هستند [۱۷].



(شکل_۱): روش‌های مختلف کنترل دسترسی

- ✓ کنترل دسترسی مبتنی بر نقش (RBAC): در این روش تصمیمات دسترسی بر اساس نقش‌هایی که اشخاص و کاربران در سازمان دارند، مشخص می‌شود. RBAC به‌دلیل سادگی آن در اداره‌کردن مجوزها برای تعداد زیادی از کاربران، به‌طور گسترده‌ای به کار گرفته شده است؛ ولی این شیوه مشکلاتی مانند دشواری در تعریف و نقش ساختار دسترسی و عدم انعطاف در محیط‌های در حال تغییر را دارد. علاوه‌بر آن به‌دلیل استفاده از نقش‌های از قبل اختصاص داده شده به افراد، تنها از کنترل دسترسی درشت‌دانه[1] و از ساختار از پیش تعیین شده پشتیبانی می‌کند.
- ✓ کنترل دسترسی مبتنی بر رمزنگاری (CBAC): در محیط‌های ابری از روش‌های مختلف رمزنگاری برای محافظت از داده‌ها در برابر دسترسی‌های غیرمجاز استفاده می‌شود. این روش‌ها شامل رمزنگاری کلید عمومی[2]، رمزنگاری کلید خصوصی[3]، رمزنگاری قابل جستجو[4]،رمزنگاری سلسله مراتبی[5]، رمزنگاری مبتنی بر شناسه[6]، رمزنگاری مبتنی بر ویژگی و ... است. در این روش‌ها فرستنده قبل از بارگذاری داده‌ها به محیط ابری اقدام به رمزکردن داده‌ها می‌کند و فقط کسانی می‌توانند داده‌ها را رمزگشایی کنند که کلید خصوصی مرتبط را داشته باشند.

سازوکارهای کنترل دسترسی DAC، MAC و RBAC محدودیت‌های مختلفی را در ارتباط با اجرای سیاست‌های کنترل دسترسی و اطمینان از محرمانه‌بودن اطلاعات ایجاد می‌کنند و تنها زمانی مناسب هستند که مالک داده و سامانهٔ

[1] Coarse grained access control

[2] Public Key Encryption
[3] private key encryption
[4] Searchable encryption
[5] Hierarchical encryption
[6] Identity based encryption

ذخیره‌ساز داده هر دو متعلق به یک دامنه اطلاعات باشند. این سازوکارها نیازمندی‌های سناریوی برون‌سپاری داده[1] را برآورده نمی‌کنند و مسائلی مانند در معرض خطر قرارگرفتن حریم خصوصی، مقیاس‌پذیری، ازدست‌دادن داده‌ها، دسترسی انعطاف‌پذیر، ابطال فوری[2] کاربران و سربار زیاد مرتبط با مدیریت کلید و بار محاسباتی و ارتباطی آن، جزء مهم‌ترین مسائل باقی‌مانده در این حوزه است. در سال‌های اخیر برای حذف مشکلات گفته‌شده و رسیدن به دسترسی ریزدانه[3] به داده‌ها و مقیاس‌پذیری خوب، روش کنترل دسترسی مبتنی بر ویژگی[4] (ABAC) معرفی شد. این روش کنترل دسترسی از رمزنگاری مبتنی بر ویژگی برای مدیریت دسترسی کاربران استفاده می‌کند و شامل روش‌های رمزنگاری مبتنی بر ویژگی با سیاست کلید[5] (KP-ABE)، رمزنگاری مبتنی بر ویژگی با سیاست متن رمزشده[6] (CP-ABE)، رمزنگاری مبتنی بر ویژگی توزیع‌شده (MA-ABE)[7] و رمزنگاری مبتنی بر ویژگی سلسله‌مراتبی است. در بخش ۳ به‌صورت مفصل به بررسی و ارائه این روش‌ها پرداخته‌ایم.

۳- کنترل دسترسی مبتنی بر ویژگی

ABE برای نخستین بار در سال ۲۰۰۵ توسط shahi و همکاران [۱۸] تحت عنوان رمزنگاری مبتنی بر هویت فوزی[8] و با در نظرگیری سناریوی برون‌سپاری داده به سرورهای غیرقابل اعتماد بیرونی ارائه شد. کنترل دسترسی مبتنی بر ویژگی، یک مدل تا حدودی تازه و در حال رشد از کنترل دسترسی است که از ویژگی‌ها و سیاست‌های دسترسی برای تعریف دسترسی افراد استفاده می‌کند. این شیوه به مالکان داده کمک می‌کند تا بتوانند به‌دلخواه، داده خود را با کاربران به اشتراک بگذارند. در این مدل یک کلید خاص فقط زمانی می‌تواند یک متن رمزشده را باز کند که بین ویژگی‌های متن رمزشده و کلید کاربر مطابقت وجود داشته باشد. ABAC به‌دلیل استفاده از ویژگی‌ها، قابلیت پشتیبانی از سیاست‌های کنترل دسترسی ریزدانه را دارد.

[1] Data outsourcing
2 Immediate revocation
[3] Fine grained
[4] Attribute-Based Access Control
[5] Key Policy Attribute Based Encryption
[6] Ciphertext Policy Attribute Based Encryption
[7] Multi authority ABE
[8] Fuzzy identity-based encryption

این سیاست‌ها برای پشتیبانی از محیط‌های ابری که در آن مجوز کاربران به‌صورت پویا در حال تغییر است، مناسب می‌باشند. به همین دلیل امروزه در بیشتر طرح‌های کنترل دسترسی در محیط‌های ابری از این تکنیک استفاده می‌شود.

این نوع رمزنگاری به چهار دسته کلی تقسیم می‌شود که در ادامه به بررسی هر کدام از آنها و روش‌های ارائه‌شده در این زمینه می‌پردازیم. در اکثر این روش‌ها به‌منظور کاهش سربار بالای محاسباتی ایجادشده به‌وسیله ABE، از روش‌های ترکیبی[9] برای رمزنگاری داده‌ها، تکنیک PRE[10] برای رمزنگاری مجدد داده‌ها در زمان ابطال کاربران و از روش برون‌سپاری رمزگشایی[11] برای کاهش بار محاسباتی رمزگشایی داده توسط کاربر استفاده شده است. در روش ترکیبی، مالک داده به‌منظور کاهش سربار بالای رمزنگاری، ابتدا داده‌ها را با رمزنگاری متقارن رمز و سپس کلید رمزنگاری متقارن را با رمزنگاری مبتنی بر ویژگی رمز می‌کند. این کار باعث می‌شود تا حجم داده‌های رمزشده به‌وسیله رمزنگاری مبتنی بر ویژگی کم شده و درنتیجه سربار محاسباتی کل سامانه کاهش پیدا می‌کند. در PRE، مالک با ارسال کلیدهای رمزنگاری مجدد برای سرور ابری، وظیفه رمزنگاری مجدد داده‌ها در زمان ابطال را به سرورهای بیرونی برون‌سپاری می‌کند. در برون‌سپاری رمزگشایی، کاربر یک کلید رمزگشایی جزئی را تولید کرده و با ارسال آن برای مهیاکننده خدمات ابری بخش عظیمی از رمزگشایی را به سرور ابری واگذار می‌کند. در این روش سرور ابری نمی‌تواند از ماهیت داده‌ها باخبر شود و محرمانگی داده‌ها حفظ می‌شود.

۳-۱- رمزنگاری مبتنی بر ویژگی با سیاست کلید (KP-ABE)

در KP-ABE داده‌ها به‌وسیله مجموعه‌ای از ویژگی‌های توصیفی رمز می‌شوند و ساختار دسترسی مشخص‌شده توسط مالک در کلید خصوصی قرار داده می‌شود. کاربر تنها زمانی می‌تواند متن رمزشده را رمزگشایی کند که ساختار دسترسی موجود در کلید خصوصی‌اش به‌وسیله ویژگی‌های موجود در متن رمزشده برآورده شوند [۱۹]. Yu و همکاران

[9] Hybrid
[10] Proxy re-encryption
[11] Outsourcing decryption

[۱۲] با ترکیب KP-ABE و PRE روشی را برای کنترل دسترسی کاربران در محیط‌های ابری معرفی کردند. این روش به‌طور هم‌زمان از مفهوم ریزدانگی، قابلیت توسعه و محرمانگی داده‌ها پشتیبانی می‌کند. در این روش مالک داده می‌تواند بیشتر بار محاسباتی مانند ابطال کاربران را بدون فاش‌شدن اطلاعات، به سرورهای ابری برون‌سپاری کند؛ اگرچه با این کار ممکن است بعضی از ویژگی‌ها و کلیدهای مخفی کاربران برای محیط ابری نمایان شود. Wang و همکاران [۲۰] با استفاده از طرح رمزنگاری مبتنی بر شناسه فراگیر[1] یک طرح KP-ABR با طول کلید ثابت را پیشنهاد دادند. در این طرح که از ساختار دسترسی یکنواخت برای بیان سیاست دسترسی استفاده کرده است، طول متن رمزشده مستقل از تعداد ویژگی‌ها است و تعداد عمل‌گرهای دودویی به مقدار ثابتی کاهش یافته است. اگرچه تاکنون روش‌های مختلفی پیشنهاد شده است که از KP-ABE برای اعمال کنترل دسترسی استفاده می‌کنند [۲۱]،[۲۷]، ولی به‌دلیل محدودیت‌هایی که این روش نسبت به CP-ABE ایجاد می‌کند، بهتر است از طرح CP-ABE برای مدیریت کنترل دسترسی کاربران در محیط‌های ابری استفاده شود.

۳-۲- رمزنگاری مبتنی بر ویژگی با سیاست متن رمز شده (CP-ABE)

در مقابل KP-ABE مفهوم رمزنگاری مبتنی بر ویژگی با سیاست متن رمزشده توسط Sahai معرفی شد [۲۸]. در این مدل، ساختار دسترسی در متن رمزشده و ویژگی‌های هر کاربر در کلید خصوصی‌اش قرار می‌گیرد. KP-ABE دارای سه عیب اساسی زیر است که همین امر باعث شده است بیشتر پژوهشگران از روش CP-ABE برای برون‌سپاری اطلاعات در محیط‌های ابری استفاده کنند.

- ✓ در KP-ABE سیاست‌های دسترسی در کلید کاربران تعریف می‌شود و رمزکننده کنترل مستقیم بر روی سیاست رمزنگاری ندارد و باید به مرجع صادرکننده کلید اعتماد کند؛ درحالی‌که در CP-ABE مالک داده مشخص می‌کند که چه کسی می‌تواند به داده‌های رمز شده دسترسی داشته باشد.
- ✓ در هنگام ابطال کاربران نیاز است تا ضمن رمزنگاری مجدد داده‌ها، برای کاربران ابطال‌نشده کلید رمزنگاری مجدد ارسال شود. در KP-ABE این کار باعث ایجاد مشکلات قابل توجه در پیاده‌سازی می‌شود و کارایی و انعطاف‌پذیری سامانه را کاهش می‌دهد.
- ✓ در KP-ABE نیاز است تا تمامی ویژگی‌های کاربران از ابتدا مشخص باشد که در محیط‌های ابری این کار عملی نیست.

در سال‌های اخیر کارهای زیادی در زمینه برون‌سپاری اطلاعات با استفاده از مدل CP-ABE در محیط‌های ابری صورت گرفته است که ما در ادامه به بررسی جدیدترین روش‌های ارائه‌شده در این زمینه می‌پردازیم.

Huang و همکاران [۲۹] با استفاده از مدیریت حق دسترسی دیجیتال[2] (DRM) مدلی را برای مدیریت کلید امن و کنترل حق دسترسی در محیط‌های ابری پیشنهاد دادند. DRM روشی است که در آن می‌توان با استفاده از تکنیک‌های رمزنگاری و کنترل دسترسی، حق رونوشت محتوا را حفظ کرد. در DRM مالک بعد از رمزکردن داده‌ها برای هر کاربر یک مجوز[3] صادر می‌کند تا کاربران بر اساس آن به محتوا دسترسی پیدا کنند. در این طرح مهیاکنندهٔ داده ابتدا داده‌ها را با استفاده از کلید CEK[4] که به دو قسمت CMK[5] و AK[6] تقسیم می‌شود، رمز می‌کند. قسمت CMK با استفاده از رمزنگاری CP-ABE رمز می‌شود و به همراه متن رمزشده برای محیط ابری فرستاده می‌شود؛ درحالی‌که قسمت AK با استفاده از تکنیک PRE رمز و در مجوزهای کاربران توزیع می‌شود. کاربران زمانی می‌توانند متن رمزشده را رمزگشایی کنند که علاوه بر ارضای سیاست دسترسی موجود در متن رمزشده، حق دسترسی استفاده را نیز داشته باشند. مدل پیشنهادی در مقابل حملات تبانی بین دو یا چند کاربر مقاوم است و علاوه بر حفظ محرمانگی داده باعث گمنامی کاربر نیز می‌شود.

مرجع [۳۰] به حل مشکلات و چالش‌های ذخیره داده بر روی سامانه‌های ذخیره ابری Peer-to-Peer پرداخته است. در این مقاله برای دستیابی به سازوکار کنترل

1 identity-based broadcast

[2] Digital right management
[3] license
[4] Content Encryption Key
[5] Content Master Key
[6] Assistant Key

دسترسی امن، مؤثر و مبتنی بر ریزدانگی روشی به‌نام ACPC مطرح شده که ترکیبی از دو تکنیک CP-ABE و PRE است. از آنجا که CP-ABE برای رمزنگاری مستقیم داده‌ها مؤثر نیست، در ACPC رمزکننده ابتدا داده‌ها را با استفاده از رمزنگاری متقارن رمز و سپس کلید رمزنگاری متقارن را با استفاده از تکنیک PCCP-ABE رمز می‌کند. PCCP-ABE گسترش‌یافتهٔ CP-ABE است که از ساختار دسترسی گویا برای رمزنگاری داده استفاده می‌کند. همچنین در این طرح وظایف ابطال کاربران به سرورهای ابری برون‌سپاری شده است که باعث کاهش سربار محاسباتی مالک داده در هنگام ابطال کاربران شده است

Zhang Yو همکاران [۳۱] یک روش رمزنگاری ترکیبی مبتنی بر رمزنگاری متقارن و CP-ABE را پیشنهاد دادند که علاوه‌بر محرمانگی داده و مقاوم‌بودن در برابر حملات تبانی، هزینهٔ محاسباتی ثابت[1] و سربار ارتباطی پایین دارد. الگوریتم رمزنگاری در این طرح به این صورت است که ابتدا رمزکننده یک طرح رمزنگاری متقارن و دو تابع هش H_1^{hash} و H_2^{hash} را انتخاب می‌کند؛ زمانی که مالک داده می‌خواهد فایل F را به اشتراک بگذارد، به‌صورت تصادفی مقدار $M \in MS$[2] را انتخاب و سپس با استفاده از توابع هش مقدار $\mathbf{s = H_1^{hash}(M \,||\, F)}$ و کلید متقارن $\mathbf{k = H_2^{hash}(M)}$ را محاسبه می‌کند. s مقدار مخفی مورد استفاده در الگوریتم رمزنگاری و k کلید رمزنگاری متقارن است؛ سپس مالک یک سیاست دسترسی W مبتنی بر AND^*_m برای فایل تعریف و ابتدا فایل F را به‌وسیله کلید خصوصی K و سپس مقدار تصادفی M را با رمزنگاری ABE و سیاست دسترسی W رمز می‌کند. این مقادیر به‌صورت زیر محاسبه می‌شوند: $\mathbf{C_M = Encrypt(PK, M, W)}$و $\mathbf{C_F = E^{sym}(F, K)}$. مالک داده زوج دادهٔ رمزشده $\mathbf{CT_W = (C_F, C_M)}$ را برای ابر می‌فرستد. در زمان رمزگشایی نیز ابتدا کاربر $\mathbf{CT_W = (C_F, C_M)}$ را از ابر دریافت می‌کند؛ سپس $\mathbf{M^* = Decrypt(PK, C_M, SK_L)}$ را با استفاده از کلید مخفی SK_L محاسبه و سپس $\mathbf{K^* = H_2^{hash}(M^*)}$، $\mathbf{F^* = D^{sym}(C_F, K^*)}$و $\mathbf{S^* = H_1^{hash}(M^* \,||\, F^*)}$ را محاسبه می‌کند. امنیت این طرح در مدل پیش‌گوی تصادفی[3] و تحت فرضیه مسئله تصمیم دیفی-هلمن[4] اثبات شده است.

Hur و همکاران [۳۲] یک طرح CP-ABE را برای به‌اشتراک‌گذاری داده در سامانه‌های شبکه هوشمند[5] پیشنهاد دادند. در این طرح کاربران با ایجاد توکن‌های رمزگشایی و ارسال آن برای سرور، حجم عظیمی از سربار محاسباتی رمزگشایی را به سرورهای بیرونی برون‌سپاری می‌کنند؛ ولی مشکل اصلی این طرح اعتبار دائمی توکن‌ها و عدم منقضی‌شدن آنهاست که این طرح را در برابر حملات منع سرویس (DOS) آسیب‌پذیر کرده است. همچنین طرح آنها فاقد روشی مناسب برای ابطال کاربران است. برای غلبه بر این مشکلات M Bayat و همکاران [۳۳] طرح پیشنهادی Hur را توسعه دادند و دو نیاز امنیتی ابطال کاربران و مقاوم‌بودن در مقابل حملات DOS را فراهم کردند. آنها با اضافه‌کردن یک مهر زمان[6] به توکن تولیدی توسط کاربر مدت زمام معتبربودن توکن را محدود کردند که این امر باعث می‌شود در صورت دزدیده‌شدن توکن توسط یک کاربر غیرقانونی امکان بروز حمله DOS وجود نداشته باشد.

Li Jin و همکاران [۳۴] با برون‌سپاری جزئی رمزگشایی داده به یک مهیاکنندهٔ خدمات رمزگشایی[7] (DSP) و برون‌سپاری جزئی تولید کلید به یک مهیاکنندهٔ تولید کلید (KGSP)، تا حد زیادی سربار بالای محاسباتی رمزگشایی داده‌ها توسط کاربر و مدیریت کلید توسط مراجع تولید کلید را کاهش دادند. در این طرح علاوه بر سیاست دسترسی مهیاشده توسط مالک، از یک سیاست جزئی نیز استفاده شده است. این دو سیاست دسترسی به‌وسیله یک گیت AND به یکدیگر متصل شده‌اند. KGSP وظیفه تولید کلید برای سیاست کاربران را بر عهده دارد و بنابراین نمی‌تواند به کلید رمزگشایی اصلی دسترسی داشته باشد چون سیاست جزئی را نمی‌داند. کاربر نیز با تولید یک کلید رمزنگاری مجدد و تحویل آن به DSP موجب برون‌سپاری رمزگشایی داده‌ها می‌شود. همچنین برای کاهش قابلیت اعتماد به KGSP، مدل ABE برون‌سپاری‌شده در مدل RDoC[8] در نظر گرفته شده است که در آن به‌جای استفاده

[1] Constant computation cost

[2] MS فضای پیام مورد استفاده در CP-ABE است.

[3] random oracle model
[4] decisional Bilinear Diffi-Hellman
[5] Smart grid
[6] Timestamp
[7] Decryption Service Provider
[8] refereed delegation of computation

از یک سرور KGSP از تعداد زیادی KGSP برای تولید کلید برای مراجع صدور استفاده شده است. کاربران نیز با اضافه‌کردن k بیت صفر اضافی به داده اصلی می‌توانند از فعالیت نادرست و متقلبانه DSP باخبر شوند.

به‌منظور کاهش بار محاسباتی رمزنگاری داده Nabeel و همکاران [۳۵] روشی بر مبنای رمزنگاری دولایه‌ای برای داده‌های بارگذاری‌شده در محیط ابر پیشنهاد دادند و آن را رمزنگاری دولایه‌ای[1] (TLE) نامیدند. در روش TLE سیاست کنترل دسترسی به دو زیرمجموعه تقسیم می‌شود که مجموع آنها سیاست کنترل دسترسی اولیه را تشکیل می‌دهند. این تقسیم‌بندی، به‌نحوی صورت می‌گیرد که کمترین تعداد ویژگی‌ها به مالک واگذار می‌شود و همچنین داده‌ها از دید ابر محرمانه می‌ماند. مالک داده ابتدا برای تضمین محرمانگی داده از ابر، رمزنگاری مبتنی بر درشت دانگی را بر روی داده انجام می‌دهد؛ سپس ابر بر اساس سیاست کنترل دسترسی مهیاشده به‌وسیله مالک، رمزنگاری مبتنی بر ریزدانگی با سیاست متن رمزشده را بر روی داده‌هایی که درقبل توسط مالک رمز شده است، انجام می‌دهد. ابطال کاربران در این روش فقط با به‌روزرسانی لایهٔ بیرونی رمزنگاری توسط محیط ابر صورت می‌گیرد و نیازی به انتقال داده بین مالک داده و ابر نیست.

Yang و همکاران [۳۶] برای دستیابی به اشتراک داده مبتنی بر ریزدانگی و قابل ابطال در سرویس‌های ذخیره‌ساز ابر از مفهوم CPRE[2] استفاده کردند. در CPRE کاربران در داخل متن رمزشده یک مقدار w را قرار می‌دهند و کلید رمزنگاری مجدد[3] که توسط کاربر A برای کاربر B صادر شده حاوی یک مقدار 'w است. متن رمزشده تنها زمانی توسط کلید رمزنگاری مجدد انتقال پیدا می‌کند که w= w' باشد. مشکل اساسی اکثر طرح‌های CPRE رایج این است که فقط با شروط ساده و مبتنی بر کلمات کلیدی کار می‌کنند که این محدودیت یک مانع بزرگ برای استفاده از آنها در محیط‌های ابری است. در این طرح برای حل مشکل ذکرشده از شروط مبتنی بر ریزدانگی برای رمزنگاری مجدد داده‌ها استفاده شده است. ابطال کاربران نیز بسیار ساده و با حذف کلیدهای رمزگشایی کاربران ابطال‌شده از محیط ابری صورت می‌گیرد و نیاز به هیچ‌گونه به‌روزرسانی کلید، توزیع کلید مجدد و به‌روزرسانی متن رمزشده نیست.

[1] two layer encryption
[2] conditional proxy re-encryption
[3] re-encryption key

Dong X و همکاران [37] با ترکیب CP-ABE و IBE[4] یک طرح انعطاف‌پذیر و قابل گسترش و مؤثر برای به‌اشتراک‌گذاری داده در محیط‌های ابری پیشنهاد دادند. در این طرح به هر ویژگی یک جفت کلید عمومی و خصوصی نسبت داده شده است و کلید مخفی کاربران از ترکیب یک شناسهٔ منحصربه‌فرد و کلید مخفی ویژگی‌ها به‌وجود می‌آید. داده‌ها بوسیله مولفه‌های کلید عمومی و ماتریس دسترسی[5] رمز می‌شوند و کاربر فقط زمانی می‌تواند به داده‌ای دسترسی پیدا کند که صفات موجود در کلیدش بتوانند ساختار دسترسی موجود در متن رمزشده را برآورده سازد.

Green و همکاران روشی جدید را برای کاهش سربار فرآیند رمزگشایی پیشنهاد دادند و آن را رمزگشایی برون‌سپاری شده نامیدند [۳۸]. این روش به یک سرور ابری این اجازه را می‌دهد تا یک متن رمزشده با CP-ABE را با استفاده از کلیدی که به‌وسیله کاربر مهیا شده است، به یک متن رمزشدهٔ ساده تبدیل کند. این کار سربار رمزگشایی در سمت کاربر را به‌طور چشم‌گیر کاهش می‌دهد؛ ولی هیچ تضمینی روی درستی و صحت انتقالات انجام‌شده به‌وسیله سرور وجود ندارد. برای تضمین اینکه سرور بیرونی به‌درستی محاسبات برون‌سپاری را انجام می‌دهد، Lai و همکاران [۳۹] مفهوم قابلیت بازبینی[6] را به رمزگشایی برون‌سپاری‌شده اضاف کردند. قابلیت بازبینی کاربر را توانا می‌سازد تا درستی اطلاعات انتقال‌یافته به‌وسیله نهاد سومی را بررسی کند. در این طرح آنها رمزشدهٔ یک مقدار تصادفی را به الگوریتم‌های رمزنگاری و رمزگشایی اضافی کردند و از آن برای بازبینی[7] اطلاعات استفاده کردند. مشکل اصلی این روش این است که طول متن رمزشده به‌دلیل اضافه‌شدن مقدار تصادفی نسبت به طرح اولیه ABE دو برابر می‌شود و همچنین هزینه محاسباتی رمزنگاری و رمزگشایی نیز نسبت به طرح‌های پیشین افزایش می‌یابد. به‌منظور ازبین‌بردن این مشکلات Lin و همکاران [۴۰] یک تکنیک جدید را بر اساس AB-KEM[8] پیشنهاد دادند. در این طرح از مفهوم رمزنگاری ترکیبی و پروتکل تعهد[9] برای اضافه‌کردن مقدار تصادفی به متن رمزشده استفاده شده است که باعث می‌شود به‌راحتی بتوان بازبینی را انجام داد. پروتکل تعهد از دو الگوریتم

[4] Identity based encryption
[5] Access matrix
[6] verifiability
[7] Check ability
[8] attribute-based key encapsulation mechanism
[9] commitment

(commit,Decommit) تشکیل شده است. در مرحلهٔ commit فرستنده یک مقدار تصادفی r را به پیام M اضافه می‌کند ($\hat{C}$ = Commit (M)). در مرحلهٔ Decommit فرستنده مقادیر (M,r) را برای گیرنده ارسال می‌کند و گیرنده بررسی می‌کند آیا $Decommit_r$ ($\hat{C}$) = M می‌شود یا نه. همچنین در این طرح از یک الگوریتم تصدیق برای بررسی‌کردن صحت محاسبات برون‌سپاری‌شده استفاده شده است. داده‌ها تنها زمانی می‌توانند رمزگشایی شوند که الگوریتم بازبینی[1] خروجی صحیح را برگرداند.

یک روش دیگر برای بررسی صحت متن رمزشدهٔ انتقال‌یافته در یک سامانه رمزنگاری مبتنی بر ویژگی در [۴۱] ارائه شده است. در این طرح مالک ابتدا پیام را با رمزنگاری متقارن رمز می‌کند و سپس کلید رمزنگاری متقارن را به‌وسیله رمزنگاری مبتنی بر ویژگی با سیاست کلید رمز می‌کند. برای بررسی صحت داده‌های انتقال‌یافته از یک کلید بازبینی به‌عنوان ورودی الگوریتم رمزگشایی استفاده شده است. کلید بازبینی همان‌طور که در (شکل_۱ مشخص است از اعمال تابع هش بر روی هش کلید متقارن و متن رمزشده ایجاد می‌شود. Tag_0 در این شکل همان متن رمزشده به‌وسیله رمزنگاری متقارن است. کاربر تنها زمانی می‌تواند داده‌ها را رمزگشایی کند که مقدار VK با مقدار VK' محاسبه‌شده برابر باشد، در غیر این صورت قادر به رمزگشایی داده‌ها نیست. مشکل اصلی طرح های پیشنهادشده در [۳۹] ، [۴۰] و [۴۱] این است که در هیچ کدام از آنها به حل مشکلات امنیتی موجود در ABE و ارائه روشی موثر برای ابطال ویژگی‌ها و کاربران اشاره‌ای نشده است که می‌تواند به‌عنوان کار آینده برای این طرح‌ها در نظر گرفته شود.

۳-۳- رمزنگاری مبتنی بر ویژگی با چندین مرجع صدور

طرح‌های رمزنگاری مبتنی بر ویژگی که در قسمت‌های قبل گفته شد؛ همگی از یک مرجع صدور برای مدیریت تمامی ویژگی‌ها استفاده می‌کنند و ازاین‌رو برای سامانه‌های با مقیاس بالا مناسب نیستند. Chase و همکاران [۴۲] برای نخستین بار یک سامانهٔ KP-ABE مبتنی بر چندین مرجع صدور و یک مرجع مرکزی را پیشنهاد دادند. مرجع مرکزی کلیدهای مخفی مرتبط با سایر مراجع را می‌داند و کاربر تنها زمانی می‌تواند داده‌ها را رمزگشایی کند که کلیدهای مخفی مرتبط با ویژگی‌هایش را از مراجع مرتبط دریافت کند. در این روش ویژگی‌ها به چندین مجموعهٔ گسسته تقسیم می‌شوند و این مجموعه‌ها توسط مراجع متفاوت که متعلق به یک دامنه مدیریتی یکسان هستند، مدیریت می‌شوند. این ساختار باعث افزایش امنیت، افزایش مقیاس‌پذیری سامانه و کاهش خطر افشای اطلاعات در صورت خراب‌شدن یکی از مراجع می‌شود. Chase و همکاران در [۴۳] طرح قبلی خود را [۴۲] بهبود دادند و با حذف مرجع مرکزی یک طرح KP-ABE مبتنی بر چندین مرجع صدور را پیشنهاد دادند. آنها همچنین در این طرح مشکلات حریم خصوصی مرتبط با کاربران را نیز بهبود دادند.

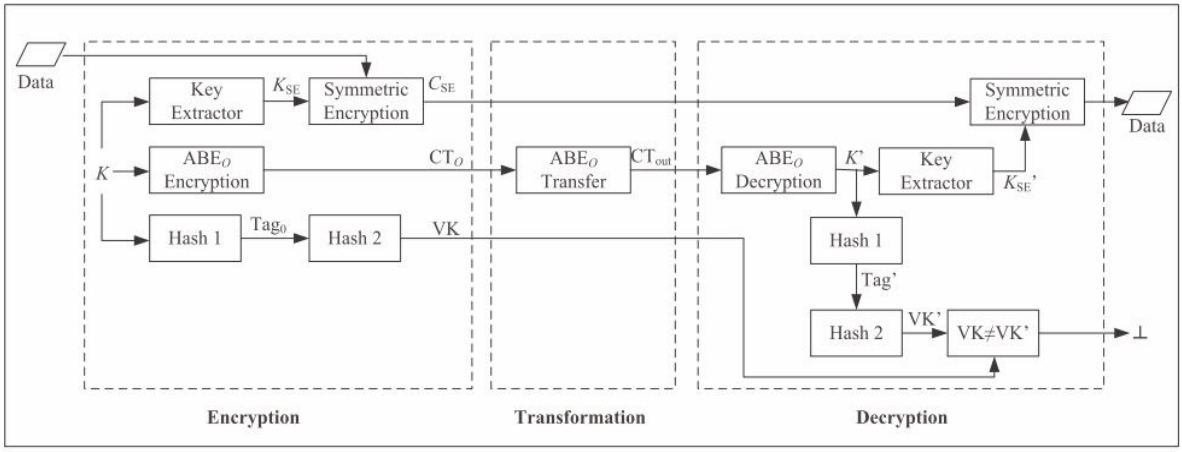
T Jungو همکاران [۴۴] یک طرح کنترل دسترسی مبتنی بر چندین منبع صدور را برای حفظ محرمانگی داده‌ها و اطلاعات هویت[2] کاربران پیشنهاد دادند. در این طرح دو روش AnonyControl و AnonyControl-F معرفی شده است که به سرورهای ابری اجازه می‌دهد امتیازات[3] کاربران را بدون شناخت اطلاعات هویتی آنها کنترل کنند.

در AnonyControl فرض بر این است که مراجع صدور سه برای به‌دست‌آوردن هویت کاربر با یکدیگر تبانی نمی‌کنند که یک فرض ضعیف است؛ زیرا اگر اطلاعات همه مراجع با یکدیگر ترکیب شود، مجموعه‌ای کامل از صفات کاربر ایجاد و هویت کاربر فاش می‌شود. AnonyControl-F با استفاده از تکنیک 1-Out-of-n Oblivious Transfer این ضعف را برطرف کرده است. در 1-Out-of-n Oblivious Transfer مراجع صدور تمامی کلیدهای ویژگی[4] تولیدی را برای کاربر ارسال می‌کنند؛ ولی کاربر فقط می‌تواند کلیدهای مرتبط با ویژگی‌های خود را ، بدون اینکه ماهیت سایر کلیدها فاش شود، دیافت کند. در این روش هیچ راه‌حلی برای ابطال کاربران و صفات در نظر گرفته نشده است که به‌عنوان کار آینده برای این مقاله می‌توان در نظر گرفت.

Yang و همکاران در [۴۵] طرح CP-ABE پیشنهاد شده به‌وسیله Water [۴۶] را برای چندین منبع صدور توسعه دادند و مدلی را برای ذخیرهٔ امن داده با استفاده از رمزنگاری مبتنی بر ویژگی پیشنهاد دادند. معماری این طرح از یک مرجع مرکزی[5] (CA) و چندین مرجع صدور تشکیل شده است.

[1] Verification

[2] Identity
[3] Privilege
[4] Attribute key
[5] Central Authority



(شکل ـ ۱): یک چارچوب نمونه برای بررسی صحت داده‌های انتقال یافته در CP-ABE [۴۱]

رمزنگاری داده‌ها بر اساس کلیدهای عمومی صادرشده به‌وسیلهٔ مراجع صدور مختلف و پارامترهای عمومی جهانی صادرشده توسط CA انجام می‌شود که این کار باعث جلوگیری از رمزگشایی داده‌ها به‌وسیله CA می‌شود. همچنین برای ابطال ویژگی‌ها به هر ویژگی یک شماره نسخه[1] نسبت داده شده است. زمانی که صفتی ابطال می‌شود، فقط مؤلفه‌های مرتبط با صفت ابطال‌شده در کلید خصوصی و متن رمزشده به‌روزرسانی می‌شوند که باعث کاهش سربار رمزنگاری مجدد داده می‌شود.

مرجع [۴۷] از دو تکنیک PRE و CP-ABE برای دستیابی به روش کنترل دسترسی مبتنی بر ریزدانه، قابل ابطال و امن در محیط‌های توزیع‌شده و حاوی چند مرجع صدور استفاده کرده است و روش MPRE-CPABE[2] را پیشنهاد داده است. در این روش ابتدا داده‌ها به دو قسمت کوچک[3] و بزرگ[4] تقسیم می‌شوند و مالک از قسمت کوچک‌تر به‌عنوان کلید خصوصی برای رمزکردن قسمت بزرگ استفاده می‌کند. همچنین قسمت کوچک با رمزنگاری مبتنی بر ویژگی رمز می‌شود. مزیت این روش این است که حتی اگر قسمت بزرگ بارگذاری‌شده بر روی ابر توسط کاربران غیرقانونی دزدیده شود، کاربران نمی‌توانند به اطلاعات کامل فایل دسترسی پیدا کنند. برای ابطال صفات نیز از یک پروکسی استفاده شده است که وظیفه رمزنگاری مجدد متن رمزشده و کلید خصوصی را در زمان ابطال صفات کاربران بر عهده دارد.

Yang و همکاران [۴۸] یک طرح کنترل دسترسی مبتنی بر ویژگی را برای محیط‌های ذخیره‌سازی ابر با چندین مرجع صدور پیشنهاد دادند و آن را DAC-MAC[5] نامید. در این طرح برای افزایش کارایی رمزگشایی از توکن استفاده شده است و بیشتر عملیات محاسباتی رمزگشایی به سرور ابری برون‌سپاری می‌شود. همچنین برای مقابله با حملات تبانی و حواله کلید به ترتیب دو راه حل زیر در نظر گرفته شده است: ۱- یک شناسهٔ منحصر به‌فرد[6] به هر کاربر اختصاص داده شده است که مانع از ترکیب کلیدهای خصوصی کاربران با هم می‌شود. ۲- در رمزنگاری داده‌ها از کلیدهای عمومی صادرشده توسط تمامی مراجع صدور استفاده شده است که از رمزگشایی داده‌ها توسط مرجع مرکزی جلوگیری می‌کند. ابطال ویژگی‌ها نیز با اختصاص شماره نسخه[7] به هر ویژگی انجام می‌شود. عیب این روش این است که هنگام ابطال صفات، هر مرجع صدور باید یک کلید برای کاربران ابطال‌نشده ایجاد کند که این کار سربار محاسباتی بالایی را برای مراجع صدور ایجاد می‌کند. همچنین یک آسیب‌پذیری امنیتی دیگر توسط Hong و همکارانش [۴۹] برای این روش اثبات شد. آنها نشان دادند

[1] Version
[2] multi-authority proxy re-encryption based on ciphertext-policy attribute-based encryption
[3] Small block
[4] Big block

[5] Data Access Control for Multi-Authority Cloud Storage
[6] Unique ID
[7] Version Number

که یک کاربر ابطال‌شده می‌تواند همچنان بـه مـتن رمزشـدهٔ جدید دسترسی داشته باشد و آن را رمزگشایی کند.

Li و همکاران [۵۰] با استفاده از رمزنگاری مبتنی بـر ویژگی طرحی را برای ذخیره و به اشتراک‌گـذاری امـن داده سلامت الکترونیک بیمـاران بـر روی سـرورهای نیمـه‌معتمـد ابری در محیط‌های چندمالکه[1]، چنـدکـاربره[2] و چنـدمرجـع پیشنهاد دادند. در این طرح به‌منظور کاهش پیچیدگی تولید و توزیـع کلیـد، سـامانه بـه دو دامنـهٔ امنیتـی عمـومی[3] و شخصـی[4] تقسـیم شـده اسـت. در دامنـهٔ شخصـی وظیفـه مدیریت کلید کاربران بر عهده مالک و در دامنـهٔ عمـومی بـر عهده مراجع صدور کلید است. هر منبـع صـدور مجموعـه‌ای گسسته از ویژگی‌هـای کـاربران را نگـه مـی‌دارد، کـه باعـث جلوگیری از حمله تبانی[5] و حواله کلید[6] توسط مراجع صدور می‌شود. همچنین در این طرح برای کاهش سربار رمزنگاری، از رمزنگاری ترکیبی استفاده شده اسـت. ابطـال کـاربران در این طرح به این صورت است که یک مرجع صدور می‌تواند با رمزنگاری مجدد داده‌ها و به‌روزرسـانی کلیـدهای رمـز، یـک کاربر یا مجموعه‌ای از ویژگی‌هـای کـاربران را ابطـال کنـد و برای بهبود کارایی حجم عظیمی از ایـن کـار بـه سـرورهای بیرونی برون‌سپاری‌شده است. این طرح گسترش‌یافتـهٔ طـرح پیشنهادشـدهٔ قبلـی توسـط Li و همکـاران [۵۱] اسـت کـه علاوه‌بر بهبود سازوکار ابطال فوری و بر حسب تقاضا کاربران، مقیاس‌پذیری سامانه را نیز بهبود داده است.

در [۵۲] Li Q و همکـارانش یـک روش کنتـرل دسترسی بنام MAACS[7] بـرای محیط‌هـای ذخیره‌سـاز ابـر پیشنهاد دادند. طرح آنها از تکنیک CP-ABE بهمراه چندین مرجع صدور برای صدور کلید برای کاربران استفاده می‌کنـد. در MAACS مالک داده برای کاهش بـار رمزنگـاری از روش ترکیبی استفاده کرده است به این صورت که ابتدا داده‌هـا را بـا رمزنگـاری متقـارن رمـز و سـپس کلیـد خصوصـی را بـا رمزنگاری مبتنی بر ویژگی رمز می‌کند. در زمـان رمزگشـایی نیـز از تکنیـک برون‌سـپاری رمزگشـایی بـرای کـاهش بـار رمزگشایی در سمت کاربر استفاده شده است. در ایـن طـرح مرجع اصلی به هر کاربر یک شناسهٔ منحصربه‌فرد اختصـاص داده است کـه مـانع از تبـانی کـاربران بـا یکـدیگر می‌شـود. همچنین ابطال کاربران نیز در سطح ویژگی انجام می‌شـود و بـا ابطـال بعضـی از صـفات یـک کـاربر، آن کـاربر همچنـان می‌تواند با سایر صفاتش متن رمزشده را رمزگشایی کند.

Horváth و همکاران [۵۳] طرح MA-CPABE[8] را برای مدیریت کنترل دسترسی داده‌های ذخیره‌شده در محیط‌های ابری دارای چند مرجع صدور اسـتفاده کردنـد و طـرح MA-CPABE را پیشنهاد دادنـد. MA-CPABE گسـترش‌یافتـهٔ طـرح Waters [۵۴] اسـت کـه در آن بـرای بـرای ابطـال کاربران از روش ابطال مبتنی بر هویت[9] استفاده شـده اسـت. در الگـوریتم رمزنگـاری، فهرسـت کـاربران ابطـال‌شـده[10] به‌عنوان ورودی دریافت می‌شود و این فهرست همراه با مـتن رمزشده برای سرور ابر فرستاده می‌شود. در هنگام رمزگشایی فقط کاربرانی می‌توانند داده‌ها را رمزگشایی کنند که شناسه آنها در فهرست ابطال نباشد. از آنجا کـه ابطـال کـاربران بـر اساس هویت آنها انجام می‌شود، هیچ تـأثیری بـر روی سـایر ویژگی‌های کاربران نمی‌گذارد و نیـاز بـه بـه‌روزرسـانی مـتن رمزشده و کلید سایر کاربران ابطال‌نشده نیست. عیب اساسی این روش این است که بدلیل اسـتفاده از فهرسـت ابطـال در زمان ابطال کاربران ویژگی امنیت پس‌سو[11] فراهم نمی‌شـود زیرا زمانی‌که کاربری از سامانه حذف شود همچنان می‌توانـد به داده‌های قبلی دسترسی داشته باشد.

K Han و همکاران [۵۵] یک طـرح مبتنـی بـر ویژگـی توزیع‌شده[12] برای به اشتراک‌گذاری داده در محیط‌های ابری پیشنهاد دادند. معماری مـدل پیشـنهادی آنهـا از پـنج نهـاد مالک داده، کاربر، سرور ابری، مرکز تولید کلیـد[13] و چنـدین مرکز صدور گواهی ایجاد شده است. مرکز تولید کلید، وظیفه صدور پارامترهای کلید خصوصی و عمومی را بـرای سیسـتم بر عهـده دارد. مراجـع صـدور نیـز وظیفـه ارسـال، ابطـال و بروزرسانی پارامترهای مخفی جهت محاسبه کلیدهای ویژگی کاربران را بر عهده دارنـد. در ایـن طـرح بـرای جلـوگیری از حمله تبانی برای هر کاربر یک شناسهٔ منحصربه‌فـرد در نظـر

[1] Multi owner
[2] Multi user
[3] Public
[4] Private
[5] Collusion attack
[6] key escrow
[7] Multi-Authority Access Control System

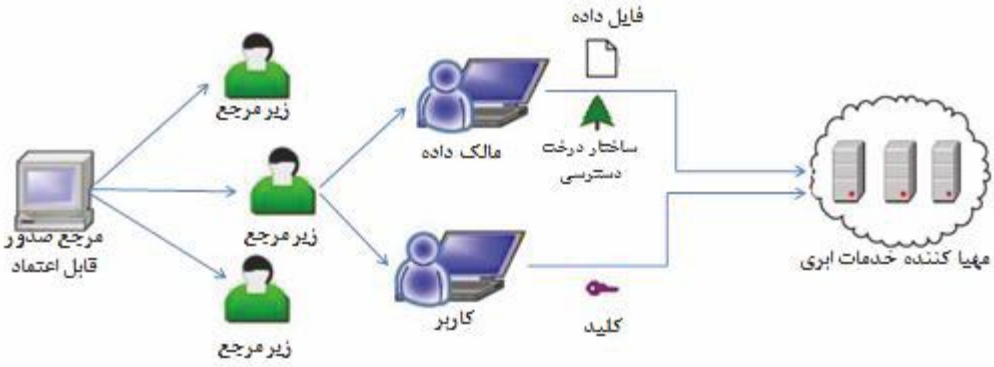
[8] Multi authority Ciphertext policy attribute based encryption
9 identity-based revocation
10 Revoked list
11 Backward Security
12 Decentralize attribute base
13 Key Generation Center

گرفته شده است. این شناسه در تولید کلیدهای ویژگی کاربران استفاده می‌شود و بنابراین کاربران مختلف دارای کلیدهای ویژگی متفاوتی هستند و نمی‌توانند آنها را با هم ترکیب کنند. همچنین برای اینکه از تبانی بین مراکز صدور گواهی جلوگیری شود یک عدد تصادفی توسط سرور ابری در کلید مخفی کاربر قرار داده می‌شود؛ چون مراکز صدور گواهی این مقدار تصادفی را نمی‌دانند درنتیجه با تبانی نیز نمی‌توانند به کلید کاربر دسترسی پیدا کنند.

طرح‌های بیشتری از رمزنگاری مبتنی بر ویژگی با چندین مرجع صدور در [۵۶]،[۶۰] بیان شده است.

۳-۴- رمزنگاری مبتنی بر ویژگی سلسله مراتبی

مفهوم رمزنگاری مبتنی بر ویژگی سلسله‌مراتبی برای نخستین بار توسط Gentry و همکارانش [۶۱] پیشنهاد شد. تاکنون طرح‌های CP-ABE سلسله‌مراتبی زیادی پیشنهاد شده است [۶۲]،[۶۴]. برای مثال Wang و همکاران [۶۵] یک طرح کنترل دسترسی سلسله‌مراتبی را پیشنهاد دادند که مبتنی بر رمزنگاری مبتنی بر شناسهٔ سلسله‌مراتبی و CP-ABE است. ساختار این طرح به‌صورت سلسله‌مراتبی است که در راس آن یک ریشهٔ اصلی وجود دارد و در سطح بعدی مراجع صدور دامنه وجود دارند که برای کاربران کلید تولید می‌کنند. اگرچه پیچیدگی این سامانه بالا می‌باشد زیرا برای هر نهاد تعداد زیادی کلید لازم است.



(شکل ـ ۲): یک نمونه از ساختار سلسله‌مراتبی مورد استفاده در ABE [۶۶]

Wan و همکاران [۶۶] یک مدل کنترل دسترسی مبتنی بر ریزدانگی را پیشنهاد دادند و آن را طرح رمزنگاری سلسله‌مراتبی مبتنی بر مجموعه ویژگی[1] نامیدند. (شکل ۲_ مدل سامانه مورد استفاده در این طرح را نشان می‌دهد. همان‌طور که مشخص است در این طرح یک مرجع صدور قابل اعتماد، وظیفهٔ تولید و توزیع پارامترهای سامانه و کلیدهای اصلی را برای مراجع سطح بعد برعهده دارد. در سطح دوم مراجع صدور دامنه وجود دارند که وظیفه تخصیص کلید به مراجع سطح بعدی یا کاربران را در دامنه خودشان بر عهده دارند.

هر کاربر در سامانه یک ساختار کلید دارد که صفات مرتبط با کلید رمزگشایی‌اش را مشخص می‌کند. در این سامانه، مالکان یا کاربران داده نیاز نیست که همیشه برخط باشند و فقط در زمان مورد نظر برخط می‌شوند؛ ولی مهیاکنندگان سرویس ابر، مرجع صدور قابل اعتماد و مراجع صدور دامنه باید همیشه برخط باشند. ملاحظات امنیتی نشان می‌دهد که طرح پیشنهادی در مقابل حملات تبانی بین کاربران امن است، اگرچه به‌دلیل استفاده از یک زمان انقضا در کلید کاربران فاقد سازوکار موثر و فوری برای ابطال کاربران است.

۴- تحلیل امنیتی و عملکردی

در این قسمت به بررسی و مقایسه روش‌های ارائه‌شده در بخش ۳،۱ می‌پردازیم و آنها را از لحاظ ویژگی‌های عملکردی و نحوه ابطال کاربران جدول (۱) و ویژگی‌های امنیتی جدول (۲) مقایسه می‌کنیم. همان‌طور که در جدول ۱ مشخص است،اکثر طرح‌های بررسی‌شده از چندین مرجع صدور برای صدور کلیدهای خصوصی کاربران استفاده می‌کند [۴۴]،[۵۰]،[۴۵]،[۶۶]،[۴۷]،[۴۸]،[۵۲]،[۵۳]،[۵۵].

دلیل آن این است که در محیط ابری چون ویژگی‌های

[1] hierarchical attribute-set-based encryption

کاربران بوسیله مراجع مختلف صادر می‌شود استفاده از کنترل دسترسی مبتنی بر چند مرجع نسبت به کنترل دسترسی مبتنی بر یک مرجع کاربردی‌تر است. همچنین استفاده از طرح‌های مبتنی بر چندین مرجع امکان حمله حواله کلید و دستیابی یک مرجع صدور به کلید کاربران را تا حد امکان از بین می‌برد. یکی از ویژگی‌های مهم دیگر در این حوزه مباحث مرتبط با روش‌های اثبات امنیت طرح های پیشنهادی و مقاوم بودن در مقابل حملات مختلف است. اکثر روش‌های بیان‌شده از روش گروه دوخطی عمومی[1] و مدل‌های پیش‌گوی تصادفی[2] برای اثبات امنیت طرح‌های خود استفاده کرده‌اند. چهار حمله متداول و رایج در این حوزه وجود دارد که در هنگام طرح‌ریزی یک معماری کنترل دسترسی مبتنی بر ویژگی باید برای مقابله با آنها راه‌کارهایی را در نظر گرفت. این چهار حمله و روش‌های بیان‌شده برای مقابله با آنها در ادامه آورده شده است:

حمله تبانی[3]: یکی از ویژگی‌های امنیتی مهم در ABE که در اکثر طرح‌ها به آن اشاره شده است حملات تبانی است. حمله تبانی زمانی اتفاق می‌افتد که دو یا چند کاربر غیرمجاز با ترکیب کلیدهای خصوصی خود بتوانند داده‌هایی را رمزگشایی کنند که به‌تنهایی قادر به رمزگشایی‌شان نیستند. یکی از روش‌های رایج برای مقابله با این حمله، اختصاص یک شناسهٔ منحصر به‌فرد برای هر کاربر است. در این حالت کلیدهای خصوصی مرتبط با هر کاربر حاوی یک مقدار یکتا به‌نام شناسهٔ منحصربفرد[4] است و درنتیجه کاربران متفاوت جهت رمزگشایی داده نمی‌توانند کلیدهایشان را با هم ترکیب کنند.

حملهٔ حواله کلید: این حمله به معنی دسترسی مرجع یا مراجع صدور کلید به کلید خصوصی کاربران و رمزگشایی داده‌ها است. این حملات در طرح‌هایی که از یک مرجع مرکزی برای صدور کلید استفاده می‌کنند، رایج‌تر و بهترین روش مقابله با آن استفاده از چندین مرجع صدور برای تولید پارامترهای رمزنگاری و رمزگشایی است.

حمله جستجوی کامل[5]: این حمله بیشتر در طرح‌هایی که از روش‌های ترکیبی برای رمزنگاری داده‌ها استفاده می‌کنند، ممکن است به وقوع بپیوندد و به معنی تلاش متعدد حمله‌کننده برای به‌دست‌آوردن کلید رمزگشایی است. روش پیشنهادی در [۴۷] برای مقابله با این حمله به این صورت است که هنگام استفاده از رمزنگاری ترکیبی ابتدا داده‌ها را به دو قسمت کوچک و بزرگ تقسیم کرده و سپس از قسمت کوچک‌تر به‌عنوان کلید خصوصی برای رمزنگاری متقارن قسمت بزرگ‌تر استفاده می‌شود. همچنین قسمت کوچک‌تر با رمزنگاری مبتنی بر ویژگی رمز می‌شود. با استفاده از این روش حتی اگر قسمت بزرگ بارگذاری‌شده بر روی ابر توسط حمله جستجوی کامل رمزگشایی شود، کاربران نمی‌توانند به اطلاعات کامل فایل دسترسی پیدا کنند.

حمله منع سرویس (DOS). حمله DOS به حملاتی گفته می‌شود که با هدف ازکارانداختن سرویس یا سرویس‌هایی خاص از یک سرور صورت می‌گیرد. در ABE این دسته از حملات زمانی ممکن است اتفاق بیفتد که جهت رمزگشایی جزئی داده‌ها از توکن استفاده شود. در این حالت اگر یک کاربر غیرمجاز به توکن دسترسی پیدا کند، می‌تواند باعث بروز حمله DOS بر روی سرور شود. راه‌حل پیشنهادی در [۳۳] استفاده از یک مهر زمان برای محدودکردن زمان اعتبار توکن‌ها است.

سایر معیارهای درنظرگرفته‌شده جهت مقایسه طرح‌های بررسی‌شده عبارتند از: حفظ هویت کاربران، برون‌سپاری رمزگشایی، قابلیت بازبینی داده‌های برون‌سپاری‌شده، رمزنگاری ترکیبی و ابطال کاربران. نتایج مقایسه به‌ترتیب در جدول (۱) و (۲) نشان داده شده است. در این جداول نشان‌های √ و X به‌ترتیب نشان‌دهنده این است که آیا معیار موردنظر به‌وسیله طرح پیشنهادی برآورده شده است یا خیر. همچنین علامت – به این معنی است که هیچ اشاره‌ای راجع به معیار مورد نظر نشده است. همچنین در جدول ۳ نیز مزایا و معایب هر کدام از روش‌های بررسی‌شده در بخش ۱,۳ ارائه شده است.

[1] generic bilinear group
[2] random oracle models
[3] Collusion
[4] Unique ID
[5] brute force

(جدول_ ۱): مقایسه اجرایی و فنی راه‌حل‌های ارائه‌شده در کنترل دسترسی مبتنی بر ویژگی

Scheme	CP/KP	Multi-authority	Decryption Outsourcing	verifiability	Symmetric encryption	Revocation / (method)	Key update by	ciphertext update by	Immediate revocation	Attribute/user revocation
[۵۵]	CP	√	X	X	X	X	X	X	X	X
[۴۱]	CP	X	X	X	√	√	System peers	Cloud Server	√	both
[۶۱]	CP	√	X	X	√	√	Authority	Proxy	√	both
[۴۰]	CP	X	√	X	√	√			√	both
[۵۶]	CP	√	X	X	√	√	Authority	Cloud Server	√	attribute
[۷۷]	CP	√	X	X	√	√	Authority	Cloud Server	X	user
[۵۰]	CP	X	√	√	X	X	X	X	X	X
[۵۱]	CP/KP	X	√	√	√	X	X	X	X	X
[۵۲]	CP/KP	X	√	√	√	X	X	X	X	X
[۵۸]	CP	√	X	X	√	√	proxy authority	Proxy authority	√	User revocation
[۴۵]	CP/KP	X	√	√	X	X	X	X	X	X
[۵۹]	CP	√	√	X	√	√	Non-revoked Users	Cloud Server	√	Attribute revocation
[۴۶]	-	X	X	X	X	√	X	Cloud Server	√	User revocation
[۴۴]	CP	X	√	X	X	√	X	X	√	User revocation
[۶۳]	CP	√	√	X	√	√	Authority	Cloud Server	√	Attribute revocation
[۴۷]	CP	X	√	X	X	√	X	X	√	User revocation
[۴۲]	CP	X	X	X	√	√	Authority	Cloud Server	√	Attribute revocation
[۶۴]	CP	√	X	X	√	√	-	-	√	User revocation
[۶۶]	CP	√	X	X	X	√	Cloud Server	Data owner	√	Attribute revocation
[۴۸]	CP	X	X	X	X	√	-	Data owner	√	both

(جدول _۲): مقایسه امنیتی راه‌حل‌های ارائه‌شده در کنترل دسترسی مبتنی بر ویژگی

Scheme	Security Approval	Security Assumption	Collusion Attack resistant	Key escrow Attack resistant	Brute force attack resistant	Dos Attack resistant	Identity Privacy
[۵۵]	-	DBDH	√	√	X	X	√
[۴۱]	Selective	DBDH	√	X	X	X	√
[۶۱]	Selective	–	√	√	X	X	X
[۴۰]	Semantic	-	√		X	X	
[۵۶]	-	q-parallel BDHE	√	√	X	X	X
[۷۷]	-	–	√	X	X	X	X
[۵۰]	Selective	-	X	X	X	X	X
[۵۱]	Selectively	q-parallel BDHE	X	X	X	X	X
[۵۲]	Selective	-	X	X	X	X	X
[۵۸]	–	DBDH	√	√	√	X	X

[۴۵]	Selective	DBDH	√	X	X	X	X
[۵۹]	Selective	q-parallel BDHE	√	√	X	X	X
[۴۶]	-	-	X	X	X	X	√
[۴۴]	-	-	√	X	X	√	X
[۶۳]	Adaptive	-	√	√	X	X	X
[۴۷]	-	-	X	X	X	X	X
[۴۲]	Selective	n-BDHE	√	X	X	X	X
[۶۴]	-	-	√	√	X	X	X
[۶۶]	-	-	√	√	X	X	X
[۴۸]	Semantic	-	√	√	X	X	√

(جدول_۳): مزایا و معایب روش‌های بررسی شده

طرح	مزایا	معایب
[۴۴]	حفظ محرمانگی داده و هویت کاربران.	الگوریتم AnonyControlF به دلیل استفاده از تکنیک 1-Out-of-n Oblivious Transfer سربار محاسباتی بیشتری را تولید می‌کند. عدم وجود سازوکاری برای ابطال کاربران و صفات.
[۳۰]	کاهش بار محاسباتی ابطال کاربران در سمت مالک و سامانه ابری.	عدم مقابله در برابر حملات حواله کلید.
[۵۰]	کاهش سربار مدیریت کلید. ابطال مؤثر کاربران.	عدم بیان سیاست دسترسی در مقاله.
[۲۹]	کنترل دسترسی امن با استفاده از DRM.	عدم مقابله در برابر حملات حواله کلید
[۴۵]	مقاوم‌بودن در برابر حملات تبانی و حواله کلید.	طول کلید رمزگشایی با تعداد صفات رابطه خطی دارد. سربار محاسباتی بالا در زمان رمزنگاری مجدد داده‌ها.
[۶۶]	مقیاس‌پذیری و انعطاف‌پذیری بالا.	عدم پشتیبانی از دو ویژگی امنیت پس‌سو و امنیت پیش‌سو در هنگام ابطال کاربران.
[۳۹]	حل مشکل بازبینی اطلاعات برون سپاری‌شده.	افزایش سربار رمزنگاری و رمزگشایی داده‌ها. افزایش طول متن رمزشده.
[۴۰]	کاهش سربار رمزنگاری در سمت کاربر به دلیل استفاده از رمزنگاری ترکیبی.	اثبات امنیت به‌صورت انتخابی[1] صورت گرفته است.
[۴۱]	کاهش سربار رمزنگاری در سمت کاربر به دلیل استفاده از رمزنگاری ترکیبی. مقاوم‌بودن در برابر حملات برخوردی[2]	کاربر نمی‌تواند داده‌ها را به‌صورت مستقیم و بدون استفاده از رمزگشایی برون‌سپاری‌شده، رمزگشایی کند.
[۴۷]	مقاوم در برابر حملات جستجوی کامل. ابطال مؤثر کاربران.	سربار محاسباتی بالای پروکسی در زمان ابطال.
[۳۴]	کاهش بار محاسباتی در سمت کاربر و مرجع صدور.	عدم وجود سازوکاری برای ابطال کاربران. عدم مقابله با حملات حواله کلید.

1 Selectively
2 Collision

[۴۸]	کاهش سربار محاسباتی رمزگشایی. مقاوم در برابر حملات تبانی.	اعمال سربار محاسباتی سنگین به مرجع صودر کلید در مرحلهٔ ابطال کاربر.
[۳۵]	کاهش سربار رمزنگاری مالک داده.	مشکل‌بودن تقسیم سیاست دسترسی به دو سیاست مجزا برای مالک و ابر.
[۳۳]	مقاوم بودن در مقابل حملات DOS.	سربار رمزنگاری بالا.
[۵۲]	سربار رمزنگاری پایین. روش ابطال مؤثر کاربر در سطح ویژگی.	بار محاسباتی بالا برای تولید کلید به‌روزرسانی در زمان ابطال کاربران توسط AA.
[۳۶]	سربار محاسباتی پایین هنگام ابطال کاربر. سربار محساباتی پایین رمزگشایی برای کاربر.	عدم مقابله با حملات حواله کلید و تبانی.
[۳۱]	هزینه محاسباتی ثابت و سربار ارتباطی پایین.	استفاده از یک مرجع صدور گواهی.
[۵۳]	مقاوم‌بودن در برابر حملات تبانی وحواله. کلید	عدم امکان ابطال ویژگی و عدم پشتیبانی از ویژگی. امنیت پس‌سو
[۵۵]	ابطال مؤثر کاربران. مقاوم‌بودن در برابر حملات تبانی و حواله کلید.	سربار رمزنگاری بالا در سمت کاربر.
[۳۷]	ابطال فوری کاربران و صفات. مقاوم در برابر حملات تبانی.	سربار محاسباتی بالا در سمت کاربر به‌دلیل رمزنگاری داده‌ها، تولید کلید خصوصی برای کاربران و رمزنگاری مجدد داده‌ها هنگام ابطال کاربران.

۵- نتیجه گیری و کارهای آینده

در این مقاله به بررسی روش‌های رمزنگاری مبتنی بر ویژگی و کاربرد آن در مدیریت کنترل دسترسی در محیط‌های ابری پرداختیم. همچنین طرح‌های مختلف کنترل دسترسی را که از رمزنگاری مبتنی بر ویژگی برای حفظ محرمانگی داده‌های ذخیره‌شده در محیط‌های ابری استفاده می‌کنند بررسی و سعی کردیم مقایسه‌هایی از نظر امنیت و کارایی آنها ارائه دهیم. با توجه به مطالب بیان‌شده، طرح‌های رمزنگاری مبتنی بر ویژگی کنونی را می‌توان به چهار دسته تقسیم کرد: ۱- رمزنگاری مبتنی بر ویژگی با سیاست متن رمزشده، ۲- رمزنگاری مبتنی بر ویژگی با سیاست کلید، ۳- رمزنگاری مبتنی بر ویژگی سلسله‌مراتبی و ۴- رمزنگاری مبتنی بر ویژگی با چندین مرجع صدور. می‌توان نتیجه گرفت که در محیط‌های توزیع‌شده مانند رایانش ابری، روش رمزنگاری مبتنی بر ویژگی با سیاست متن رمزشده به‌دلیل مزایا و ویژگی‌های زیر چه در حوزه دانشگاهی و چه در حوزه صنعت بیشتر از سایر روش‌ها مورد استفاده قرار می‌گیرد:

در CP-ABE سیاست‌های دسترسی در متن رمزشده تعریف می‌شود و رمزکننده کنترل مستقیم بر روی سیاست رمزنگاری دارد و مشخص می‌کند که چه کسی می‌تواند به داده‌های رمزشده دسترسی داشته باشد.

در هنگام ابطال کاربران نیاز است تا ضمن رمزنگاری مجدد داده‌ها، برای کاربران ابطال‌نشده کلید رمزنگاری مجدد ارسال شود. در KP-ABE این کار باعث ایجاد مشکلات قابل توجه در پیاده‌سازی می‌شود و کارایی و انعطاف‌پذیری سامانه را کاهش می‌دهد.

در KP-ABE نیاز است تا تمامی ویژگی‌های کاربران از ابتدا مشخص باشد که در محیط‌های ابری این کار عملی نیست.

همچنین پیشنهاد می‌شود با توجه به افزایش روزافزون خدمات ابری در کشور، سازمان‌ها و افراد جهت ذخیرهٔ داده‌های خود بهتر است که از این روش کنترل دسترسی برای افزایش امنیت و محرمانگی داده‌ها خود استفاده کنند.

۶- منابع

[1] C. R, "Intermediaries in cloud-computing: A new computing paradigm," INFORMS Meet., 1997.

[2] M. Ali, S. U. Khan, and A. V Vasilakos, "Security in cloud computing : Opportunities and challenges," Inf. Sci. (Ny)., vol. 305, pp. 357–383, 2015.

[3] N. H. Hussein, "A survey of Cloud Computing Security challenges and solutions II- Infrastructure as Services," International Journal of Computer Science and Information Security, vol. 14, no. 1, pp. 52–56, 2016.

[4] M. Ali, S. U. Khan, and A. V Vasilakos, "Security in Cloud Computing : Opportunities and Challenges," INFORMATION SCIENCES, Inf. Sci. (Ny)., 2015.

[5] F. Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges , Approaches and Solutions," Procedia Computer Science. Sci., vol. 37, pp. 357–362, 2014.

[6] C. Modi, D. Patel, and B. Borisaniya, "A survey on security issues and solutions at different layers of Cloud computing," The Journal of Supercomputing, 2012.

[7] Z. Xiao, Y. Xiao, and S. Member, "Security and Privacy in Cloud Computing," IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, 2013.

[8] F. Sabahi, "Cloud Computing Security Threats and Responses," Communication Software and Networks, pp. 245–249, 2011.

[9] J. Che, Y. Duan, T. Zhang, and J. Fan, "Procedia Engineering," Procedia Eng., vol. 23, pp. 586–593, 2011.

[10] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a Service Security : Challenges and Solutions." Informatics and Systems Conference, vol. 12, no. 2, pp. 245–861, 2010.

[11] N. Meghanathan, "R EVIEW OF ACCESS CONTROL MODELS FOR CLOUD COMPUTING," CS & IT-CSCP, no. i, pp. 77–85, 2013.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure , Scalable , and Fine-grained Data Access Control in Cloud Computing," IEEE INFOCOM, 2010.

[13] R. Sandhu and Q. Munawer, "to do Discretionary Access Control Using Roles *,"3rd ACM workshop, pp. 47–54.

[14] S. Osborn, R. Sandhu, and Q. Munawer, "Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies," ACM Transactions on Information and System Security, vol. 3, no. 2, pp. 85–106, 2000.

[15] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models yz 1 INTRODUCTION," vol. 29, no. 2, pp. 38–47, 1996.

[16] V. Hu and D. F. Ferraiolo, "Assessment of Access Control Systems," IEEE Computer, no. January 2007, 2016.

[17] W. Lafayette, W. Lafayette, and G. Ghinita, "Towards Mechanisms for Detection and Prevention of Data Exfiltration by Insiders." ASIACCS, 2011.

[18] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," EUROCRYPT, pp. 457–473, 2005.

[19] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," CCS, pp. 89–98, 2006.

[20] C. Wang and J. Luo, "An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length," Concurrency Computat, vol. 2013, 2013.

[21] Y. Rouselakis and B. Waters, "Practical Constructions and New Proof Methods for Large Universe Attribute-Based Encryption Categories and Subject Descriptors," ACM, pp. 463–474, 2013.

[22] R. Ostrovsky, "Attribute-Based Encryption with Non-Monotonic Access Structures," CCS, pp. 195–203, 2007.

[23] T. Okamoto, "Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption *," no. 2, pp. 191–208, 2011.

[24] C. Ciphertexts and N. Attrapadung, "Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts,"PKC, pp. 1–22, 2011.

[25] C. Gentry and B. Waters, "Attribute-Based Encryption for Circuits from Multilinear Maps," pp. 1–25.

[26] A. Lewko, "Fully Secure Functional Encryption : Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,"EUROCRYPT, vol. 02, no. subaward 641, pp. 1–56. 2010.

[27] B. Waters, "Functional Encryption for Regular Languages," Advances in Cryptology–CRYPTO 2012., pp. 1–18.

[28] J. Bethencourt and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," IEEE

symposium on security and privacy (SP'07) 2007.

[29] H. Qinlong, M. A. Zhaofeng, Y. Yixian, N. I. U. Xinxin, and F. U. Jingyi, "Attribute Based DRM Scheme with Dynamic Usage Control in Cloud Computing," pp. 50–63.

[30] H. He, R. Li, X. Dong, and Z. Zhang, "Secure , Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud," IEEE Transactions on Cloud Computing2.4 (2014), vol. 2, no. 4, pp. 471–484, 2014.

[31] Y. Zhang, D. Zheng, X. Chen, J. Li, and H. Li, "Efficient attribute-based data sharing in mobile clouds ☆," Pervasive Mob. Comput., 2015.

[32] J. Hur, "Attribute-Based Secure Data Sharing with Hidden Policies in Smart Grid," IEEE Transactions on Parallel and Distributed Systems vol. 24, no. 11, pp. 2171–2180, 2013.

[33] M. Bayat and H. Reza, "A revocable attribute based data sharing scheme resilient to DoS attacks in smart grid," Wireless Networks, pp. 871–881, 2015.

[34] J. Li, X. Huang, J. Li, X. Chen, Y. Xiang, and S. Member, "Securely Outsourcing Attribute-Based Encryption with Checkability," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201–2210, 2014.

[35] M. Nabeel and E. Bertino, "Privacy Preserving Delegated Access Control in Public Clouds," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 9, pp. 2268–2280, 2014.

[36] Y. Yang, H. Zhu, H. Lu, J. Weng, and Y. Zhang, "Cloud based data sharing with fine-grained proxy," Pervasive Mob. Comput., 2015.

[37] X. Dong, J. Yu, Y. Luo, Y. Chen, and G. Xue, "ScienceDirect Achieving an effective , scalable and privacy-preserving data sharing service in cloud computing," Comput. Secur., vol. 42, pp. 151–164, 2013.

[38] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts." USENIX Security Symposium. Vol. 2011. No. 3. 2011.

[39] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-Based Encryption With Veri fi able Outsourced Decryption," IEEE Transactions on information forensics and security, vol. 8, no. 8, pp. 1343–1354, 2013.

[40] S. Lin, R. Zhang, H. Ma, and M. Wang, "Revisiting Attribute-Based Encryption With Verifiable Outsourced Decryption," IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2119–2130, 2015.

[41] B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption," IEEE Transactions on Information Forensics and Security, vol. 6013, no. c, pp. 1–10, 2015.

[42] M. Chase, "Multi-Authority Attribute Based Encryption." Theory of Cryptography Conference. Springer Berlin Heidelberg, 2007.

[43] M. Chase, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009.

[44] T. Jung, X. Li, S. Member, Z. Wan, and M. Wan, "Control Cloud Data Access Privilege and Anonymity With Fully Anonymous," IEEE Transactions on Information Forensics and Securit , vol. 10, no. 1, 2015.

[45] K. Yang, S. Member, and X. Jia, "Expressive , Efficient , and Revocable Data Access Control for Multi-Authority Cloud Storage," IEEE transactions on parallel and distributed systems, vol. 25, no. 7, pp. 1735–1744, 2014.

[46] A. Lewko and B. Waters, "New Proof Methods for Attribute-Based Encryption : Achieving Full Security through Selective Techniques." Advances in Cryptology–CRYPTO 2012. Springer Berlin Heidelberg, 2012.

[47] X. Xu, J. Zhou, X. Wang, and Y. Zhang, "Multi-authority proxy re-encryption based on CPABE for cloud storage systems," Journal of Systems Engineering and Electronics, vol. 27, no. 1, pp. 211–223, 2016.

[48] K. Yang, S. Member, X. Jia, K. Ren, and S. Member, "DAC-MACS : Effective Data Access Control for Multi-Authority Cloud Storage Systems," no. c, pp. 1–12, 2013.

[49] J. Hong, K. Xue, and W. Li, "Security Analysis of Attribute Revocation in Multi-Authority Data Access Control for Cloud Storage System," International Conference on Security and Privacy in Communication Systems. Springer Berlin Heidelberg, vol. 6013, no. c, pp. 1–2, 2015.

[50] M. L. Member, S. Yu, Y. Zheng, S. Member, and K. Ren, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption," IEEE transactions on parallel and distributed systems, vol. 24, no. 1, pp. 1–14, 2013.

[51] M. Li, S. Yu, K. Ren, and W. Lou, "Securing

Personal Health Records in Cloud Computing : Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings," IEEE transactions on parallel and distributed systems, pp. 89–106, 2010.

[52] R. Li, X. Liu, J. Xiong, D. Chen, R. Li, X. Liu, J. Xiong, and D. Chen, "Secure , efficient and revocable multi-authority access control system in cloud storage," Computers & Security , 2016.

[53] Horváth, Máté. "Attribute-based encryption optimized for cloud computing." International Conference on Current Trends in Theory and Practice of Informatics. Springer Berlin Heidelberg, 2015..

[54] A. Lewko, "Decentralizing Attribute-Based Encryption," Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg,, vol. 02, pp. 1–31, 2006.

[55] N. Science, C. Phenomena, K. Han, Q. Li, and Z. Deng, "Security and efficiency data sharing scheme for cloud storage," Chaos, Solitons & Fractals, vol. 86, pp. 107–116, 2016.

[56] Z. Liu, Z. Cao, Q. Huang, and D. S. Wong, "Fully Secure Multi-authority Ciphertext-Policy Attribute-Based Encryption without Random oracles," European Symposium on Research in Computer Security. Springer Berlin Heidelberg, no. 61033014, pp. 278–297.

[57] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority q," Inf. Sci. (Ny)., vol. 180, no. 13, pp. 2618–2632, 2010.

[58] Moreno, Edward David. Transactions on Computational Science X: Special Issue on Security in Computing. Eds. Marina L. Gavrilova, and CJ Kenneth Tan. Vol. 6340. Springer, 2010.

[59] J. Han, S. Member, W. Susilo, and S. Member, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 11, 2012.

[60] V. Božovi, "Multi-authority attribute-based encryption with honest-but-curious central authority," International Journal of Computer Mathematics, vol. 89, no. 3, pp. 268–283, 2012.

[62] Z. O. U. Xiubin, "A Hierarchical Attribute-Based Encryption Scheme," Wuhan University Journal of Natural Sciences, vol. 18, no. 3, pp. 259–264, 2013.

[63] L. You and L. Wang, "Hierarchical Authority Key-Policy Attribute-Based Encryption," 2015 IEEE 16th International Conference on Communication Technology (ICCT, pp. 868–872.

[64] H. Deng, Q. Wu, B. Qin, J. Domingo-ferrer, L. Zhang, and J. Liu, "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," Inf. Sci. (Ny)., vol. 275, pp. 370–384, 2014.

[65] G. Wang and Q. Liu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proceedings of the 17th ACM conference on Computer and communications security. ACM, pp. 1–3, 2010.

[66] Z. Wan, J. Liu, R. H. Deng, and S. Member, "HASBE : A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing," IEEE transactions on information forensics and security, vol. 7, no. 2, pp. 743–754, 2012.

سعید رضائی مدرک کارشناسی خود را در رشته مهندسی فناوری اطلاعات از دانشگاه دولتی جهرم در سال ۱۳۹۲ اخذ نمود و هم‌اکنون بعنوان دانش‌پژوه مقطع کارشناسی ارشد در رشته فناوری اطلاعات گرایش امنیت اطلاعات در دانشگاه شاهد مشغول می‌باشد. زمینه‌های پژوهشی مورد علاقه ایشان شامل رمزنگاری، حریم خصوصی و امنیت رایانش ابری می‌باشد.

محمدعلی دوستاری در سال ۱۳۵۴ وارد دانشکده مهندسی دانشگاه شیراز شد و در رشته مهندسی کامپیوتر به تحصیل پرداخت. از سال ۱۳۶۶ الی۱۳۷۲ با اخذ بورسیه دولتی ژاپن جهت گذراندن یک دوره تحقیقاتی، دوره کارشناسی ارشد و دوره دکتری به کشور ژاپن عزیمت نمود و در دانشگاه صنعتی کیوتو در زمینه الکترونیک و اطلاعات به تحصیل پرداخت. ایشان پس از بازگشت از تحصیل، در گروه مهندسی کامپیوتر دانشکده فنی و مهندسی دانشگاه شاهد همکاری خود را با آن دانشگاه آغاز نمود. در حال حاضر تمرکز پژوهش‌های ایشان در زمینه امنیت اطلاعات، کارت هوشمند، زیر ساخت کلید عمومی، شناسایی هویت و بیومتریک می باشد.

مجید بیات در سال ۹۳ دکترای خود را در رشته رمزنگاری از دانشگاه خوارزمی اخذ نموده است. پس از آن به صورت پژوهشگر پسا دکتری در دانشگاه صنعتی شریف مشغول شد. ایشان هم‌اکنون استادیار گروه مهندسی کامپیوتر دانشکده فنی و مهندسی دانشگاه شاهد می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان شامل پروتوکل‌های رمزنگاری و امنیت شبکه‌های توزیع شده است.