مرور طرح‌های رمزگذاری قابل جستجو: رده‌بندی، روش‌ها و تحولات اخیر

محمد حسین نوراله‌زاده[1]، احمد غلامی[2] و رضا علیمرادی[3]

[1]دانشجوی دکتری ریاضی دانشکده علوم پایه، دانشگاه قم، قم، ایران
Mh.noorallahzadeh@stu.qom.ac.ir

[2]دانشیار دانشکده علوم ریاضی، دانشگاه قم، قم، ایران
a.gholami@qom.ac.ir

[3]استادیار گروه ریاضی و علوم کامپیوتر دانشکده علوم پایه، دانشگاه قم، قم، ایران
alimoradi@qom.ac.ir

چکیده

با پیدایش رایانش ابری، مالکان داده تمایل دارند تا داده‌های خود را به سرورهای ابری بسپارند و به کاربران اجازه دهند تا در صورت لزوم به داده‌ها دسترسی پیدا کنند. با این حال، برون سپاری داده‌های حساس مسائل حریم خصوصی را به دنبال خواهد داشت. رمزگذاری داده‌ها قبل از برون سپاری، مسائل حریم خصوصی را حل می‌کند، اما در این حالت، قابلیت جستجو در داده‌ها را از دست خواهیم داد. برای دستیابی به این قابلیت یعنی جستجو در داده‌های رمزگذاری شده بدون به خطر انداختن حریم خصوصی، طرح‌های رمزگذاری قابل جستجو (SE)[1] پیشنهاد شده است. با این روش هم از از اطلاعات حساس کاربر محافظت می‌شود و هم قابلیت جستجو در داده‌های رمزگذاری شده را خواهیم داشت. در این مقاله، طرح‌های مختلف SE را مرور می‌کنیم. در این مرور، رده بندی طرح‌های SE را ارائه می‌نماییم: رمزگذاری قابل جستجوی متقارن[2]، رمزگذاری قابل جستجوی کلید عمومی[3] و طرح‌های رمزگذاری قابل جستجو ویژگی مبنا[4]، و سپس بحث مفصلی در مورد طرح‌های SE از نظر ساختار نمایه[5] و قابلیت جستجو[6] ارائه می‌کنیم. همچنین مقایسه‌ای درمورد تحلیل طرح‌های SE از نظر امنیت و عملکرد و کارایی ارائه شده است. علاوه بر این، در مورد چالش‌ها، مسیرهای پیشرو و کاربردهای طرح‌های SE نیز صحبت کرده‌ایم.

واژگان کلیدی: فضای ذخیره‌سازی ابر، رمزگذاری قابل جستجو، حفظ حریم خصوصی، قابلیت جستجو، امنیت

۱- مقدمه

با توسعهٔ سریع رایانش ابری، بسیاری از مردم علاقه‌مند هستند که داده‌های خود را برون سپاری نمایند [۲۵ ، ۳۱ ، ۴۸ ، ۴۹]. فضای ذخیره‌سازی ابری مزایایی دارد از جمله: دسترسی آسان به داده‌ها، استفاده کمتر از تجهیزات ذخیره‌سازی فیزیکی و کاهش زیرساخت‌ها برای نگهداری داده‌ها. علاوه بر این، کاربران ابر تنها با اتصال به اینترنت می‌توانند به داده‌های خود در هر مکان و در هر دستگاهی دسترسی داشته باشند. اگرچه فضای ذخیره‌سازی ابری مزایای بسیاری را برای کاربران فراهم می‌کند، اما حفظ حریم خصوصی داده‌های حساس، همچنان مسأله‌ای چالش برانگیز است (داده‌های حساس مانند: سوابق پزشکی شخصی، اسناد محرمانه، عکس‌های خصوصی و هر سندی که برای کاربر شخصی باشد). این مسأله به این دلیل است که وقتی داده‌ها به سرور ابری برون سپاری می‌شوند، کاربر کنترل فیزیکی داده‌های خود را از دست می‌دهند. بیشتر سرورهای ابری صادق اما کنجکاو[7] هستند، به‌عنوان مثال، می‌توانیم به ارائه‌دهندگان خدمات ابری برای خدمات آن‌ها اعتماد کنیم، اما ممکن است آن‌ها تمایل داشته باشند تا به داده‌های ما دسترسی داشته باشند. از این رو، اکنون لازم است از حریم خصوصی داده‌های حساس در ابر محافظت شود. رایج‌ترین راه‌حل برای تضمین حریم خصوصی کاربر، رمزگذاری داده‌های کاربر قبل از برون‌سپاری در ابر است. با این

[1] Searchable encryption
[2] symmetric searchable encryption
[3] public key searchable encryption
[4] attribute-based searchable encryption schemes
[5] Index
[6] search functionality
[7] Honest but curious

*نویسندهٔ عهده‌دارمکاتبات: احمد غلامی

وجود، رمزگذاری داده‌ها به دلیل مشکلی که در جستجوی داده‌های رمزگذاری شده وجود دارد، نمی‌توانند مزایای مورد نیاز را ایجاد کنند. برای حل این مشکل، از طرح‌های رمزگذاری قابل جستجو (SE) استفاده می‌شود. طرح‌های SE به سرور ابری اجازه می‌دهد تا داده‌های رمزگذاری شده را بدون دانستن اطلاعات مربوط به متن اصلی یا کلیدواژه‌ها جستجو کند. پس از آن، بسیاری از طراحان، طرح‌های مختلف SE را بر اساس روش‌های رمزگذاری پیشنهاد داده‌اند مانند: رمزگذاری قابل جستجوی متقارن (SSE[1])، رمزگذاری قابل جستجوی کلیدعمومی (PSE[2])، و رمزگذاری قابل جستجوی ویژگی مبنا(ABSE[3]). SSE با کلید محرمانه سروکار دارد و به کاربری که کلید محرمانه را در اختیار دارد امکان ایجاد یک دریچه[4] را می‌دهد. PSE با زوج کلید عمومی و خصوصی سروکار دارد و به دارندگان داده اجازه می‌دهد تا برای رمزگذاری از کلید عمومی و برای ایجاد دریچه از کلید خصوصی استفاده کنند. در ABSE، مرجع شخص ثالث مورد اعتماد (TA[5]) کلیدهای خصوصی را تولید می‌کند و دارندگان داده اسناد را تحت سیاست‌های دسترسی تعریف شده رمزگذاری می‌کنند، به طوری که کاربران فقط در صورتی مجاز به رمزگشایی اسناد هستند که ویژگی‌ها با خط‌مشی دسترسی مطابقت داشته باشد. یک بررسی جامع در مورد رمزگذاری قابل جستجو در [۲۴ ، ۴۵ ، ۴۶ ، ۶۳] ارائه شده است. نویسندگان در [۲۴] در مورد ویژگی‌های مختلف جستجو بحث و SE را به سه دسته تقسیم کردند مانند مدل‌های Server-User (S-U)، User-Server-User (U-S-U) و UserA-Server-UserB (U_A-S-U_B) با این حال، آن‌ها در مورد رهنمودهای تحقیق برای آینده توضیح بیشتری نداده‌اند. در مرجع [۶۳] نویسندگان در مورد مدل SE صحبت کرده و طرح‌های مختلفی را بر اساس SSE و PSE ترسیم کرده‌اند. با این حال، آن‌ها ABSE را به‌عنوان رده‌بندی اصلی در نظر نگرفته‌اند از آنجایی که ABSE از نظر کنترل دسترسی کاربر کارآمد است جای پرداختن به این طرح خالی باقی مانده است. در مرجع [۴۶] نویسندگان درباره‌ی رمزگذاری قابل جستجو متقارن از نظر اهداف طراحی، ساختار و عملکرد پرسمان[6] به طور مفصل بحث کرده‌اند. آن‌ها در آن مرور چالش‌های حاصل را شناسایی و چند مسیر برای آینده ارائه دادند. با این حال، مقاله فقط محدود به طرح‌های SSE است. در مرجع [۴۵] نویسندگان چارچوبی برای طرح‌های SE مبتنی بر ابر ارائه داده‌اند و طرح‌های مختلف موجود را بر اساس معیارهای امنیتی بررسی کرده‌اند. نویسندگان همچنین چندین کاربرد SE را مورد بحث قرار داده و جهت‌گیری‌های مفید در آینده را معرفی کرده‌اند. اما هنوز، رده‌بندی مقاله بر اساس قابلیت جستجو است و آن‌ها روش‌های رمزگذاری را در نظر نگرفته‌اند.

در این مقاله ابتدا، یک مرور محدود از طرح‌های رمزگذاری قابل جستجو در رایانش ابری ارائه می‌گردد. قسمت اصلی این مقاله به موارد زیر می‌پردازد:

- کاربردهای SE شناسایی می‌شود و چالش‌ها و مسیرهای پیش‌رو برای رسیدن به آن‌ها معرفی می‌گردد.
- طرح‌های مختلف رمزگذاری قابل جستجو (SE) بر اساس روش‌های رمزگذاری مانند SSE، PSE و ABSE بررسی می‌شوند،
- طرح‌های SE از نظر قابلیت جستجو مانند جستجوی تک کلمه‌ای[7] ، جستجوی چند کلمه ای[8] ، جستجوی قابل تأیید[9] ، جستجوی پویا[10] و جستجوی ویژگی مبنا[11] بررسی می‌شوند.
- حملات مختلف قابل تصور به طرح‌های SE تعریف و مدل امنیتی طرح‌های SE به صورت جدول ارائه می‌گردد.
- کارایی طرح‌های مختلف SE بر اساس مدت زمان ایجاد نمایه، مدت زمان جستجو و مدت زمان ایجاد دریچه مورد تجزیه و تحلیل قرار می‌گیرد.

باقی مقاله بدین شرح است: کاربردهای رمزگذاری قابل جستجو در بخش ۲ شرح داده شده است. رمزگذاری قابل جستجو و معماری آن در بخش ۳ آمده. رده‌بندی SE و طرح‌های مختلف SSE، PSE و ABSE در بخش ۴ آورده شده است. تحلیل امنیتی طرح‌های مختلف SE در بخش ۵ آمده. تجزیه و تحلیل کارایی طرح‌های مختلف SE در بخش ۶ آورده شده است. کاربردهای رمزگذاری قابل جستجو در بخش ۶ آمده. چالش‌ها و مسیرهای پیش‌رو در بخش ۷ ارائه شده است. سرانجام، نتیجه گیری در بخش ۸ آمده است.

[1] Symmetric searchable encryption
[2] Public-key searchable encryption
[3] Attribute-based searchable encryption
[4] Trapdoor
[5] third-party authority
[6] Query
[7] Single-keyword search
[8] Multi-keyword search
[9] Verifiable keyword search
[10] Dynamic keyword search
[11] Attribute-based keyword search

۲- کاربردهای رمزگذاری قابل جستجو

در این بخش، طرح‌های SE را در وضعیت دنیای واقعی بررسی می‌کنیم.

ابرهای بهداشت و درمان[1]: در رایانش ابری برای مراقبت‌های بهداشتی، بیماران می‌توانند داده‌های پزشکی خود را برون سپاری کنند. برون سپاری داده‌های پزشکی به ابر در بسیاری از کاربردهای پزشکی درحال تبدیل شدن به روند بوده زیرا هزینه نگهداری سوابق الکترونیکی سلامت (EHR) را کاهش می‌دهد. از آنجا که داده‌های بهداشتی افراد حساس هستند ، بنابراین باید قبل از برون سپاری به ابر رمزگذاری شود. با این حال، از آنجایی که رمزگذاری قابلیت جستجو برای کاربران را فراهم نمی‌کند. از این رو، SE به عنوان یک راه‌حل عملی برای تأمین حریم خصوصی داده‌ها در نظر گرفته می‌شود. لیانگ و سوسیلو [۳۷] سازوکاری را برای ارائه بستر برون سپاری مراقبت های بهداشتی پیشنهاد دادند. به همین ترتیب، بسیاری از طرح‌ها در دوره‌های اخیر در این حوزه قرار گرفته اند.

ابرهای قابل حمل امروزی[2]: بسیاری از برنامه‌های کاربردی تلفن همراه[3] در یک فضای ابری در حال اجرا هستند. دستگاه‌های قابل حمل، عمده فروشندگان ابر هستند. با افزایش استفاده از دستگاه‌های همراه، ابر از روی دسک تاپ به تلفن همراه تبدیل شده است. ابر قابل حمل، تمام عملیات محاسبات موبایل را با استفاده از منابع ابری قابل حمل به صورت امن ارائه می‌دهد. برای ایجاد حریم خصوصی هنگام جستجوی اطلاعات از ابر، SE یک راه‌حل است و SE هنوز در رایانش ابری قابل حمل رشد می‌کند.

بخش بانکی[4]: بخش‌های بانکی برای بهبود توانایی خود در فناوری اطلاعات (IT[5]) از رایانش ابری استفاده می‌کنند. با این حال، بیشتر داده‌های بانکی حساس هستند. از این رو، آن‌ها با بسیاری از مسائل حریم خصوصی روبرو هستند. برای حفظ حریم خصوصی داده‌ها، سازمان‌های بانکی در حال بکارگیری طرح‌های SE برای انجام عملیات جستجوی امن بر روی داده‌های رمزگذاری‌شده که در فضای ابری ذخیره شده هستند.

جمع‌سپاری[6]: جمع سپاری با مدل پرداخت در ازای عملکرد ارائه شده است. ما هزینه‌ی منابع را پرداخت نمی‌کنیم، اما هزینه‌ی راه‌حل‌ها را پرداخت می‌کنیم. استفاده گسترده از رایانش ابری مزایا و معایب زیادی ازجمله کاهش هزینه تا بسیاری از نگرانی‌های امنیتی دارد. با این حال، برای کاربران ارائه قابلیت جستجو همراه با محافظت از حریم خصوصی داده‌هایشان چالش برانگیز است. از این رو، SE راه‌حلی برای مسأله فوق الذکر است.

اینترنت اشیا (IoT[7]): اینترنت اشیا به طور فزاینده‌ای یکی از روندهای محبوب فناوری است. اینترنت اشیا به قابلیت کنترل و حفظ داده‌های حریم خصوصی قوی نیاز دارد زیرا مقدار زیادی داده از طریق حسگرها تولید می‌کند و آن‌ها را در فضای ابری ذخیره می‌کند. راه‌حل نهایی برای این سناریو رمزگذاری قابل جستجو در ابر است. داده‌های این سنسورها در ابرهایی بارگذاری می‌شوند که به کاربران امکان دسترسی از طریق عملیات جستجو را می‌دهند.

رایانش مه[8]: رایانش مه توسعه‌ای از رایانش ابری است و داده‌های حساس رمزگذاری شده را در چندین گره مه مهار می‌کند تا از ازدحام شبکه و تأخیر در لبه اینترنت اشیا جلوگیری کند. با این حال، حریم خصوصی داده‌ها در رایانش مه نگران کننده است. از این رو، SE یک راه‌حل مطلوب برای تأمین حریم خصوصی داده‌ها است.

داده‌های بزرگ[9]: داده‌های بزرگ تأثیر بسزایی در زندگی امروز ما دارند و توجه رایانش ابری را برای ذخیره‌سازی و پردازش مقدار زیادی از داده‌ها به سمت خود جلب می‌کنند. امنیت و حریم خصوصی چالش‌های اصلی برای داده‌های بزرگ است. از این رو، رمزگذاری قابل جستجو یک راه‌حل اصلی برای تأمین حریم خصوصی داده‌های بزرگ است.

بسیاری از برنامه‌های دیگر رمزگذاری قابل جستجو وجود دارد، که با ارائه کارایی و دقت بهتر، بسیاری از سناریوهای واقعی را تحت تأثیر قرار می‌دهد.

۳- رمزگذاری قابل جستجو

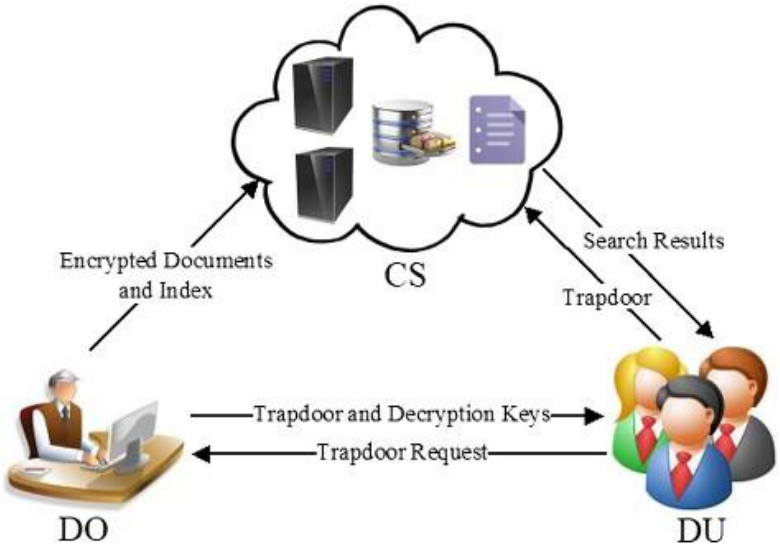
رمزگذاری قابل جستجو یک روش رمزنگاری است که به کاربران اجازه می‌دهد تا داده‌های رمزگذاری شده را با استفاده از کلیدواژه‌های امن و بدون رمزگشایی جستجو کنند. در طرح‌های SE ، مالک داده قبل از اینکه داده را به سرور ابری بسپارد، نمایه و مجموعه اسناد را رمزگذاری می‌کند. نمایه شامل مجموعه کلیدواژه‌های تمامی اسناد است. برای انجام جستجو، کاربر یک دریچه تولید می‌کند و آن را به سرور ابری می‌فرستد. سرور ابری اسنادی را که

[1] Healthcare clouds
[2] Mobile clouds Nowadays
[3] mobile applications
[4] Banking sector
[5] information technology
[6] Crowdsourcing
[7] Internet of Things
[8] Fog computing
[9] Big data

مربوط به دریچه‌ی تولید شده است برمی‌گرداند. طرح SE اولین بار توسط Song و همکاران پیشنهاد شد [۵۳] تا به کاربران امکان دسترسی امن به اسناد ذخیره شده در ابر را بدهد. در طرح آن‌ها جستجوی کنترل شده، ایزوله و پنهان کردن پرسمان برای بهبود بیشتر حریم خصوصی ارائه شده است. SE به کاربران این امکان را می‌دهد تا پرسمآن‌های خود را رمزگذاری کنند، که به نوبه خود حریم خصوصی داده‌ها را تضمین می‌کند. با استفاده از طرح‌های SE، اطمینان حاصل می‌کنیم که مهاجم نتواند به این راحتی به داده‌ها حمله کند. از طرح‌های SE به طور گسترده‌ای در پلت فرم رایانش ابری استفاده می‌شود زیرا حریم خصوصی و امنیت، پارامترهای دارای معیار اندازه‌گیری در ابر هستند.

(شکل-۱): معماری رمزگذاری قابل جستجوی متقارن

۳-۱- معماری طرح‌های SE



طرح‌های SE بر اساس مدل کلاینت/ سرور ایجاد می‌شوند، جایی که سرور ابری (CS[1]) به‌عنوان یک سرور و صاحبان داده (DOs[2]) و کاربران (DUs[3]) به‌عنوان کلاینت در هنگام ذخیره‌سازی و بازیابی عمل می‌کنند. شکل (۱) معماری رمزگذاری قابل جستجو متقارن را به تصویر می‌کشد.

مالک داده: نقش DO برون سپاری مجموعه اسناد $D = d_1 و d_2 و \dots و d_k$ و نمایه‌ی از کلیدواژه‌ها $W = w_1 و w_2 و \dots و w_n$ است که رمزگذاری شده است. مالک داده، قبل از برون سپاری، باید اسناد و مجموعه کلیدواژه‌ها را رمزگذاری کند تا مجموعه کلیدواژه‌های رمزگذاری شده، قابل جستجو باشد. توجه نمایید که، تعداد مالکان داده مستقل از طرح SE است.

سرور ابری: سرور ابری اسناد ارسال شده توسط مالک داده را ذخیره می‌کند و همچنین کارهای جستجو را انجام می‌دهد. وقتی کاربر یک دریچه را که حاوی یک کلیدواژه است را پرسمان می‌کند، سرور کلیدواژه‌های رمزگذاری شده را جستجو می‌کند و پس از اتمام جستجو، اسناد حاوی کلیدواژه‌ها را به کاربر برمی‌گرداند. فرض بر این است که CS صادق اما کنجکاو است. یعنی CS پروتکل‌ها را به‌درستی اجرا می‌کند، اما ممکن است داده‌ها یا الگوهای پرسمان را ارزیابی کند.

کاربر: DU با ارسال دریچه به CS مجاز به بازیابی داده‌ها از ابر است. هنگامی که نتایج به‌دست آمد، DU می‌تواند نتایج را رمزگشایی کند.

۳-۲- اهداف طراحی SE

در مورد برخی از اهداف طراحی طرح‌های رمزگذاری قابل جستجو صحبت می‌نماییم.

حفظ حریم خصوصی داده‌ها: داده‌های ذخیره شده در فضای ابری نباید برای اشخاص غیر مجاز افشا شود.

حفظ حریم خصوصی نمایه: حریم خصوصی نمایه نشان می‌دهد که سرور نباید از کلیدواژه‌های تعبیه شده در نمایه آگاهی داشته باشد.

حفظ حریم خصوصی کلیدواژه‌ها: سرور نمی‌توانند کلیدواژه‌ها موجود در دریچه یا برچسب‌های احراز هویت ایجاد شده توسط کاربر را بیاموزد.

[1] cloud server
[2] data owners
[3] data users

الگوی جستجو: الگوی جستجو به عنوان اطلاعاتی قابل استخراج در مورد اینکه دو یا چند نتیجه جستجو از یک کلیدواژه هستند تعریف شده است. حفظ الگوی جستجو یکی از اهداف طراحی تلقی می‌گردد.

الگوی دسترسی: الگوی دسترسی به اطلاعاتی اطلاق می‌شود که می‌تواند از دنباله‌ای از نتایج جستجو که حاوی کلیدواژه است، استخراج شود. حفظ الگوی دسترسی یکی از اهداف طراحی تلقی می‌گردد.

کارایی: کاربر باید بتواند دریچه تولید کند و نتایج جستجو را به طور کارآمد به‌دست آورد. از طرف دیگر، سرور ابری باید بتواند جستجوی کلیدواژه‌ها را به طور کارآمد انجام دهد.

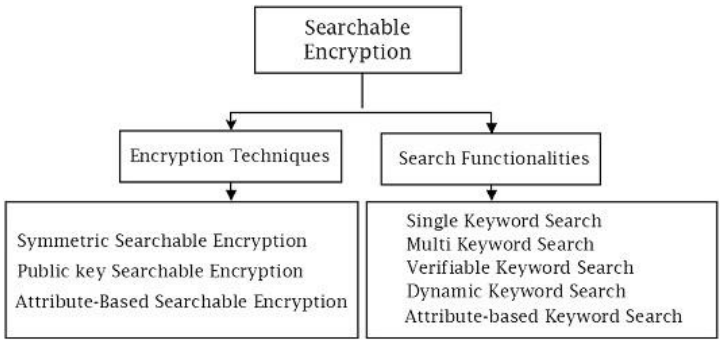
راستی آزمایی: علی رغم حریم خصوصی داده‌ها، نتایج به‌دست‌آمده از ابر باید بررسی شوند تا یکپارچگی داده‌ها سنجیده شود.

کنترل دسترسی: کنترل دسترسی از دسترسی غیرمجاز جلوگیری می‌کند. از دسترسی کاربرانی که اجازه دسترسی به داده‌ها را ندارند، با انجام عملیات حذف کاربر می‌توان به این نوع کنترل دست یافت.

چندین طرح رمزگذاری قابل جستجو بعد از طرح Song و همکارانش [۵۳] و بر اساس آن ارائه شده است. شکل (۲) رده‌بندی رمزگذاری قابل جستجو را نشان می‌دهد. در این بخش، به تفصیل درباره هر یک از روش‌های رمزگذاری صحبت می‌نماییم. علاوه بر این، در هر یک از روش‌های رمزگذاری، طرح‌های مختلفی را بررسی می‌کنیم. بیشتر این طرح‌ها بین سال های ۲۰۱۵ و ۲۰۱۹ منتشر شده و این طرح‌ها بر اساس قابلیت جستجوی کلیدواژه‌ها تقسیم‌بندی خواهند شد.

(شکل-۲): رده‌بندی رمزگذاری قابل جستجو

۴- رده‌بندی SE



۴-۱- رمزگذاری قابل جستجو متقارن

در SSE، اسناد با استفاده از روش‌های رمزگذاری متقارن/ کلید محرمانه رمزگذاری می‌شوند. همانطور که در شکل (۱) نشان داده شده است، سرور ابری بین DO و DU قرار دارد. در این حالت، DO اسناد را به‌همراه نمایه رمزگذاری کرده و به سرور ابری می‌فرستد، و بعد از آن DU می‌تواند با تولید دریچه و ارسال آن برای سرور ابری به داده‌های رمزگذاری شده دسترسی پیدا کند. سرور ابری جستجو در داده‌های رمزگذاری شده را انجام می‌دهد و نتایج را به DU برمی‌گرداند سپس کاربر با استفاده از کلید محرمانه می‌توان نتایج به‌دست‌آمده را رمزگشایی کند.

اگر KeyGen، BuildIndex، Enc، genTrapdoor، Search و Dec الگوریتم‌های زمان چندجمله‌ای برای مجموعه کلیدواژه‌های W باشند، الگوریتم‌های SSE به شرح زیر بیان خواهد شد:

K KeyGen(s): الگوریتم KeyGen اولین الگوریتم SE است و توسط DO اجرا می‌شود. پارامتر s را به‌عنوان ورودی می‌گیرد و کلید خصوصی K را به‌عنوان خروجی ارائه می‌کند.

I BuildIndex (w): این الگوریتم توسط DO اجرا می‌شود این الگوریتم مجموعه‌ای از کلیدواژه‌های w که $W = w_1$ و ... و w_2 و w_n که از مجموعه اسناد استخراج شده را به‌عنوان ورودی می‌گیرد و نمایه قابل جستجوی I را به‌عنوان خروجی تولید می‌کند.

Ed, Ei Enc(D, I, K): این الگوریتم توسط DO اجرا می‌گردد و مجموعه سند D را که $D = d_1$ و d_2 و ... و d_k، نمایه I و کلید K را به عنوان ورودی می‌پذیرد و اسناد رمزگذاری شده Ed[1] و نمایه رمزگذاری شده Ei[2] را به‌عنوان خروجی تولید می‌کند.

T genTrapdoor(K, q): این الگوریتم توسط DU اجرا می‌شود و کلید محرمانه K و کلیدواژه(ها)ی پرسمان q را

[1] encrypted documents
[2] encrypted index

به‌عنوان ورودی می‌پذیرد. اگر هدف جستجوی تک کلمه‌ای باشد، q فقط یک کلیدواژه دارد. در غیر این صورت، حاوی بیش از یک کلیدواژه است. سپس، با رمزگذاری q با K، دریچه T را به عنوان خروجی تولید می‌کند.

Ed Search(Ei, T): این الگوریتم توسط CS اجرا می‌شود. این الگوریتم دریچهٔ T و نمایه رمزگذاری شده Ei را به‌عنوان ورودی می‌پذیرد و قبل از تولید نتایج جستجو رمزگذاری شده Ed به عنوان خروجی، سپس عملیات جستجو را با دریچه‌ی دریافتی در نمایه رمزگذاری شده انجام می‌دهد و دست آخر Ed را به عنوان خروجی تولید می‌کند.

D Dec(Ed, K): این الگوریتم توسط DU اجرا می‌شود. این الگوریتم نتایج جستجو Ed و کلید محرمانه K را به‌عنوان ورودی می‌گیرد و با رمزگشایی Ed اسناد اصلی D را به‌عنوان خروجی ارائه می‌دهد.

۱-۱-۴- جستجوی تک کلیدواژه

جستجوی تک کلیدواژه‌ای به کاربران اجازه می‌دهد تا فقط با یک کلیدواژه روی داده‌های رمزگذاری شده‌ی ذخیره شده در سرور ابر، جستجو کنند. پرسمان کاربر باید دقیقاً شامل یک کلیدواژه برای تولید دریچه باشد و سپس، CS نتیجه مربوط به آن کلیدواژه را برمی‌گرداند. بسیاری از کارهای ارائه شده بر اساس سازوکار جستجوی یک کلیدواژه می‌باشد. برخی از این طرح‌ها به شرح زیر هستند:

Goh [23] برای دستیابی به امنیت نمایه، نمایه‌های امن را تعریف کرد و امنیت طرح‌ها را برای دستیابی به نمایه امن فرموله کرد. سپس یک طرح ساختاری نمایه امن به نام Z_IDX را بر اساس bloom filters و توابع شبه تصادفی معرفی کرد. bloom filters برای حافظه دارای ساختار کارآمد هستند و توابع شبه تصادفی توابع قطعی و کارآمدی هستند که مقادیر شبه تصادفی غیر قابل تشخیص از توالی‌های تصادفی را تولید می‌کنند. Z_IDX برای اجرای جستجوها در داده‌های رمزگذاری شده آزمایش شد. این روش در هنگام در نظر گرفتن به روزرسانی‌های نمایه کارآمد است اما از نظر زمان جستجو (در سرور ابری) کارآمد نیست.

برای بهبود کارایی جستجو، Chang و Mitzenmacher [9] این طرح را برای بازیابی فایل‌ها با جستجوی کاراتری با کلیدواژه‌ها نمایه شده ارائه دادند. در این طرح، آن‌ها از بیت‌های شبه تصادفی برای پوشاندن کلیدواژه‌ها نمایه شده استفاده کردند و آن‌ها را به سرور ارسال کردند با این حال، کل پایگاه داده باید برای یک جستجوی خاص جستجو شود، که باعث افزایش سربار محاسبات و همچنین نیاز به سربار ذخیره‌سازی اضافی می‌شود. بعلاوه، چیس و کامارا [۱۰] طرح‌هایی را برای انجام پرسمان بر روی داده‌های ساخت یافته پیشنهاد دادند.

در این قسمت، پرسمآن‌ها بر روی داده‌های دارای برچسب اعمال می‌شوند. هنگام رمزگذاری، داده‌ها به کمک دنباله زنی دارای طول یکسان خواهند شد و به داده‌های دارای برچسب تبدیل می‌شوند. با این حال، فقط یک برچسب به کل پایگاه داده اختصاص داده شده است. بنابراین، برای دستیابی به امنیت نیاز به دنباله زنی کل نتیجه است. اما Cash [8] برای هر سندی از یک برچسب استفاده کرد که حاوی کلیدواژه است، اگر کلیدواژه حاوی k سند باشد، از k برچسب مختلف استفاده می‌کند. طرح او از دنباله زنی اضافی جلوگیری می‌کند و همچنین جستجوی موازی را امکان پذیر می‌کند.

تمام طرح‌های مورد بحث در بالا برای بازیابی نتایج جستجو بر اساس مطابقت دقیق هستند. یعنی هرگونه اشتباه تایپی و انواع اشتباهات جزئی دیگر که توسط کاربر صورت گیرد در نتایج جستجو تاثیر دارد. بنابراین، لی و همکارانش [۳۳] اولین طرح کلیدواژه فازی[1] را پیشنهاد دادند-طرحی مبتنی بر این که بر ایرادات شایع غلبه می‌کند. این طرح اسناد منطبق بر کلیدواژه‌ها را برمی‌گرداند حتی اگر کلیدواژه دارای ایراد نوشتاری جزئی باشد، با استفاده از تشابه معنایی کلیدواژه، اسنادی را که با نزدیک ترین کلیدواژه از نظر معنایی منطبق هستند، برمی‌گرداند. آن‌ها از فاصله ویرایشی برای اندازه گیری شباهت معنایی استفاده کردند و همچنین از پروتکل‌های امنیتی و حریم خصوصی برای اطمینان از حریم خصوصی استفاده نمودند. با این حال ، این طرح نمی‌توانند نیازهای سطح بالای خدمات مانند تجربه جستجوی کاربر و قابلیت استفاده از سیستم را تضمین کند. همچنین، این طرح مخصوص اندازه‌گیری فاصله مشخصی است. بنابراین، کوزو و همکاران [۳۲] از روش‌های حساس‌سازی محلی چکیده (LSH) برای راه‌حل‌های عمومی تر در اندازه گیری فاصله استفاده کرده و یک نمایه LSH امن برای گواهی حریم خصوصی و امنیت ساخته شده است. معمولا LSH

[1] fuzzy

برای کمک به جستجوی تقریبی یا همسایگی نزدیک در فضاهای با ابعاد بالا استفاده می‌شود.

هرچند، از جستجوی تک کلیدواژه برای جستجوی در سرور ابری استفاده می‌شود که در آن فقط یک کلیدواژه جستجو می‌شود، اما این گونه جستجوها برای برنامه‌های زمان واقعی (real-time) مناسب نیست. زیرا جستجو با تنها یک کلیدواژه ممکن است فایل مورد نیاز را به طور دقیق شناسایی نکند. بنابراین، جستجوی چند کلیدواژه برای بهبود کارایی جستجو و گرفتن نتایج دقیق معرفی شد.

۲-۱-۴- جستجوی چند کلیدواژه

جستجوی چند کلیدواژه یک طرح جستجوی محبوب در برنامه‌های ابری است و به شما امکان می‌دهد به جای فقط یک کلیدواژه، با چندین کلیدواژه در پرسمان، جستجو کنید. با استفاده از کلیدواژه‌های متعدد، می‌توان به کارآیی در جستجو و نتایج دقیق‌تر دست یافت. بر اساس جستجوی چند کلیدواژه، چندین طرح پیشنهاد شده است و هنوز هم بسیاری از آن‌ها برای حفظ حریم خصوصی جستجو در زیرساخت‌های ابری دستاوردهایی دارند. این طرح‌ها را به چندین نوع دسته بندی کردیم که عبارتند از: جستجوی کلیدواژه‌ها رتبه‌بندی شده[۱]، جستجوی کلیدواژه فازی، جستجوی کلیدواژه‌ها مترادف[۲]، جستجوی معنایی کلیدواژه[۳] و جستجوی کلیدواژه‌ها عطفی[۴].

۱-۲-۱-۴- جستجوی رتبه‌بندی شده کلیدواژه‌ها

در این جستجوی کلیدواژه‌ها، اسناد با درنظرگرفتن وزن کلیدواژه‌ها بازیابی می‌شوند. به‌علاوه، این وزن‌ها با استفاده از مدل رتبه‌بندی $TF^5 * IDF^6$ تعیین می‌شوند. در اینجا، TF یک ترم فرکانس در یک سند خاص است و IDF یک فرکانس سند معکوس است. IDF را می‌توان به‌صورت زیر محاسبه کرد:

$$IDF_t = log\frac{N}{DF_t}$$

که در آن N تعداد اسناد و DF_t تعداد اسناد دارای ترم t است. نمره شباهت بین سند Dj و پرسمان Q را می‌توان به‌صورت زیر محاسبه کرد:

$$Score\left(D_j, Q\right) = \frac{1}{|D_j|}\sum TF_{i,j} \cdot IDF_i$$

$$|D_j| = \sqrt{\sum_{w_i \in D_j}\left(TF_{i,j}\right)^2}$$

جایی که $|D_j|$ نشان‌دهنده طول اقلیدسی D_j می باشد و w_i کلیدواژه در سند D_j است.

وانگ و همکاران [۶۱] یک جستجو کلیدواژه رتبه‌بندی امن را بر روی داده‌های ابری تعریف کردند، که توسط پیاده سازی رمزگذاری حفظ سفارش (OPE[7]) رمزگذاری شده است. در این طرح، امتیازات مربوطه و شناسه فایل برای ساخت یک نمایه قابل جستجوی امن استفاده می‌شود. برای محافظت ازحساسیت رابطه امتیازات، یک روش نگاشت حفظ سفارش یک به چند، توسعه یافته است. همچنین این طرح به همان قدرت طرح‌های جستجوی رتبه‌بندی پیشین است. OPE از نظر کارایی برای مقایسه داده‌های رمز شده بدون رمزگشایی آن‌ها مناسب است. با این حال، یو و همکاران. [۷۲] گفتند که OPE به نشت حریم خصوصی داده‌ها منجرمی‌شود و طرحی را به نام رمزگذاری دو دور قابل جستجو (TRSE[8]) ارائه دادند که از جستجوی چند کلیدواژه TOP-K با استفاده از رمزگذاری هوموفیک پشتیبانی می‌کند. در این طرح، مدل فضای برداری برای ساخت نمایه استفاده می‌شود. TRSE امنیت داده‌ها و حذف نشت اطلاعات را تضمین می‌کند. با این حال، این طرح پویا نیست. دو و همکاران [۱۶] شناسایی کردند که حملات تزریق فایل زمانی که به روز رسانی کلیدواژه به صورت پویا انجام می‌شود وجود دارد و طرح‌هایی را با توابع پیش‌سو برای حریم خصوصی پیش‌سو پیشنهاد دادند که یک قدم جلوتر از حملات تزریق فایل است. سپس آن‌ها یک ساختار سبد نمایه رمزنگاری را با یک مولد تصادفی (BEIS-I[9]) پیشنهاد کردند تا نمایه را با رمزگذاری بردارهای شناسه داده‌ها (DIV[10] ها) و بردارهای بیت تعیین کنند. آن‌ها همچنین ساختار سبد نمایه رمزگذاری را با یک مولد هوموفیک (BEIS-II[11]) را برای کنترل پهنای باند در طی پردازش پرسمان پیشنهاد کردند. این طرح با استفاده از مدل حمله کلیدواژه تطبیقی[۱۲] (CKA2) و مدل پیش‌سوی حریم خصوصی[۱۳] پشتیبانی می‌کند که از

[1] ranked keyword search
[2] synonym keyword search
[3] semantic keyword search
[4] conjunctive keyword search
[5] term frequency
[6] inverse document frequency

[7] order-preserving encryption
[8] two-round searchable encryption
[9] bucket-encrypting index structure
[10] data identifier vectors
[11] bucket-encrypting index structure with a homomorphic generator
[12] chosen keyword attack
[13] forward-privacy model

پردازش پرسمان چند کلیدواژه پشتیبانی می‌کند، اما این طرح نتایج جستجو را تأیید نمی‌کند.

طرح‌های جستجو کلیدواژه رتبه‌بندی شده جستجوی چند کلیدواژه را در مورد داده‌های رمزگذاری شده ارائه می‌دهند، اما آن‌ها خطاپذیری[1] ندارند، یعنی زمانی که کاربر خطاهای تایپی دارد، دقیق کار نمی‌کنند.

۴-۱-۲-۲- جستجوی کلیدواژه فازی

جستجوی کلیدواژه فازی به کاربران اجازه می‌دهد تا با وجود اشتباهات جزئی در کلیدواژه، به جستجو بپردازند. فاصله: $F \times F \rightarrow r$ یک تابع است که فاصله بین دو کلیدواژه را تعریف می‌کند و مقادیر آستانه برای اندازه گیری شباهت است به‌طوری که $\alpha < \beta$. بنابراین، جستجوی کلیدواژه فازی به شرح زیر تعریف می‌گردد.

جستجوی کلیدواژه فازی(I,Q) این جستجو را در نمایه I بر اساس کلیدواژه‌ها F(Q) انجام می‌گیرد و مجموعه‌ای از اسناد D، که رمزگذاری شده است را به‌عنوان خروجی ارائه می‌کند. فرض کنید F_j کلیدواژه مربوط به D_j است. بنابراین، با احتمال بالا، $D_j \in D$ اگر $\exists f_i(distance(f_i, f) \leq \alpha)$ و $D_j \notin D$، اگر $\forall f_i(distance(f_i, f) \geq \beta)$ که $f_i \in F_j$.

Z Fu et al.[۲۰] یک طرح جستجوی چندکلیدواژه فازی مبنا را براساس طرح [۶۰] پیشنهاد دادند، که اولین طرح در نوع خودش بود. این طرح یک روش تغییر شکل کلیدواژه را براساس Uni-Gram برای بررسی ایرادات املایی و بهبود دقت پیشنهاد کرد. علاوه بر این، الگوریتم برای پرسمان از کلیدواژه‌ها با بردار ریشه و نمایه یکسان با وزن کلیدواژه‌ها، برای جستجو در نمایه استفاده می‌کند. اما هنوز، این طرح در برابر حملات مختلفی آسیب‌پذیر است [۵۰]. برای بهبود امنیت، Ahsan و همکاران. [۱] یک ساختار مجموعه کلیدواژه تغییر شکل یافته را برای پیدا کردن کلمه اصلی با وجود خطای تایپی و علاوه بر این از ماتریس شباهت Jaccard برای رسیدن به حداکثر شباهت استفاده کردند. در این طرح، نویسندگان محدود به دقت خاصی هستند. برای بهبود دقت، یوان و همکاران. [۷۳] سه طرح را برای انجام جستجوی شباهت، امنیت، دقت و مقیاس پذیری طراحی کردند. حساب برخورد حساس به مکان (LSH) برای جستجوی شباهت امن استفاده می‌شود، طرح‌های مخفی‌کننده فرکانس پرسمان برای شاهد امنیت مورد استفاده قرار می‌گیرند و در نتیجه طرح‌های پرسمان به اشتراک گذاری برای بهبود مقیاس پذیری اجرا می‌شود.

۴-۱-۲-۳- جستجو کلیدواژه‌ها مترادف/ معنایی

این سناریو را در نظر بگیرید که در آن یک کاربر قصد دارد تا کلیدواژه که در نمایه موجود نیست را جستجو نماید، اما با درنظرگرفتن معنی مشابه یا مترادف آن کلیدواژه، کاربر می‌تواند اسناد را بازیابی کند. این سناریو اهمیت جستجوی معنایی کلیدواژه و جستجوی مترادف کلیدواژه را نشان می‌دهد. بسیاری از نویسندگان طرح‌هایی مربوط به جستجوی معنایی و مترادف کلیدواژه را پیشنهاد کرده‌اند که برخی از این طرح‌ها، کارایی بهتری نسبت به نتایج جستجو همراه با حریم خصوصی فراهم می‌نماید. فو و همکاران [۲۱] بیان کردند که رابطه گرامری بین کلیدواژه‌ها پرسمان در هنگام بررسی دیدگاه کاربر مهم است و اولین طرح را برای بررسی رابطه بین کلیدواژه‌ها در پرسمان پیشنهاد دادند. به این دلیل، آن‌ها یک الگوریتم جستجوی وزنی کلیدواژه را طراحی کردند تا اهمیت واگرایی را نشان دهند. علاوه بر این، آن‌ها یک طرح جستجوی کلیدواژه معنایی را برای ارائه دقت و کارایی در کلیدواژه مکان مرکزی که کاربر علاقه‌مند به یافتن آن است، طراحی کرده است. برای بهبود کارایی، Fu و همکاران [۲۲] طرح جستجوی معنایی کلیدواژه مبتنی بر دو سرورابری[2] (ECSED) بر اساس سلسله مراتب مفهومی پیشنهاد دادند تا جستجوی مبتنی بر معنایی یا جستجوی مبتنی بر محتوا را مؤثرتر کند. در این طرح، یک سرور ابر برای ذخیره اسناد رمزگذاری شده استفاده می‌شود و نتایج دریچه را به کاربر بازمی‌گرداند و دیگر سرور ابری برای محاسبه امتیازات شباهت استفاده می‌شود و این امتیازات را به سرور اول برمی‌گرداند. این طرح از یک نمایه مبتنی بر درخت استفاده می‌کند تا تمام اسناد را به طور مؤثر سازماندهی کند و پرسمان را به طور مؤثر پردازش کند.

۴-۱-۲-۴- جستجوی عطفی کلیدواژه

جستجوی تک کلیدواژه معمولاً با تعداد زیادی اسناد مطابقت دارد. در این میان، فقط تعداد کمی مربوط به جستجوی کاربر است. در عوض، جستجوی عطفی کلیدواژه‌ها (CKS[3]) به کاربران امکان می‌دهد با کلیدواژه‌ها متفاوتی جستجو کنند تا به نتایج جستجوی منفردی را تولید کنند و سپس برای ایجاد یک نتیجه

[1] fault tolerant

[2] two-cloud-server-based semantic search scheme

[3] conjunctive keyword search

نهایی، همه نتایج جداگانه را اشتراک می‌گیرند. این نتیجه نهایی شامل اسناد مربوط به جستجوی کاربر است.

کای و همکاران [۶] آسیب‌پذیری مربوط به حملات رابطه شمول (IR[1]) را شناسایی کرد و طرحی را با نام safe-CKS بر اساس bloom filter ارائه کردند. این طرح پرسمان را به فرم تصادفی و یکپارچه تبدیل می‌کند تا یافتن هرگونه رابطه در میان پرسمآن‌های مختلف دشوار باشد. اگرچه این طرح برای حملات رابطه شمول موثر است، اما به حملات دیگر نمی‌پردازد. برای بهبود بیشتر امنیت، علی و لو [۲] یک طرح CKS بدون فیلد کلیدواژه پیشنهاد کردند تا از ترتیب کلیدواژه در دریچه جلوگیری شود. سپس برای امن‌سازی نمایه، یک مدل امنیتی تمایزناپذیری را تحت حملهٔ کلمه کلیدواژهٔ انتخابی (IND-CKA[2]) معرفی کرد. مدل امنیتی مبتنی بر bloom filter و توابع شبه تصادفی است. با این حال، این طرح عملیات به روز رسانی پویا را ارائه نمی‌دهد.

۴-۱-۳- جستجوی کلیدواژه قابل تایید

اکثر طرح‌های SSE بر اساس مدل سرور ابری صادقانه اما کنجکاو طراحی شده‌اند. متأسفانه، در عمل، این فرض همیشه برقرار نیست، زیرا ممکن است سرورهای ابری تحت حملات خارجی قرار گیرند، اشکالات نرم‌افزاری پیدا کنند، اشتباهات پیکربندی داخلی و حتی تهدیدات داخلی در مورد آن‌ها صورت گیرد [۵۷]. همه این تأثیرات ممکن است باعث شود که سرور ابری فراتر از مدل صادقانه اما کنجکاو عمل کند. از طرف دیگر، برای حل کردن اینگونه مشکلات، طرح‌های جستجوی قابل تأیید برای تضمین یکپارچگی داده‌ها ارائه شده است. در طرح‌های قابل تأیید، نتایج اسناد به‌دست‌آمده از یک جستجو، قبل از رمزگشایی، تأیید می‌شوند. الگوریتم قابل تأیید به شرح زیر است:

(reject or $K(w_i)$) <-- KeywordTest(pk,T_{w_i},K): این الگوریتم کلید عمومی pk و دریچه‌ی T_{w_i} و فایل‌های رمز K را به عنوان ورودی می‌گیرد و اگر w_i در مجموعه موجود باشد $K(w_i)$ را به‌عنوان خروجی می‌دهد، در غیر این صورت خروجی رد را ارائه می‌کند.

(reject یا f) <--VerifyDecrypt(sk,K): اگر KeywordTest در اصطلاح پاس شود این الگوریتم کلید خصوصی کاربر و فایل‌های رمز K را به عنوان ورودی می‌گیرد و در صورت پذیرش ، مشتری می‌تواند فایل‌ها را رمزگشایی کند، در غیر این صورت رد و این اطلاعات را به سرور ارسال می‌کند.

چنگ و همکاران [۱۲] طرحی را برای جلوگیری از سرورهای مخرب و ایجاد محیطی برای نتایج جستجوی قابل تأیید پیشنهاد دادند. این طرح بر اساس مبهم سازی تمایزناپذیری امن (iO[3]) ساخته شده است تا قابلیت تأیید را به همراه جستجوی کارآمد کلیدواژه‌ها فراهم کند. از مبهم سازی به عنوان فرآیندی استفاده می‌شود که بر روی اطلاعات اعمال می‌شود تا بدون دانستن الگوریتمی که به کار رفته است، برگشت آن را دشوار کند. با این حال، این طرح حریم خصوصی را فراهم نمی‌کند. بنابراین، [۴] طرحی با همان عملکردِ [۱۲] را پیشنهاد داد. علاوه بر این، حریم خصوصی پیش‌سو فراهم می‌شود تا جستجو در برابر مهاجمان فعال امن باشد. و همچنین اوگاتا و کوروساوا [۴۳] روشی را برای تبدیل هر روش SSE به طرح SSE قابل تأیید بدون فرهنگ‌لغت پیشنهاد کردند. بعلاوه، این موضوع به مشکلات نگهداری کلیدواژه‌ها با یک جدول هش می‌پردازد. با این حال، همه طرح‌ها [۴ ، ۱۲ ، ۴۳] مدل‌های تک کاربره هستند، یعنی مدل‌های دو طرفه. با این حال، ارائه دهندگان خدمات ابری خدماتی را برای مدل‌های چند کاربره، به عنوان مثال، مدل‌های سه طرفه فعال می‌کنند. مرجع [۷۸] با این انگیزه، اولین طرح عمومی رمزگذاری متقارن قابل جستجو قابل تأیید (GSSE[4]) را برای پشتیبانی از مدل چند کاربره با مالک واحد ارائه داد. این طرح از قابلیت تأیید بیشتری نسبت به هر طرح SSE دیگری دارد. GSSE اثبات نمایه خود را با استفاده از هش افزایشی [۳] (IH[5]) و درخت مرکل پاتریشیا پویا ایجاد و حفظ می‌کند، که یکپارچگی داده‌ها را بیشتر تضمین می‌کند. همچنین، برای حفظ طراوت داده‌ها بر روی چندین کاربر، آن‌ها یک زنجیره زمانبر را پیشنهاد کردند. ایده IH این است که اگر قبلاً هش را برای برخی از سندها محاسبه کرده‌ایم و اگر بعضی از قسمت‌های سند در زمان بعدی اصلاح شده باشد، به جای محاسبه مقدار هش به و روزرسانی کامل سند، فقط باید به روز شده مقدار هش برای قسمت اصلاح شده را محاسبه کنیم. Merkle Patricia Tree درختی از هش است. هر گره در درخت حاوی هش فرزندان خود به همراه مقدار گره است.

[1] inclusion relation
[2] indistinguishability under chosen keyword attack
[3] indistinguishability obfuscation
[4] generic verifiable symmetric searchable encryption
[5] Incremental Hash

۴-۱-۴- جستجوی کلیدواژه‌های پویا[1]

تمام طرح‌هایی که تاکنون مورد بحث قرار گرفتند، تنها از عملیات ایستا[2] پشتیبانی می‌کنند، یعنی هیچ قانونی برای افزودن یا حذف اسناد بدون نمایه‌سازی مجدد کل داده‌ها وجود ندارد. علاوه بر این، جستجوی کلیدواژه‌های پویا به کاربران امکان می‌دهد داده‌های خود را به صورت انعطاف پذیر به روز کنند. برخی از طرح‌های جستجوی کلیدواژه‌های پویا در SSE به شرح زیر است.

کائو و همکاران [۷] اولین جستجوی رتبه‌بندی شده با چند کلیدواژه را بر روی داده‌های رمزگذاری شده (MRSE[3]) در فضای ابری طراحی کردند، که در آن اسناد و سؤالات به‌عنوان بردار نشان داده می‌شوند. آن‌ها برای اطمینان از حفظ حریم خصوصی از روش‌های امن استفاده از داده‌های ابری بهره بردند. در این طرح، مطابقت مختصات برای بررسی شباهت انتخاب شده است، یعنی اسناد را برمی‌گرداند که تا آنجا که ممکن است مطابقت دارند. برای بهبود بیشتر امنیت، یان و همکاران [۷۰] برای ایجاد امنیت بیشتر در جستجو و حفظ حریم خصوصی، جستجوی چند کلیدواژه‌ی پویا جدید ارائه داد. آن‌ها از رمزگذاری داخلی محصول برای پنهان‌سازی برای تشدید امنیت به همراه جلوگیری از نشت الگوی جستجو استفاده کردند. این طرح از یک ساختار باینری درخت برای نمایه‌سازی استفاده می‌کند تا کارایی و به‌روزرسانی پویا را تضمین کند. به همین ترتیب، شیا و همکاران [۶۶] یک طرح امن برای پشتیبانی از حذف و اضافه پویای اسناد ارائه دادند، که از مدل وزنی TF * IDF و مدل فضای برداری برای ساختن نمایه و همچنین ساختن پرسمان استفاده شده است. در کنار آن، یک جستجوی حریصانه عمق اول و یک ساختار نمایه درختی خاص برای ارائه یک جستجوی رتبه‌بندی شده به صورت پویا با چند کلیدواژه استفاده می‌شود. این طرح از الگوریتم امن رمزگذاری KNN برای رمزگذاری نمایه و کلیدواژه پرسمان استفاده می‌کند و ترم های فریبنده[4] به پرسمان و همچنین به نمایه برای مقابله با حملات آماری اضافه می‌شوند.

علاوه بر این، فو و همکاران [۱۹] به جستجوی رتبه‌بندی مبتنی بر واژه مترادف کمک کردند. در این طرح، جستجوی واژه مترادف از جستجوی کلیدواژه‌هایی که معنای مشابهی دارند پشتیبانی می‌کند و ساختار نمایه بر اساس درختان باینری بصورت پویا ساخته می‌شود. سپس، لی و همکاران [۳۵] یک طرح SSE پویا برای پشتیبانی از جستجوی عطفی کلیدواژه با مکانیزم احراز هویت پیشنهاد کردند. این طرح با در نظر گرفتن یک کلیدواژه واحد جستجو می‌کند و نتایج حاصل از هر جستجو با یکدیگر اشتراک گرفته می‌شود. در این طرح، از درخت مرکل برای اطمینان از درستی یکپارچگی استفاده می‌شود. نگاشت دو خطی مسئول تضمین نتیجه نهایی است که زیر مجموعه‌ای از نتایج تمام جستجوها است. این طرح در برابر مهاجمان تطبیقی فراموش نشدنی است. در مدل مهاجم تطبیقی، آن‌ها پرسمان‌های مداومی را برای کلید محرمانه ایجاد می‌کنند. این طرح دربرابر حمله‌ی کلیدواژه‌ی انتخابی تطبیقی امن است. با این حال، این طرح با پارامترهای امنیتی بیشتری که دارد ناکارآمد شده است. برای تأمین کارآیی، وان و دنگ [۵۹] برای رسیدن به جستجوی کلیدواژه‌ی قابل تایید با حفظ حریم خصوصی (VPSearch)، از روش تلفیق طرح‌های جستجوپذیر با حفظ حریم خصوصی و کدهای احراز اصالت پیام (MAC) همریخت[5] کمک گرفتند. آن‌ها به کاربران داده پیشنهاد دادند تا نتایج جستجوی خود را بدون ذخیره‌سازی محلی به‌صورت کارآمد تأیید کنند و برای ساختن سند نمایه و پرسمان از یک بردار بیت استفاده کردند. در این طرح، مشتری، داده‌ها را رمزگذاری می‌کند و سپس با استفاده از MAC همریخت، تأیید اعتبار می‌شود. داده‌های تأیید شده رمزگذاری شده به یک سرور ابر برون سپاری می‌شوند. با دریچه‌ی تأیید شده، مشتری می‌تواند در ابر به جستجو بپردازد.

برای بهبود بیشتر امنیت و کار با داده‌های بزرگ، وانگ و همکاران [۷۴] طرحی را برای پشتیبانی از جستجوی مبتنی بر مشابهت برای مقیاس بزرگ پیشنهاد دادند. این طرح از یک بردار ویژگی با ابعاد بالا به عنوان معیار جستجو استفاده می‌کند. این بردارهای ویژگی به bloom filters فازی نگاشته می‌شوند که بیشتر از LSH برای رمزگذاری شاخص استفاده می‌کنند. این طرح تحت حمله‌ی پرسمان انتخاب شده تطبیقی (AQA2[6]) و حریم خصوصی پیش‌سو، امن است. این طرح، یک طرح جستجوی مبتنی بر کلیدواژه نیست و به جای آن، یک جستجوی مبتنی بر بردار ویژگی با ابعاد بالا است.

برخی از طرح‌های اخیر SSE با ویژگی‌های جستجو و همچنین ساختارهای نمایه در جدول (۱) نشان داده شده است. مشاهده می‌کنیم که هر قابلیت جستجو مزایای خاص خود را دارد. هنوز هم، در مقایسه با سایر قابلیت‌های جستجو، جستجوی کلیدواژه‌های پویا بیشتر

1 Dynamic
2 static
3 multi-keyword ranked search over encrypted data
4 phantom terms

5 homomorphic
6 adaptive chosen query attack

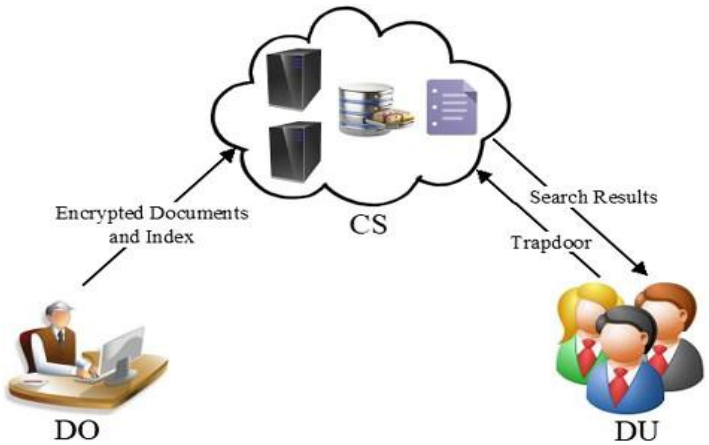
مورد توجه قرار می‌گیرد، زیرا در بسیاری از برنامه‌های دنیای واقعی، داده‌ها به صورت پویا تغییر می‌کنند. بنابراین این طرح باید انعطاف‌پذیر باشد تا با چنین داده‌هایی کار کند. علاوه بر این، طرح‌های SSE برای تبادل کلید محرمانه بین صاحب داده و کاربران داده به یک کانال امن اضافی نیاز دارند. با این حال، در دنیای واقعی چنین کانال مطمئنی وجود ندارد.

(جدول-۱): مقایسه طرح‌های SSE مدرن بر اساس قابلیت جستجو و ساختار نمایه

ردیف	نام طرح	سال	قابلیت جستجو	ساختار نمایه
۱	Xia et al. [66]	۲۰۱۶	جستجوی کلیدواژهٔ رتبه‌بندی شده	درخت
۲	Fu et al. [20]	۲۰۱۶	جستجوی کلیدواژهٔ فازی	بردار
۳	Bost et al. [4]	۲۰۱۶	جستجوی کلیدواژهٔ قابل تایید	درخت
۴	Yan et al. [70]	۲۰۱۶	جستجوی کلیدواژهٔ رتبه‌بندی شده	درخت
۵	Ali and Lu [2]	۲۰۱۶	جستجوی کلیدواژهٔ عطفی	درخت
۶	Fu et al. [21]	۲۰۱۷	جستجوی کلیدواژهٔ معنایی	بردار
۷	Yuan et al. [73]	۲۰۱۷	جستجوی کلیدواژه‌ی فازی	نمایه معکوس
۸	Liu et al. [39]	۲۰۱۷	جستجوی تک کلیدواژه	درخت
۹	Li and Liu [34]	۲۰۱۷	جستجوی کلیدواژهٔ عطفی	Bloom غیر filter
۱۰	Ahsan et al. [1]	۲۰۱۷	جستجوی کلیدواژهٔ فازی	نمایه معکوس
۱۱	Li et al. [35]	۲۰۱۸	جستجوی کلیدواژهٔ عطفی	فهرست معکوس
۱۲	Du et al. [16]	۲۰۱۸	جستجوی کلیدواژهٔ رتبه‌بندی شده	نمایه معکوس
۱۳	Fu et al. [22]	۲۰۱۸	جستجوی کلیدواژهٔ معنایی	درخت
۱۴	Zhu et al. [78]	۲۰۱۸	جستجوی کلیدواژهٔ قابل تایید	MPT
۱۵	Wu and Li [65]	۲۰۱۹	جستجوی کلیدواژهٔ عطفی	درخت باینری مجازی

۴-۲- رمزگذاری قابل جستجوی کلیدعمومی

در طرح‌های SSE برای به اشتراک گذاشتن کلید محرمانه بین DO وDU به یک کانال امن اضافی نیاز داریم، اما نمی‌توانیم تضمین کنیم که کانال امن به خطر نیفتد. در طرح‌های PSE از روش‌های رمزگذاری کلید عمومی استفاده می‌شود که در آن از دو کلید برای رمزگذاری و رمزگشایی استفاده می‌شود: کلید عمومی و کلید خصوصی. همانطور که در شکل (۳) نشان داده شده است، DO اسناد را به‌همراه نمایه با کلید عمومی کاربر رمزگذاری می‌کند و اسناد را به همراه نمایه به سرور ابری برون سپاری می‌کند. اکنون DU می‌تواند دریچه را به سرور ابری ارسال تا نتیجه بگیرد. هنگامی که DU نتایج را به‌دست آورد، می‌تواند با استفاده از کلید خصوصی کاربر، نتایج را رمزگشایی کند.



(شکل-۳): معماری رمزگذاری قابل جستجوی کلیدعمومی

اگر KeyGen، BuildIndex، Enc، genTrapdoor ، Query و Dec الگوریتم‌های زمان چند جمله‌ای در مجموعه کلیدواژه‌های W باشند، شرح الگوریتم‌های PSE در زیر آمده است:

KeyGen(s) (PK, SK): الگوریتم KeyGen اولین الگوریتم در فرآیند SE است و توسط DO آغاز می‌شود. پارامتر s را به‌عنوان ورودی می‌گیرد و کلید عمومی PK و کلید خصوصی SK را به عنوان خروجی ارائه می‌دهد.

BuildIndex I: این الگوریتم توسط DO اجرا می‌شود. مجموعه‌ی کلیدواژه‌های w را که در آن $W = w_1$ و w_2 و ... و w_n و از مجموعه اسناد D حاصل شده را به‌عنوان ورودی می‌گیرد و نمایه‌ی قابل جستجوی I را به‌عنوان خروجی تولید می‌کند.

Enc(PK, D, I) E_d, E_i: این الگوریتم توسط DO آغاز شده است. این مجموعه سند D را که $D = d_1$ و d_2 و ... و d_k نمایه I و کلید عمومی PK را به‌عنوان ورودی قبول می‌کند و اسناد رمزگذاری شده E_d و E_i را به‌عنوان خروجی تولید می‌کند.

genTrapdoor(SK, q) T: این الگوریتم توسط DU اجرا می‌شود. کلید خصوصی SK و کلیدواژه(ها) $q \in I$ را به‌عنوان ورودی قبول می‌کند. اگر جستجوی تک کلیدواژه‌ای باشد، q فقط یک کلیدواژه دارد. در غیر این صورت، حاوی بیش از یک کلیدواژه است. سپس، با رمزگذاری q به کمک SK، دریچه‌ی T را به‌عنوان خروجی می‌دهد.

Query(E_i, T) E_d : این الگوریتم توسط CS اجرا می‌شود. این الگوریتم دریچه T و نمایه رمزگذاری شده E_i را به‌عنوان ورودی می‌پذیرد و قبل از تولید مجموعه نامزد اسناد رمزگذاری شده E_d به عنوان خروجی، عملیات جستجو را با دریچه در نمایه رمزگذاری شده انجام می‌دهد.

Dec(E_d, SK) D: این الگوریتم توسط DU آغاز می‌گردد. نتایج جستجو E_d و کلید خصوصی SK را به‌عنوان ورودی می‌گیرد و با رمزگشایی E_d نسخه اصلی اسناد را به عنوان خروجی می‌دهد.

۴-۲-۱- جستجوی تک کلیدواژه‌ای

جئونگ و همکاران [۳۰] نشان دادند که ایجاد یک طرح PSE امن در برابر حمله حدس کلیدواژه هنگامی که یک چند جمله‌ای تعداد کلیدواژه‌ها را محدود کند امکان پذیر نیست. علاوه بر این، Xu و همکاران [۶۸] طرحی را برای پشتیبانی از جستجوی کلیدواژه‌های فازی پیشنهاد دادند. در این طرح، کلیدواژه‌ها، دریچه‌ی کلیدواژه فازی منحصر به فردی را به اشتراک می‌گذارند، بدین ترتیب سرور ابری چیزی در مورد کلیدواژه‌ی دقیق، متوجه نمی‌شود. با این حال، این طرح دارای محدودیت‌هایی در مورد کارایی و امنیت است. برای تأمین امنیت، چن و همکاران [۱۱] طرحی را به نام طرح PSE دو سرور با استفاده از توابع چکیده ساز تصویری ساده[1] برای تأمین امنیت در برابر حمله‌ی حدس کلیدواژه پیشنهاد کردند. جستجوی تک کلیدواژه‌ای برای برنامه‌های کاربردی در زمان واقعی[2] توصیه می‌شود. طرح‌های جستجوی چند کلیدواژه توجه زیادی را به خود معطوف داشته‌اند که در ادامه به آن‌ها خواهیم پرداخت.

۴-۲-۲- جستجوی چند کلیدواژه‌ای

۴-۲-۲-۱- جستجوی رتبه‌بندی شده

ژانگ و همکاران [۷۵] برای جستجوی رتبه‌بندی‌شدهٔ چند کلیدواژه‌ای به همراه حفظ حریم خصوصی در مدل چند مالک، (PRMSM[3]) چند طرح را ارائه کردند. در این طرح، پروتکل‌های جستجوی امن جدیدی ساخته شده‌اند تا امنیت هردوی کلیدواژه و دریچه را تأمین کند. آن‌ها همچنین یک خانواده سفارش addictive جدید و تابع نگهداری از حریم خصوصی را برای رتبه‌بندی نتایج جستجو و ارایه حریم خصوصی برای ارتباط بین امتیازات کلیدواژه‌ها و اسناد پیشنهاد کردند. علاوه بر این، آن‌ها پروتکل احراز هویت کاربر داده جدید و پروتکل تولید کلید خصوصی پویا را برای احراز هویت کاربران داده و جلوگیری از حمله به کلیدهای خصوصی پیشنهاد کردند. برای بهبود بیشتر کارایی، Pasupuleti و همکاران [۴۴] طرحی را برای کاهش سربار محاسباتی هنگام انجام رمزگذاری و رمزگشایی پیشنهاد دادند. این طرح از فرآیند رتبه‌بندی برای بازیابی اسناد دارای بالاترین رتبه بر اساس امتیازات مرتبط بودن، بدون درز اطلاعات در مورد اسناد و کلیدواژه‌ها، استفاده می‌کرد. برای بهبود امنیت، ژانگ و همکاران [۷۶] اولین طرح مبتنی بر بازدارندگی را با استفاده از رمزنگاری Paillier پیشنهاد دادند که متعلق به رمزگذاری کلید عمومی با یک مدل چند مالک بر اساس روش رتبه‌بندی است. در این طرح، سرور ابری نمی‌داند که چند مالک داده یا صاحبان داده در حال تبادل داده‌ها

[1] smooth projective hash functions
[2] real-time applications
[3] privacypreserving multi-keyword ranked search in a multi-owner model

هستند. با این حال، این طرح‌ها تحمل خطا ندارند، به‌عنوان مثال، خطاهای تایپی کاربر در کلیدواژه‌های دریچه در نظر گرفته نمی‌شوند.

۴-۲-۲-۲- جستجوی کلیدواژه‌های فازی

Xu و همکاران [۶۹] رمزگذاری کلید عمومی با جستجوی کلیدواژه فازی (PEFKS[1]) را ارائه دادند. در PEFKS، دریچه به دو قسمت تقسیم شده است، (۱) جستجوی دقیق کلیدواژه‌های دریچه و (۲) جستجوی کلیدواژه‌های فازی دریچه، فقط کلیدواژه‌های فازی دریچه به سرور ابری داده می‌شود تا اسناد منطبق را بازیابی کند، و سپس کاربر می‌تواند با صدور جستجوی دقیق کلیدواژه‌های دریچه به‌صورت محلی، نتایج را بیشتر فیلتر کند. بعلاوه، آن‌ها یک طرح تبدیل را پیشنهاد دادند که می‌تواند هر طرح رمزنگاری مبتنی بر شناسه را به طرح PEFKS تبدیل کند. این طرح در برابر حمله حدس کلیدواژه امن است.

۴-۲-۲-۳- جستجوی کلیدواژه عطفی

دینگ و همکاران [۱۵] طرحی را برای ارائه جستجوی کلیدواژه عطفی با استفاده از رمزگذاری کلید عمومی پیشنهاد دادند. در این طرح، هیچ عملیات زوج‌سازی هنگام رمزگذاری و هنگام تولید دریچه، استفاده نمی‌گردد. به‌علاوه، هوانگ و همکاران [۲۹] شناسایی کردند که طرح‌های موجود در برابر حملات حدس کلیدواژه غیربرخط[2] آسیب پذیر هستند و طرحی را برای فعال کردن جستجوی کلیدواژه عطفی با استفاده از زوج سازی دو خطی پیشنهاد کردند. این طرح از نظر معنایی در برابر حملات حدس کلیدواژه غیربرخط امن است حتی اگر کاربر از دستگاه ضعیف استفاده کند. با این حال، طرح‌ها [۱۵ ، ۲۹] هنگام تولید دریچه به لیست کامل کلیدواژه‌ها در نمایه نیاز دارند. این امر منجر به نشت اطلاعات و عدم رعایت حریم خصوصی پرسمان می‌شود. بنابراین، یانگ و ما [۷۱] یک رویکرد جدید به نام Re-dtPECK، یک طرح رمزگذاری قابل جستجو وابسته به زمان برای پشتیبانی از جستجوی پیوندی ارائه دادند. این در برابر حملات کلیدواژه انتخابی، حملات زمان انتخابی و همچنین حملات حدس کلیدواژه غیربرخط، امن است. امنیت طرح به جای مدل اوراکل تصادفی بر اساس مدل استاندارد ساخته شده است. با این حال، در این طرح، صحت نتایج جستجو تضمین نشده است [۴۱]. علاوه بر این، Xu و همکاران [۶۷] به کمک گروه دوخطی مرتبه ترکیبی به عنوان یک ویژگی پیشنهادی برای افزایش امنیت ارائه دادند. این طرح صحت و ثبات نتایج جستجو را تضمین می‌کند. علاوه بر این، در برابر حملات حدس کلیدواژه مقاومت می‌نماید. Farras و Gonzalez [17] برای بهبود اندازه‌ی نمایه و همچنین زمان تولید دریچه، طرحی را پیشنهاد کردند که از جستجوی کلیدواژه عطفی پشتیبانی می‌کند. این طرح در مقایسه با طرح‌های موجود در بیشتر معیارهای حیاتی مانند اندازه، زمان و عملکرد کارآمد است.

[1] public key encryption with a fuzzy keyword search
[2] offline keyword guessing attacks

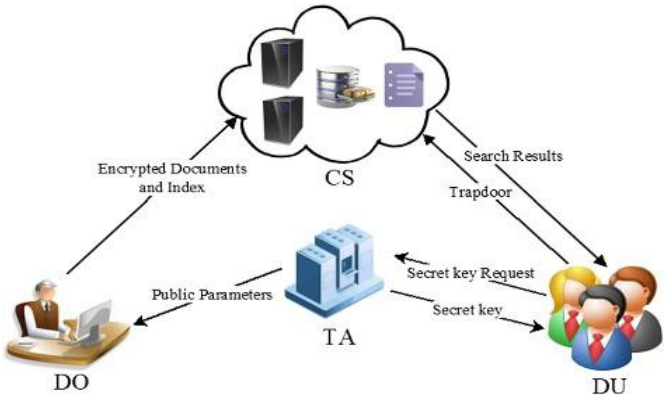
(جدول-۲): مقایسه طرح‌های مختلف PSE و BASE مبتنی بر قابلیت جستجو و ساختار نمایه

ردیف	نام طرح	سال	رمزگذاری	قابلیت جستجو	ساختار نمایه
۱	Liang and Susilo [36]	۲۰۱۵	ABSE	جستجوی کلیدواژهٔ ویژگی مبنا	ماتریس
۲	Yang and Ma [71]	۲۰۱۶	PSE	جستجوی کلیدواژهٔ عطفی	بردار
۳	Zhang et al. [75]	۲۰۱۶	PSE	جستجوی کلیدواژهٔ رتبه‌بندی شده	بردار
۴	Chen et al. [11]	۲۰۱۶	PSE	جستجوی تک کلیدواژه	بردار
۵	Pasupuleti et al. [44]	۲۰۱۶	PSE	جستجوی کلیدواژهٔ رتبه‌بندی شده	درخت
۶	Sun et al. [58]	۲۰۱۶	ABSE	جستجوی کلیدواژهٔ ویژگی مبنا	نمایه معکوس
۷	Miao et al. [41]	۲۰۱۶	PSE	جستجوی کلیدواژه‌ی عطفی	بردار
۸	Ma [40]	۲۰۱۶	PSE	جستجوی تک کلیدواژه	بردار
۹	Xu et al. [67]	۲۰۱۷	PSE	جستجوی کلیدواژهٔ عطفی	بردار
۱۰	Huang et al. [27]	۲۰۱۷	PSE	جستجوی کلیدواژهٔ قابل تایید	بردار
۱۱	Cui et al. [13]	۲۰۱۸	ABSE	جستجوی کلیدواژهٔ ویژگی مبنا	درخت
۱۲	Miao et al. [42]	۲۰۱۸	PSE	جستجوی کلیدواژه‌ی قابل تایید	درخت
۱۳	Zhang et al. [76]	۲۰۱۸	PSE	جستجوی کلیدواژه‌ی رتبه‌بندی شده	بردار
۱۴	Sun et al. [55]	۲۰۱۸	PSE	جستجوی کلیدواژه‌ی قابل تایید	بردار
۱۵	Farras and Gonzalez [17]	۲۰۱۹	PSE	جستجوی کلیدواژه‌ی عطفی	بردار

۴-۲-۳- جستجوی کلیدواژه قابل تایید

شن و همکاران [۵۱] طرح قابل جستجو و قابل تأیید توسط شخص ثالث را برای برنامه‌هایی که روی داده‌های بزرگ کار می‌کنند، ارائه داده‌اند. در این کار آن‌ها، از ساختار داده مکعبی برای ذخیره‌سازی و دسترسی راحت استفاده شده است. بعلاوه، این طرح با استفاده از امضاهای دیجیتال و پروتکل‌های توافق کلید برای یک طرح قابل جستجوی قابل تأیید به کارایی مناسبی دست یافت. این طرح در حفاظت ایمن از داده‌ها کارآمد است، اما امنیت در اشتراک داده‌ها تضمین نشده است. علاوه بر این، Wu و همکاران [۶۴] یک طرح قابل تأیید مطمئن بر اساس استانداردهای رمزگذاری هموморفیک در یک سیستم عامل چند کاربره ارائه دادند. در این مورد، از ساختار نمایه معکوس برای ساختار داده‌های معتبر استفاده می‌شود، که باعث بهبود صحت نتایج جستجو می‌شود. برخی از طرح‌های اخیر PSE و ABSE[1] با قابلیت جستجوی خود و همچنین ساختارهای نمایه در جدول (۲) نشان داده شده است. مشاهده می‌کنیم که طرح‌های PSE در مقایسه با SSE از امنیت بیشتری برخوردار هستند زیرا هیچ ارتباط اضافی بین DO وDU به طور مخفی وجود ندارد. با این حال، محدودیت‌های PSE عبارتند از: (۱) مدیریت کلید توسط DO مراقبت می‌شود و نیاز است که DO آنلاین باشد، زیرا هر بار که کاربر جدیدی در سیستم ثبت نام می‌کند، به DO نیاز دارد. و (۲) احراز هویت کاربر، کنترل دسترسی کاربر و لغو کاربر عملیات دشواری در طرح‌های PSE است. رمزگذاری قابل جستجو بر اساس ویژگی ABSE یک راه‌حل برای محدودیت‌های فوق الذکر است.

[1] Attribute-based searchable encryption



(شکل-۴): معماری رمزگذاری قابل جستجوی ویژگی مبنا

ردیف	نام طرح	سال	رمزگذاری	SKS	FKS	RKS	SeKS	VKS	CKS	ABSE	DKS
۱	Cao et al. [7]	۲۰۱۴	SSE	خیر	خیر	بله	خیر	خیر	خیر	خیر	بله
۲	Fu et al. [19]	۲۰۱۴	SSE	خیر	خیر	بله	بله	خیر	خیر	خیر	بله
۳	Hwang et al. [29]	۲۰۱۴	PSE	خیر	خیر	خیر	خیر	خیر	بله	خیر	خیر
۴	Wang et al. [60]	۲۰۱۴	SSE	خیر	بله	خیر	خیر	خیر	خیر	خیر	بله
۵	Cash et al. [8]	۲۰۱۴	SSE	بله	خیر	خیر	خیر	خیر	خیر	خیر	خیر
۶	Liang and Susilo [36]	۲۰۱۵	ABSE	خیر	خیر	خیر	خیر	خیر	خیر	بله	خیر
۷	Yan et al. [70]	۲۰۱۶	SSE	خیر	خیر	بله	خیر	خیر	خیر	خیر	بله
۸	Sun et al. [58]	۲۰۱۶	ABSE	خیر	خیر	خیر	خیر	بله	خیر	بله	بله
۹	Ali and Lu [2]	۲۰۱۶	SSE	خیر	خیر	خیر	خیر	خیر	بله	خیر	خیر
۱۰	Xia et al. [66]	۲۰۱۶	SSE	خیر	خیر	بله	خیر	خیر	خیر	خیر	بله
۱۱	Chen et al. [11]	۲۰۱۶	PSE	بله	خیر	خیر	خیر	خیر	خیر	خیر	خیر
۱۲	Fu et al. [21]	۲۰۱۷	SSE	خیر	خیر	خیر	بله	خیر	خیر	خیر	خیر
۱۳	Miao et al. [42]	۲۰۱۷	PSE	خیر	خیر	خیر	خیر	بله	خیر	خیر	خیر
۱۴	Cui et al. [13]	۲۰۱۷	ABSE	خیر	خیر	خیر	خیر	خیر	خیر	بله	بله
۱۵	Li et al. [35]	۲۰۱۷	SSE	خیر	خیر	خیر	خیر	بله	بله	خیر	بله
۱۶	Xu et al. [67]	۲۰۱۷	PSE	خیر	خیر	خیر	خیر	بله	خیر	خیر	خیر
۱۷	Wan and Deng [59]	۲۰۱۸	SSE	خیر	خیر	بله	خیر	بله	خیر	خیر	بله
۱۸	Fu et al. [22]	۲۰۱۸	SSE	خیر	خیر	بله	بله	خیر	خیر	خیر	خیر
۱۹	Wang et al. [74]	۲۰۱۸	SSE	خیر	بله	خیر	خیر	خیر	خیر	خیر	بله
۲۰	Wang et al. [62]	۲۰۱۸	ABSE	خیر	خیر	بله	خیر	خیر	خیر	بله	بله

(جدول-۳): مقایسه طرح‌های مختلف SSE، PSE و ABSE بر اساس قابلیت جستجو

SKS single-keyword search, FKS fuzzy keyword search, RKS ranked keyword search, SeKS semantic keyword search, VKS verifiable keyword search, CKS conjunctive keyword search, ABSE attribute-based keyword search, DKS dynamic keyword search

۴-۳- رمزگذاری قابل جستجو ویژگی مبنا

SSE و PSE می‌توانند حریم خصوصی داده‌ها را فراهم کنند، اما هنگام صحبت در مورد مجوز دسترسی کارآیی ندارند. هر کاربر با یک کلید خصوصی می‌تواند به سازوکارهای SSE و PSE دسترسی پیدا کند. رمزگذاری قابل جستجوی ویژگی مبنا ABSE کاملاً متفاوت است، و یک سیاست دسترسی همراه با اسناد رمزگذاری شده، برای کنترل دسترسی کاربر درنظر می‌گیرد. خط‌مشی دسترسی شامل اطلاعاتی درباره همه کاربرانی است که می‌توانند به سند دسترسی داشته باشند. اگر ویژگی‌های کاربر (به‌عنوان مثال، نام، بخش، دوره، جنسیت) با خط‌مشی دسترسی تعریف شده، تفاوت داشته باشد، کاربر مجاز به دسترسی به اسناد نیست. شکل (۴) معماری رمزگذاری قابل جستجو ویژگی مبنا را به تصویر می کشد،

جایی که مرجع معتبر (TA[1]) وظیفه تولید پارامترهای عمومی و کلیدهای اصلی محرمانه را برای کاربر دارد. ABSE به دو نوع تقسیم می‌شود: ABSE سیاست گذاری کلید (KP-ABSE[2]) و ABSE سیاست‌گذاری متن رمز (CP-ABSE[3])، فرآیند تولید کلید و رمزگذاری در هر دو سیاست دارای تفاوت است. در KP-ABSE، کلید اصلی محرمانه با استفاده از سیاست دسترسی P تولید می‌شود و اسناد و نمایه با استفاده از مجموعه‌ای از ویژگی‌ها رمزگذاری می‌شوند. در CP-ABSE، کلید خصوصی با استفاده از مجموعه‌ای از ویژگی‌ها تولید می‌شود و اسناد و نمایه با استفاده از خط‌مشی دسترسی رمزگذاری می‌شوند. اگر Setup، KeyGen، Enc، Trapdoor و Query الگوریتم‌های زمان چند جمله‌ای روی مجموعه کلیدواژه‌ها W باشند، الگوریتم‌های CP-ABSE به شرح زیر است:

Setup (λ, U) (PK, MK) : این الگوریتم توسط TA آغاز می‌گردد. این الگوریتم پارامتر امنیتی λ و ویژگی‌های سراسری U را به‌عنوان ورودی می‌گیرد و کلید عمومی PK و کلید اصلی محرمانه MK را به‌عنوان خروجی ارائه می‌دهد.

KeyGen(PK, MK, S) sk : این الگوریتم توسط TA آغاز می‌گردد. با پذیرش PK، MK و ویژگی کاربر S به‌عنوان ورودی. الگوریتم کلید محرمانه sk را برای کاربران تولید خواهد کرد.

Enc(W, p) cp : این الگوریتم توسط DO آغاز می‌گردد. این رمزگذاری مجموعه کلیدواژه W با سیاست دسترسی P را برای به‌دست‌آوردن متن رمز cp انجام می‌دهد.

Trapdoor(sk, w) t : این الگوریتم توسط DU آغاز می‌شود. این الگوریتم اجازه می‌دهد تا با توجه به sk و کلیدواژه w یک دریچه برای جستجو ایجاد نمایید.

Query(cp, t) ۰ یا ۱ : این الگوریتم توسط CS آغاز می‌شود. این الگوریتم اگر کلیدواژه در نمایه با کلیدواژه در دریچه مطابقت داشته باشد، ۱ را برمی‌گرداند، در غیر این صورت ۰ را برمی‌گرداند.

۴-۳-۱- جستجوی کلیدواژهٔ ویژگی مبنا

لیو و همکاران [۳۸] یک روش جدید برای تأیید نتایج حاصل شده از سرور ابری که از KP-ABSE استفاده می‌کند را ارائه دادند. این طرح می‌تواند به طور کارآمد یکپارچگی و درستی نتایج جستجو را تأیید کند. علاوه بر این، این طرح اطمینان می‌دهد که از حملات حدس کلیدواژه غیربرخط جلوگیری می‌شود. سپس، Hur و Noh [28] برای دستیابی به سیاست‌های کنترل دسترسی با قابلیت حذف کاربر همراه با قابلیت جستجوی کارآمد ویژگی مبنا، یک طرح رمزگذاری مبتنی بر سیاست گذاری متن رمز پیشنهاد کردند. علاوه بر این برای بهبود کارایی، ژنگ و Xu [77] یک طرح جستجوی ویژگی مبنا قابل تأیید برای حل مشکلاتی مانند جستجو در داده‌های رمزگذاری شده ارائه دادند، این طرح تأیید می‌کند که آیا سرور ابری صادقانه عملیات جستجو را انجام داده است یا خیر. در این طرح برای کنترل دسترسی از درختان دسترسی استفاده می‌شود. با این حال، از به اشتراک گذاری داده‌ها از داده‌های رمزنگاری‌شده پشتیبانی نمی‌کند . لیانگ و سوسیلو [۳۶] برای به اشتراک گذاری کارآمد داده‌ها و به روزرسانی انعطاف پذیر کلیدواژه‌ها، از قابلیت جستجوی کلیدواژه‌های ویژگی مبنا و رمزگذاری مجدد پروکسی ویژگی مبنا[4] استفاده کردند. با استفاده از این ادغام، دارندگان داده می‌توانند به طور کارآمد داده‌های خود را با کاربرانی که خط‌مشی دسترسی را برآورده می‌کنند، به اشتراک بگذارند. سپس، میائو و دیگران [۴۲] طرح جستجوی کلیدواژه‌های قابل تأیید ویژگی مبنا را پیشنهاد کردند تا به کاربران امکان بررسی صحت نتایج را بدهد. این طرح به کنترل دسترسی ریز دسترسی می‌یابد و همچنین از درخت اولویت ویژگی مبنا برای ارائه کنترل دسترسی از داده‌های مشابه استفاده می‌نماید. علاوه بر این، این طرح در برابر حملهٔ CKA امن است. با این حال، این طرح از ساختار درختی با کارایی کمتری بهره می برد [۵۵].

برای بهبود کارایی، سان و همکاران [۵۸] طرح جستجوی کلیدواژه‌ها مقیاس پذیر مبتنی ABSE برای مدل پشتیبانی چند کاربره و چند مالک را طراحی کردند. این طرح با ارائه مقیاس پذیری بهتر می‌تواند در جستجوی خطی با احراز هویت جزئی تر در سطح فایل اجرا شود. حذف کاربر می‌تواند از نظر محاسباتی کارآمد باشد زیرا مالک داده می‌تواند مهمترین وظایف سرور ابری را به طور مؤثر مدیریت کند. این طرح در برابر حمله‌ی CKA امن است. با این حال، این طرح در برابر انواع دیگر حملات از نظر امنیتی مناسب نیست. علاوه بر این، کوی و همکاران [۱۳] یک طرح جستجوی مالک چند کاربره به نام

[1] trusted authority
[2] Key-policy ABSE
[3] Ciphertextpolicy
[4] attribute-based proxy reencryption

جستجوی کلیدواژه‌ها ویژگی مبنا با یک طرح حذف کارآمد (AKSER[1]) را پیشنهاد کرد.

این طرح با توجه به حذف کاربر کارآمد است و جستجوی مجاز برای کلیدواژه‌ها را فراهم می‌کند. این طرح همچنین به اهداف امنیتی مانند محرمانگی کلیدواژه‌ها، امنیت معنایی کلیدواژه‌ها، دریچه‌های ارتباط ناپذیر و مقاومت در برابر برخورد، دست یافته است. با این حال، کاربر هربار که عمل حذف اتفاق می‌افتد، نیاز به ثبت نام جدید دارد. سپس، وانگ و همکاران [۶۲] اولین طرح رمزگذاری ویژگی مبنا سلسله مراتبی را برای مجموعه اسناد ارائه داد. با استفاده از طرح‌های جستجوی ویژگی مبنا، منابعی مانند فضای ذخیره‌سازی متن رمز و زمان رمزگذاری/ رمزگشایی ذخیره می‌شوند. در این طرح، فهرست با درخت ویژگی‌های بازیابی ویژگی مبنا (ARF[2]) برای مجموعه اسناد ساخته می‌شود. کارایی جستجو با استفاده از الگوریتم پیمایش جستجو برای اولین بار در درخت ARF و با استفاده از محاسبات موازی بهبود یافت.

مشاهده کردیم که از نظر امنیت طرح‌های ABSE در مقایسه با طرحهای SSE و PSE از ویژگی‌های بیشتری برخوردار هستند. علاوه بر این، جستجوی کلیدواژه پویا با ABSE در دنیای واقعی مفیدتر است. جدول (۳) طرح‌های مختلف SE را همراه با قابلیت جستجوی موجود در آن‌ها نشان می‌دهد. مشاهده شده است که برخی از طرح‌ها بیش از یک قابلیت جستجو دارند. در این جدول اگر طرحی شامل قابلیت جستجوی خاصی باشد، با (بله) و در غیر این صورت با (خیر) نمایش داده می‌شود.

۵- مدل امنیتی طرح‌های رمزگذاری قابل جستجو

سیستم SE باید ثابت کند که می‌تواند حریم خصوصی داده‌های کاربر را حفظ کرده و از نشت اطلاعات جلوگیری کند. در این بخش، نقاط قوت امنیتی طرح‌های SE را ارائه می‌دهیم، عمدتا به حملات مختلفی که به طرح‌های SE وارد است و راه‌حل‌های ارائه شده برای جلوگیری از این حملات توسط نویسندگان مختلف خواهیم پرداخت.

حمله متن اصلی انتخابی (CPA[3]) در این حمله، مهاجم ممکن است برای بدست آوردن متن رمزهای مربوطه، متنهای تصادفی که رمزگذاری شده‌اند را انتخاب کند. چندین کار برای امن‌سازی در برابر این حمله پیشنهاد شده است [۱۴ ، ۵۲ ، ۵۴]. در مدل حمله متن اصلی شناخته شده، سرور ابری می‌تواند جفت متن اصلی متن رمز را مجموعه داده به‌دست آورد. با استفاده از این اطلاعات، سعی دارد تا با به‌دست‌آوردن کلید محرمانه عملیات رمزگشایی را بدست آورد.

حمله کلیدواژه انتخابی (CKA[4]) در این حمله، مهاجم ممکن است به طور انتخابی به کلیدواژه‌ها حمله کند تا رمزگشایی کلیدواژه‌های انتخاب شده را بدست آورد. وانگ و همکاران [۶۰]، علی و لو [۲]، شیا و دیگران. [۶۶]، یوان و همکاران [۷۳]، فو و همکاران [۲۱]، Du و همکاران [۱۶]، لی و همکاران [۳۵]، Farras و Gonzalez [17] و Curtmola و همکاران [۱۴] طرح‌هایی پیشنهادی برای امن‌سازی در برابر حمله‌ی CKA ارائه دادند. تمایزناپذیری تحت مدل حمله کلیدواژه انتخاب شده (IND-CKA) این مفهوم را که اسناد یا نمایه آشکار نمی‌شود را تداعی می‌کند. در ابتدا، به‌عنوان پشتوانهٔ این مدل ازbloom filters و توابع شبه تصادفی استفاده می‌شود.

حمله حدس کلیدواژه (KGA[5]) در طرح‌های PSE، مهاجم ممکن است برچسب‌های رمزگذاری شده مربوط به تمام کلیدواژه‌ها ممکن را برای تولید دریچه برای تعیین اسناد بیشتر ایجاد نماید. حملات حدس کلیدواژه‌ها زمانی بسیار زیاد امکان‌پذیر است که فرستنده و گیرنده معمولاً از کلیدواژه‌ها معمول مانند "مهم"، "اقدام" یا "خوشحال" استفاده کنند. مشخص شده است که تعداد کلیدواژه‌ها متداول چندان زیاد نیست. چندین نویسنده طرح‌هایی [۱ ، ۱۱ ، ۲۷ ، ۲۹ ، ۳۰ ، ۶۸ ، ۶۹ ، ۷۱] را برای امن‌سازی در برابر حملهٔ KGA پیشنهاد داده‌اند.

مدل متن رمز شناخته شده (KCM[6]) در این مدل، CS می‌تواند از نمایه‌های امن، فایل‌های رمزگذاری شده و دریچه‌ها مطلع شود [۲۰ ، ۲۱]. علاوه بر این، CS می‌تواند نتایج جستجو را بداند و ثبت کند. در مدل حمله متن رمز انتخابی، مهاجم می‌تواند با به‌دست‌آوردن رمزگشایی متن رمز انتخابی خود، اطلاعاتی را جمع‌آوری کند [۳۶ ، ۳۷ ، ۴۰ ، ۴۴ ، ۵۵].

مدل پس زمینه شناخته شده (KBM[7]) در این مدل، CS تحلیل آماری را برای به دست آوردن اطلاعات خاص در مورد کلیدواژه انجام می‌دهد، که می‌تواند بیشتر

[1] attribute-based keyword search with an efficient revocation scheme
[2] attribute-based retrieval features
[3] Chosen plaintext attack

[4] Chosen keyword attack
[5] Keyword guessing attack
[6] Known ciphertext model
[7] Known background model

با اطلاعات پس زمینه ترکیب شود تا از کلیدواژه‌ای که توسط کاربر جستجو شده مطلع شود با استفاده از این تحلیل آماری، سرور ابری می‌تواند حمله آماری فرکانس دوره (TF[1]) را برای استنباط یا حتی تشخیص کلیدواژه‌ها با تحلیل هیستوگرام‌ها انجام دهد [۵۶]. چندین نویسنده‌ی دیگر نیز طرح‌هایی را برای مقابله با این حمله پیشنهاد کردند [۲۱ ، ۲۲ ، ۶۶].

حمله پیام انتخابی (CMA[2]) این حمله به طرح‌های امضا امکان پذیر است که در آن مهاجم می‌تواند امضای پیام‌های انتخابی خود را دریافت کند [۴]. در بسیاری از موارد، این مدل حمله برای محافظت از کدهای احراز اصالت پیام (MAC) استفاده می‌شود.

انواع مختلفی از حملات مانند حملات رابطه ورود[3]، حملات شناسه انتخابی[4]، حملات تزریق فایل[5] و حملات جستجوی کامل[6] وجود دارد که حریم خصوصی را تهدید می‌کنند. جداول (۴ و ۵) به ترتیب طرح‌های مختلف SSE و PSE و حملات مختلفی را نشان می‌دهند که طرح در برابر آن‌ها امن است.

(جدول-۴): مدل‌های امنیتی طرح‌های مختلف SSE

KBM known background model, KCM known ciphertext model,
CMA chosen message attack, CKA chosen keyword attack

ردیف	نام طرح	مدل امنیتی
۱	Xia et al. [66]	KBM
۲	Fu et al. [20]	KCM, KBM
۳	Bost et al. [4]	CMA
۴	Yan et al. [70]	CKA
۵	Ali and Lu [2]	CKA
۶	Fu et al. [21]	KCM, KBM
۷	Yuan et al. [73]	CKA
۸	Liu et al. [39]	CKA
۹	Li and Liu [34]	CKA
۱۰	Ahsan et al. [1]	CKA
۱۱	Li et al. [35]	CKA
۱۲	Du et al. [16]	CKA
۱۳	Fu et al. [22]	KBM
۱۴	Zhu et al. [78]	CKA
۱۵	Wu and Li [65]	CKA

جدول۵ : مدل امنیتی مورد استفاده در طرح‌های مختلف PSE و ABUSE

CCA chosen ciphertext attack, KGA keyword guessing attac k, CKAchosen keyword attack, CPA chosen plaintext attack

ردیف	نام طرح	مدل امنیتی
۱	Liang and Susilo [36]	CCA
۲	Yang and Ma [71]	KGA
۳	Zhang et al. [75]	CKA
۴	Chen et al. [11]	KGA
۵	Pasupuleti et al. [44]	CCA
۶	Sun et al. [58]	CKA
۷	Miao et al. [41]	KGA
۸	Ma [40]	CCA
۹	Xu et al. [67]	KGA
۱۰	Huang et al. [27]	KGA
۱۱	Shen et al. [52]	CKA
۱۲	Miao et al. [42]	CKA
۱۳	Zhang et al. [76]	CKA
۱۴	Sun et al. [55]	CCA
۱۵	Farras and Gonzalez [17]	CKA

۶- تحلیل کارایی

در این بخش، عملکردهای مختلف SE را در مورد زمان تولید نمایه، زمان جستجو و زمان دریچه، مرور خواهیم کرد.

زمان تولید نمایه: زمان تولید نمایه به تعداد کلیدواژه‌هایی که از همه اسناد بدست می آید بستگی دارد. ایجاد نمایهٔ کارآمد تضمین می‌کند که فرآیند جستجو به زمان کمتری نیاز دارد. روش‌های مختلفی برای ایجاد نمایه وجود دارد، نمایه معکوس یک روش محبوب برای ساخت نمایه است. مدل فضای برداری یک روش گسترده در سناریوهای جستجوی چند کلیدواژه است. ساخت نمایه مبتنی بر درخت باعث بهبود کارایی در فرآیند جستجو می‌شود.

زمان جستجو: زمان جستجو به عملکرد جستجو بستگی دارد. کارایی هر طرح SE بستگی به زمان جستجو دارد. بنابراین، معیار محاسباتی به یک معیار مهم تبدیل می‌شود. طرح‌های دارای نمایه معکوس به زمان O(r) نیاز دارند، که r تعداد اسناد مطابق با کلیدواژه‌ی جستجو است. از طرف دیگر، طرح‌هایی با نمایه درختی به زمان O(logn) نیاز دارند که n تعداد کل اسناد است. از این رو، هنگامی که طرح‌های SE طراحی می‌شوند باید دقت کرد که زمان جستجو کارآمد باشد.

زمان دریچه: زمان دریچه به زمان اختصاص داده شده برای تولید دریچه به منظور جستجوی کلیدواژه معطوف است. تعداد کلیدواژه‌های موجود در پرسمان، سربار دریچه را تعیین می‌کند.

وقتی امنیت طرح SE افزایش می‌یابد، به دلیل اضافه شدن سربارهایی، کارایی کاهش می‌یابد. بنابراین، باید یک توازن متعادل بین امنیت و کارایی وجود داشته

[1] term frequency
[2] Chosen message attack
[3] inclusion relation attacks
[4] chosen identity attacks
[5] file-injection attacks
[6] brute-force attacks

باشد. جداول (۶ و ۷) انواع کارایی SE را بر اساس معیارهای بیان‌شده در بالا نشان می‌دهد که در آن M تعداد کل کلیدواژه‌ها را نشان می‌دهد، N تعداد کل اسناد را نشان می‌دهد، D نشانگر اندازه مجموعه داده است، B نشان دهنده تعداد سطل‌ها[1] است، L نمایانگر تعداد سطرهای ماتریس است، A نشان‌دهنده تعداد ویژگی در مجموعه ویژگی‌ها است، C نشان‌دهنده هزینه محاسباتی نگاشت‌های دو خطی است، V نشان‌دهنده بعد بردار است، F نشان دهنده شماره فایل است، T نمایانگر کلیدواژه‌ها متمایز در پرسمان است، R نشان‌دهنده تعداد کلیدواژه‌ها در پرسمان است، و S نشان‌دهنده اندازه فرهنگ لغت است.

[1] buckets

(جدول-۶):تحلیل کارایی طرح‌هایی با اندازه‌های مختلف بر اساس زمان جستجو، زمان تولید نمایه و زمان دریچه

ردیف	نام طرح	زمان جستجو	زمان تولید نمایه	زمان دریچه
۱	Xia et al. [66]	O(M log N)	O(MN2)	O(M2)
۲	Fu et al. [20]	O(N)	O(M)	O(M)
۳	Bost et al. [4]	O(N log N)	O(M)	O(S)
۴	Yan et al. [70]	O(D)	O(N)	O(S)
۵	Ali and Lu [2]	O(D)	O(N)	O(M)
۶	Fu et al. [21]	O(S)	O(SV)	O(S)
۷	Li et al. [35]	O(M log M)	O(N)	O(F + R log T)
۸	Yuan et al. [73]	O(M)	O(N)	O(M)
۹	Liu et al. [39]	O(R)	O(N)	O(M)
۱۰	Li and Liu [34]	O(MlogN)	O(NlogN)	O(M)
۱۱	Wang and Deng [59]	O(N + M)	O(N)	O(S)
۱۲	Du et al. [16]	O(N)	O(NB)	O(C)
۱۳	Fu et al. [22]	O(D)	O(MnlogN)	O(M)
۱۴	Wu and Li [65]	O(RlogN)	O(MlogN)	O(S)
۱۵	Zhu et al. [78]	O(M)	O(MlogN)	O(M)

(جدول-۷): تحلیل کارایی طرح‌های مختلف PSE و ABUSE بر اساس بر اساس زمان جستجو، زمان تولید نمایه و زمان دریچه

ردیف	نام طرح	زمان جستجو	زمان تولید نمایه	زمان دریچه
۱	Liang and Susilo [36]	O(AC)	O(N2)	O(L2)
۲	Yang and Ma [71]	O(D)	O(MN)	*O*(*M*)
۳	Shen et al. [51]	O(M)	O(N)	*O*(*M*)
۴	Chen et al. [11]	O(R)	O(MN)	*O*(*C*)
۵	Pasupuleti et al. [44]	O(R)	O(N)	*O*(*M*)
۶	Sun et al. [58]	O(N)	O(M)	*O*(*R*)
۷	Miao et al. [41]	O(M)	O(D)	*O*(*R*)
۸	Ma [40]	O(R)	O(N)	*O*(*R*)
۹	Xu et al. [67]	O(D)	O(N)	*O*(*M*)
۱۰	Cui et al. [13]	O(M)	O(A)	*O*(*C*)
۱۱	Miao et al. [42]	O(N)	O(M)	*O*(*A*)
۱۲	Huang et al. [27]	O(M)	O(M)	*O*(*C*)
۱۳	Zhang et al. [76]	O(M)	O(MN)	*O*(*M*)
۱۴	Sun et al. [55]	O(C)	O(M)	*O*(*C*)
۱۵	Farras and Gonzalez [17]	O(C)	O(MC)	*O*(*C*)

۷- چالش‌ها و مسیرهای پیشرو

در این بخش، در مورد چالش‌ها و مسیرهای تحقیق در مورد طرح‌های رمزگذاری قابل جستجو بحث می‌کنیم.

۷-۱- بهره‌وری در ایجاد نمایه

در بخش ۳، مشاهده کردیم که اکثر طرح‌ها از ساختار داده‌ای کاملاً مشخصی برای ایجاد نمایه از فرهنگ لغت‌ها به درختان جستجوی دودویی متعادل استفاده می‌کنند. در مستندات، شاخص معکوس [۱ ، ۱۶ ، ۳۵ ، ۵۸ ، ۷۳] به طور گسترده‌ای از ساختار داده در روش‌های جستجوی تک کلیدواژه استفاده می‌نماید و مدل فضای برداری با استفاده از فاکتور TF*IDF برای رتبه‌بندی فرکانس کلیدواژه به مزایای بسیاری دست یافت [۱۱ ، ۱۷ ، ۲۰ ، ۲۱ ، ۲۷ ، ۴۰ ، ۴۱ ، ۵۵ ، ۶۷ ، ۷۱ ، ۷۵ ، ۷۶]. به همین ترتیب، پس از آن، درختان جستجوی باینری با پیچیدگی زمانی O(logn) که n تعداد اسناد است، سربار محاسباتی

را کاهش دادند [۲ ، ۴ ، ۳۹]. به نظر می‌رسد که شاخص معکوس و مدل فضای بردار هنوز به عنوان روش‌های نمایه‌سازی اصلی عمل می‌کنند. با این حال، علاوه بر این، ساختارهای درخت و گراف را می‌توان با هم برای کشف خواص جدید و بهبود کارایی در ایجاد یک نمایه استفاده کرد.

۷-۲- قابلیت جستجوی کارآمد

گفتیم که مرحله اولیه طرح‌های SE بر اساس قابلیت جستجو با یک کلیدواژه ساخته شده است، اما در این طرح‌ها دقت نتایج کمتر است [۸-۱۱ ، ۲۳ ، ۶۸]. بعد از آن، بسیاری از طرح‌های SE در یک سناریوی چند کلیدواژه‌ای ارائه شدند که در آن پرسمان به جای فقط یک کلیدواژه، شامل چندین کلیدواژه است. جستجوی کلیدواژه‌ها مبتنی بر رتبه‌بندی یکی از کاربردهای گسترده‌ای است که در آن اسناد با در نظر گرفتن رتبه کلیدواژه‌های داده شده بازیابی می‌شوند [۱۶ ، ۴۴ ، ۶۱ ، ۶۶ ، ۷۰ ، ۷۲ ، ۷۵ ، ۷۶]. به همین ترتیب، می‌توان با استفاده از جستجوی کلیدواژه فازی، اسناد را بازیابی کرد و از انواع اشتباهات کوچک تایپی کاربر اجتناب نمود [۱ ، ۲۰ ، ۳۲ ، ۳۳ ، ۵۰ ، ۶۰ ، ۶۹ ، ۷۳]. همچنین برای جستجوی کلیدواژه عطفی جستجوی تک کلیدواژه‌ای برای هر کلیدواژه که در پرسمان است انجام می‌شود و نتایج همه‌ی جستجوها با هم اشتراک گرفته می‌شود و نتیجه‌ی نهایی برای جستجوی کلیدواژه عطفی ارائه می‌گردد [۲ ، ۶ ، ۱۵ ، ۲۹ ، ۴۱ ، ۷۱]. ولی، سازوکارهای مختلف جستجو برای انواع پرسمان‌های غنی‌تر مانند پرسمان زیرمجموعه و پرسمان دامنه، تحقیقات بیشتری نیاز دارد.

۷-۳- روش‌های رمزگذاری امن

در ابتدا، طرح‌های SE بر اساس روش رمزگذاری قابل جستجو متقارن (SSE) ایجاد شدند. این طرح‌ها به یک کانال امن اضافی برای به اشتراک گذاشتن کلید خصوصی در بین مالکان و کاربران نیاز داشتند. با این حال، هیچ تضمینی برای ایمن‌بودن یک کانال امن وجود ندارد. سپس، روش رمزگذاری قابل جستجوی کلیدعمومی (PSE) معرفی شد که آن‌ها هرگز به یک کانال امن برای برقراری ارتباط بین مالک و کاربران احتیاج ندارند زیرا PSE از دو کلید استفاده می‌کند: یکی برای رمزگذاری (کلید عمومی) و دیگری برای رمزگشایی (کلید خصوصی). براساس دامنه PSE، رمزگذاری قابل جستجوی مبتنی بر شناسه (IBSE) و رمزگذاری قابل جستجو ویژگی مبنا (ABSE) به‌ترتیب به برای حذف کاربر و کنترل دسترسی دقیق، معیارهای امنیتی را در اختیار شما قرار می‌دهند. علاوه بر این، با وجود دوران پسا کوانتومی، تمام طرح‌هایی که بر اساس فرض زوج‌سازی دو خطی ساخته می‌شوند، توسط رایانه‌های کوانتومی مورد حمله قرار می‌گیرند. از این رو، باید با در نظر گرفتن حملات کوانتومی، طرح‌های جدیدی ایجاد شود.

۷-۴- جستجوی پویای امن

افزودن کلیدواژه‌ها جدید به یک نمایه که از قبل ساخته شده است در طرح‌های SE ایستا، بدون نمایه‌سازی مجدد کل داده‌ها امکان پذیر نیست. با مروری که انجام دادیم، مشاهده کردیم که طرح‌های SE پویا به کاربران امکان می‌دهند تا عملیات به‌روزرسانی پویا مانند اضافه کردن، حذف و اصلاح داده‌هایی را که قبلاً به سرور ابری سپرده شده را انجام دهند [۷ ، ۱۳ ، ۱۸ ، ۱۹ ، ۳۵ ، ۵۸ ، ۵۹ ، ۶۲ ، ۶۶ ، ۷۰ ، ۷۴]. از طرف دیگر، به‌روزرسانی پیام‌ها به صورت پویا و بدون در نظر گرفتن ساختار نمایه، به راحتی توسط سرور ابری مشاهده می‌شود. این امر نشان می‌دهد که طرح‌های جستجوی پویا از حریم خصوصی پیش‌سو و رو به عقب برخوردار نیستند. اگر سرور نتواند بداند که پیام تازه اضافه شده دارای کلیدواژه‌ای است که قبلاً جستجو شده همچنین سرور نتواند به ترتیب بر روی پیام های حذف شده جستجو کند، گفته می‌شود که طرح‌های جستجوی پویا دارای حریم خصوصی پیش‌سو و رو به عقب هستند. جستجوی پویا برای برنامه‌هایی که در دنیای واقعی بکار می‌روند مناسب است زیرا داده‌ها در دنیای واقعی متغیر هستند. به طور کلی طرح‌های پویا اطلاعات بیشتری را در مقایسه با طرح‌های ایستا نشت می‌دهند. از این رو، ساخت طرح‌های پویای امن نیاز به مطالعه بیشتری دارد.

۷-۵- قابلیت تأیید

همراه با حریم خصوصی داده‌ها، یکپارچگی داده‌ها نیز برای امن‌سازی طرح SE مهم است. عدم یکپارچگی داده‌ها از بسیاری جهات ممکن است در اشکالات نرم‌افزاری، تهدیدات داخلی و حملات خارجی اتفاق افتد. از آنجا که نتایج به‌دست‌آمده از سرور ابری ممکن است تمام مدت صحیح نباشد، تأیید نتایج جستجو می‌تواند گواه بر داده‌های صحیح باشد. در این بررسی مشاهده کردیم که بسیاری از نویسندگان، طرح‌های مختلف قابل تأیید را برای تایید نتایج به‌دست‌آمده از ابر ارائه کرده‌اند [۴ ، ۱۲ ،

۳۸ ، ۴۲ ، ۴۳ ، ۵۱ ، ۵۵ ، ۵۷ ، ۶۴ ، ۷۸]. طرح‌های جستجوی قابل تأیید باید بدون به خطر انداختن ویژگی‌های اساسی مانند به‌روزرسانی داده‌های پویا و برخی از ویژگی‌های مهم جستجو ساخته شوند. علاوه بر این، هزینه تأیید، صرف نظر از جمع آوری داده‌های بزرگ، باید برای کاربران، ناچیز و مقرون به صرفه باشد. از این رو، طرح‌های جستجوی قابل تأیید با حداقل هزینه و بدون از دست دادن ویژگی‌های اساسی مورد نیاز است.

۷-۶- مشکل کلیدسپاری[1]

در مرور مستندات، مشاهده کردیم که طرح‌های ABSE هویت کاربر را به مجموعه‌ای از ویژگی‌ها تقسیم می‌کنند و به هر کاربر این امکان را می‌دهند تا یک مجموعه ویژگی منحصر به فرد داشته باشد [۱۳ ، ۲۸ ، ۳۶ ، ۴۷ ، ۵۸ ، ۶۲ ، ۷۷]. با این حال، رایج‌ترین مشکلی که در طرح‌های ABSE وجود دارد، مسألهٔ کلید سپاری است. این اتفاق زمانی رخ می‌دهد که مرجع معتمد (TA) که به عنوان تولیدکننده یک کلید خصوصی برای کاربران شناخته می‌شود، دسترسی غیرمعمولی به کلیدها داشته باشد، به عنوان مثال، TA پیام را رمزگشایی می‌کند و ممکن است آسیب‌پذیر باشد. از این رو، طرح‌های ABSE باید بدون مشکل کلیدسپاری طراحی شوند.

۷-۷- فناوری زنجیرقالب[2] در رمزگذاری قابل جستجو

با پیشرفت فناوری، فناوری زنجیرقالب جنبه‌های جذاب و امیدوار کننده‌ای نشان داد و توجه بیشتری را از رویکرد SE کسب نمود. چندین پیشنهاد برای استفاده از فناوری زنجیرقالب در رمزگذاری قابل ارائه شده است [۵ ، ۲۶]. کار کای و همکاران [۵] اولین کاری است که رمزگذاری قابل جستجو و زنجیرقالب را ادغام می‌نماید. با این وجود، برای توسعه‌ی طرح‌های بالغ‌تر در آینده، به مطالعه و آزمایشات بیشتری نیاز دارد.

۸- نتیجه‌گیری

در این مقاله، طرح‌های مختلف رمزگذاری قابل جستجو در رایانش ابری را مرور کردیم. اهداف اصلی طرح‌های SE حریم خصوصی داده‌ها، کارایی، امنیت و پرسمان روشن است. در این بررسی، با در نظر گرفتن معماری، الگوریتم‌ها و اهداف طراحی، رمزگذاری قابل جستجو را مرور کردیم. SE را به طرح‌های SSE، PSE و ABSE طبقه‌بندی کردیم و از نظر قابلیت جستجو، ساختار نمایه، معیارهای امنیتی و کارایی، با یکدیگر مقایسه کردیم. سپس، امنیت طرح‌های رمزگذاری قابل جستجو فعلی را بر اساس انواع مختلف حملات ممکن تحلیل کردیم. تحلیل کارایی طرح‌های رمزگذاری قابل جستجو را بر اساس زمان جستجو، زمان ایجاد نمایه و زمان دریچه انجام دادیم. علاوه بر این، در مورد کاربردهای مختلف طرح‌های SE بحث کردیم. بر اساس بررسی، چالش‌هایی مانند کارایی در ایجاد نمایه، روش‌های رمزگذاری امن، کارایی در قابلیت جستجو، جستجوی پویای امن، قابل تأیید، مشکل کلیدسپاری و فناوری زنجیرقالب در رمزگذاری قابل جستجو را شناسایی کردیم. به منظور پیشنهاد کارهای آینده، می‌توان روی رمزگذاری قابل جستجو ویژگی مبنا برای حل مشکل کلیدسپاری و مقاومت در برابر حملات کوانتومی کار کرد.

[1] Key escrow problem
[2] Blockchain

۹- مراجع

[1] Ahsan MAM, Chowdhury FZ, Sabilah M, Wahab A, Idris B (2017) An efficient fuzzy keyword matching technique for searching through encrypted cloud data. In: International Conference on Research and Innovation in Information Systems (ICRIIS). https://doi.org/10.1109/ICRIIS.2017.8002456

[2] Ali FS, Lu S (2016) Searchable encryption with conjunctive field free keyword search scheme. In: 2016 International Conference on Network and Information Systems for Computers (ICNISC), IEEE, pp 260-264. https://doi.org/10.1109/ICNISC.2016.064

[3] Bellare M, Goldreich O, Goldwasser S (1994) Incremental cryptography: the case of hashing andsigning. In: Annual International Cryptology Conference, Springer, Berlin, pp 216-233

[4] Bost R, Fouque PA, Pointcheval D (2016) Verifiable dynamic symmetric searchable encryption: optimality and forward security. IACR Cryptology ePrint Archive p 62

[5] Cai C, Yuan X, Wang C (2017) Towards trustworthy and private keyword search in encrypted decentralized storage. In: 2017 IEEE International Conference on Communications (ICC), IEEE, pp 1-7. https://doi.org/10.1109/ICC.2017.7996810

[6] Cai K, Hong C, Zhang M, Feng D, Lv Z (2013) A secure conjunctive keywords search over encrypted cloud data against inclusion-relation attack. In: 2013 IEEE 5th

International Conference on Cloud Computing Technology and Science, IEEE, vol 1, pp 339-346. https://doi.org/10.1109/ CloudCom.2013.51

[7] Cao N, Wang C, Lia M, Ren K, Lou W (2014) Privacy-preserving multi-keyword ranked search
over encrypted cloud data. IEEE Trans Parallel Distrib Syst 25(1):222-233. https://doi.org/10.1109/ TPDS.2013.45

[8] Cash D, Jaeger J, Jarecki S, Jutla CS, Krawczyk H, Rosu MC, Steiner M (2014) Dynamic searchable encryption in very-large databases: data structures and implementation. In: NDSS, Citeseer, vol 14, pp 23-26. https://doi.org/10.14722/ndss.2014.23264

[9] Chang YC, Mitzenmacher M (2005) Privacy preserving keyword searches on remote encrypted data. In: International Conference on Applied Cryptography and Network Security, Springer, pp 442-455. https://doi.org/10.1007/11496137_30

[10] Chase M, Kamara S (2010) Structured encryption and controlled disclosure. In: International Con-ference on the Theory and Application of Cryptology and Information Security, Springer, pp 577-594. https://doi.org/10.1007/978-3-642-17373-8_33

[11] Chen R, Mu Y, Yang G, Guo F, Wang X (2016) Dual-server public-key encryption with key-word search for secure cloud storage. IEEE Trans Inf Forensics Secur 11(4):789-798. https://doi. org/10.1109/TIFS.2015.2510822

[12] Cheng R, Yan J, Guan C, Zhang F, Ren K (2015) Verifiable searchable symmetric encryption from indistinguishability obfuscation. In: Proceedings of the 10th ACM Symposium on Informa-tion, Computer and Communications Security, ACM, pp 621-626. https://doi.org/10.1145/27145 76.2714623

[13] Cui J, Zhou H, Zhong H, Xu Y (2018) Akser: attribute-based keyword search with efficient revoca-tion in cloud computing. Inf Sci 423:343-352. https://doi.org/10.1016/j.ins.2017.09.029

[14] Curtmola R, Garay J, Kamara S, Ostrovsky R (2006) Searchable symmetric encryption: improved definitions and efficient constructions. In: 13th ACM Conference on Computer and Communica-tions Security

[15] Ding M, Gao F, Jin Z, Zhang H (2012) An efficient public key encryption with conjunctive keyword search scheme based on pairings. In: 2012 3rd IEEE International Conference on Network Infra-structure and Digital Content, IEEE, pp 526-530. https://doi.org/10.1109/ICN-IDC.2012.6418809

[16] Du M, Wang Q, He M, Weng J (2018) Privacy-preserving indexing and query processing for secure dynamic cloud storage. IEEE Trans Inf Forensics Secur 13(9):2320-2332. https://doi.org/10.1109/ TIFS.2018.2818651

[17] Farràs O, Ribes-González J (2019) Provably secure public-key encryption with conjunctive and sub-set keyword search. Int J Inf Secur. https://doi.org/10.1007/s10207-018-00426-7

[18] Fu Z, Shu J, Sun X, Linge N (2014a) Smart cloud search services: verifiable keyword-based semantic search over encrypted cloud data. IEEE Trans Consum Electr 60(4):762-770. https://doi. org/10.1109/TCE.2014.7027353

[19] Fu Z, Sun X, Linge N, Zhou L (2014b) Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query. IEEE Trans Consum Electr 60(1):164-172. https://doi.org/10.1109/TC-E.2014.6780939

[20] Fu Z, Wu X, Guan C, Sun X, Ren K (2016) Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. IEEE Trans Inf Forensics Secur 11(12):2706-2716. https://doi.org/10.1109/TIFS.2016.2596138

[21] Fu Z, Wu X, Wang Q, Ren K (2017) Enabling central keyword-based semantic extension search over encrypted outsourced data. IEEE Trans Inf Forensics Secur 12(12):2986-2997. https://doi. org/10.1109/TIFS.2017.2730365

[22] Fu Z, Xia L, Sun X, Liu AX, Xie G (2018) Semantic-aware searching over encrypted data for cloud computing. IEEE Trans Inf Forensics Secur 13(9):2359-2371. https://doi.org/10.1109/ TIFS.2018.2819121

[23] Goh EJ et al (2003) Secure indexes. IACR Cryptol ePrint Archive 2003:216

[24] Han F, Qin J, Hu J (2016) Secure searches in the cloud: a survey. Fut Gener Comput Syst 62:66-75.
https://doi.org/10.1016/j.future.2016.01.007

[25] Höfer C, Karagiannis G (2011) Cloud computing services: taxonomy and comparison. J Internet Serv Appl 2(2):81-94. https://doi.org/10.1007/s13174-011-0027-x

[26] Hu S, Cai C, Wang Q, Wang C, Luo X, Ren K (2018) Searching an encrypted cloud meets block-chain: a decentralized, reliable and fair realization. In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications, IEEE, pp 792-800. https://doi.org/10.1109/INFOCO-

M.2018.8485890

[27] Huang Q, Li H (2017) An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks. Inf Sci 403:1-14. https://doi.org/10.1016/j.ins.2017.03.038

[28] Hur J, Noh DK (2011) Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Trans Parall Distrib Syst 22(7):1214-1221. https://doi.org/10.1109/TP-DS.2010.203

[29] Hwang MS, Hsu ST, Lee CC (2014) A new public key encryption with conjunctive field keyword search scheme. Inf Technol Control 43(3):277-288. https://doi.org/10.5755/j01.itc.43.3.6429

[30] Jeong IR, Kwon JO, Hong D, Lee DH (2009) Constructing PEKS schemes secure against keyword guessing attacks is possible? Comput Commun 32(2):394-396. https://doi.org/1-0.1016/j.comco m.2008.11.018

[31] Kalapatapu A, Sarkar M (2012) Cloud computing: an overview. Cloud Comput Methodol Syst
Appl. https://doi.org/10.1201/b11149-8

[32] Kuzu M, Islam MS, Kantarcioglu M (2012) Efficient similarity search over encrypted data. In: 2012 IEEE 28th International Conference on Data Engineering, IEEE, pp 1156-1167. https://doi. org/10.1109/ICDE.2012.23

[33] Li J, Wang Q, Wang C, Cao N, Ren K, Lou W (2010) Fuzzy keyword search over encrypted data in cloud computing. In: Proceedings 2010 IEEE INFOCOM, IEEE, pp 1-5. https://doi.org/10.1109/ INFCOM.2010.5462196

[34] Li R, Liu AX (2017) Adaptively secure conjunctive query processing over encrypted data for cloud computing. In: 2017 IEEE 33rd International Conference on Data Engineering (ICDE), IEEE, pp 697-708. https://doi.org/10.1109/ICDE.2017.122

[35] Li Y, Zhou F, Qin Y, Lin M, Xu Z (2018) Integrity-verifiable conjunctive keyword search-able encryption in cloud storage. Int J Inf Secur 17(5):549-568. https://doi.org/10.-1007/s1020 7-017-03-94-9

[36] Liang K, Susilo W (2015a) Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. IEEE Trans Inf Forensics Secur 10(9):1981-1992. https://doi.org/10.1109/ TIFS.2015.2442215

[37] Liang K, Susilo W (2015b) Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. IEEE Trans Inf Forensics Secur 10(9):1981-1992. https://doi.org/10.1109/ TIFS.2015.2442215

[38] Liu P, Wang J, Ma H, Nie H (2014) Efficient verifiable public key encryption with keyword search based on kp-abe. In: 2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications, IEEE, pp 584-589. https://doi.org/10.1109/BWCCA.2014.119

[39] Liu Z, Lv S, Wei Y, Li J, Liu JK, Xiang Y (2017) Ffsse: flexible forward secure searchable encryp-tion with efficient performance. IACR Cryptol ePrint Archive 2017:1105

[40] Ma S (2016) Identity-based encryption with outsourced equality test in cloud computing. Inf Sci 328:389-402. https://doi.org/10.1-016/j.ins.2015.08.053

[41] Miao Y, Ma J, Liu X, Liu Z, Shen L, Wei F (2016) Vmkdo: verifiable multi-keyword search over encrypted cloud data for dynamic data-owner. Peer-to-Peer Netw Appl. https://doi.org/10.1007/ s12083-016-0487-7

[42] Miao Y, Ma J, Jiang Q, Li X, Sangaiah AK (2018) Verifiable keyword search over encrypted cloud data in smart city. Comput Electr Eng 65:90-101. https://doi.or-g/10.1016/j.compelecen g.2017.06.021

[43] Ogata W, Kurosawa K (2016) Efficient no-dictionary verifiable SSE. IACR Cryptol ePrint Archive 2016:981

[44] Pasupuleti SK, Ramalingam S, Buyya R (2016) An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. J Netw Comput Appl 64:12-22. https://doi.org/10.1016/j.jnca.2015.11.023

[45] Pham H, Woodworth J, Salehi MA (2018) Survey on secure search over encrypted data on the cloud. arXiv preprint arXiv:181109767

[46] Poh GS, Chin JJ, Yau WC, Choo KKR, Mohamad MS (2017) Searchable symmetric encryption: designs and challenges. ACM Comput Surv (CSUR) 50(3):40. https://doi.org/10.1145-/3064005

[47] Premkamal PK, Pasupuleti SK, Alphonse P (2018) A new verifiable outsourced ciphertext-policy attribute based encryption for big data privacy and access control in cloud. J Ambient Intell Human Comput 10:2693-2707

[48] Qian L, Luo Z, Du Y, Guo L (2009) Cloud computing: An overview. In: IEEE International Confer-ence on Cloud Computing, Springer, pp 626-631. https://doi.org/10.1007/978-3-642-10665-1_63

org/10.1109/TDSC.2016.2635128

[60] Wang B, Yu S, Lou W, Hou YT (2014) Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud. IEEE INFOCOM 2014-IEEE Conference on Computer Communica-tions pp 2112-2120. https://doi.org/10.1109/INFOCOM.2014.6848153

[61] Wang C, Cao N, Ren K, Lou W (2012) Enabling secure and efficient ranked keyword search over outsourced cloud data. IEEE Trans Parallel Distrib Syst 23(8):1467-1479. https://doi.org/10.1109/ TPDS.2011.282

[62] Wang N, Fu J, Bhargava BK, Zeng J (2018) Efficient retrieval over documents encrypted by attributes in cloud computing. IEEE Trans Inf Forensics Secur 13(10):2653-2667. https://doi.org/10.1109/TIFS.2018.2825952

[63] Wang Y, Wang J, Chen X (2016) Secure searchable encryption: a survey. J Commun Inf Netw 1(4):52-65. https://doi.org/10.1007/BF0-3391580

[64] Wu D, Gan Q, Wang X (2018) Verifiable public key encryption with keyword search based on homomorphic encryption in multi-user setting. IEEE Access 6:42445-42453. https://doi.org/10.1109/ACCESS.2018.2861424

[65] Wu Z, Li K (2019) Vbtree: forward secure conjunctive queries over encrypted data for cloud com-puting. VLDB J 28(1):25-46. https://doi.org/10.1007/s00778-018-0517-6

[66] Xia Z, Wang X, Sun X, Wang Q (2016) A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans Parallel Distrib Syst 27(2):340-352. https://doi.org/10.1109/TPDS.2015.2401003

[67] Xu K, Wang G, Wang S, Zhao Z, Wang J (2017) A secure channel free conjunctive keyword search without random oracle under simple assumption. In: 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN), IEEE, pp 1467-1476. https://doi.org/10.1109/ICCSN.2017.8230352

[68] Xu P, Jin H, Wu Q, Wang W (2013a) Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack. IEEE Trans Comput 62(11):2266-2277. https://doi.org/10.1109/TC.2012.215

[69] Xu P, Jin H, Wu Q, Wang W (2013b) Public-key encryption with fuzzy keyword search: a provably secure scheme under keyword guessing attack. IEEE Trans Comput 62(11):2266-2277. https://doi.org/10.1109/TC.2012.215

[49] Sarga L (2012) Cloud computing: an overview. J Syst Integr 3(4):3-14. https://doi.org/10.20470/jsi. v3i4.131

[50] Shen J, Shen J, Chen X, Huang X, Susilo W (2017a) An efficient public auditing protocol with novel dynamic structure for cloud data. IEEE Trans Inf Forensics Secur 12(10):2402-2415. https://doi.org/10.1109/TIFS.2017.2705620

[51] Shen J, Wang C, Wang A, Ji S, Zhang Y (2018) A searchable and verifiable data protection scheme for scholarly big data. IEEE Trans Emerg Topics Comput. https://doi.org/10.1109/ TETC.2018.2830368

[52] Shen Z, Shu J, Xue W (2017b) Keyword search with access control over encrypted cloud data. IEEE Sens J 17(3):858-868. https://doi.org/10.1109/JSEN.2016.2634018

[53] Song DX, Wagner D, Perrig A (2000) Practical techniques for searches on encrypted data. In: Pro-ceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000, IEEE, pp 44-55. https://doi.org/10.1109/SECPRI.2000.848445

[54] Su S, Teng Y, Cheng X, Xiao K, Li G, Chen J (2015) Privacy-preserving top-k spatial keyword queries in untrusted cloud environments. IEEE Trans Serv Comput. https://doi.org/10.1109/ TSC.2015.2481900

[55] Sun J, Wang X, Wang S, Ren L (2018) A searchable personal health records framework with fine-grained access control in cloud-fog computing. PloS One 13(11):e0207543. https://do-i.org/10.1371/journal.pone.0207543

[56] Sun W, Wang B, Cao N, Li M, Lou W, Hou YT, Li H (2013) Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking. In: Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, ACM, pp 71-82

[57] tch you if you lie to me: Efficient verifiable conjunc-tive keyword search over large dynamic encrypted cloud data. In: 2015 IEEE Conf Comput Commun (INFOCOM), IEEE, pp 2110-2118

[58] Sun W, Yu S, Lou W, Hou YT, Li H (2016) Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. IEEE Trans Parallel Dis-trib Syst 27(4):1187-1198. https://doi.org/10.1109/TPDS.2014.2355202

[59] Wan Z, Deng RH (2018) Vpsearch: achieving verifiability for privacy-preserving multi-keyword search over encrypted cloud data. IEEE Trans Depend Secure Comput 15(6):1083-1095. https://doi.

[70] Yan J, Zhang Y, Liu X (2016) Secure multi-keyword search supporting dynamic update and ranked retrieval. China Commun 13(20):209-221. https://doi.org/10.1109/CC.2016.7733045

[71] Yang Y, Ma M (2016) Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds. IEEE Trans Inf Forensics Secur 11(4):746-759. https:// doi.org/10.1109/TIFS.2015.2509912

[72] Yu J, Lu P, Zhu Y, Xue G, Li M (2013) Toward secure multikeyword top-k retrieval over encrypted cloud data. IEEE Trans Depend Secure Comput 10(4):239-250. https://doi.org/10.1109/ TDSC.2013.9

[73] Yuan X, Wang X, Wang C, Yu C, Nutanong S (2017) Privacy-preserving similarity joins over encrypted data. IEEE Trans Inf Forensics Secur 12(11):2763-2775. https://doi.org/10.1109/ TIFS.2017.2721221

[74] Wang Q, He M, Du M, Chow SS, Lai RW, Zou Q (2018) Searchable encryption over fea-ture-rich data. IEEE Trans Depend Secure Comput 15(3):496-510. https://doi.org/10.1109/ TDSC.2016.2593444

[75] Zhang W, Lin Y, Xiao S, Wu J, Zhou S (2016) Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing. IEEE Trans Comput 65(5):1566-1577. https://doi. org/10.1109/TC.2015.2448099

[76] Zhang W, Lin Y, Qi G (2018) Catch you if you misbehave: ranked keyword search results veri-fication in cloud computing. IEEE Trans Cloud Comput 6(1):74-86. https://doi.org/10.1109/ TCC.2015.2481389

[77] Zheng Q, Xu S, Ateniese G (2014) Vabks: verifiable attribute-based keyword search over outsourced encrypted data. In: IEEE INFOCOM 2014-IEEE Conference on Computer Communications, IEEE, pp 522-530. https://doi.org/10.1109/INFOCOM.2014.6847976

[78] Zhu J, Li Q, Wang C, Yuan X, Wang Q, Ren K (2018) Enabling generic, verifiable, and secure data search in cloud services. IEEE Trans Parallel Distrib Syst 29(8):1721-1735. https://doi.org/10.1109/ TPDS.2018.2808283