فصلنامه علمی-ترویجی پدافند غیرعامل

سال هشتم، شماره ۲، تابستان ۱۳۹۶، (پیاپی ۳۰): صص ۴۲-۳۵

بررسی و ارزیابی مدل‌های جدید امنیت داده در رایانش ابری

وحید شاهی[۱]، مهدی نقوی[۲*]

تاریخ دریافت: ۱۳۹۵/۰۳/۰۸
تاریخ پذیرش: ۱۳۹۵/۱۱/۲۴

چکیده

رایانش ابری یک مدل پردازشی است که به‌دلایل قابلیت انعطاف‌پذیری، گسترش سریع و هزینه پایین، مورد توجه پژوهشگران قرارگرفته و استفاده اشتراکی سرویس‌ها را بدون نیاز به حق مالکیت و مدیریت منابع در محیط شبکه فراهم می‌نماید. با توجه به ذخیره و بازیابی داده‌های کاربران سرویس‌های ابر، امنیت داده یکی از چالش‌های عمده رایانش ابری محسوب می‌شود. برای مقابله با این چالش‌ها، مدل‌های مختلف امنیت داده در سطح ابر ارائه شده است که در این مقاله برخی از این مدل‌ها را بررسی و ارزیابی کرده‌ایم. نتیجه ارزیابی‌ها نشان می‌دهد که مدل امنیت داده ترکیبی، بیشترین امنیت را زمانی داراست که داده‌ها علاوه‌بر رمزنگاری، طبقه‌بندی و نمایه‌گذاری نیز شوند. هم‌چنین مدل مبتنی بر سطح، با تقسیم داده به دو سطح و احراز هویت دومرحله‌ای درصدد امن‌کردن داده‌های سطح ابر است. مدل کسب وکار امنیت داده نیز با توجه به فعالیت مستقل سرویس‌های ابر، سرباری پایین‌تری نسبت به سایر مدل‌های امنیت داده دارد.

کلیدواژه‌ها: **رایانش ابری، امنیت داده، مدل ترکیبی، مدل مبتنی بر سطح، مدل کسب و کار**

۱- دانشجوی کارشناسی ارشد کامپیوتر، دانشگاه جامع امام حسین(ع)

۲- استادیار گروه کامپیوتر، دانشگاه جامع امام حسین(ع) ، Email:mnaghavi@ihu.ac.ir- نویسنده مسئول

۱- مقدمه

رایانش ابری نوعی از پردازش موازی و توزیع شده است که در سال ۲۰۰۷ شرکت هایبزرگیچون گوگل، آمازون، IBM و دانشگاه‌های بزرگ و معتبر جهان، یک پروژه تحقیقاتی در این زمینه را آغاز کردند و با توجه به ویژگی‌های مثبت و چشم‌گیری که با خود به ارمغان آورد، سازمان‌های بزرگ و معتبر بسیاری به آن روی آوردند [۱]. رایانش ابری مدلی برای فراهم‌کردن دسترسی آسان به مجموعه‌ای از منابع رایانشی قابل تغییر است که مبتنی بر تقاضای کاربر بوده و از طریق شبکه و با کمترین نیاز به مدیریت منابع، به سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها متصل است [۲].

رایانش ابری به‌عنوان یک مفهوم جدید در فنّاوری و تجارت است که از دید افراد مختلف رویکردهای متفاوتی داشته و برای توسعه‌دهندگان و به یک سکوی توسعه و محیط اجرای نرم‌افزار در مقیاس اینترنت و برای مدیران و فراهم‌کنندگان ارتباطات زیرساخت، یک زیرساخت مبتنی بر مراکز داده‌ای توزیع‌شده و عظیم است که از طریق شبکه به‌هم متصل هستند [۳].

رایانش ابری، برنامه‌های کاربردی و بانک‌های اطلاعاتی را به سمت مراکز داده بسیار بزرگ سوق می‌دهد که در آن مدیریت داده‌ها و سرویس قابل اعتماد نیست. این ویژگی رایانش ابری، چالش‌های امنیتی زیادی را به دنبال دارد. گسترش رایانش ابری و انتقال داده‌ها به فضای ابر، افزایش حجم ذخیره‌سازی داده را به دنبال دارد که در اصطلاح به آن داده‌های کلان گویند. مفهوم داده‌های کلان بیان‌گر این است که بسیاری از برنامه‌های کاربردی که از مجموعه داده‌های کلان استفاده می‌نمایند قادر به ذخیره‌سازی و پردازش این حجم داده‌ها با استفاده از منابع محلی نیستند [۴].

با توجه به گزارش IDC[1] امنیت، کارایی و دسترس‌پذیری از چالش‌های اصلی رایانش ابری هستند و امنیت مهم‌ترین موضوعی است که به‌منظور استفاده گسترده از رایانش ابری باید مورد توجه قرار گیرد [۵]. امنیت داده نیز مهم‌ترین بحث امنیت رایانش ابری است که شامل دو مؤلفه مؤثر تفکیک داده و جلوگیری از فاش‌شدن داده است. تفکیک داده با توجه به ذخیره داده‌ها در توده ابر در یک محیط اشتراکی، این قابلیت را فراهم می‌کند که از عدم دسترسی دیگران به داده‌های خود مطمئن شد. همچنین با توجه به این‌که اطلاعات حساس مربوط به سازمان در خارج از مرزهای آن، ذخیره شده و یا پردازش می‌شوند، باید کنترل دسترسی لازم برای جلوگیری از فاش‌شدن داده‌ها در ابر صورت‌گیرد [۶].

برخی از مدل‌های امنیتی وجود دارند که موفق به امن‌سازی داده‌های مشتری در سطح فضای ابر می‌شوند. بررسی‌های امنیتی نشان می‌دهد که روش‌های رمزنگاری RSA در رایانش ابری مورد نیاز بوده و برای جلوگیری از حملات کاربران بدخواه برای دسترسی به داده‌ها و صحت ذخیره‌سازی داده‌ها در سطح ابر به‌کار می‌رود [۷]. در بخش دوم این مقاله، کارهای مرتبط با موضوع مقاله بیان شده است. در بخش سوم به بیان مدل‌های اولیه امنیت داده پرداخته و در بخش چهارم برخی از مدل‌های جدید امنیت داده را مورد بحث و بررسی قرار می‌دهیم؛ در بخش پنجم مدل‌های ارائه شده را مورد ارزیابی قرار داده و در بخش ششم از بحث‌های انجام شده نتیجه‌گیری خواهد شد.

۲-کارهای مرتبط

مطالعات، تحقیقات و پژوهش‌های زیادی در زمینه مدل‌های امنیت داده صورت گرفته است که در این بخش به برخی از آنان اشاره می‌نماییم. در بحث مدل و معماری‌های امنیت داده در رایانش ابری، محققین دانشگاه شاندونگ در مقاله‌ای [۸] یک مدل امنیت داده پیشنهاد داده‌اند که سازوکارهای رمزنگاری مؤثر برای محافظت از داده کاربران را می‌پذیرد. همان‌طورکه داده‌های رمزنگاری‌شده به‌سختی بازیابی می‌شوند، در این مدل یک متد بازیابی متن رمز ارائه شده است. نتایج آزمایش‌ها روی مدل ارائه شده، بیانگر این است که این مدل می‌تواند قابلیت اعتماد و جامعیت را تضمین نماید. این مدل به‌خوبی قابل استفاده بوده و مقیاس‌پذیر است.

در پژوهشی دیگر، طراحی یک مدل امنیت داده در رایانش ابری [۹] بر روی یک محیط کسب‌وکار صورت گرفته که آن شامل عملگر داده‌ها نیز هست. پیاده‌سازی مدل ارائه شده به‌وسیله UML صورت گرفته است. این مدل به ۷ واحد تقسیم شده است که هر قسمت به‌صورت مستقل، اصلاحات امنیت داده را معین می‌کند. مبتنی بر این مدل، تبدیل پیاده‌سازی ابر به محیط سرمایه‌گذاری امکان‌پذیر است.

در تحقیقی‌که در زمینه مدل‌های امنیت داده در رایانش ابری صورت گرفته است، برخی از مدل‌ها برای امنیت مراحل مختلف داده‌ها ازجمله ذخیره‌سازی و رمزنگاری بررسی و مقایسه شده است [۱۰].. اگر قرار است داده به‌مدت طولانی ذخیره شود، قابلیت اطمینان و مالکیت داده‌ها بسیار مهم است.

۳- مدل‌های اولیه امنیت داده در رایانش ابری

یک مدل صحیح امنیت داده، با استفاده از روش‌های رمزنگاری سنتی جامعیت داده را محافظت می‌کند. یکی از این روش‌ها استفاده از تابع درهم‌ساز MAC[2] است. کاری‌که MAC می‌کند این است که یک کلید رمز را به‌همراه یک پیام به‌عنوان ورودی قبول می‌کند و یک خروجی به‌نام کد تصدیق پیام می‌دهد. کاربرد اصلی این تابع این است که موقع ارسال پیام برای فردی دیگر، آن فرد بتواند از هویت

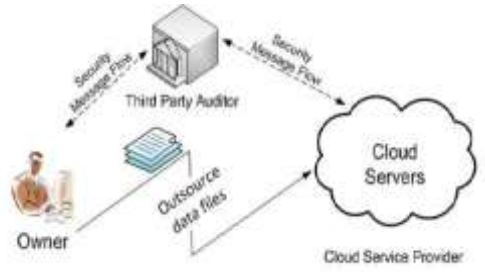
1- International Data Corporation- www.idc.com

۲- Message Authentication Code (MAC)

اصلی فرد فرستنده اطمینان حاصل کند و مطمئن شود تا فردی پیام را برایش ارسال کرده که آن انتظارش را داشته و ارسال کننده اصلی پیام است.

در واقع MAC داده‌ای است که در انتهای پیام ارسالی قرار می‌گیرد و از طریق استفاده از آن، حفظ جامعیت پیام و صحت آن را تأیید می‌کند. طرفین از کلید مشترک یک‌سانی که برای تولید این داده استفاده می‌شود، مطلع هستند. از این‌رو در خانواده رمزنگاری‌های متقارن قرار می‌گیرد.

برای تأیید جامعیت و صحت داده‌ها، مدلی برای حفظ حریم خصوصی و نظارت و بررسی‌های عمومی به‌منظور امنیت داده‌ها توسعه یافت. این مدل که با نام TPA[1] است در حفاظت از حریم خصوصی قابل توجه است؛ زیرا کاربران ابر درحال انتقال و برون‌سپاری داده‌های خود به سمت ابر هستند. TPA به‌منظور افزایش کارایی می‌تواند وظایف نظارتی خود را به‌صورت دسته‌ای انجام دهد. TPA فقط داده‌ها را در ابر بررسی نموده و قادر به کپی آن‌ها نخواهد بود. TPA نباید آسیب جدی برای امنیت داده‌های کاربر ایجاد کند. نقش TPA در برون‌سپاری داده‌ها به ابر و پیام رمزشده سرور ابر به مالک داده از طریق TPA در شکل (۱) نشان داده شده است [۱۱].



شکل ۱- معماری ذخیره‌سازی داده در ابر با TPA [۱۱]

کنترل دسترسی برای محیط محاسبات ابری لازم و ضروری به‌نظر می‌رسد. کنترل دسترسی به‌طور عمومی یک سیاست و یا روالی است که دسترسی به یک سیستم را محدود و یا رد می‌کند. کنترل دسترسی هم‌چنین ممکن است تلاش کاربران برای دسترسی به سیستم‌های غیرمجاز را نیز تشخیص دهد و سازوکاری است که برای محافظت از امنیت کاربر بسیار مهم می‌باشد.

۴- مدل‌های جدید امنیت داده در رایانش ابری

در این بخش برخی از مدل‌های جدید ارائه شده در مقوله امنیت داده رایانش ابری را ارائه می‌دهیم و آن‌ها را از دید طبقه‌بندی، رمزنگاری و کد تصدیق پیام بررسی می‌کنیم.

۴-۱- مدل امنیت داده ترکیبی

رویکرد ترکیبی جهت اطمینان از امنیت داده در رایانش ابری که توسط سندیپ سود ارائه شده، یک راه برای محافظت داده و بررسی احراز هویت و جامعیت داده به‌وسیله سازوکارهای صنعتی ممکن را فراهم می‌سازد [۱۲]. این روش، تقسیم داده به چندین بخش، نمایه‌سازی، رمزنگاری و کد تصدیق پیام و احراز هویت دومرحله‌ای یک کاربر توسط مالک داده و ابر را مطرح می‌کند.

این مدل دسترس‌پذیری داده را توسط بسیاری از اعمال شبیه تشخیص دسترسی غیرمجاز از یک فراهم‌کننده سرویس ابر تأمین می‌کند. مدل پیشنهادی به دسترسی بالا، قابلیت اعتماد و جامعیت انتقال داده از طریق مالک داده به ابر و از ابر به کاربر نایل می‌شود. علاوه بر این، انعطاف و توانایی بیشتری برای پاسخ‌گویی به تقاضاهای روزمره پیچیده شبکه داشته و این قابلیت را به کاربر می‌دهد تا فایل‌های مورد نظر را از فضای ابر، به‌وسیله جستجو بر داده‌های رمزشده بازیابی نماید.

مدل پیشنهادی برای فراهم‌نمودن امنیت کامل داده از طریق انجام همه فرایندهای رایانش ابری ساخت یافته است؛ بنابراین سازوکارهای چندگانه و فنون دسترس‌پذیر برای محافظت داده‌های حیاتی از دسترسی‌های غیرمجاز انجام می‌شوند. چارچوب پیشنهادی به دو فاز تقسیم شده است. فاز اول اقدام به فرایند انتقال و ذخیره‌سازی امن داده‌ها به فضای ابر می‌نماید.

فاز دوم نیز اقدام به بازیابی داده از ابر و نمایش تولید درخواست برای دسترسی داده، احراز هویت دومرحله‌ای، تصدیق امضای دیجیتال و جامعیت داده می‌نماید.

فاز اول با برخی متدها و سازوکارهای ذخیره‌سازی و امنیت داده‌ها از ابتدای کار و انتقال داده به‌صورت رمزنگاری‌شده سمت فضای ابر صورت می‌پذیرد. این فاز مجدداً به سه بخش تقسیم می‌شود. این تقسیم شامل طبقه‌بندی، ساخت و رمزنگاری نمایه و MAC است که MAC گام‌به‌گام، جزئیات فعالیت‌های انجام‌شده روی داده‌ها را فراهم می‌نماید.

طبقه‌بندی: همان‌طورکه داده‌ها در ابر ذخیره شده‌اند، یک روش برای ذخیره‌سازی داده‌ها در بخش‌های مختلف ابر، براساس سه پارامتر محرمانگی، دسترس‌پذیری و جامعیت وجود دارد. این مقادیر توسط خود مشتری و رتبه‌بندی پارامترها با استفاده از الگوریتم شکل (۲) فهرست خواهد شد. مقدار C بیانگر سطح خصوصی مورد نیاز برای هر مرحله از پردازش داده‌ها است. مقدار I نیز مبنی بر اندازه صحت داده، قابلیت اطمینان اطلاعات و محافظت داده‌ها از دسترسی‌های غیرمجاز است. مقدار A نیز بیانگر این است که داده

۱- Third Party Auditor (TPA)

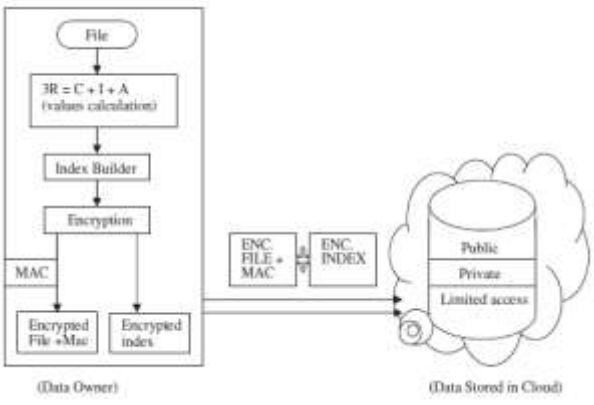
چگونه قابل دسترس بوده و هنگام درخواست چگونه به‌سرعت دردسترس درخواست‌کننده خواهد بود.

```
1. Input: Data, protection section, D [] array of n integer size.
   Where D[ ] array consisting of C, I, A, SR, R of n integer size.
2. Output: Categorized data for corresponding section.
3. For i=1 to n
        3.1 C [i]=Value of Confidentiality.
        3.2 I [i]=Value of Integrity.
        3.3 A [i] =Value of Availability.
        3.4 Calculate SR [ i ]=(C[ i ]+[1/A[ i]]*10+I[ i ] )/2   /*security and confidentiality is directly
                                                                  proportional to integrity and availability is
                                                                  inversely proportional to security*/
4. For j=1 to 10
        For i=1 to n
        IF SR [ i ]== 1||2||3 then                                /* where || represents OR operation.
        S[ i ]=3                                                  /* Section 3 allotted to D[i]th data.
        IF SR[ i ]== 4||5||6 then
        S[ i ] =2                                                 /* Section 2 allotted to D[i]th data.
        IF SR [i]== 8||9||10 then
        S[ i ] =1                                                 /* Section 1 allotted to D[i]th data.
```

شکل ۲- الگوریتم رتبه‌بندی پارامترهای ذخیره‌سازی [۱۲].

در الگوریتم شکل (۲)، وظیفه اصلی مالک داده، طبقه‌بندی داده‌ها بر اساس سه پارامتر رمزنگاری‌شده C، I و A است. آرایه D نشان‌دهنده این است که کاربر و داده باید مقادیر C، I و A را به‌عنوان ورودی وارد کنند تا مقدار SR محاسبه گردد. مقدار SR قابل استفاده برای یکی از بخش‌های سه‌گانه ابر هست.

ساخت و رمزنگاری نمایه: پس از تخصیص موفق مقادیر به داده‌ها، اکنون داده‌ها باید به سایر سازوکارهای پردازشی انتقال یابند. از آنجائی‌که داده روی ابر باید به‌صورت رمزشده ذخیره و بازیابی شوند، بنابراین نیاز به ایجاد یک نمایه به‌وسیله نمایه‌ساز شکل (۳) داریم. پس موقع بازیابی داده، می‌توان عمل جستجو را بر روی داده‌های رمزنگاری‌شده انجام داد. پس از ساخت نمایه، نوبت به رمزنگاری آن می‌رسد که می‌تواند با MAC و یا بدون MAC در فضای ابر ذخیره‌سازی شود.



شکل ۳- نمایه‌ساز داده [۱۲]

کد تصدیق پیام: پس از رمزنگاری داده‌ها، یک کد تصدیق پیام تولیدشده و با داده رمزشده سمت ابر ارسال می‌شود. این کد یک بلاک ثابتی از داده است که سایز کمی دارد. در واقع روال ذخیره داده در ابر به این صورت است که ابتدا مقدار SR=C+I+A از داده‌های فایل به‌دست آورده شده و سپس با استفاده از آن نمایه‌سازی صورت می‌گیرد. پس از نمایه‌سازی، داده‌ها به‌صورت رمز درمی‌آیند و با استفاده از MAC که شامل رمز K_I روی داده C_I است در فضای ابر ذخیره می‌شود. به‌فرض مثال اگر SR<=3 باشد، داده‌ها باید در سطح عمومی ذخیره شوند. اگر مقدار SR بین مقدار ۳ و ۶ باشد، در سطح خصوصی و در غیر این صورت در سطح مالک داده ذخیره شود.

۴-۲- مدل امنیت داده مبتنی بر سطح

امنیت داده در مدل مبتنی بر سطح توسط شرما مورد بررسی قرار گرفته است [۱۳]. مدل پیشنهادی به‌گونه‌ای طرح شده است که داده علاوه بر خود ابر، در حین انتقال نیز امنیت داشته باشد. مدل پیشنهادی از چهار بخش مالک داده، کاربر، ارائه‌دهنده سرویس ابر نامطمئن و شخص ثالث نامعتبر تشکیل شده است. داده در برابر نفوذگر شبکه، ارائه‌دهنده سرویس و کاربر غیرمجاز محافظت می‌شود. مؤلفه‌های مدل امنیت داده مبتنی بر سطح، به شرح ذیل هستند.

طبقه‌بندی: رمزنگاری داده، فن مورد استفاده در مدل پیشنهادی است. رمزنگاری داده با توجه به حساسیت و اهمیت داده انجام می‌شود. داده به دو نوع صفر و یک طبقه‌بندی می‌شود. داده نوع صفر، بیانگر غیرحساس‌بودن داده و داده نوع یک، بیانگر حساس‌بودن داده است. داده نوع یک، به‌خاطر حساس‌بودن لازم است قبل از بارگذاری در ابر رمزنگاری شود.

رمزنگاری و رمزگشایی: در این‌جا شخص ثالث نقش یک زیرساخت برای مدیریت کلید را ایفا می‌کند. مسئولیت شخص ثالث، مدیریت کلید و ذخیره‌سازی آن است. ذخیره‌سازی کلید شامل تولید کلید، حفاظت و ذخیره‌کردن آن است. مدیریت کلید نیز شامل ارائه کلید به کاربر مجاز است؛ یعنی بعد از تصدیق کلیدهایی که هویت کاربر را احراز می‌کنند. کلیدها با کد عبور، رمزنگاری می‌شوند. در این مدل فرض بر این است که شخص ثالث چیزی در رابطه با ارائه‌دهنده سرویس ابر نمی‌داند. الگوریتم‌های استانداردی مثل RSA و AES برای رمزنگاری و رمزگشایی استفاده می‌شود.

جامعیت داده: در راستای بررسی جامعیت داده، یعنی این‌که آیا داده در مسیر انتقال روی شبکه دستکاری شده است یا خیر؛ کد تصدیق پیام محاسبه می‌شود. در این مدل بعد از عمل رمزنگاری، کد تصدیق پیام از روی داده رمزنگاری‌شده، محاسبه گردیده و حین بارگذاری در ابر، ضمیمه داده رمزنگاری‌شده می‌شود. زمانی که کاربر یا

مالک داده به داده نیاز پیدا می‌کنند، آن را از ابر بارگیری کرده و جامعیت داده را با محاسبه MAC بررسی می‌کنند. کاربر یا مالک، MAC محاسبه شده را با MAC ضمیمه‌شده تطبیق می‌دهد. الگوریتم استاندارد چکیده‌سازی پیام MD5 برای جامعیت داده استفاده می‌شود.

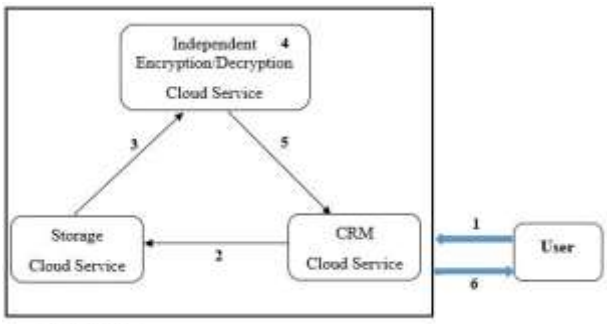
احراز هویت: برای احراز هویت کاربر، ابتدا توسط شخص ثالث و سپس توسط مالک داده احراز هویت دومرحله‌ای انجام می‌شود. مالک داده فهرستی از کاربران مجاز را همراه با شناسه ورود و رمز عبور به شخص ثالث می‌دهد. شخص ثالث یک پایگاه داده برای اعتبارسنجی کاربر می‌سازد. زمانی که کاربر با شناسه کاربری و رمز عبور وارد پایگاه داده می‌شود، شخص ثالث کاربر را با بررسی پایگاه داده خود تصدیق می‌کند. اگر کاربر مجاز باشد، شخص ثالث کلید محرمانه را بدون کد عبور، صادرکرده و مالک داده را نیز باخبر می‌سازد. از این به‌بعد، احراز هویت توسط مالک داده انجام می‌شود. مالک داده کاربری را که از کارت هوشمند مورد تأیید استفاده می‌کند، تصدیق کرده و شناسه ورود به ابر، رمز عبور و کد عبور کلید محرمانه را در یک قالب رمزنگاری‌شده به کاربر ارائه می‌دهد. داده رمزنگاری‌شده با استفاده از کارت هوشمند رمزگشایی می‌شود. کاربر، شناسه کاربری را به ابر می‌فرستد تا ارائه‌دهنده سرویس ابر به کاربر، اجازه ورود به ابر و دسترسی به داده را بدهد. اکنون کاربر وارد ابر شده و به داده دسترسی پیدا می‌کند. یک روش دسترسی مبتنی بر نقش وجود دارد که کاربر می‌تواند با نقشی که مالک داده برای او تعریف می‌کند اعمال حذف، به‌روزرسانی و خواندن را انجام دهد.

۴-۳- مدل امنیت داده کسب‌وکار

مدل های امن در رایانش ابری توسط ردما و همکارش مورد بررسی قرارگرفته و یک مدل جدید ارائه شده است [۱۴]. یک مدل ارائه شده امن، سرویس ذخیره‌سازی داده را از سرویس رمزنگاری و رمزگشایی جدا می‌کند سرویس ذخیره سازی توسط یک ارائه دهنده سرویس ابر و سرویس رمزنگاری و رمزگشایی توسط ارائه دهنده سرویس دیگر عرضه می‌شود. این جداسازی ضروری است؛ چراکه مدیران ارائه‌دهنده سرویس ابر ممکن است دسترسی غیرقانونی به داده کاربران داشته باشند. برای ممانعت از بروز چنین امری سرویس‌هایی مثل ذخیره‌سازی و رمزنگاری و رمزگشایی از یکدیگر جدا شده و به سرویس‌دهنده‌های ابر دیگر منتقل می‌شوند. درکل، کاربران از محیط ابر برای منظورهای خاصی استفاده می‌کنند. سرویس CRM[1] نمونه‌ای از این سرویس‌ها است. داده تولیدشده از این عملیات در ابر ذخیره می‌شود. با این حال، این مطالعه از سرویس دهنده های ابری که به فعالیت‌های رمزنگاری و رمزگشایی مستقل از سرویس ذخیره‌ساز توجه دارند، حمایت می‌کند. این مسئولیت تقسیم‌شده بین سرویس‌دهنده‌ها باعث تقسیم کار در عملکرد می‌شود که نتیجه آن امنیت بیشتر برای داده کاربر است.

سازوکار ذخیره‌سازی داده بدین‌گونه است که CRM کاربر، برای نمایش مدل کسب وکاری جدید مورد استفاده قرار می‌گیرد. طبق این مدل، کاربران با سرویس ابر CRM در تعامل هستند. سپس سرویس CRM با هر دو سرویس ذخیره‌ساز و هم‌چنین سرویس رمزنگاری و رمزگشایی ارتباط برقرار می‌کند و تعامل بین آن‌ها دوطرفه است. سرویس ذخیره‌ساز ابر و سرویس رمزنگاری و رمزگشایی و سرویس CRM بین خود ارتباطات دوطرفه دارند.

قبل از هر چیز، گواهی‌نامه‌های کاربران توسط سرویس ابر CRM احراز هویت می‌شود. با انجام احراز هویت، کاربر می‌تواند به سرویس‌دهنده CRM دسترسی پیدا کرده و از آن طریق، اعمال ذخیره و بازیابی داده را انجام دهد. با هر دستورالعمل، کاربر CRM با سرویس ذخیره‌ساز ابر ارتباط برقرار کرده و یک درخواست استفاده از داده ایجاد می‌کند. سپس سرویس ذخیره‌ساز ابر، درخواستی برای رمزگشایی داده به‌وسیله سرویس رمزنگاری و رمزگشایی می‌فرستد. سرویس رمزنگاری و رمزگشایی، داده رمزنگاری‌شده را گرفته و با رمزگشایی آن، داده رمزگشایی‌شده را به سرویس ابر CRM می‌فرستد. برای کارهای رمزنگاری و رمزگشایی از SSL[2] استفاده می‌شود. آخرین گام این است که سرویس ابر CRM داده درخواستی را به کاربر نهایی ارسال می‌کند. درنتیجه، ارتباط امن به‌عنوان قسمتی از سازوکار بازیابی داده در همه قسمت‌ها برقرار می‌شود. شکل (۴) عملیات بازیابی داده در این مدل را با جزئیات نمایش می‌دهد.



شکل ۴- سازوکار بازیابی داده در مدل کسب‌وکار [۱۴].

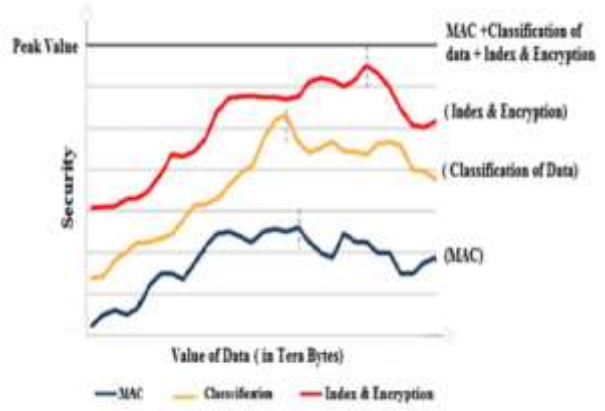
۵- ارزیابی مدل‌های ارائه‌شده

بررسی مدل پیشنهادی ترکیبی، برای امنیت همه داده‌ها در طول انتقال داده به ابر، بیانگر این است که این مدل برای مواجهه با اعمال

۱- Customer Relationship Management (CRM)

۲- Secure Sockets Layer (SSL)

امنیتی بسیار مؤثر مثل جلوگیری از افشای داده و ویرایش داده در سطح ابر که آسیب‌پذیر هستند، طراحی شده است. یک مدل امنیت داده ابر، باید قادر به انجام همه اعمال ممکن در رایانش ابری باشد. برخی از این اعمال اعم از احراز هویت، جامعیت، رمزنگاری داده، نمایه‌سازی داده و حفظ محرمانگی داده‌ها است. بررسی این مدل نشان می‌دهد که بیشتر نگرانی‌های امنیتی احتمالی با فراهم‌کردن برخی اعمال و فن‌هایی که مناسب با مسائل امنیتی رایانش ابری هستند، مرتفع می‌شود. این مدل روی شبیه‌ساز رایانش ابری، موسوم به شبیه‌ساز هدوپ آزموده شده است که نتیجه آن در شکل (۵) نمایش داده شده است.



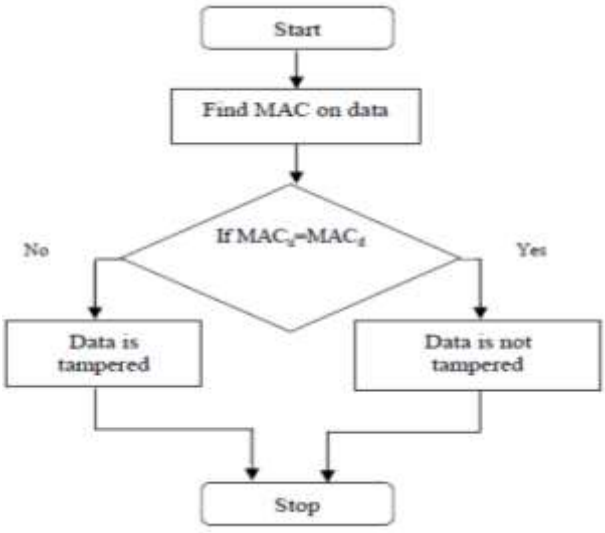
شکل ۵- ارزیابی امنیت مدل ترکیبی [۱۲].

بیشترین حالت امن برای داده‌ها، زمانی است که داده‌ها طبقه‌بندی، نمایه و رمزنگاری شوند و همراه با آن یک کد تصدیق پیام سمت ابر ارسال شود. مدل ترکیبی از یک روش رمزنگاری دومرحله‌ای که یکی توسط مالک داده و دیگری با استفاده از SSL صورت می‌گیرد، استفاده می‌کند. فرایند رمزنگاری وابسته به قدرت پردازش بوده و باعث می‌شود تا حدودی حمله نفوذگرها خنثی شود. این روش نه‌تنها باعث حفاظت داده در رسانه‌های ذخیره‌سازی می‌شود، بلکه به مشتریان این تضمین را می‌دهد که داده درحال انتقال نیز دارای امنیت است. گواهی SSL که ارتباطات خصوصی اینترنتی را رمزنگاری می‌کند، با استفاده از کلید عمومی امکان‌پذیر است. SSL دارای یک کلید عمومی و یک کلید خصوصی است که فقط با کلید مالک داده، قابل رمزگشایی است.

مدل پیشنهادی مبتنی بر سطح به‌گونه‌ای سازمان‌دهی شده است که امنیت داده را در رایانش ابری و در سطوح مختلف ارائه می‌دهد. این سطوح می‌تواند شامل سطح کاربر، ارائه‌دهنده سرویس ابر، شخص ثالث و سطح نفوذگر شبکه باشد؛ بنابراین داده در همه سطوح محافظت می‌شود. احراز هویت دومرحله‌ای کاربر، مبنی بر نقش صورت می‌گیرد؛ یعنی زمانی که کاربر نیاز به داده دارد، لازم است یک احراز هویت دومرحله‌ای توسط شخص ثالث و مالک داده صورت گیرد. وقتی کاربر توسط مالک داده و شخص ثالث، احراز هویت شد، می‌تواند به داده ابر دسترسی پیدا کند. همان‌طورکه گفته شد دسترسی به داده مبنی بر نقش است و کاربر مجاز پس از تعریف نقش از سوی مالک داده می‌تواند داده را خوانده، به‌روزرسانی و یا حذف نماید. بدین ترتیب داده در برابر دسترسی‌های غیرمجاز محافظت می‌شود.

در مدل مبتنی بر سطح، مفروض است که شخص ثالث چیزی در رابطه با ارائه‌دهنده سرویس ابر نمی‌داند. حتی اگر شخص ثالث چیزی در رابطه با ارائه‌دهنده سرویس ابر بداند، شناسه ورود و رمزعبور کاربر مجاز و هم‌چنین شخص ثالث نمی‌توان شناسه ورود و رمز ابر را به‌دست آورد. در این مدل، امنیت داده به‌طور مساوی بین شخص ثالث و مالک داده تقسیم می‌شود. درنتیجه سربار کمتری به مالک داده تحمیل می‌شود. دسترسی مبتنی بر نقش داده و احراز هویت دومرحله‌ای از طریق کارت هوشمند، دسترسی به داده را بسیار امن می‌کند. مدل مبتنی بر سطح، کیفیت داده‌ها را تضمین نموده و به کاربران این ضمانت را می‌دهد تا داده‌های خود را بدون تغییر و منحصربه‌فرد ذخیره و بازیابی نمایند.

برای بررسی جامعیت داده، MAC محاسبه شده و پس از رمزنگاری داده، دوباره MAC محاسبه و ضمیمه داده رمزنگاری شده می‌شود. سمت گیرنده، MAC محاسبه شده با MAC ضمیمه داده مقایسه می‌شود. اگر هردو باهم برابر باشند، بدین معنی است که داده دست‌کاری نشده است. درغیراین‌صورت داده دست‌کاری شده‌است. شکل (۶) نحوه بررسی جامعیت داده در مدل مبتنی بر سطح را نشان می‌دهد.



شکل ۶- بررسی جامعیت داده در مدل مبتنی بر سطح [۱۳].

مدل کسب‌وکار، یک سازوکار امنیتی جدید را برای حفاظت از داده کاربران ابر ارائه کرده است که شامل جداسازی سرویس ذخیره‌سازی و سرویس رمزنگاری و رمزگشایی به دو ارائه‌دهنده سرویس ابر متفاوت می‌شود. ذخیره‌سازی داده در سرویس‌دهنده ابر اتفاق می‌افتد درحالی‌که سازوکارهای امنیتی در یک سرویس‌دهنده ابر دیگر به‌کار گرفته می‌شود. این کار شفافیت را در ذخیره‌سازی و بازیابی تضمین می‌کند. زمانی که کاربر داده را به ارائه‌دهنده سرویس ابر ارسال می‌کند مجبور است آن را به شکل متن قابل مشاهده برای ارائه‌دهنده سرویس رمزنگاری و رمزگشایی بفرستد.

سپس ارائه‌دهنده سرویس رمزنگاری و رمزگشایی، داده را رمز نموده و آن را به ارائه‌دهنده سرویس دیگری که مسئول ذخیره‌سازی است، می‌فرستد؛ بنابراین ذخیره امن داده تضمین می‌شود. زمانی‌که کاربر می‌خواهد اطلاعات را از سرویس‌دهنده ابر بگیرد، یک درخواست ساخته شده و سرویس‌دهنده‌ای که داده را ذخیره کرده است، داده رمزنگاری‌شده را به سرویس‌دهنده ابری که مسئول رمزنگاری و رمزگشایی است ارسال می‌کند. سرویس‌دهنده داده را رمزگشایی نموده و درنهایت، متن قابل خواندن به‌طور امن برای کاربر ارسال می‌شود. در جدول (۱) مدل‌های ارائه شده ازنظر چندین معیار مقایسه شده‌اند.

جدول ۱- مقایسه مدل‌های امنیت داده در رایانش ابری

معیار/مدل	مدل ترکیبی	مدل مبتنی بر سطح	مدل کسب‌وکار
قابلیت اعتماد	دارد	دارد	دارد
جامعیت داده با MAC	دارد	دارد	ندارد
دسترسی بالا با نمایه‌سازی داده	دارد	ندارد	ندارد
طبقه‌بندی میزان حساسیت داده	سه نوع (C-I-A)	دو نوع (صفر و یک)	ندارد
کارایی	بالا	خوب	خوب
مدیریت کلید	مالک داده	شخص ثالث	سرویس ابر
رمزنگاری/رمزگشایی	رمزنگاری متقارن	کارت هوشمند (AES)	SSL
احراز هویت	دومرحله‌ای	دومرحله‌ای	تک مرحله
اعتبارسنجی	MAC	MAC	CRM
کاهش سرباری به دلیل جداسازی سرویس	ندارد	ندارد	دارد

۶- نتیجه‌گیری

رایانش ابری یک مدل محاسباتی است که اجازه دسترسی به نرم‌افزار، سکو، زیرساخت و سرویس‌های اینترنتی را فراهم می‌آورد. مشتریان این سرویس‌ها انتظار دارند داده‌هایشان امنیت داشته و دور از دسترس سایرین باشد. در این مقاله ضمن بررسی مدل‌های امنیت داده رایانش ابری، مقایسه‌ای بین مدل‌های ارائه شده انجام داده و آن‌ها را از دید تقسیم داده، کارایی، احراز هویت و مدیریت کلید، ارزیابی نمودیم. نتایج بررسی‌ها نشان می‌دهد در مدل پیشنهادی ترکیبی امنیت داده، طبقه‌بندی، نمایه‌سازی، رمزنگاری و ایجاد کد تصدیق برای داده‌ها، جامعیت و امنیت آن‌ها را بالا برده و منجر به کارایی و قابلیت اعتماد بیشتر آن‌ها در رایانش ابری خواهد بود. مدل مبتنی بر سطح نیز داده‌ها را از نظر سطح حساسیت به دو نوع صفر و یک تقسیم نموده و با اعتبارسنجی دومرحله‌ای امنیت داده‌ها را تأمین می‌نماید. مدل کسب‌وکار امنیتی نیز با جداسازی سرویس‌های ابر و سرویس رمزنگاری-رمزگشایی سربار پایین‌تری به سطح ابر تحمیل می‌نماید.

۷- منابع

1. F. Borivoje and A. Escalante, “Handbook of cloud computing,” vol. 3, New York: Springer, 2010.
2. M. Peter and T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology, Gaithersburg, 2011.
3. M. Dan, “Cloud computing: Theory and practice,” AMSTERDAM: Morgan Kaufmann, 2012.
4. F. Gen, “IT Cloud Services User Survey, pt.2: Top Benefits & Challenges,” 2011.
   [Online].Available:http://blogs.idc.com/ie/?p=210.
5. R. R. Velumadhava and K. Selvamani, “Data Security Challenges and Its Solutions in Cloud Computing,” International Conference on Computer, Communication and Convergence(ICCCN), pp. 204-209, 2015.
6. T. San and X. Wang, “Research of Data Security Model in Cloud Computing Platform for Smes,” International Journal of Security and Its Applications(IJSIA), vol. 7, no. 6, pp. 97-108, 2013.
7. L. Geng, D. Fu, J. Zho, and G. Dasmalchi, “Cloud computing: IT as a service,” IT professional Journal(IPJ), vol. 11, no. 2, pp. 10-13, 1 Mar 2009.
8. V. Chandu and P. Khobragade, “Data Security in Cloud Computing,” International Journal on Recent and Innovation Trends in Computing and Communication(IJRITCC), vol. 3, no. 5, pp. 167–170, 2015.
9. Z. Priscakova and I. Rabova, “Model of solutions for data security in Cloud Computing,” International Journal of Computer Science, Engineering and Information Technology(IJCSEIT), vol. 3, no. 1, pp. 11-23, 2013.
10. N. Mazher and I. Ashraf, “A Survey on data security models in cloud computing,” International Journal of Engineering Research and Applications(IJERA), vol. 3, no. 6, pp. 413-417, 2013.

11. S. Ramasami and P. Umamaheswari, “Survey on Data Security Issues and Data Security Models in Cloud Computing,” International Journal of Engineering and Innovative Technology (IJEIT), vol. 1, no. 3, pp. 56-60, 2012

12. S. Sood, “A combined approach to ensure data ecurity in cloud computing,” journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831–1838, 2012.

13. M. Sharma, “Level-Based Data Security Model in Cloud Computing,” International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 4, no. 2, pp. 68-71, 2014.

14. Y. Reddemma, L. Thirupathi, and S. Gunti, “Secure Model for Cloud Computing Based Storage and Retrieval,” IOSR Journal of Computer Engineering (IOSRJCE), vol. 6, no. 1, pp. 1-5, 2012.