بررسی امنیت داده ها در محاسبات ابری با استفاده از روش رمزنگاری بیضوی

مرضیه خاکزادی[*1]، فاطمه مهری[2]، محبوبه شمسی[3]، عبدالرضا رسولی کناری[3].

۱- دانشجوی کارشناسی ارشد، موسسه آموزش عالی تعالی، hkhakzadi@hotmail.com

۲- دانشجوی کارشناسی ارشد، موسسه آموزش عالی تعالی، Fatemeh.mehri68@gmail.com

۳- استادیار دانشکده برق و کامپیوتر دانشگاه صنعتی قم، shamsi@qut.ac.ir

۴- استادیار دانشکده برق و کامپیوتر دانشگاه صنعتی قم، rasouli@qut.ac.ir

چکیده

محاسبات ابری مجموعه ایی از منابع مجازی و مقیاس پذیر است که قابلیت ارائه خدمات مورد نیاز کاربران را با پرداخت بر اساس میزان استفاده آنها از سرویس را دارا می باشد. امروزه امنیت و حریم خصوصی ابر مسئله‌ی مهمی است. امنیت، حریم خصوصی و ذخیره‌ی ایمن داده دو مانع برای انتخاب محاسبات ابری از سوی سازمان‌ها و کاربران هستند. باید بر امنیت، حریم خصوصی و ثبات فناوری‌ها و محاسبات مبتنی بر ابر تاکید کرد تا موجب تحسین آن در بین محیط چند-مستاجره‌ی شرکتی شود.

در این مقاله، ابتدا به مفاهیم پایه‌ای ابر می‌پردازیم و به مدل‌های مختلف به کار رفته در آن نگاهی خواهیم داشت. اهمیت امنیت، حفظ حریم خصوصی و مسائل مربوط به اعتماد در محیط های محاسبات ابری را بیان می‌کنیم. در ادامه ساختار و سرویس‌های ابر را بیان کرده و راه‌حل های موجود جهت افزایش امنیت و استراتژی ها و مدل‌های امنیتی آن را به صورت مختصر شرح داده و مقایسه‌ای را بین روش‌های رمزنگاری مانند RSA و ECC انجام خواهیم داد. رمزنگاری خم بیضوی را به عنوان روشی مناسب جهت استفاده در محاسبات ابری برای بالا بردن امنیت داده‌ها در ابر بررسی خواهیم کرد، که ضمن فراهم آوردن سطح امنیتی یکسان در مقایسه با سایر روش ها، به دلایل پایه ریاضی قوی تر و در نتیجه استفاده از کلید کوچکتر، پیچیدگی زمانی به مراتب کمتر و کارایی بهتری برای اجرا دارند.

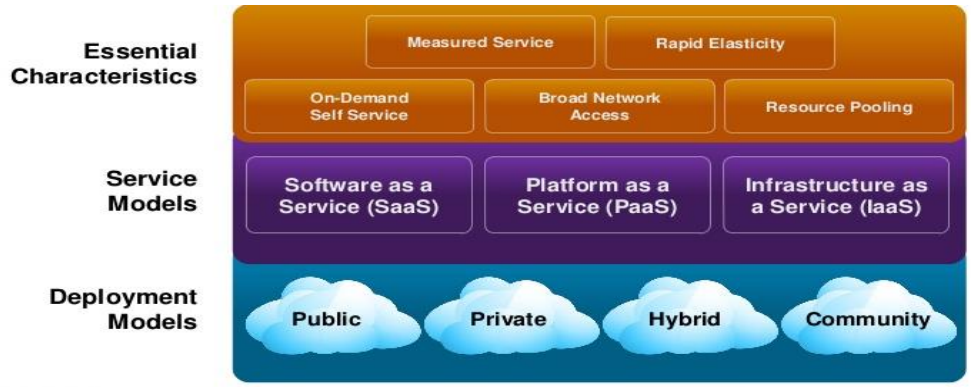
کلمات کلیدی: محاسبات ابری، امنیت، رمزنگاری، خم‌بیضوی، شبیه‌ساز ابر.

۱– مقدمه

موضوع محاسبات ابری در دهه گذشته انقلابی در صنعت فناوری اطلاعات ایجاد کرده است. این تکنولوژی جدید و رو به گسترش باعث افزایش کارایی، قابلیت دسترسی منابع و در عین حال کاهش هزینه های نگهداری و مدیریت آن ها می شود. در دنیای محاسبات ابری گذشته از مزایا و فوایدی که در استفاده از این سبک محاسباتی وجود دارد با چالش های پیچیده ایی نیز مواجه هستیم. مهم ترین چالش در این زمینه پر کردن شکاف امنیت، حریم خصوصی و کنترل دسترسی های غیر مجاز به داده های ذخیره شده در ابر می باشد[۱]. محاسبات ابری یک مدل برای ارائه خدمات فنآوری

اطلاعات است که منابع از اینترنت به وسیله‌ی ابزارها و برنامه‌های کاربردی مبتنی بر وب به جای اتصال مستقیم به یک سرور، دریافت می‌شوند. داده‌ها و بسته های نرم‌افزاری در سرور ذخیره می‌شود. با این حال ساختار محاسبات ابری اجازه دسترسی به اطلاعات را به همان اندازه که دستگاه های الکترونیکی اجازه دسترسی به اینترنت را دارند می‌دهد. محاسبات-ابری با چالش های امنیتی زیادی مواجه است.کاربران داده های خود را در ابر قرار می دهند و آن را از یک فضای ابری به یک فضای ابری دیگر انتقال می دهند، به خطر افتادن حریم خصوصی کاربران ناشی از آخرین مرحله کنترل داده می باشد. معمولا کاربران بیشتر نگران امنیت اطلاعات خود هستند، بنابراین امنیت مجازی و امنیت اطلاعاتی، مشکلات اصلی در امر حفاظت محاسبات ابری می باشد[۳]. یکی از استفاده های اولیه از محاسبات ابری، ذخیره سازی داده هاست، با ذخیره-سازی ابری، داده ها روی قسمت سوم سرور بجای سرور های اختصاصی روی شبکه های سنتی ذخیره می شود.

مفهوم محاسبات ابری برای چندین سال است که مطرح گردیده است با این حال هنوز تفاسیر مختلفی در رابطه با اینکه محاسبات ابری چیست وجود دارد. موسسه ملی استاندارد و فناوری (NIST) محاسبات ابری را به شرح زیر تعریف می-کند: "محاسبات ابری مدلی برای فعال سازی آسان و راحت دسترسی در شبکه مورد تقاضا به یک منبع مشترک از منابع محاسبات قابل پیکربندی (از جمله شبکه ها، سرورها، ذخیره سازی، برنامه های کاربردی و خدمات) است که این منابع به سرعت و با حداقل تلاش مدیریتی یا تراکنش ارائه دهنده سرویس نظارت و منتشر شود". تعریف NIST از محاسبات ابری شامل پنج خصیصه اصلی، سه مدل سرویس و چهار مدل گسترش است که در شکل ۱ نشان داده شده است. در اینجا پنج خصیصه اصلی شامل اشتراک منبع محاسبه مجازی، دسترسی شبکه گسترده، الاستیسیته سریع، خدمات بر حسب تقاضا، خدمات اندازه گیری شده و سه مدل سرویس عبارتند از زیر ساخت به عنوان یک سرویس(IaaS)، پایگاه به عنوان یک سرویس (PaaS) و نرم افزار به عنوان یک سرویس (SaaS) و نهایتا چهار مدل گسترش شامل ابر شخصی، ابر گروهی، ابر-عمومی و ابر ترکیبی می‌باشند[۵, ۶]. شکل ۱ مدل توصیفی NIST از محاسبات ابری است.

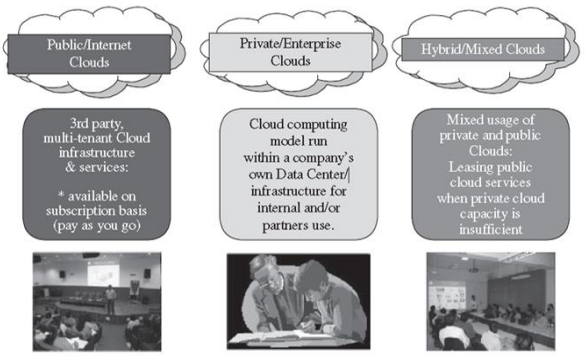


شکل ۱ – مدل توصیفی NIST از رایانش ابری[۵].

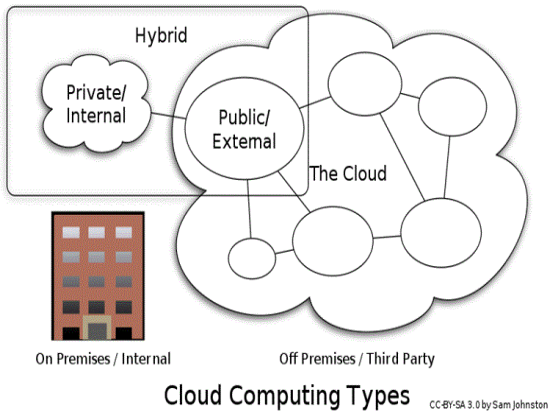
بررسی‌های اخیر نشان می‌دهد که امنیت داده ها و خطرات حفظ حریم خصوصی به دغدغه های اصلی مردم برای استفاده از محاسبات ابری تبدیل شده‌اند. رمزنگاری یکی از راهکارهای حفظ امنیت و حریم خصوصی در ابر می‌باشد. باتوجه به اینکه رمزنگاری باعث کاهش کارایی می‌شود بنابراین باید اطمینان حاصل شودکه رمزنگاری فقط بر روی داده هایی که نیاز

به محافظت دارند متمرکز شده است نه همه داده ها. برای حفظ امنیت داده ها می توان قبل از ارسال، آنها را با الگوریتم-های مختلف رمزنگاری کرد. ویژگی مهم یک الگوریتم رمز، پیچیدگی مناسب برای کاهش احتمال رمزگشایی توسط غیر است و در نتیجه ارتقاء سطح امنیت است. امنیت بالا در واقع برای مقاومت در برابر حملات ایجاد می شود. از اینرو الگوریتم های متفاوتی برای رمزنگاری مطرح می شود. یکی از مهمترین آنها سیستم رمزنگاری منحنی بیضوی با طول کلید ۱۶۰ بیت و سطح امنیتی بالاست[۷].

در این مقاله، در ابتدا به مفاهیم پایه‌ای ابر می پردازیم و به مدل‌های مختلف به کار رفته در آن نگاهی خواهیم داشت و رمزنگاری را در ابر بررسی می‌کنیم و برای بالا بردن استفاده از رمزنگاری در محاسبات ابری، روش رمزنگاری را انتخاب کرده ایم که علاوه بر حفظ امنیت بالا، دارای پیچیدگی و سربار کمتری باشد. بررسی ما بر روی رمزنگاری منحنی بیضوی شکل (ECC) است که برای تبادل کلید، رمزگذاری، رمزگشایی داده و تولید امضای دیجیتال استفاده می شود. استفاده کمتر از عملوند ها در ECC به نسبت RSA با همان میزان امنیت موجب کاربرد گسترده آن گشته است. شکل۲ انواع ابر و شکل۳ می‌تواند راه‌گشای درک ساختار ابر ترکیبی باشد.



شکل ۲- انواع ابر بر اساس گسترش مدل[۸].



شکل۳- انواع ابر[۸].

۲.امنیت ابر

امروزه امنیت و حریم خصوصی ابر مسئله‌ی مهمی است. امنیت، حریم خصوصی و ذخیره‌ی ایمن داده دو مانع برای انتخاب محاسبات ابری از سوی سازمان‌ها و کاربران هستند. باید بر امنیت، حریم خصوصی و ثبات فناوری ها و محاسبات مبتنی بر ابر تاکید کرد تا موجب تحسین آن در بین محیط چند مستاجره‌ی شرکتی شود. داده ها صرف نظر از اینکه در کجا ذخیره شده اند در برابر حملات آسیب پذیرند[۴, ۹]. امنیت داده نه تنها شامل رمزگذاری داده می‌شود، بلکه پیاده-سازی و اعمال سیاست های مناسب برای اشتراک داده ها و تایید اعتبار کاربری که باید به این داده ها در ابر دسترسی داشته باشد را نیز در برمی‌گیرد. این کار شامل برنامه‌ریزی برای تهیه پشتیبان از داده‌ها و ذخیره‌ی امن وسیله های پشتیبان نیز می‌شود. اما علاوه بر آن باید به مسائل عمده‌ای که وجود دارد نیز توجه کرد. برای رفع این مسائل باید مدلی امنیتی پدید آورد که CIA (محرمانه بودن، یکپارچگی، در دسترس بودن) را تضمین کند[۲]. همگام با افزایش تعداد

کاربران، با قابلیت ارائه شده از سوی سیستم‌های ابری، احتمال وقوع جرایم سایبری نیز افزایش می‌یابد. مسئله امنیت در محاسبات ابری یکی از مسائل پیچیده به شمار رفته که تمامی سه لایه ابر همچنین مسئولیت هایی که بین کاربران و ارائه دهندگان تقسیم می شود و نهایتا شخص ثالث را درگیر می کند[۱۰]. اگر تمام ارائه دهندگان ابر تدارک اقدامات امنیتی کافی را نبینند، آنگاه این ابرها به اهداف اصلی مجرمان سایبری بدل خواهند شد. از آنجایی که سیستم‌های ابری معماری موروثی دارند، موقعیتی برای حمله‌گر فراهم می‌آورد که با یک حمله خرابکارانه تعداد زیادی از سایت‌ها را تحت تاثیر قرار-دهد. (شکست در امنیت ابر می تواند نزاع میان ارائه دهنده سرویس و کاربران آن را به همراه داشته باشد. از طرفی از دیدگاه کاربر از دست رفتن اطلاعات یا قطعی در ارائه سرویس ها می تواند هزینه های مالی هنگفتی را در پی داشته-باشد). از طرفی از دیدگاه ارائه دهنده سرویس ارائه خدمات با کیفیت مختل شده و بدین ترتیب توافقات سطح سرویس (SLA) محقق نمی شود. مسائل اصلی امنیت محاسبات ابری در مدل‌های مختلف در شکل ۴ مورد مقایسه قرار می گیرند:

شکل ۴- مسائل امنیتی در معماری ابرهای مختلف(A. Kumar, 2012)

محاسبات، ارزیابی ریسک امنیتی را به طور عمده از نقطه فروشندگان در مورد توانایی های امنیتی مورد تجزیه تحلیل و ریسک امنیتی توسط ابر را گزارش می دهند. در جدول ۱ لیست خطرات امنیتی را شرح می دهیم:

جدول۱- آیتم‌های امنیتی در محاسبات ابری[۳]

آیتم امنیتی	شرح
دسترسی کاربر ممتاز	با توجه به نوع کاربر، مسائل مربوط به مالکیت داده‌ها را شامل می‌شود.
رعایت مقرارت	کاربران به انتخاب خود، یکی از ارائه دهندگانی را که سطوح امنیتی شان قبلاً مورد بررسی قرار گرفته است را انتخاب می کنند.
مکان داده	کاربران ازخدمات ارائه شده توسط ارائه دهندگان بدون آگاهی از مکان منابع استفاده می کنند.
تجزیه داده	ممکن است اطلاعات رمزنگاری شده چندین شرکت در یک فضا ذخیره شود، بنابراین باید مکانیزمی توسط ارائه دهندگان در نظر گرفته شود که بتواند، داده‌ها را جداسازی کند.
بازیابی	هر ارائه دهنده برای حفاظت از داده‌های کاربر، باید یک پروتکل بازیابی داشته باشد. یک ارائه دهنده ابر باید به شما بگوید که برای داده های شما چه اتفاقی خواهد افتاد و سرویسی که در مورد یک فاجعه پیش می آید.
پشتیبانی تحقیقی	اگر یک کاربر، فعالیت خطایی را از سوی ارائه دهنده تشخیص دهد، ممکن است راه های قانونی زیادی را برای انجام بازرسی برایش وجود نداشته باشد.

۳. تدابیر امنیتی پیشنهادی

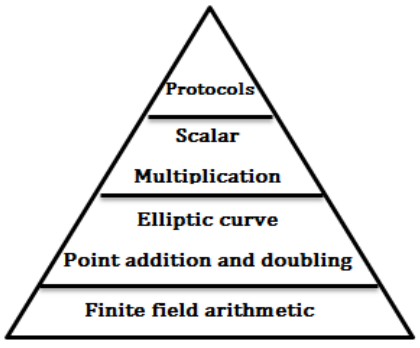
ارائه دهنده ابر برای کسب اطمینان از محرمانه بودن، سندیت، تمامیت و حصول پذیری داده، باید رمزگذاری ذیل را در برنامه خود بگنجاند:

- **رمزگذاری:** حساسیت داده می تواند رمزگذاری انبوه داده ای شبکه در ماشین مجازی را ایجاب کند، که این رمز گذاری با استفاده از نرم افزار سیستم عامل میزبان صورت می گیرد.
- **امنیت فیزیکی:** سیستم مجازی و میزبان های مدیریت ابری را امن و پشت درهای الکترونیک و ایمن از نظر محیطی نگهداری کنید.
- **کنترل دسترسی و دستیابی:** قابلیت های تصدیق در سیستم مجازی شما باید مطابق با شیوه ی سندیت دادن در سایر سیستم های فیزیکی باشد. کلمه عبور دفعه ای و بیومتریک ها، همه باید به شیوه یکسان به اجرا درآیند. تصدیق در زمان ارسال داده یا پیام از یک ابر به ابر دیگر الزامی است.
- **تفکیک وظایف:** هر چه سیستم پیچیده تر می شود، احتمال بروز پیکر بندی نادرست، به دلیل فقدان مهارت به همراه ارتباط ناکافی بیشتر می شود. اطمینان حاصل کنید که حداقل ایمنی و کمترین میزان کنترل دستیابی و جوابگویی را مورد نیاز باشد.
- **پیکره بندی، کنترل تغییر و مدیریت patch ها:** این امر، بسیار مهم است و گاهی اوقات در سازمان های کوچکتر نادیده گرفته می شود. پیکره بندی، کنترل تغییر، مدیریت patch ها و فرایند های به روز رسانی شده باید همانند دنیای مجازی، به عنوان دنیای فیزیکی نیز حفظ و نگهداری شوند.

- **تشخیص نفوذ و ممانعت از آن**: آنچه به شبکه شما وارد و از آن خارج می شود باید شناسایی شود. یک سیستم منع-نفوذ میزبان محور، به همراهی یک هاپیروایزر به عنوان راه حل، می تواند رفت و آمد های شبکه مجازی را مورد بررسی قرار دهد.

۴. سیستم رمز منحنی بیضوی

یکی از سیستم هایی که در سال های اخیر، برای انجام عملیات رمز نگاری مورد استفاده قرار گرفته، سیستم رمز-نگاری مبتنی بر خم بیضوی است. در سال ۱۹۸۵ نیل کبلیتز و ویکتور میلر[1] به طور مستقل استفاده از منحنی‌های بیضوی را به منظور طراحی سیستم های رمزنگاری کلید عمومی پیشنهاد دادند و در اواخر دهه۱۹۹۰، ECC توسط تعدادی سازمان به صورت استاندارد درآمد و شروع به دریافت پذیرش تجاری کرد[۳]. به تدریج سیستم‌های رمزنگاری کلید-عمومی، جای خود را به سیستم رمزنگاری خم بیضوی می‌دهند، چرا که قدرت محاسباتی تکامل می یابد، در حالی که اندازه کلید در سیستم های متداول جهت تامین این قدرت محاسباتی نیاز به افزایش طول کلید به طرز چشمگیری را دارند. اندازه منحنی بیضوی تعیین کننده سختی مسئله است و امنیت این مکانیزم رمزنگاری مبتنی بر دشواری حل مسئله لوگاریتم بر روی منحنی بیضوی استوار است. مزیت اصلی ECC، یک کلید با اندازه کوچکتر است که این موضوع به معنی کاهش ذخیره سازی و انتقال است. سیستم منحنی بیضوی می تواند همان سطح از امنیت را که یک سیستم مبتنی بر RSA با ماژول های بزرگ و طول بلند کلید فراهم می کند را ایجاد کند. بدیهی است با کاهش طول کلید، می توان سیستم های رمزنگاری کلید عمومی پر سرعت تر، کم حجم تر و دارای توان پردازشی بالاتر با صرفه جویی در منابع سخت افزاری طراحی نمود. سیستم‌های رمزنگاری را می‌توان در دو دسته تقسیم کرد: رمزنگاری کلیدخصوصی[2] و رمز-نگاری کلیدعمومی[3]. در رمز نگاری کلید خصوصی که به عنوان رمزنگاری متقارن[4] نیز شناخته می‌شود یک کلید برای رمزگذاری و رمزگشایی استفاده می‌شود. رمزنگاری منحنی بیضوی یک رمزنگاری کلید عمومی است[۱، ۳]. مشکل اصلی و متداول سیستم‌های رمزنگاری کلید عمومی، اندازه کلید است که باید به اندازه کافی بزرگ باشد تا به سطح بالایی از امنیت مورد نیاز ما برسد. در نتیجه سرعت پایین آمده و مصرف پهنای باند نیز بالا می‌رود که بدین منظور برای افزایش سرعت، سیستم رمز منحنی بیضوی سیستم مناسب تری است[۱]. ساختار کلی استفاده از رمزنگاری منحنی بیضوی در شکل ۵ نمایش داده شده است.



[1] V.S.Miller
[2] Secret key cryptography
[3] Public key cryptography
[4] Symmetric cryptography

شکل ۵- ساختار سیستم ECC(Verbauwhede, 2008)

روش‌های رمزگذاری و رمزگشایی ECC تنها می‌توانند نقطه‌ای روی خم ایجاد کند نه برای اینکه پیام ها را رمزگذاری یا رمزگشایی کنند. متاسفانه تاکنون الگوریتم زمانی چند جمله‌ای برای یافتن تعداد زیادی از نقاط در خم دلخواه به دست-نیامده است. در واقع در این کار به دنبال نقاط تصادفی روی E نبوده اند بلکه به دنبال راهی متقارن برای یافتن نقاط روی $E_p(a,b)$ بوده‌اند که به نحوی مرتبط با متن پیام باشد. بنابر این روش‌های کدینگ (پیام به یک نقطه) و دیکدینگ (یک نقطه به پیام) در طول رمزگذاری و رمزگشایی مهم هستند.

۵. مزیت ها و چالش ها امنیت محاسبات ابری :

سرویس های ابری چالش های بسیاری را برای یک سازمان به وجود می آورند. هنگامی که یک سازمان در مصرف سرویس های ابری و به خصوص سرویس های ابری عمومی افراط می کند، بخش اعظم زیر بنای سیستم رایانشی تحت-کنترل ارائه دهنده ی سرویس ابری قرار خواهد گرفت. بسیاری از این چالش ها را باید به وسیله ی نوآوری های مدیریتی مورد ملاحظه قرار داد. این نوآوری های مدیریتی قوانین مالکیتی و مسئولیتی را ایجاب خواهند کرد که باید هم برای ارائه دهنده ی سرویس ابری و هم برای سازمانی که نقش مشتری را دارد به روشنی توصیف شوند. مدیران امنیتی باید بتوانند موارد کنترل تشخیصی و پیشگیرانه ی موجود را بشناسند تا بدین وسیله وضعیت امنیتی سازمان را به درستی تعریف و مشخص کنند. با این وجود، نظارت های امنیتی مناسب باید بر مبنای سرمایه، خطر و ماتریس های ارزیابی ریسک آسیب پذیری به ~~اجرا درآیند. گزارش ارزیابی ریسک~~ امنیتی رایانش ابری، صرفا از منظر فروشنده و درباره ظرفیت های امنیتی و تحلیلی از ریسک های امنیتی است که ابر با آن مواجه می باشد. در جدول ۲ مزیت ها و ریسک های امنیتی را مشاهده می کنید.[2, 3]:

جدول۲- مزیت ها و چالش های محاسبات ابری

مزایا محاسبات ابری	چالش ها در محاسبات ابری
✓ **سهولت مدیریت:** هزینه های کامپیوتری کمتر، هزینه های نرم-افزاری کمتر، ارتقای نرم افزاری سریع و دائم و نیز زیر ساخت های عمومی برای حمایت ذخیره سازی توسط نرم افزار های کاربردی خیلی ساده است.	✓ **پشتیبانی** : تلاش برای کسب اطلاعات یا دست زدن به اقدام غیر قانونی و نامربوط در رایانش ابری غیر ممکن می باشد.
✓ **برنامه ریزی ساده:** راه حل های ذخیره سازی ابری مدیر فناوری اطلاعات را از جزئیات کل برنامه ریزی راحت می کند. این راه حل ها انعطاف پذیر هستند.	✓ **جداسازی و تفکیک داده** : داده در ابر، از فضای مشترکی در کنار داده های سایر مشتریان استفاده می کند.
✓ **آمادگی در مقابل بلایا:** پشتیبان گیری از داده های مهم. سرویس های ذخیره سازی ابری به تنهایی نمیتواند داده ها را	✓ **بازیابی :** حتی اگر ندانید داده شما کجاست، یک ارائه دهنده ی ابر باید به شما بگوید که در صورت بروز سانحه، چه اتفاقی برای

نگهداری کند اما آنها همیشه این افزونگی و بهبود فاجعه را تضمین می کنند.	داده و سرویس شما روی خواهد داد.
✓ فضای ذخیره سازی نامحدود برای ذخیره سازی داده های کاربر	✓ **محل داده** : هنگامی که از فضای ابری استفاده می کنید، احتمالا اطلاع دقیقی از محل میزبانی داده ندارید.
✓ مستقل از سخت افزار سازگاری بیشتر فرمت اسناد	✓ **چند اجاره ایی:** چالشی برای حفاظت داده های کاربران در برابر دسترسی غیر مجاز از فرایندهای اجراشده کاربران دیگر بر روی سرورهای فیزیکی مشابه می باشد.

۶. کارهای مربوطه

RSA اولین وکاربردی‌ترین روش رمزنگاری کلید عمومی است. این روش درسال ۱۹۷۷ ابداع و در سال ۱۹۷۸ توسط سه دانشمند به نام‌های ریوست[1]، شامیر[2] و ادلمن[3] به چاپ رسید. بهترین مقایسه امنیت ECC و RSA نتایجی است که توسط آقای کاترین طی سال ۲۰۱۰ در مقاله الگوی امنیتی RFID، برای طول کلید متفاوت آورده شده است. درطول سالهای گذشته محققان، سیستم های امنیتی متعددی را توسعه داده اند که این سیستم ها بر ویژگی های ماشین های مجازی برای فراهم کردن یک سطح امنیتی بالاتر تکیه کرده اند[۱۱]. در سال های اخیر به منظور ذخیره سازی و دسترسی امن به داده ها در ابر طرح های بسیاری ارائه شده است. درسال۱۹۷۸ لنسترا به قابلیت این شاخه از ریاضیات در تجزیه اعداد پی برد. سپس کوبلیتز و میلر، مستقلاً پروتکل‌های رمزنگاری که بر خم‌های بیضوی استوارشده‌اند را ارائه دادند. در بخش زیر، یک بازبینی مختصری بر روی بعضی از فعالیت های مرتبط با مدل های ذخیره سازی دادهای ابری، که تا-کنون صورت گرفته است، ارائه شده است.

- در مقاله [۱]، سه مدل ذخیره سازی دادهای ابری، پیشنهاد داده شد که در آن راه حل های رمزنگاری برای اطمینان کاربر علاوه بر ذخیره داده هایش در ابر، می تواند داده های کاربران را با تصدیق چندگانه با امنیت و وعده بهره وری به اشتراک گذارد. علاوه بر این ECC برای همه عملیاتهای رمزنگاری پیشنهاد شده که به دلیل فراهم کردن امنیت قابل-توجه و با طول کلید کوتاهتر نسبت به دیگر روش های رمزنگاری کلید عمومی، هزینه محاسبات و ارتباط کمتر، این طرح را کارامدتر می سازد.
- این مقاله[۲]، مدلی را توسط انجمن صنعت ذخیره سازی شبکه طراحی و توسعه داده است که انواع متعددی از رابط-های ذخیره داده ابری را نشان می دهد که هم توانایی پشتیبانی از اپلیکیشن های قدیمی را دارند و هم اپلیکشن های جدید را پشتیبانی می کند و تمام این رابط ها امکان ذخیره سازی و ارائه فضای ذخیره بر اساس تقاضا از میان انباری از منابع را فراهم می کنند و ظرفیت مورد نظر از بین انباری از ظرفیت های ذخیره شده توسط سرویس های ذخیره سازی

[1] Rivest
[2] Shamir
[3] Adleman

گرفته می شود ونیز سرویس های داده، بر اساس آنچه در فراداده ی سیستم داده ها مشخص شده است در مورد هر یک از عناصر داده به کار گرفته می شود.

- آقای گامپالا[1] سال ۲۰۱۲ در مقاله [۳] امنیت داده‌ها در محاسبات ابری با رمزنگاری منحنی بیضوی، امنیت داده‌ها در محاسبات ابری را با اجرای امضای دیجیتال و رمزنگاری منحنی‌بیضوی شرح داد تا از محرمانه بودن و صحت داده بین ابرها اطمینان حاصل شود، که البته به صورت موازی این روش رمزنگاری را به کار نبرده است.

- روش ارائه شده در[۴]، یک اثبات ذخیره سازی پروتکل اجرا شده بین کلاینت و سرور است که با کدام سرور می توان به کلاینت اثبات کرد و نیاز به دستکاری داده ها وجود ندارد. کلاینت با کدگذاری داده ها، قبل از ذخیره سازی انها در ابر آغاز می شود. یک اثبات قابل بازبینی خصوصی از ذخیره سازی تنها به کلاینت اجازه می دهد به منظور بررسی یکپارچگی داده ها، با یک اثبات قابل بازبینی عمومی برای ذخیره سازی اقدام نماید، از سوی دیگر هر کسی کلید-عمومی کلاینت را داشته باشد می تواند جامعیت داده ها را بررسی کند.

- مدل ارائه شده در[۱۲]، اجازه می دهد کاربر بصورت امن داده هایش را در ابر ذخیره کند و از طریق اینترنت به آنها دسترسی داشته باشد. در این مدل از رمزنگاری ECC برای رمزنگاری و رمزگشایی داده ها در ابر استفاده می شود و تنها کاربر داده هایش را با کاربران دیگر در گروه یکسان به اشتراک می گذارد.

- در این مقاله [۱۳]، این امکان وجود دارد تا مهاجم با یک IP جعلی و ساخت یک هویت جعلی خود را به عنوان یک آغازگر یا مخاطب قانونی جلوه دهد. در این مقاله رمزنگاری منحنی بیضوی در نسخه دوم IKE پیاده سازی میشود و برای کم کردن سربار حاصل از گواهی دیجیتال و نیز کاهش طول پیام ها، از هش موارد ارسالی به جای ارسال کامل اطلاعات استفاده می شود.

- سیستم پیشنهادی در مقاله[۱۴]، طرح یک سیستم ذخیره سازی ابری ایمن را تضمین می کند و همچنین رمز گذاری را با ارسال داده تلفیق می نماید. به موجب رمز گذاری و آشکار سازی با استفاده از کد تصحیح خطا، از اندازه کلید تا حد زیادی کاسته می شود و از این رو در پهنای باند شبکه صرفه جویی می شود. به عبارت دیگر، از آنجا که تبادل داده توسط افراد غیر مجاز، به وسیله موبایل به اطلاع مالکین داده می رسد، هشدار آنلاین موجب حفاظت اطلاعاتی بیشتر شده و از بروز تاخیر در انتقال بسته های اطلاعاتی می کاهد.

- در این مقاله[۱۵]، مشکل امنیت داده ها در ذخیره سازی ابری مورد بررسی قرار داده شده و یک طرح ذخیره سازی ابری ایمن که به کاربر نه تنها اجازه ذخیره سازی امن و دسترسی به داده ها در ابر را می دهد بلکه اجازه اشتراک گذاری داده-های کاربران با کاربران متعدد را نیز می دهد. روش ECC پیشنهاد شده بر اساس تابع گواهی PKI دارای محاسبات پایین-تر و هزینه های ارتباطی کمتر را فراهم می کند. در این روش سایز کلید کوچکتر همان سطح از امنیت RSA را ارائه می دهد.

- در این مقاله[16] ، ارسال داده ایمن در ذخیره سازی ابری با استفاده از روش پاک کردن کد انجام می شود که تبادلات فوق امنیتی را بدون نیاز به تایید طرف سوم امکان پذیر می کند. امنیت در ذخیره سازی ابری با به کارگیری کلید-خصوصی، کلید عمومی و با استفاده از تکنیک رمز گذاری مجدد قابل دستیابی می باشد. تایید و تصدیق به وسیله ی

[1] Gampala

طرف سوم منجر به نقض امنیت می شود. فرایند رمز گذاری مجدد در زمان ذخیره سازی اطلاعات در محیط ابری، امنیت را افزایش می دهد این مکانیسم های امنیتی سطح بالا، نقض امنیتی در هنگام ذخیره فایل ها در محیط ابری را کاهش می دهند و موجب تبادل فایل ایمن بین کاربران در محیط ابری می شود.

۷– بررسی امنیت سیستم ECC

هر الگوریتم بر اساس یک مساله سخت ریاضی بنا نهاده شده است. ثابت شده است که مساله لوگاریتم گسسته روی خم بیضوی (ECDLP) از هر دو مساله سخت دیگر یعنی تجزیه عدد صحیح (IFP) و لوگاریتم گسسته (DLP)، پیچیده-تر و دشوارتر است. این امر مهمترین دلیلی است که موجب شده روش‌هایECC از امنیت بالاتری نسبت به RSA برخوردار باشند. راه ساده برای شکستن رمزکلید عمومی به دست آوردن کلید خصوصی ازکلید عمومی است. اما این نیاز به محاسبات سنگین معادلی برای حل این مسائل سخت ریاضی می‌باشد. بهترین معیار برای مقایسه امنیت ECC و RSA نتایجی است که در جدول۳ برای امنیت ثابت و طول کلید متفاوت آورده شده است[۱۷].

جدول۳ - مقایسه ECC و RSA برای امنیت ثابت و طول کلید متفاوت

Time to break(In MIPS years)	RSA key size(in bits)	ECC key size(in bits)	RSA/ECC key size ratio
10^4	512	106	**5:1**
10^8	768	132	**6:1**
10^{11}	1024	160	**7:1**
10^{20}	2048	210	**10:1**
10^{78}	21000	600	**35:1**

الگوریتم ECC با کلیدی خیلی کوچکتر از کلید RSA، قادر به فراهم کردن امنیتی مشابه RSA می‌باشد. همان‌طور که مشخص است، عمل اصلی ECC ضرب نقطه KP می‌باشد. همان طور که دیدیم k عدد صحیح بوده و p نقطه‌ای روی منحنی بیضوی E می‌باشد. پردازنده‌های مؤثر برای اجرای ضرب نقطه منحنی بیضوی و محاسبات واحدی کلی (جمع‌ها و ضرب‌ها)، که نیاز به پروتکل‌های رمزنگاری دارند. بنابراین کاهش ضرب نقطه و محاسبات واحد تا حد ممکن ضروری می‌باشد.

۸- نتیجه

امروزه محاسبات ابری با چالش های امنیتی زیادی مواجه است. کاربران داده های خود را در ابر قرار می دهند و آن را از یک فضای ابری به یک ابر دیگر انتقال می دهند، به خطر افتادن حریم خصوصی کاربران ناشی از آخرین مرحله کنترل داده می باشد. معمولا کاربران بیشتر نگران امنیت اطلاعات خود هستند، بنابراین امنیت مجازی و امنیت اطلاعاتی مشکلات اصلی در امر حفاظت محاسبات ابری می باشد. در این مقاله، مسئله ی امنیت داده ها را به کمک رمز نگاری منحنی بیضوی مورد بررسی قرار دادیم تا از محرمانه بودن و صحت داده بین ابرها اطمینان حاصل شود. به طور کلی الگوریتم های مبتنی بر مساله لوگاریتم گسسته برای منحنی بیضوی ضمن فراهم آوردن سطح امنیتی یکسان در مقایسه با سایر روش ها، به دلایل پایه ریاضی قوی تر و در نتیجه استفاده از کلید کوچکتر، پیچیدگی زمانی به مراتب کمتر و کارایی بهتری برای اجرا دارند. در آینده بیشتر به مسائل امنیتی محاسبات ابری رسیدگی خواهیم کرد و سعی می کنیم تا با استفاده از رمز نگاری، راه حل های بهتری بیابیم. در جدول ۴ مقایسه ای بین روش های امنیت و ذخیره سازی در محیط ابری ارائه شده است.

جدول ۴- مقایسه ای بین روش های امنیت و ذخیره سازی در محیط ابری

عنوان	متد/الگوریتم	نتایج
Data Security In Cloud Computing With Elliptic Curve Cryptography	✓ امنیت داده ها جهت بهبود احراز هویت و اطمینان بین داد های ابر همراه با رمز نگاری منحنی بیضوی	✓ اطمینان از محرمانه بودن و صحت داده ها در ابر ✓ تصدیق و رمزگذاری به منظور انتقال داده ایمن از یک ابر به ابر دیگر

PKI-Based Cryptography for Secure Cloud DataStorage Using ECC	✓ راه حلی برای امنیت برون سپاری داده در ابر ارائه شد. ✓ الگوریتم رمزنگاری منحنی بیضوی	✓ کاهش اندازه کلید ✓ دسترسی امن کاربران به داده ها ✓ اشتراک گذاری امن داده ها ✓ ذخیره داده ها به طور امن ✓ محاسبات کم ✓ کاهش هزینه های ارتباطی
Security in Data Forwarding Through Elliptic Curve Cryptography in Cloud	✓ طراحی سیستم ذخیره سازی ابری ایمن ✓ رمزنگاری به روش ECC	✓ تضمین حجم وسیعی از داده ها ✓ استفاده از اطلاعات محرمانه گروه، اشتراک گذاری گروه را کارامدتر می سازد. ✓ استفاده از امضاء برای تصدیق هویت داده ✓ استفاده از درهم سازی برای تایید درستی داده ها ✓ داده در تمام طول چرخه حیات رمزگذاری شده است. ✓ تضمین امنیت حجم وسیعی از داده ها
An Efficient and Secured Data Storage Scheme in Cloud Using ECC-based PKI computing	✓ روش ECC بر اساس تابع گواهی PKI	✓ کااهش اندازه کلید ✓ صرفه جویی در پهنای باند ✓ حفاظت از اطلاعات بوسیله هشدار آنلاین ✓ کاهش بروز تاخیر در انتقال بسته ها ✓ هزینه محاسبات با توجه به زمانی که برای محاسبه الگوریتم های مختلف صرف شده است تعیین می شود. ✓ امنیت با دو مورد سر وکار دارد: امنیت سیستم ذخیره سازی ابری و امنیت پیام ارسال شده.
A Secure Data Forwarding In Cloud Storage	✓ الگوریتم RSA در این روش رمزگذاری ، به رمز دراوردن و ارسال را ادغام می کند. شامل چهار مرحله: راه اندازی سیستم، داده ذخیره-سازی، حمل داده ها و بازیابی داده ها.	✓ افزایش امنیت توسط فرآیند رمزگذاری مجدد در زمان ذخیره سازی اطلاعات در محیط ابر ✓ کاهش نقض امنیتی در هنگام ذخیره فایل ها در محیط ابر ✓ تبادل فایل ایمن بین کاربران در محیط ابر

منابع:

۱. Yin, X., et al. *PKI-based cryptography for secure cloud data storage using ECC*. in *Information and Communication Technology Convergence (ICTC), ۲۰۱٤ International Conference on*. ۲۰۱٤. IEEE.

۲. Wu, J., et al. *Cloud storage as the infrastructure of cloud computing*. in *Intelligent Computing and Cognitive Informatics (ICICCI), ۲۰۱۰International Conference on*. ۲۰۱۰. IEEE.

.٣ Gampala, V., S. Inuganti, and S. Muppidi, *Data security in cloud computing with elliptic curve cryptography*. International Journal of Soft Computing and Engineering (IJSCE), ٢٠١٢. ٢(٣): p. ١٤١.-١٣٨

.٤ Joshi, M. and Y.S. Moudgil, *Secure cloud storage.* International Journal of Computer Science & Communication Networks, ٢٠١١. ١(٢): p. ١٧٥.-١٧١

.٥ Atayero, A.A. and O. Feyisetan, *Security issues in cloud computing: The potentials of homomorphic encryption.* Journal of Emerging Trends in Computing and Information Sciences, ٢٠١١. ٢(١٠): p. ٥٥٢.-٥٤٦

.٦ Mell, P. and T. Grance, *Effectively and securely using the cloud computing paradigm.* NIST, Information Technology Laboratory, ٢٠٠٩: p. ٣١١.-٣٠٤

.٧ Dyka, Z. and P. Langendoerfer. *Area efficient hardware implementation of elliptic curve cryptography by iteratively applying Karatsuba's method*. in *Design, Automation and Test in Europe, ٢٠٠٥. Proceedings*. ٢٠٠٥. IEEE.

.٨ Buyya, R., J. Broberg, and A.M. Goscinski, *Cloud computing: principles and paradigms*. Vol. ٨٧. ٢٠١٠: John Wiley & Sons.

.٩ Kumar, A., *World of Cloud Computing & Security.* International Journal of Cloud Computing and Services Science (IJ-CLOSER), ٢٠١٢. ١(٢): p. ٥٨.-٥٣

.١٠ Sharma, S., S. Soni, and S. Sengar. *Security in cloud computing*. in *National Conference on Security Issues in Network Technologies*. ٢٠١٢.

.١١ Maiero, C. and M. Miculan. *Unobservable intrusion detection based on call traces in paravirtualized systems*. in *Security and Cryptography (SECRYPT), ٢٠١١ Proceedings of the International Conference on*. ٢٠١١. IEEE.

.١٢ Yin, X., N. Thiranant, and H. Lee, *Secured Data Storage Scheme in Cloud Computing using Elliptic Curve Cryptography*. ٢٠١٣, APICIST.

.١٣ Ray, S., R. Nandan, and G. Biswas, *ECC based IKE protocol design for internet applications.* Procedia Technology, ٢٠١٢. ٤: p. ٥٢٩.-٥٢٢

.١٤ Divya, S. and R. Shaji. *Security in data forwarding through elliptic curve cryptography in cloud*. in *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), ٢٠١٤International Conference on*. ٢٠١٤. IEEE.

.١٥ Yin, X.C., Z.G. Liu, and H.J. Lee. *An efficient and secured data storage scheme in cloud computing using ECC-based PKI*. in *Advanced Communication Technology (ICACT), ١٦ ٢٠١٤th International Conference on*. ٢٠١٤. IEEE.

.١٦ Prabha, K. and S. Nalini. *A secure data forwarding in cloud storage*. in *Optical Imaging Sensor and Security (ICOSS), ٢٠١٣International Conference on .٢٠١٣* . IEEE.

.١٧ Hankerson, D., A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography;* ٢٠٠٤. to. ١٠١: p. .٩٨