

## امنیت در محاسبات ابری سیار

محمد بخشنده باورساد<sup>۱</sup>

<sup>۱</sup> دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش نرم‌افزار موسسه آموزش عالی بهمنیار کرمان

نام و نشانی ایمیل نویسنده مسئول:

محمد بخشنده باورساد

[bav\\_1999@yahoo.com](mailto:bav_1999@yahoo.com)

### چکیده

محاسبات ابری سیار، شیوه‌ای برای ارائه منابع محاسباتی و سرویس‌ها از طریق اینترنت به کاربران گوشی‌های همراه است. از مزایای محاسبات ابری می‌توان به کاهش هزینه‌ها، نگهداری آسان، قابلیت دسترسی و تامین منابع اشاره کرد. افزایش تقاضای کاربران گوشی‌های همراه برای برنامه‌های کاربردی ابر منجر به افزایش نیاز به مکانیزم‌های امنیتی شده است. محرمانه بودن، یکپارچگی اطلاعات و احراز هویت از مسائل مهم مربوط به امنیت محاسبات ابری سیار می‌باشند. در این مقاله ابتدا چالش‌های مربوط به امنیت و حریم خصوصی در پردازش ابری سیار بررسی می‌شوند و در ادامه راه‌های مقابله با این چالش‌ها مرور می‌شوند.

**واژگان کلیدی:** محاسبات ابری سیار، امنیت، حریم خصوصی، تشخیص هویت

## مقدمه

در سال‌های اخیر محاسبات ابری به محبوب‌ترین تکنولوژی در میان سایر تکنولوژی‌ها تبدیل شده است. ابر گروهی از رایانه‌ها (اعم از رایانه‌های شخصی یا سرور) است که یک خوشه را تشکیل می‌دهند تا سرویسی را براساس تقاضای کاربر ارائه دهند [۱]. ایده اصلی محاسبات ابری بسیار این است که داده‌ها و برنامه‌ها می‌توانند به طور مرکزی در ابر ذخیره شوند و از هرجایی از طریق گوشی همراه قابل دسترسی باشند [۲]. یکی از ویژگی‌های مهم محاسبات ابری این است که کاربران ابر، تنها برای منابع اختصاص داده شده به آن‌ها، هزینه پرداخت می‌کنند<sup>۱</sup> و این امر باعث می‌شود محاسبات ابری موجب بهره‌وری هزینه و انعطاف پذیری بالا گردد [۳]. با استفاده از محاسبات ابری، کاربران اینترنت می‌توانند خدمات را از ابر درخواست کنند، همچنین می‌توانند داده‌ها را به جای ذخیره‌سازی در دستگاه‌های خود در ابر ذخیره کنند و به همین دلیل دسترسی به داده‌ها در همه جا امکان پذیر می‌باشد [۴]. موسسه ملی فناوری و استانداردها (NIST) محاسبات ابری را اینگونه تعریف می‌کند [۱]: محاسبات ابری مدلی است برای فراهم کردن دسترسی آسان براساس تقاضای کاربر از طریق شبکه به مجموعه‌ای از منابع محاسباتی قابل تغییر و پیکربندی (مثل شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) که این دسترسی بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم فراهم کننده سرویس به سرعت فراهم شده یا آزاد گردد. ابر سرویس‌های زیادی از جمله مقیاس پذیری، سرویس‌های مشورتی، سرویس مدیریت سرویس‌ها، سرویس مالی، سرویس ذخیره سازی داده، قابلیت اطمینان و قابلیت دسترسی به منابع را در اختیار کاربران قرار می‌دهد. در اصل کاربران به اندازه‌ی مصرف سرویس‌ها، پول پرداخت می‌کنند.

## ۲- مدل‌های گسترش یافته محاسبات ابری

- **ابر عمومی:** در این مدل که فراگیرترین مدل ارائه سرویس ابر است یک فراهم کننده، سرویس‌های نرم افزاری و یا سخت افزاری را برای استفاده عموم فراهم می‌کند مانند GOOGLE DRIVE.
- **ابر خصوصی:** یک فراهم کننده ابر است که در درون یک سازمان سرویس‌هایی را برای پرسنل درون سازمان و یا شرکای خود فراهم می‌کند.
- **ابر ترکیبی:** ترکیبی از ابر خصوصی و عمومی است و هنگامی استفاده می‌شود که ابر خصوصی کافی نیست.
- **ابر انجمنی:** این واژه برای سرویس ابر انجمن‌هایی مانند انجمن‌های آموزشی و انجمن‌های پزشکی مورد استفاده قرار می‌گیرد.

## ۳- سرویس محوری

- **زیر ساخت به عنوان سرویس (IAAS<sup>۲</sup>):** در این سرویس، ابر منابعی از قبیل حافظه، پردازنده و سایر منابع جانبی را از طریق شبکه در اختیار کاربران قرار می‌دهد.
- **سکو به عنوان سرویس (PAAS<sup>۴</sup>):** در این سرویس، ابر سکویی کامل از سخت افزار و نرم افزار در اختیار برنامه‌نویسان قرار می‌دهد.
- **نرم افزار به عنوان سرویس (SAAS<sup>۵</sup>):** در این سرویس نرم افزار به عنوان سرویس در اختیار کاربران قرار می‌گیرد. به عنوان مثال GOOGLE DOC نرم افزار پردازش کلمه را به شکل آنلاین در اختیار کاربران قرار می‌دهد.

در محاسبات ابری بسیار هم از مزایای بسیار بودن گوشی همراه و هم از کارایی و منابع غنی محاسبات ابری به طور همزمان استفاده می‌شود [۵]. در این زمینه بسیاری از محاسبات گوشی همراه به ابرها فرستاده می‌شوند و پس از انجام محاسبات نتایج به گوشی

<sup>1</sup> pay-as-you-go

<sup>2</sup> National Institute of Standards and Technology

<sup>3</sup> Infrastructure as a Service

<sup>4</sup> Platform as a Service

<sup>5</sup> Software as a Service

همراه فرستاده می‌شوند. بنابراین بسیاری از منابع گوشی همراه حفظ می‌شوند. این تکنیک تقسیم بار به عنوان Offloading شناخته می‌شود. توانایی‌ها و منابع گوشی همراه بسیار محدود هستند بنابراین با استفاده از منابع ابری می‌توانند قدرت محاسباتی خود را ارتقاء داده و در ضمن عمر باتری خود را نیز افزایش دهند. بدین ترتیب گوشی‌های همراه نیز می‌توانند برنامه‌های سنگین را اجرا کنند.

#### ۴- مزایای استفاده از محاسبات ابری سیار

- **قابلیت محاسباتی بالا:** امکان انجام محاسبات سنگین روی سرورهای راه دور باعث می‌شود تا گوشی‌های همراه بتوانند برنامه‌های سنگین‌تر از قدرت پردازش خود را اجرا نمایند.
- **افزایش عمر باتری:** برنامه‌های سنگین باتری را زیاد مصرف می‌کنند. با انجام محاسبات روی ابر گوشی‌های همراه می‌توانند شارژ باتری کمتری مصرف کنند.
- **ارتقاء ظرفیت حافظه:** سرورهای ابر می‌توانند حافظه‌ای را به گوشی‌های همراه اختصاص می‌دهند تا محدودیت فضای حافظه کم گوشی‌های همراه از بین برود.
- **افزایش قابلیت اطمینان:** داده‌ها در محاسبات ابری سیار گم نمی‌شوند چرا که روی کامپیوترهای متعددی قرار می‌گیرند بنابراین قابلیت اطمینان افزایش می‌یابد.

#### ۵- معماری سیستم محاسبات ابری سیار

محاسبات ابری سیار به چهار لایه تقسیم می‌شوند: لایه دسترسی، لایه مدیریت، لایه مجازی و لایه فیزیکی [۶]. در ادامه به توضیح هر چهار لایه خواهیم پرداخت.

- **لایه دسترسی:** این لایه واسطی است بین کاربر و ابر. این لایه از معماری نحوه ثبت نام و دسترسی به سرویس‌ها را برای کاربر شرح می‌دهد.
- **لایه مدیریت:** این لایه برای مدیریت سرویس‌ها مورد استفاده قرار می‌گیرد. بخش مدیریت کاربر، پیکربندی محیط، تعامل و سیستم پرداخت را مدیریت می‌کند. بخش مدیریت کارها، زمانبندی و اجرای کارها را بر عهده دارد. بخش مدیریت منابع، پخش بار، برطرف کردن خطاها و بازیابی اطلاعات را مدیریت می‌کند. بخش امنیت، احراز هویت، دسترسی به اطلاعات و حفاظت از اطلاعات را بر عهده دارد.
- **لایه مجازی:** لایه مجازی شامل منابع مختلفی از جمله منابع محاسباتی، منابع شبکه، منابع نرم‌افزاری و حافظه می‌باشد. این لایه محیط مجازی، سیستم مجازی و سکوی مجازی را تعریف می‌کند که در واقعیت وجود ندارند.
- **لایه فیزیکی:** وسایل جانبی مثل کامپیوتر شخصی، گوشی‌های همراه و وسایل مربوط به شبکه در این لایه قرار می‌گیرند. گوشی‌های همراه و تبلت‌ها نیازی به قدرت محاسباتی زیاد ندارند اما به منابع ورودی و خروجی نیاز دارند.

#### ۶- برنامه‌های کاربردی محاسبات ابری

برنامه‌های محاسبات ابری بسیار فراگیر شده‌اند و روز به روز بر این امر افزوده می‌شود. هر برنامه‌ای که بر روی سرور اجرا می‌شود و از طریق گوشی همراه استفاده می‌شود برنامه محاسبات ابری سیار محسوب می‌شود. برای مثال GOOGLE DRIVE که توسط گوگل ارائه شده است و سرویس SILK که توسط آمازون ارائه شده است همگی از برنامه‌های کاربردی محاسبات ابری محسوب می‌شوند. سایر برنامه‌ها بر اساس کاربردشان دسته‌بندی می‌شوند [۷]. این برنامه‌ها عبارتند از:

- **کسب و کار سیار:** هر نوع خرید و فروش سیار به عنوان کسب و کار سیار شناخته می‌شود. وقتی این امر توسط گوشی همراه انجام شود به دلیل ظرفیت محدود منابع این وسایل ممکن است مشکلات زیادی به وجود آید. برای غلبه بر این محدودیت می‌توان از منابع ابر برای این نوع کسب و کار استفاده کرد.
- **مراقبت‌های بهداشتی سیار:** در برنامه‌های درمان پزشکی محاسبات ابری سیار کاربرد دارند. ابر می‌تواند سرویس را بر اساس نیاز کاربر برای او تامین کند.
- **بانکداری سیار:** یک معامله می‌تواند از طریق پیامک و یا اینترنت گوشی همراه نیز انجام شود. بدین منظور باید برنامه مربوطه روی گوشی همراه فعال شود. امنیت و حریم خصوصی هم در سمت سرور و هم در سمت گوشی همراه باید به درستی انجام شود.

- **یادگیری سیار:** یادگیری سیار مبتنی بر ابر به خیلی از محدودیت‌های یادگیری سنتی غلبه کرده است. این امر با استفاده از منابع قدرتمند ابر مهیا شده است.

## ۷- امنیت در محاسبات ابری سیار

امنیت موضوعی مهم در محاسبات ابری سیار است. هم اکنون نگرانی‌های بسیاری درباره امنیت گوشی‌های همراه مطرح است و به طبع این نگرانی‌ها درباره برنامه‌های کاربردی سیار و همچنین محاسبات ابری سیار نیز وجود دارد [۸]. گوشی‌های همراه مانند گره‌ها در اینترنت عمل می‌کنند و در نتیجه در برابر انواع نفوذها و حمله‌ها بسیار آسیب پذیر هستند. مسائل امنیتی محاسبات ابری عبارتند از:

- **امنیت شبکه:** درگوشی‌های همراه تهدیدات بسیاری از طریق ارتباط با شبکه به وجود می‌آیند. بعضی از برنامه‌ها می‌توانند باعث به خطر افتادن حریم خصوصی کاربران شود. مشکلات امنیت شبکه همه موارد امنیتی درباره گوشی‌های همراه و اینترنت آن‌ها را در بر می‌گیرد. شبکه‌ها می‌توانند عمومی یا خصوصی باشند. شبکه‌های خصوصی که سازمان‌های شناخته شده آن را تامین می‌کنند از قابلیت اطمینان خوبی برخوردار هستند. اما زمانی که کاربران به شبکه‌های عمومی وصل می‌شوند، قابلیت اطمینان یک نگرانی بزرگ است. به عنوان مثال زمانی که مسافران از اینترنت بی‌سیم قطار استفاده می‌کنند در چنین مواردی دستگاه‌های همراه به خاطر شبکه‌ی غیرقابل اعتمادی که از آن استفاده می‌کنند بسیار آسیب پذیر هستند.
- **امنیت سطح کار بردی:** برنامه‌هایی که روی دستگاه‌های همراه نصب می‌شوند می‌توانند تهدیدی برای اطلاعات محرمانه کاربران باشند. برنامه‌های غیر قابل اعتمادی که روی گوشی همراه کاربران نصب می‌شوند می‌توانند باعث نشت اطلاعات از گوشی همراه شوند. برای حفظ اطلاعات محرمانه کاربران روی گوشی همراه در برابر این برنامه‌ها باید تدبیری جدی اندیشیده شود. کاربران نیز باید درباره نصب برنامه‌ها روی گوشی همراه مراقب باشند.
- **حریم خصوصی:** محافظت از داده‌ها در برابر دسترسی‌های فیزیکی غیر مجاز از اهمیت ویژه‌ای برخوردار است. حفاظت از اطلاعات حساس از طریق رمزگذاری باعث می‌شود تا اگر گوشی همراه گم شد اطلاعات برای دیگران قابل استفاده نباشد [۹].
- **امنیت ابر:** برای سازمان‌ها و شرکت‌های خصوصی که اطلاعات‌شان را به سرورهای ابر می‌سپارند امنیت از چند جهت مهم است: یکپارچگی، احراز هویت و مدیریت حقوق دیجیتال.
- ✓ **یکپارچگی:** هر نوع دسترسی کاربر به اطلاعات باید دارای تشخیص هویت باشد. روش‌های مختلفی برای حفظ یکپارچگی اطلاعات ذخیره شده وجود دارد که در مقاله‌ای جداگانه بررسی خواهند شد.
- ✓ **احراز هویت:** در محیط‌های سیار روش‌های متفاوتی برای احراز هویت وجود دارد. استفاده از شناسه کاربری و رمز عبور یکی از این روش‌هاست. سه مساله مهم در این بحث عبارتند از: احراز هویت، سطوح دسترسی و حسابرسی. احراز هویت مشروعیت کاربر را بررسی می‌کند. سطوح دسترسی مشخص می‌کند که کاربر به چه مجموعه‌ای از اطلاعات می‌تواند دسترسی داشته باشد. در این بین اگر چیزی اشتباه شد با حسابرسی می‌توان دلایل آن را فهمید که این امر قابلیت اطمینان را افزایش می‌دهد [۱۰].
- ✓ **مدیریت حقوق دیجیتال:** توزیع غیر قانونی محتوای دیجیتال مثل ویدئو، عکس، فایل صوتی و کتاب‌های الکترونیکی روز به روز رایج‌تر می‌شود. امضای دیجیتال و رمزگذاری روشی امن برای دسترسی به اطلاعات است.

## ۸- کارهای انجام شده

امنیت محاسبات ابری سیار در تحقیقات بسیاری مورد بحث قرار گرفته است. در [۱۱] فریم ورکی پیشنهاد شده است برای برنامه‌های گوشی همراه که همزمان از چند نقطه قابل دسترسی هستند. هر گره به محض وصل شدن به این برنامه بهنگام سازی می‌شود. [۱۲] فریم ورکی را معرفی می‌کند که بر اساس محل، سرویس‌ها را زمانبندی می‌کند. این فریم ورک از الگوریتم  $IJS^6$  استفاده می‌کند و از رمزگذاری برای تشخیص هویت کاربران بهره می‌برد. سیستم پیشنهادی [۱۳] از سه قسمت تشکیل شده است: کاربر گوشی همراه، فراهم کننده سرویس ابر و شرکت ثالث. شخص با گوشی همراه خود درخواستی را به سرور می‌فرستد و فراهم کننده سرویس ابر بر اساس

<sup>6</sup> IMSI-based Join Secure

درخواست، منابع مورد نیاز را تامین می‌کند. این روش بسیار مفید است اما محدودیت اصلی آن کمبود امنیت داده در ابر عمومی است. در [۱۴] روشی برای رمزنگاری داده‌ها در سرویس ابر پیشنهاد شده است که بار محاسباتی کمتری دارد و بسیار بهینه است. در [۱۵] فریم‌ورک پیشنهادی بر اساس داده‌هایی که در گذشته در ابر ذخیره شده‌اند می‌تواند تعداد زیادی کاربر آنلاین را پشتیبانی کند. این رویه سربرار ارتباط و پردازش را حداقل می‌کند. در [۱۶] سیستمی مجازی بر اساس IP برای گوشی‌های هوشمند پیشنهاد شده است که به کاربران کمک می‌کند تا از اطلاعات خود نسخه پشتیبان تهیه کنند. کاربران به سادگی می‌توانند این نرم‌افزار را نصب کنند.

#### ۹- نتیجه گیری

تعداد کاربران استفاده کننده از گوشی همراه در حال افزایش است و سناریوهای استفاده از آن نیز روز به روز در حال تغییر هستند. کاربران به سمت کسب و کار سیار سوق پیدا کرده‌اند بنابراین در گوشی‌های همراه اطلاعات حساسی وجود دارد. در نتیجه گوشی‌های همراه بسیار مورد توجه هکرها و نفوذگران قرار گرفته است. بنابراین امنیت در گوشی‌های همراه از اهمیت ویژه‌ای برخوردار است و ایجاد سیستم محاسبات ابری امن برای گوشی‌های همراه به امری جدی بدل شده است. هدف از محاسبات ابری سیار ارائه منابع به کاربران و بالا بردن کارایی گوشی‌های همراه آنان می‌باشد. در این مقاله، درباره مسائل مختلف محاسبات ابری سیار و تهدیدات آن بحث شد. نتایج مقالات دیگر در زمینه امنیت محاسبات ابری سیار بررسی و تهدیدات به دو دسته اصلی طبقه بندی شدند: تهدیدات سمت گوشی همراه و تهدیدات سمت ابر.

## منابع و مراجع

1. The NIST Definition of Cloud Computing, "*National Institute of Standard and Technology*".
  2. Ryan, M., "*Cloud computing security: The scientific challenge, and a survey of solutions*", The Journal of Systems and Software 86, 2263– 2268, 2013.
  3. Bashir Shaikh, F., Haider, S., "Security Threats in Cloud Computing", in 6th international conference internet technology and secured transition, 2011.
  4. Subashini, S., Kavitha, V., "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol. 34, pp. 1–11, 2011.
  5. Chen, Y.J. and Wang, L.C., "A security framework of group location-based mobile applications in cloud computing", International Conference on Parallel Processing Workshops, ICPPW '11 Taipei, Taiwan, 2011.
  6. Wang, S. and Wang, X., "*In-device spatial cloaking for mobile user privacy assisted by the cloud*", 11th International Conference on Mobile Data Management, MDM '10, Missouri, USA, 2010.
  7. Huang, D., Zhou, Z., Xu, L., Xing, T., Zhong, Y., "*Secure Data Processing Framework for Mobile Cloud Computing*", IEEE INFOCOM Workshop on Cloud Computing, 2011.
  8. Boldyreva, A. and Grubbs, P., "*Making encryption work in the cloud*", Network Security, pp. 8-10, 2014.
  9. Godarzi, K., karimi, A., " *Cloud Computing Security by Integrating Classical Encryption*", International Conference on Robot PRIDE, Procedia Computer Science, Vol. 42, pp. 320-326, 2014.
  10. Tebaa, M., Hajji, S.E., Ghazi, A.E., "*Homomorphic Encryption Applied to the Cloud Computing Security*", Proceedings of the World Congress on Engineering, 2012.
  11. Chun, B.G., Ihm, S., Manitis, P., Naik, M. and Patti, A., "*Clone Cloud : Elastic Execution between Mobile Device and Cloud*", Proceedings of 6th Conference On Computer Systems, pp. 301-314, 2011.
  12. Itani, W., Kayssi, A. and Chehab, A., "*Energy- Efficiency incremental integrity for securing storage in mobile cloud computing*", Proceeding International Conference on Energy Aware Computing, ICEAC '10, 2010.
  13. Ren, W., Yu, L., Gao, R. and Xiong, F., "*Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing*", Journal of Tsinghai Science and Technology, pp. 520–528, 2011.
  14. Jia, W., Zhu, H., Cao, Z., Wei, L., and Lin, X., "*SDSM: a Secure data service mechanism in mobile cloud Computing*", Proceeding IEEE Conference on Compute Communications Workshops, INFOCOM WKSHPS, Shanghai, China, 2011.
  15. Zonouz, S., Houmansadr, A., Barthier, R., Borisov, N. and Sanders, W., "*Seccloud: A cloud based comprehensive and lightweight security solution for smartphones*", Science Direct journal of Computers and security, Vol. 37, pp. 215-227, 2013.
- Eric Y. Chen Mistutaka Itoh, "*Virtual Smartphone over IP*", Copyright © IEEE , 2010