احراز هویت کاربر با استفاده از پروفایل در محاسبات ابری سیار

ولی الله وحیدی نژاد

دانشجوی کارشناسی ارشد مهندسی نرم افزار گرایش نرم افزار ، دانشگاه پیام نور واحد تهران ، ایران

vahidi.best90@yahoo.com

مریم اسکندر پور

فارغ التحصیل کارشناسی ارشد مهندسی فناوری اطلاعات گرایش سیستمهای چند رسانه ای ، دانشگاه پیام نور واحد عسلویه ، ایران

mohandes.eskandarpour@gmail.com

چکیده

همان طور که محاسبات ابری به گستردگی توسعه می یابند، کاربران و خدمات توسعه یافته نیز توانایی کاربرد منابع یا خدمات ارزان و ساده را بدون مالکیت همه ی منابع مورد نیاز خواهند داشت. هرچندکه، محاسبات ابری، تکنولوژی مجازی سازی، تکنولوژی پردازش توزیع گسترده، دسترسی به خدمات، پردازش با ترافیک بالا، به دلایل مختلف رخ خواهند داد. در سال های اخیر، بسیاری از این مشکلات در کاربرد ایمنی، کنترل در دسترس، احراز هویت، و رمز عبور و موارد بسیار دیگر، مورد تحقیق قرار گرفته اند. احراز هویت کاربری در محیط سیار، به ویژه اهمیت و ایمنی اعتبار آن، مورد نیاز می باشد. دراین تحقیق، محیط سیار برای سطح بالای ایمنی احراز هویت با کاربرد تکنیک پروفایل برای کنترل در دسترس و احراز هویت کاربری، پیشنهاد شده است.

کلید واژه ها: محاسبات ابری سیار، پروفایل، امنیت، کنترل دسترسی، احرازهویت کاربر

۱. مقدمه

بازار سیارات اخیرا" سرعت یافته است و محاسبات ابری در سیارات به خوبی توسعه یافته است. به عبارت دیگر، این بدین دلیل است که محاسبات ابری سیار، امروزه به موضوع جدیدی تبدیل شده است. محاسبات ابری، محاسبه ای ست که منابع مجازی IT را به عنوان خدماتی با کاربرد تکنولوژی اینترنت، توسعه می بخشد. در محاسبات ابری، کاربر به منابع IT مورد نیاز (نرم افزار، ذخیره سازی، سرور، شبکه) گرایش دارد، از آنها استفاده می کند، از مقیاس پذیری آنها در زمان حقیقی حمایت می کنند، و آنچه را که می خواهند پرداخت می کنند.

محاسبات ابری سیار، شانس تازه ای برای صنعت IT ایجاد کرده است، زیرا این محاسبات کاربرد بهتری دارند و از لحاظ اقتصادی اثر همکاری بیشتری را ترسیم می کنند. البته محاسبات ابری سیار به بنیانی ارجاع داده می شوند که درآن پردازش و ذخیره ی اطلاعات در خارج از ابزار سیار و با کاربرد محاسبات ابری و ملاحظه ی نوع ابزار سیار، انجام می شوند.

احراز هویت و ایمنی داده ها در تکنولوژی محاسبات ابری، دراین بخش بیان شده است. لیم این تکنولوژی را در ۸ رده، در مقاله ی خود توصیف کرده است، ترایان آندری نیز به ذکر موارد مشابه با اظهارات گارتنر، پرداخته است. بنابراین، همان طور که ایمنی داده ها فردی یا شرکتی ست، تکنولوژی احرازهویت می بایست به طور اساسی پیشنهاد شود. دسترسی به یک سیستم کلی-به ویژه در محاسبات ابری- هنگامی می تواند با خطا روبه رو شود که ایمنی حجم گسترده ای از داده ها، برای این موقعیت بکار رود. همچنین وقتی که در سرور کلید ذخیره، مواردی رخ دهد، این امر در دسترسی کاربر به داده، ممکن نمی باشد، بدین ترتیب باید بر کلید مدیریت تحقیقاتی انجام شود. این تحقیق بر خطای حامل و تکنولوژی های پوشش دهنده ی داده ها، وقتی اهمیت می یابد که واقعه ی در پیشگیری از قطع خدمات یا داده های از دست رفته، رخ داده باشد. مثال های قطع خدمات ابری واز دست دادن داده مشکلاتی هستند که هنگام عدم تناسب کار مکانیسم ها ایجاد می شوند. او همچنین راهنماهای ایمنی را در کاربرد محاسبات ابری بیان شده توسط گارتنر، توصیف می کند. آنها همچنین دسترسی کاربر، انطباق منظم، جایگاه داده، تفکیک داده، پوشش، حمایت از بررسی ها، و توانایی درازمدت، را امتیاز می بخشند.

بنابراین، تکنیک پروفایل، برای توسعه ی خدمات متناسب جهت اطلاعات پروفایل کاربری و شخصی در محیط سیار، مورد مطالعه قرار گرفته است. دراین سیستم، یک مدل معمولی برای اطلاعات پیشنهادی مورد نیاز توسعه یافته است. هرچندکه، برای این مدل ساختارهای تکنیکی وجود دارد، چراکه این مدل به خودی خود نمی تواند طبق منابع ابزار محدوده شده، برای برنامه های سیار بکار رود، بنابراین، این تحقیق با تکیه بر خدمات سیار در برنامه های سیار، هنوز هم کافی نمی باشد. مزیت اخیر مرتبط با ابر سیار، تلفن های شخصی هوشمند می باشند.

بنابراین، دراین تحقیق، پروفایلی براساس مدل برنامه ی ابری سیار طراحی شده است و ایمنی تضمین داده ها را از طریق احرازهویت کاربر توسعه می بخشد.

۲. کارهای مرتبط

هدف آگاهی از محاسبات ابری سیار که از محاسبات محیطی پیشین متفاوت می باشد، انسان نیست بلکه ابزار است. این بدان معناست که اطلاعات شخصی سازی می شوند. اطلاعات به صورت فعال جهت خدمات مختلف و آگاهی از روند و تفکرات بشری، توسعه می یابند. برای حل این مشکل در محاسبات ابری سیار، موقعیتی نشان داده شده است که توانایی درک رفتارهای بشری جمع آوری شده از حسگرهای مختلف را دارد. و این مورد، خدمات و اطلاعات را از طریق مفاهیم استنباط شده کاربری، توسعه می بخشد. به طور کلی، موقعیت به وجود آمده حول بشر، قابلیت جمع آوری از حسگرها را دارد، اما تمایلات و تفکرات بشری را به

همراه ندارد. بنابراین، آنها از روش ذخیره ی اطلاعات شخصی برای تحلیل تمایلات، مثل پروفایل شخصی، تاریخچه، خاطرات، بهره می برند. همان طور که در بالا ذکر شد، کاربر محاسبات ابری سیار، خدمات مختلف رابدون تشخیص بشری با ابزار سیار، در هر مکان و هر زمان، توسعه می بخشد. بنابراین، ما مفاهیم استنباط شده ای برای توسعه خدمات به کاربر داریم. پس، آنها بر تکنیک استنباط مفاهیم، جهت کاربرد تمایلات و اطلاعات شخصی، مطالعه می کنند. همان طور که این مورد تمایالات و اطلاعات شخصی را در استنباط مفاهیم درخواست می کند، کاربرد پروفایل کاربری برای ذخیره سازی، تحقیق بر تکنیک های پروفایل به صورت زیر بیان می شود.

پروژه ی UbiData، پردازش داده و هماهنگ سازی و بیان آنها را در سه چالش، با کاربرد یک احتکار پیشرفته و معماری شده، هماهنگ سازی، و الگوریتم های انتقال کد برای تداوم دسترسی به داده های مورد توجه کاربر سیار، توجه به ابزار سیار و کاربرد پردازش/مشاهده ی اطلاعات پیشنهاد می دهد. مانوئل کیرسچ-پینهریو، یک مفهوم مبتنی بر فرآیند فیلترینگ را با هدف تطبیق اطلاعات استنتاج شده برای کاربران سیار سیستم های وب راپیشنهاد می دهد. این فرآیند فیلترینگ پاسخی بر مدل مفاهیم است که ابعاد فیزیکی و سازمان یافته را ادغام می کند، و بازنمایی مفهوم جاری کاربری را همانند پروفایل های عمومی، دنبال می کند. این پروفایل ها مفاهیم پتانسیل کاربری و اصول فیلترینگ اطلاعات بیان شده را برای کاربرد در هنگام اتصال مفاهیم جاری کاربر به هرکدام از این قوانین، توصیف می کنند. با داشتن یک مفهوم، این قوانین ترجیحات کاربری را انعکاس می دهند. آنها چگونگی فرآیند فیلترینگ را در بخش توصیف می کنند، یکی برای تشخیص پروفایل کلی بکار رفته، و دوم برای انتخاب اطلاعات.

هرچندکه، این تکنیک های پروفایل برای محاسبات ابری سیار کافی نمی باشند. بنابراین، این تحقیق پروفایل مدیریت منابع بسیار موثر را با کاربرد اطلاعات شخصی پیشنهاد می دهد و اطلاعات را در برنامه ی سیار مدل یابی می کند.

۲.۱ تعریف محاسبه ی ابری و شکل ظاهری پیش زمینه

گارتنر محاسبات ابری را بدین صورت تعریف می کند؛ «الگویی از محاسبات که درآن قابلیت های مرتبط با مقیاس پذیری وکشسانی IT ، برای مشتریان خارجی کاربرد تکنولوژی های اینترنتی، به صورت یک خدمات توسعه می یابد.» محاسبات ابری نوعی روش محاسبات درخواست شده است که به کاربر اجازه می دهد از منابع IT ، همچون شبکه، سرور، ذخیره سازی، خدمات، برنامه های کاربردی، و غیره، از طریق اینترنت بهره ببرد. محاسبات ابری می توانند به صورت مجموعه ای از نرم افزارهای خدماتی و محاسبات سودمند مورد توجه قرار گیرند، شکل ۱ نقش کاربران یا توسعه دهندگان در محاسبات ابری را تحت مفهوم آن نشان می دهد. اولین مفهوم محاسبات ابری شکلی از آنچه که جان مک کارتی بیان می کند می باشد، او اظهار می دارد که محاسبات ممکن است به صورت یک مزیت عمومی سازمان یابند. اصطلاح «ابری» در دهه ی ۱۹۹۰، از ارتباطات از راه دور گرفته شده است، درآن هنگام،توسعه دهندگان کاربرد شبکه های مجازی خصوصی را برای ارتباط داده ها شروع کرده بودند. پس، محاسبات ابری به دلیل اینکه بنیان IT در شبکه های بی سیم/سیمی ارتباطی توسعه یافته است، سرعت بالایی دارد، مجموعه ای از بازار مختلف را دارا می باشد، از نرم افزارهای آزاد بهره می برد،و غیره، به سرعت توسعه می یابد.

۲.۲ تکنولوژی ایمن در محیط محاسبات ابری

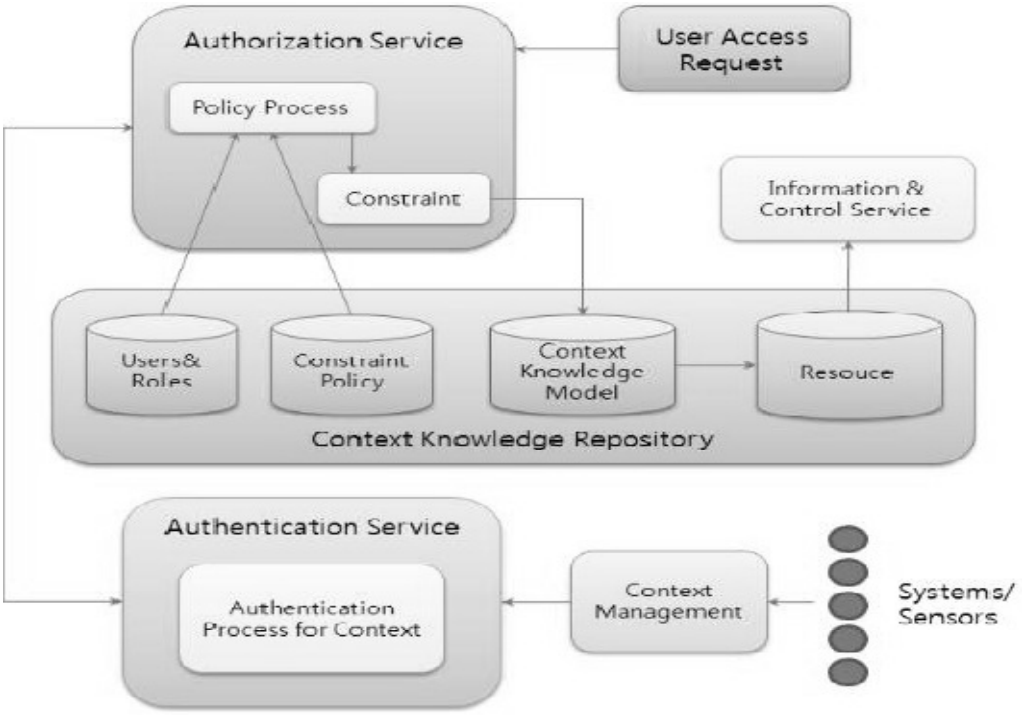
در محاسبات ابری هیچ نوع تکنولوژی ایمنی وجود ندارد، هرچندکه، اگر به محاسبات ابری به صورت تکنولوژی های IT توسعه یافته توجه کنیم، ممکن است برخی ازآنها را با هر جزء از محاسبات ابری و کاربرد آن، تقسیم کنیم. کنترل و احرازهویت کاربری، به صورت تکنولوژی ایمنی برای طرح ها بکار می روند. این تکنولوژی ها DAC، AMC، RBAC می باشند. DAC به کاربر کمک می کند که به احراز هویت منابعی که می خواهد، دسترسی یابد. AMC اصول عمودی/افقی دسترسی به سیستم استانداردو ایمن،

محدوده ی منابع، و کاربرد آنها را تثبیت می کند. RBAC دسترسی به احراز هویت را برای گروه های کاربری، براساس نقشی که در سازمان دهی ایفا می کنند، نشان می دهد. RBAC کاربرد گسترده ای دارد، زیرا برای سازمان های تجاری بسیار سودمند است. تکنولوژی های بکار رفته برای احراز هویت کاربری، رمزعبور/ID، بنیان کلید عمومی، احرازهویت چند فاکتوری، SSO، MTM، و i-Pin هستند.

۳. احراز هویت کاربر در محاسبات ابری

ارائه ی تکنولوژی های ایمنی احرازهویت کاربری که در بالا توصیف شدند، دارای برخی ضعف ها می باشند. این بخش به بیان این تکنولوژی ها و ضعف های آنها پرداخته است. رمزعبور/ID: روش ارائه ی احرازهویت کاربری ست. این روش بسیار ساده است و به آسانی به کار می رود، اما برای حفظ ایمنی، دارای عوارض است و تنظیمات آن باید تجدید شوند. PKI: احراز هویت به معنای کاربرد کلید عمومی رمزنگاری ست. این کلید توانایی احراز هویت بخش دیگر را براساس اعتبارو بدون به اشتراک گذاشتن رمز اطلاعات را دارد. در ساختار PKI ، مدیریت و بررسی فرآیند سفارش غیرممکن می باشد. چندفاکتور: روشی برای افزایش ایمنی با ترکیب چند احراز هویت. ID، رمز عبور، بیومتریک هایی چون اثر انگشت، اعتبار نامه، OTP، و غیره دراین مورد بکار می روند. اطلاعات OTP همانند رمزعبور/ID می تواند برای هجوم کننده کشف شود. SSO: نوعی گذرنامه است که اگر احرازهویت آن در سایت نشان داده شود، می تواند از طریق سایت های دیگر، بدون فرآیند احرازهویت عبور کند. استاندارد بیان شده در این مورد SAML می باشد. MTM: سخت افزار مبتنی بر مدل ایمنی: این سخت افزار استانداردی را با TCG پیشنهاد می دهد که در شرکت های نوکیا، سامسونگ، فرانس تلکام، اریکسون، و غیره وجود دارد. این سخت افزار برای پایانه ی احرازهویت از ارتباطات از را ه دور بکار می رود، هرچند که، به دلیل سازمان دهی تلفن های هوشمند، به عنوان یک روش احراز هویت محاسبات ابری با SIM مورد توجه می باشد. i-Pin: تکنیکی جهت کاربرد مشخصات کاربری ست، که در حال حاضر برای کاربران اینترنت کشور کره استفاده می شود. این تکنیک در روشی بکار می رود که سازمان ها خود مشخصات کاربر را اجرا می کنند. درمیان تکنولوژی های ایمنی ذکر شده در بالا، رمز عبور/ID و OTP ممکن است دارای یک کلید لوگ اتک، یا SSL باشند، و می توانند برای هجوم کننده کشف شود.

خدمات احرازهویت، برای خدماتی توسعه می یابد که درآن ID کاربری پس از احرازهویت از طریق اطلاعات مختلف در دسترس می باشد. خدمات احرازهویت نه تنها برای تجهیزات مرتبط با اطلاعات در دسترس کاربر انجام می شوند، بلکه بر اطلاعات همه ی ساختارها تصمیم گیری می کنند. مدل مفهوم دانش نقشه ای از دانش است که موقعیت همه ی منابع اطلاعاتی در دسترس را طبق نقش و مفهوم اطلاعات، توسعه می بخشد. این روش با منابع در دسترس در محیط پیرامون کاربر محدود می شود. شکل ۱ طرح سرویس احراز هویت را نشان می دهد.



شکل ۱. طرح سرویس احراز هویت

۴. ساختار پروفایل

یک پروفایل کاربری، اطلاعات سودمند برای یک کاربر را ویژگی می بخشد. بنابراین دراین مقاله، پروفایل شامل اطلاعات و خدمات کاربری می شود. اطلاعات کاربر، اطلاعاتی چون نام کاربر، تمایلات، علایق، و خدماتی را ذخیره می سازد که همانند نام خدمات،و توسعه دهنده ی خدمات و غیره، استفاده می شوند.

ساختار پروفایل کاربر به صورت زیر است:

-اطلاعات کاربر: نام کاربر، ID کاربر، تمایالات شخصی، علایق و غیره.

-اطلاعات خدمات: نام خدمات، توسعه دهنده ی خدمات، مفهوم خدمات، مقدار تکرار خدمات، و غیره.

به دلیل اینکه پروفایل چگونگی کاربرد اطلاعات خدمات را ذخیره می کند، ذخیره سازی نه تنها برای خدمات استفاده می شود، بلکه زمان، مکان وچگونگی کاربرد را نیز مشخص می کند. همچنین، اطلاعات باتوجه به مفهوم کاربرد ذخیره می شوند.

DTD پروفایلی که ما پیشنهاد داده ایم، به شرح زیر است:

```
<?xml version='1.0' encoding='UTF-8' ?>
<!ELEMENT ups_profiles (upsp)>
<!ELEMENT upsp(user_info, service_list?, device_info)>
<!ELEMENT user_info (username , password, hobby)>
<!ATTLIST user_info userID ID #REQUIRED >
<!ELEMENT username (firstname , lastname)>
<!ELEMENT firstname (#PCDATA)>
<!ELEMENT lastname (#PCDATA)>
<!ELEMENT password (#PCDATA)>
<!ELEMENT hobby (#PCDATA)>
<!ELEMENT service_list (service*)>
<!ELEMENT service (service_name, service_provider, service_time, service_frequency*) >
<!ELEMENT service_name(#PCDATA)>
<!ELEMENT service_provider(#PCDATA)>
<!ELEMENT service_time(#PCDATA)>
<!ELEMENT service_frequency(week_info, access_time, location)>
<!ATTLIST service_frequency value CDATA #REQUIRED >
<!ELEMENT week_info (#PCDATA)>
<!ELEMENT access_time (#PCDATA)>
<!ELEMENT location (#PCDATA)>
```

۵. جمع بندی

این مقاله درپی کنترل دسترسی و احرازهویت کاربری ست که هردو تکنولوژی های ایمنی بکار رفته در طرح محیط محاسبات ابری می باشند. در این محیط، در دسترسی به منابع احراز هویت و نقض اطلاعات شخصی سوء استفاده می شود، و می بایست برای احرازهویت یک کاربر ابری در مقایسه با مونو سیستم ها، سرعت وقدرت موثر تری داشته باشد. برای اثرپذیری احرازهویت کاربر در محیط محاسبات ابری، تکنولوژی های احرازهویت تعریف شده در بالا، با ترکیب مناسب آنها یا روش احرازهویت ایمنی کاربری استفاده می شوند. با تحقیقات بیشتر، مدل خدمات احرازهویت کاربر وپروتکل محاسبات ابری، می بایست طراحی و توسعه یابند.

منابع

[1] Gartner Says Cloud Computing Will Be As Influential As E-business, http://www.gartner.com/it/page.jsp?id=707508 (June, 2008)

[2] Lim, C.: Cloud Computing Security Technology. In Review of KIISC, V.19, n.3, pp. 14-17, ISSN:1598=3978 (2009)

[3] Andrei, T.: Cloud Computing Challenges and Related Security Issues, http://www.cs.wustl.edu/~jain/cse571-09/ftp/cloud.pdf (May, 2009)

[4] Gartner, Assessing the Security Risks of Cloud Computing, http://www.gartner.com/Display Document?id=685308 (June, 2008)

[5] M. Weiser. : Hot topics-ubiquitous computing, In: IEEE Computer, Vol. 26, No. 10(1993).

[6] Barkhuus, L., Dey, A. :Is Context-Aware Computing Taking Control away from the User Three Levels of Interactivity Examined. In: Proceedings of the 5th International Conference on Ubiquitous Computing (UbiComp'03)(2003).

[7] Elfeky, M.G., Aref, W.G., Elmagarmid, A.K. : Using Convolution to Mine Obscure Periodic Patterns in One Pass, In: Proceedings of the 9th International Conference on Extending Database Technology (EDBT)(2004).

[8] G. M. Sur, J. Hammer, : Management of user profile information in UbiData, In: Technical Report TR03-001, Dept. of CISE, University of Florida, Gainesville(2003).

[9] J. Zhang, A. S. Helal, J. Hammer. : Ubidata: Ubiquitous mobile file service, In: Eighteenth ACM Symposium on Applied Computing(2003)

[10] Manuele.Kirsch-Pinheiro, Marlene Villanova- Oliver, Jerome Gensel, Herve Martin, : Context-Aware Filtering for Collaborative Web Systems: Adapting the Awareness Information to the User's Context, In : ACM Symposium on Applied Computing(2005).

[11] Armbust, M., et al.: Above the Clouds: A Berkeley View of Cloud Computing. In: Technical Report. http://www.eeec.berkeley.edu/Pubs/TechRpts/2009/EEEC-2009-28.html (2009).

[12] Gartner Says Cloud Computing Will Be As Influential As E-business. http://www.gartner.com/it/page.jsp?id=707508 (2008).

[13] Kim, J., Kim, H.: Cloud Computing Industry Trend and Introduction Effect. In: IT Insight, National IT Industry promotion Agency (2010).

[14] http://en.wikipedia.org/wiki/Cloud_computing#History.

[15] Dikaiakos, M.D., et al.: Cloud Computing Distributed Internet Computing for IT and Scientific Research. In: IEEEInternet Computing, pp. 10-13, September/October (2009).

[16] Harauz, J., et al.: Data Security in the World of Cloud Computing. In: IEEE Security & Privacy, pp. 61-64 (2009).

[17] Lee, J.: Cloud Compting, Changes IT Industry Paradigm. In: LG Business Insight, pp. 40-46 (2009).

[18] Un, S., et al.: Cloud Computing Security Technology. In: ETRI, vol. 24, no. 4, pp. 79-88 (2009).

[19] TCG: http://www.trustedcomputinggroup.org.