3rd. International Conference on September 2017
Information Technology, Computer and Telecommunications
سومین کنفرانس بین المللی شهریورماه ۱۳۹۶
فناوری اطلاعات، مهندسی کامپیوتر و مخابرات

کنترل دسترسی در سیستم های توزیع شده با ارائه سیاست های مبتنی بر فاز دسترسی

فرهنگ پدیداران مقدم[۱]، معصومه ذبیحی[۲]، رسول عسکریان[۳]

عضو هیات علمی گروه کامپیوتر دانشگاه غیرانتفاعی اشراق بجنورد[۱]
دانشجوی کارشناسی ارشد کامپیوتر دانشگاه غیر انتفاعی اشراق بجنورد[۲]
دانشجوی کارشناسی ارشد مدیریت بازرگانی دانشگاه غیر انتفاعی حکیمان بجنورد[۳]

چکیده

کنترل دسترسی در سیستم های توزیع شده به دلیل مشارکت تعداد زیاد دستگاه ها و افراد از اهمیت زیادی برخوردار است و حفظ همخوانی و یکپارچگی داده ها و سطح مناسب دسترسی افراد به داده ها یک اصل مهم به شمار می آید. در این مقاله سیاست های کنترل دسترسی بر مبنای نوع سطح دسترسی کاربران و مجوز آن ها از بخش های مختلف، تعریف شده است که از روش های مختلفی در هر فاز استفاده می کند.

واژه های کلیدی: سطح دسترسی، سیستم های توزیع شده، حفاظت اطلاعات، همخوانی

۱- مقدمه

وقتی که درمورد کنترل دسترسی صحبت می شود، معمولا بین مدل ها و سیاست هایی که تصمیم می گیرند چه کسی باید یا نباید دسترسی داشته باشد و مکانیزم هایی که اجرا می شوند تمایز قائل می شویم.(Amoroso, 1994) در کنترل دسترسی سه نقش مهم را شناسایی می کنیم: ۱. منابع ۲. سرپرست ۳. کاربران

منابع: دارایی ارزشمندی که نیاز به محافظت دارد اگرچه تا زمانیکه یک دارایی اغلب یک شی فیزیکی و بی جان باشد، قادر نیست تا به عنوان یک واحد کنترل دسترسی عمل کند. همچنین ما اغلب از اصطلاح منبع زمانی استفاده میکنیم که به مکانیسم های کنترل دستیابی آن منبع اشاره کنیم. این مکانیسم ها قوانینی را ایجاد میکند، حق دستیابی هایی را اعطا و از افرار باز پس می گیرد. سرپرست: از اعضای تصمیم گیرنده که به منابع دسترسی دارد. کاربران: افرادی از قوانین را به منظور دسترسی به منابع به کار می گیرند.

۱-۲ مفاهیم اولیه کنترل دسترسی:

برای اینکه مکانیسم کنترل دسترسی به درستی عمل کند، تصمیمات مبنی بر دسترسی به منابع باید تنها از سوی سرپرست صادر شود.از سوی دیگر سایر احزاب مخرب می توانند تصمیمات کنترل دسترسی را صادر کنند و به شکل نادرستی به منابع دست یابند یا از دسترسی افراد دارای مجوز جلوگیری کند. همچنین، سرپرست به منظور مجوز دادن به کاربر، کاربر باید دارای مشخصه یا شناسه باشد که طبق قانون به او اختیاراتی اعطا می شود. بر اساس برنامه کاربردی، نیازی نیست که این شناسه در تمام دنیا منحصر به فرد باشد.برای اینکه هر کاربر تنها کسی باشد که از یک شناسه استفاده می کند، باید روش هایی وجود داشته باشد که به وسیله آن کاربر بتواند خود را کاربرمتناسب با قوانین معرفی کند. تفاوت قایل شدن میان شناسه (identify) و احراز هویت (authenticate.) مهم است. شناسه یعنی ما یک شخص یا گروه را شناسایی می کنیم ولی از روشی استفاده نمی کنیم تا مطمئن شویم آنها همان کسانی هستند که ادعا می کنند اما با احراز هویت ما نیازمند مدارکی برای شناسایی آنها هستیم(SANS Institute, 2013). اگرچه بیشتر سیستم های مرکزی می توانند تعداد کاربران زیادی داشته باشند، با این حال آنها اغلب تمایل دارند تا تعداد کمی منبع و سرپرست داشته باشند که به طور چشمگیر راه حل ها را ساده کند. اگر چه بیشتر سیستم های واقعی دنیا تعداد زیادی منبع و تعداد زیادی سرپرست دارند.

در رایانش ابری، محاسبات و شبکه کردن منابع میان چندین مستاجر و کاربری که از ماشین مجازی استفاده می کنند، به اشتراک گذاشته می شود. مستاجران باید از نظر امنیتی از یکدیگر مجزا باشند تا از دسترسی بدون مجوز به منابع و اطلاعات جلوگیری شود. فراهم کنندگان ابر، همانند مستاجران ابر ممکن است بخواهند با یکدیگر مشارکت کنندو زیرساخت ها و تجهیزات محاسباتی را با هم به اشتراک بگذارند.(Almutairi et al., 2012; Rujet al., 2011)امروزه سیستم های بسیاری هستند که با یکدیگر مشارکت دارند، و دسترسی هایی به سیستم های دیگر فراهم آوردند. به عنوان مثال ادوروم(Eduroam) یک شبکه دسترسی برای دانشجویان و کارمندان دانشگاه در سراسر دنیا

فراهم کرده است. این سیستم ها نیاز دارند تا مسایل کنترل دسترسی را حل کنند.(Lee and Luedemann, 2007; Kun et al., 2012؛ Alam et al., 2011; Gomi et al., 2005) شبکه های حسگر، معمولا شبکه های بدون ساختار و بی سیمی هستند که از ابزارهایی برای کنترل دنیای فیزیکی تشکیل شده اند. در بیشتر کاربردها، همانند بازیابی فاجعه و برنامه های کاربردی نظامی، حسگر ها ممکن است از سازمان های مختلف و یا بخش های مختلف یک سازمان آمده باشد که چندین کاربر دارند که نیازمند راه حل هایی برای کنترل دسترسی است.(He et al., 2011; Osmani and Slabbert2009; Maccari et al., 2008, شبکه های اجتماعی، گرافی شامل شناسه شبکه افراد به عنوان رئوس و رابطه ها به عنوان یال ها هستند. ثروتی از اطلاعات در مورد یک شخص و روابط او وجود دارد. سوال مهمی که وجود دارد اینست که چگونه یک شبکه اجتماعی ابزاری برای کنترل دسترسی این اطلاعات فراهم می کند؟!(Ahmad and Whitworth, et al., 2009، 2011; Carminati).

۲-۲ کنترل دسترسی در سیستم های توزیع شده

در شبکه ها، کنترل دسترسی توزیع شده می تواند به منظور حذف یک نقطه از خطا، افزایش مقیاس پذیری سیستم و توانمندی کنترل منترل دسترسی در محیطی که زوج ها ممکن است یکدیگر را نشناسند، استفاده شود.(Huai et al., 2005)

در سیستم های توزیع شده، تعداد زیادی از کاربران، سرپرستان و حتی منابع می توانند وجود داشته باشند و یک کاربر مجرد حتی می تواند تعداد بسیار زیادی دستگاه داشته باشد، که در این شرایط مشکلاتی می تواند رخ دهد که نیاز دارد برطرف شود:

۱) صدور قوانین: چگونه می توانیم سرپرستان را قادر سازیم تا به طور کارا قوانین مربوط به اطلاعات دریافتی منابع را صادر کنند؟
۲) هماهنگ سازی: با وجود تعداد زیاد شرکت کنندگان، چگونه کنترل دسترسی اطلاعات را هماهنگ شده حفظ کنیم ؟
۳) از دست دادن بعضی از دستگاه ها: چه اتفاقی می افتد اگر یکی از چندین دستگاه خراب یا گم شود؟
۴) قوانین باز پس گیری: چگونه مطمئن شویم که بازپس گیری یک قانون، به طور همزمان در همه منابع مربوطه اعمال می شود؟
۵) حملات DOS: چگونه می توانیم از حملات منع سرویس(DOS) و دیگر حملات جلوگیری کنیم؟
۶) کارایی: چگونه می توانیم مطمئن شویم که اطلاعات به بخش های مربوطه آن بدون ارسال سیل آسا اطلاعات غیر ضروری خواهد رسید؟
۷) حق امتیازها: چگونه می توانیم در شرایطی که منابع جایگزین زیادی وجود دارد، حق امتیاز صادر کنیم؟
۸) محرمانگی: چگونه می توانیم محرمانگی را با مسئولیت های لازم متعادل کنیم؟
۹) عدم انکار: چگونه می توانیم احزاب را به تراکنش هایی که بعدا نتوانند آنها را انکار کنند، ارتباط دهیم؟(Pesonen et al., 2006)

محدودیت های سیستم های توزیع شده

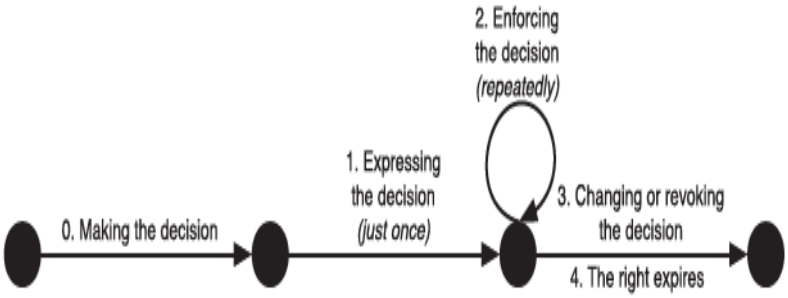
یکی از مهم ترین محدودیت های طراحی برای همه سیستم های توزیع شده، تئوری CAP است که بیان می کند، هر سیستمی می تواند حداکثر به دو مورد از این ویژگی ها دست یابد:

همخوانی (Consistency,)، دسترس پذیری (Availability) و تحمل پارتیشن(شبکه)(Partition Tolerance)((Brewer, 2000) .همخوانی (Consistency,): تمامی تصمیمات بر مبنای اطلاعات به روز شده است.. دسترس پذیری (Avilability): تصمیمات می توانند در هر زمانی انجام شوند.. تحمل پارتیشن(Partition Tolerance): راه حل ها بدون توجه به وضعیت شبکه، کار می کند. برمبنای این طبقه بندی، سه راه حل عمومی می توانیم ارایه دهیم:

CA : سازگار و دسترس پذیر، اما وضعیت شبکه قابل تحمل نیست.Cp : سازگار و شبکه تحمل پذیر، اما دسترس پذیری تضمین نمی شود. AP: دسترس پذیر و شبکه تحمل پذیر، اما سازگاری و همخوانی تضمین نمی شود. اگرچه در دنیای واقعی احتمال بروز همه باهم وجود ندارد و معمولا راحل ها AP و CP است.

۲-۳ فازهای کنترل دسترسی

می توان گفت ،فرآیند کنترل دسترسی شامل فازهای مختلف و مجزایی است که هر فاز اهداف خاص خود را دارد ولی بسیار وابسته به نوع فناوری هستند. (Kortesniemi, 2002). در شکل ۱ این فازها را می بینید.



شکل۱. فازهای کنترل دسترسی (Yki ,2014)

در فاز ۰، کسانی هستند که صاحب منابع اند یا اجازه دسترسی به آنها را دارند و اختیار صدور مجوز برای استفاده از منابع را با در نظر گرفتن محدودیت ها دارند. این تصمیمات می تواند بر مبنای شناختی که فرد مسئول از کاربر دارد هم باشد. این کاربر یا می تواند شخصی از سازمان یا استفاده کننده از خدمات باشد. این فاز می تواند با کاربر یا شخص مسئول آغاز شود.در فاز بعدی یعنی فاز ۱، سرپرست باید به گونه ای تصمیم گیری کند که بعدا بتواند مجوزهای کاربر برای استفاده از منابع را شناسایی کند.در فاز ۲، هر زمان که کاربر قصد استفاده از منابع را داشت، منابع باید اطمینان یابند که هنوز هم قوانین وجود دارند.در مقایسه با فاز۱، که فقط یک بار اتفاق می افتد، فاز ۲ می تواند چندین بار تکرار شود.بنابراین معمولا نیاز به طراحی راه حل کنترل دسترسی احساس می شود ، پس فاز۲ در صورت امکان به سادگی ارائه می شود.در فاز ۳ اگر تراکنش یا عملی از کاربر به مشکل خورد، سرپرست باید قادر به لغو و یا گرفتن حق امتیاز کاربر(مثلا در صورت گم کردن رمز) باشد. در فاز ۴ تمامی حق امتیازها بی اعتبار می شوند(در صورت اتمام کار کاربر).بنابراین در هر دو فاز ۳ و ۴، چرخه عمر کنترل دستیابی به پایان می رسد.(Yki ,2014)

۳- متدولوژی

هدف کلی فاز اول، شناسایی شخص یا ماشین و کنترل حق امتیازهای دسترسی آن است. در این فاز معمولا از روش های ساده ای مثل شناسه کاربری و کلمه و عبور استفاده می شود. اما این روش نمی تواند ادعای شخص را اثبات کند که چه کسی است. برای رفع ایم مشکل از روش های ارائه گواهی از موسسات معتبر با ارائه کلید خصوصی استفاده می شود. در این فاز می توان از یک کلید خصوصی ترکیبی استفاده کرد که به طور آنلاین توسط موسسات مجاز احراز هویت شود.

هدف فاز دوم، ارائه تصمیم بر مبنای فاز اول است. در این فاز هم معمولا برای بررسی صلاحیت افراد از گواهی نامه استفاده می کنند.اما معمولا چرخه دریافت این گواهی نامه هم مشکلاتی دارد که در تحقیقات بسیاری به ارایه الگوریتم هایی به منظور حل این مشکل پرداخته اند. لی (Li et al,2001) به مدسازی گواهینامه به صورت گراف محرمانه قابل جستجو پرداخته است. آقای (Schwoon et al,2003) از سیستم های خاموش وزن دهی شده به عنوان پایه ای برای الگوریتم گواهینامه ها پرداخته است. در این فاز پیشنهاد میشود تا کاربران بر اساس نوع مجوز دسترسی ها دسته بندی شوند و بر اساس سوابق صحت دسترسی، ضمن احراز هویت در مرحله اول اجازه دسترسی به اطلاعات طبقه بندی داده شود.

۴- نتیجه گیری

با مطالعه پژوهش های گذشته می توان دریافت که انتخاب یک روش مناسب برای کنترل دسترسی، خصوصا در سیستم های توزیع شده به شدت به نوع برنامه کاربردی بستگی دارد. نیاز برای کنترل دسترسی توزیعی، به راه حل های توانمندی نیاز دارد تا همه ابعاد احراز هویت، کنترل دسترسی، اعطا و بازپس گیری امتیاز رابررسی کند. بیشتر پژوهش ها از روش گواهی نامه برای احراز هویت کاربران استفاده کردند که در هر پژوهشی سعی شده محدودیت های این روش رفع گردد. در این مقاله سعی داریم تا با جدا کردن سطح کنترل دسترسی در هر فاز به ارائه راحل بپردازیم. در فاز اول با استفاده از گواهینامه الکترونیک آنلاین به احراز هویت پرداخته و در فاز بعد بر اساس دسته بندی های متناسب با سیاست هر محیط به دسترسی اطلاعات می پردازد.

۵- منابع

Amoroso E, Fundamentals of Computer Security Technology. Prentice Hall .1994.
Almutairi A, Sarfraz M, Basalamah S, Aref W, Ghafoor A, A distributed access control architecture for cloud computing. Softw IEEE;29(2):36-44. . 2012.

Abadi D. Problems with CAP, and Yahoo's little known NoSQLsystem.,http://dbmsmusings.blogspot.com/2010/04/problems-with-cap-and-yahoos-little.html; Apr. 2010.
Alam M, Zhang X, Khan K, Ali G. xDAuth: a scalable and Light weight framework for cross domain access control and delegation. In: Proceedings of the 16th ACM symposium on Access control models and technologies. pp. 31–40, 2011.

Brewer EA. Proceedings of the ACM Symposium on Principles of distributed computing, vol. 19. pp. 7–10. 2000.

Gomi H, Hatakeyama M, Hosono S, Fujita S, A delegation framework for federated identity management. In: Proceedings of the 2005 workshop on Digital identity management; pp. 94–103.2005.

He D, Bu J, Zhu S, Chan S, Chen C, Distributed access control with privacy support in wireless sensor networks. IEEE Trans Wirel Commun Sep;10(10):3472–81.2011.

Huai J, Zhang Y, Li X, Liu Y, Distributed access control in CROWN groups. In: Parallel Processing, 2005. ICPP 2005. International Conference on. pp. 435-42. 2005.
Maccari L, Mainardi L, Marchitti MA, Prasad NR, Fantacci R, Lightweight, distributed access control for wireless sensor networks supporting mobility. In: Communications. ICC'08. IEEE International Conference on; 2008. pp. 1441–5.2008.

Osmani F, Slabbert A, A scalable distributed security infrastructure for industrial control and sensor networks. In: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly. pp. 84–9. 2009.

Pesonen LIW, Eyers DM, Bacon J, A capability-based access control architecture for multi-domain publish/subscribe systems. In: Applications and the Internet, 2006. SAINT 2006. International Symposium on;. pp. 222–8. 2006.

Li N, Grosof BN, Feigenbaum J. Delegation logic: a logic-based approach to distribute authorization. ACM Trans Inf Syst Secur (TISSEC);6(1):128e71 .2003.
Ruj S, Nayak A, Stojmenovic I, DACC: Distributed Access Control in Clouds. In: Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on; pp. 91–8 .2011

SANS Institute, SANS: Glossary of Security Terms. 2013.
Schwoon S, Jha S, Reps T, Stubblebine S. On generalized authorization problems. In: Computer Security Foundations Workshop, 2003. Proceedings. 16th IEEE. pp. 202e16 . 2003.
Yki Kortesniemi*, Mikko Sa¨rela,2014, Survey of certificate usage in distributed access control, compute r s & s e c u r i t y 4 4 , 1 6 -3 2, 2014.

Access control in distributed systems by providing a phase-based policy

Farhang Padidaran Moghaddam[1], Masoumeh Zabihi[2], Rasool Askaryan[3]
Faculity member of Eshraq University, Bojnourd, Email: padidaran@eshragh.ac.ir
[2]Msc student of computer, Eshraq University, Bojnourd, Email: m.zabihi1394@gmail.com
[3]Msc student of commercial management, hakiman University, Bojnourd, Email: r.askaryan1394@gmail.com

Abstract. Access control in distributed systems is important because of the large number of devices and people involved and maintaining the consistency and integrity of the data and the level of access for individuals to data is an important principle. In this article, access control policies are defined based on the type of user access level and their permissions from different sectors, which uses different methods in each phase.

Keywords: access level, distributed systems, information conservation, consistency