ارزیابی سیاست های امنیتی XACML با استفاده از معیارهای شباهت

زهرا کاتبی*، دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، گروه مهندسی کامپیوتر، دانشکده مهندسی، دانشگاه بوعلی سینا، همدان

z.katebi@eng.basu.ac.ir

استاد راهنما : محمد نصیری، استادیارگروه مهندسی کامپیوتر، دانشکده مهندسی، دانشگاه بوعلی سینا

استاد مشاور : محسن رضوانی، استادیارگروه مهندسی کامپیوتر، دانشگاه صنعتی شاهرود

پاییز ۱۳۹۷

چکیده

کنترل دسترسی یکی از جنبه‌های مهم امنیت برنامه‌های کاربردی به ویژه در محیط‌های ابری است که اشتراک‌گذاری و حفاظت از منابع را برای شرکت‌ها وسازمان‌ها تسهیل می‌نماید. در همین راستا، استاندارد XACMLقواعد کنترل دسترسی را مبتنی بر ویژگی تعریف می‌کند. از طرفی ارزیابی میزان شباهت سیاست‌های امنیتی حائز اهمیت است. پیدا کردن یک ارائه-دهنده خدمات ابری که به نگرانی‌های امنیتی یک کاربر پاسخ دهد و یا یافتن همکارانی که دارای پیکربندی امنیتی مشابه هستند، از جمله مواردی است که اهمیت معیار شباهت بین دو سیاست امنیتی را نشان می‌دهد. در این نوشتار مکانیسمی سلسله مراتبی برای محاسبه میزان شباهت خط‌مشی‌های امنیتی بر اساس نسخه ۳ این استاندارد ارائه می‌شود. در معیار ارائه شده، شباهت برای مقادیر اسمی و عددی و مبتنی بر فاصله محاسبه می‌شود. در این معیار مقدار فاصله به صورت سلسله مراتبی در چهار سطح مقدار، ویژگی، قانون،سیاست محاسبه میشود. برای ارزیابی روش پیشنهادی، یک ابزار در محیط جاوا پیاده‌سازی کرده‌ایم. نتایج ارزیابی بر روی خط‌مشی‌های واقعی نشان دهنده ارتباط قوی بین تغییرات آنتروپی ویژگی‌ها با درجه شباهت ویژگی‌ها و نمایانگر ارتباط معکوس بین فاصله وشباهت می‌باشد.

واژه‌های کلیدی: کنترل دسترسی، XACML، درجه شباهت، توزیع ویژگی‌ها، Context، مقایسه خط‌مشی‌ها

۱. مقدمه

تامین امنیت کافی برای داده‌ها و سیستم‌های اطلاعاتی یک نیاز ضروری است. برای محافظت از داده‌های امنیتی، کنترل دسترسی یک مولفه کلیدی به شمار می‌رود. برای ارزیابی کارایی و عملکرد برنامه‌های‌کاربردی تحت‌وب می‌توان از XACML برای کنترل‌دسترسی به منابع استفاده نمود، که مبتنی بر یک مدل کنترل‌دسترسی ABAC می‌باشد و برپایه XMLاست و می‌تواند برای تعیین سیاست‌های کنترل دسترسی مورد استفاده قرار بگیرد[۱-۲]. در این نوشتار یک رویکرد نوین مبتنی بر فاصله برای ارزیابی شباهت بین سیاست‌های تعریف شده در XACML 3.0ارائه نموده‌ایم در این روش شباهت برای دو نوع از مقادیر بررسی می‌شود: مقادیراسمی، مقادیرعددی. برای محاسبه شباهت درهر نوع از مقادیر، متدولوژی متفاوتی در نظرگرفته شده است. معیار شباهت ارائه شده برای مقادیر اسمی از متدولوژیDILCA [۴]و برای مقادیر عددی از مفهوم فاصله و اشتراک استفاده می‌کند. با اعمال قابلیت مکانیسم‌های مذکور به استاندارد XACMLمیتوان یک ارزیابی‌کننده شباهت را طراحی کرد. به کمک این ارزیابی کننده، میتوان دیدگاه‌های مختلف را که تنها قابل تشخیص برای انسان هستند را در نظر گرفت. همچنین با کمک یک مکانیسم پایین به بالا که برگرفته از ساختار و معنای سلسله مراتبی سیاست‌ها در XACML 3.0 است، شباهت بین مولفه های یک سیاست، و در نهایت میتوان شباهت بین هر دو سیاست را محاسبه نمود.

۲. کارهای مرتبط

ویدیا و همکاران در [۲] روشی را برای محاسبه شباهت سیاست های امنیتی XACMLنسخه دوم ارائه می‌دهد. این مقاله به پیدا کردن یک سیاست سازمانی مشترک با کمترین هزینه می پردازد که در آن فاصله دو سیاست به عنوان هزینه انتقال یا جایگزینی از یک سیاست به دیگری می‌باشد. این معیار درجهت ادغام ویکپارچه سازی سیاست های سازمانی ارائه شده است.

لین و همکاران در [۳] روشی برای محاسبه درجه شباهت مجموعه خط‌مشی‌های XACML نسخه دوم ارائه کرده است که درآن هر سیاست به مجموعه قوانین permit و مجموعه قوانین deny تقسیم میشوند و درجه شباهت در هر گروه جداگانه محاسبه می گردد. این معیار شباهت را برای مقادیر اسمی از طریق رابطه درختی بین مقادیر محاسبه می‌کند .

یانهونگ و همکاران در [۵]یک معیار برای اندازه‌گیری شباهت بین دو سیاست امنیتی را بیان می‌کند و هر سیاست را به دو گروه از قوانین طبقه بندی میکند. شباهت در هر گروه به صورت سلسله‌مراتبی و مجزا محاسبه می‌شود. این معیار انتخاب سریع سرویس دهندگان تحت وب را برای کاربر امکان پذیر می‌سازد.

۳. تحلیل و ارزیابی

مقایسه سیاست‌ها: شباهت بین دو سیاست از مقایسه اجزای سلسه مراتبی سیاست‌ها بدست می آید.

شباهت مقادیر اسمی :

$$s(v_i, v_j) = \frac{1}{distance(v_i, v_j) + 1}$$

$$d(x_i, x_j) = \sqrt{\sum_{Y \in context(X)} \sum_{y_k \in Y} ((P(x_i|y_k) - P(x_j|y_k)) * 2)^2}$$

شباهت مقادیر عددی :

$$S_{(v_i,v_j)} = e^{-d} \qquad d_{(v_i,v_j)} = \frac{1}{g} \qquad g = \frac{|v_{si} - v_{ej}|}{|v_{si} + v_{ej}| - |v_{si} - v_{ej}|}$$

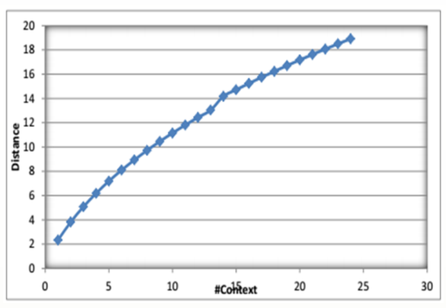
شباهت دو گروه از مجموعه قوانین:حاصل مجموع ماکزیمم شباهت هر قانون در پالیسی اول با قانون دیگر در سیاست دوم می‌باشد.

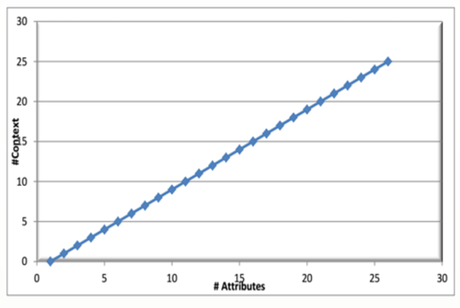
$$S^P_{rule-set} = \frac{\sum_{i=1}^{N_{PR_1}} S\_\max(r_i) + \sum_{j=1}^{N_{PR_2}} S\_\max(r_j)}{N_{PR1} + N_{PR2}}$$

$$S^D_{rule-set} = \frac{\sum_{i=1}^{N_{DR_1}} S\_\max(r_i) + \sum_{j=1}^{N_{DR_2}} S\_\max(r_j)}{N_{DR_1} + N_{DR_2}}$$

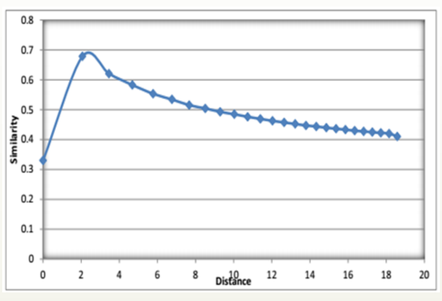
شباهت بین دو سیاست: در نهایت درجه شباهت بین دو سیاست از مجموع درجات شباهت بین مولفه‌های تشکیل دهنده آن یعنی مجموعه قوانین permit ومجموعه قوانین deny و target از دو سیاست به دست می‌آید.

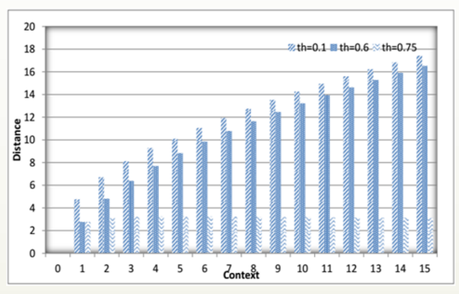
$$S(P_1, P_2) = w_t * S_T(p_1, p_2) + w_p * S^P_{rule-set} + w_d * S^D_{rule-set}$$





نمودار ۱و۲ : رابطه تعداد ویژگی های زمینه با فاصله و تعداد ویژگی های درون قوانین





نمودار ۳و۴ : رابطه فاصله با شباهت و تاثیر آستانه بر درجه فاصله

۴. نتیجه‌گیری

یک روش جدید برای ارزیابی شباهت بین سیاست‌های امنیتی توصیف شده توسط XACML 3.0 ارائه شد. این روش مبتنی بر یک معیار نوین برای محاسبه درجه شباهت بین مقادیر اسمی در این نسخه از XACMLاست. این معیار میتواند با استفاده از توزیع ویژگی ها، مقادیر اسمی را که بایکدیگر مرتبط هستند تشخیص داده و شباهت بین آنها را ارزیابی کند. این روش می‌تواند سیاست‌هایی که تنها در یک زمینه و یک مفهوم مشترک هستند را مشخص نماید.

۵. منابع

1.eXtensible Access Control Markup Language (XACML) Version 3.0. 22 January 2013. OASIS Standard. http://docs.oasis-open.org/xacml/3.0/ xacml-3.0 -core-spec-os-en.html.

2.Vaidya J, Shafiq B, Atluri V, Lorenzi D. *A Framework for Policy Similarity Evaluation and Migration Based on Change Detection.* International Conference on Network and System Security 2015 Nov 3 (pp. 191-205). Springer, Cham.

3.Lin D, Rao P, Ferrini R, Bertino E, Lobo J. *A similarity measure for comparing XACML policies*. IEEE Transactions on Knowledge and Data Engineering. 2013 Sep;25(9):1946-59.

4.Ienco D, Pensa RG, Meo R. *Context-based distance learning for categorical data clustering.* International Symposium on Intelligent Data Analysis 2009 Aug 31 (pp. 83-94). Springer, Berlin, Heidelberg.

5.Li Y, Cuppens-Boulahia N, Crom JM, Cuppens F, Frey V, Ji X. *Similarity measure for security policies in service provider selection*. International Conference on Information Systems Security 2015 Dec 16 (pp. 227-242). Springer, Cham.