Un nouveau modèle de contrôle d'accès appliqué aux environnements informatiques ; étude de cas et application en Industrie 4.0

Résumé :

L'émergence des nouvelles générations d'environnements de connectivité qui accompagnent la transformation numérique de l'industrie, tels que l'internet des objets (IdO) et le concept d'industrie 4.0 avec leurs différentes applications, fait ressortir de nouveaux défis et tendances, pour intégrer des systèmes plus intelligents et avancés dans des systèmes globaux critiques et dans des structures hétérogènes. Ce fait, en plus de la pandémie de COVID-19, a suscité un besoin plus important que jamais du contrôle d'accès (CA) en raison de la généralisation du télétravail et de la nécessité d'accéder aux ressources et aux données liées à des domaines critiques tels que les instances gouvernementales, le secteur de santé, l'industrie et d'autres applications. Tout cela ouvre de nouvelles perspectives aux systèmes d'information traditionnels et aux méthodes de CA en fusionnant de nouvelles technologies et services pour un accès transparent aux sources d'information à tout moment et n'importe où, en particulier avec la présence de cybercriminels et de cyberattaques. Dans cette réalité, toute cyberattaque ou attaque physique réussie peut perturber les opérations ou même réduire les services essentiels rendus à la société. Pour assurer la sécurité et la confidentialité, plusieurs mécanismes de sécurité ont été utilisés et le CA est l'une des exigences de sécurité essentielles dans ce domaine. Ce qui rend cette réalité également difficile, c'est la diversité et l'hétérogénéité des modèles du CA qui sont mis en œuvre et intégrés à d'innombrables systèmes d'information. L'importance des exigences de sécurité, de protection des données et de confidentialité augmente avec la présence massive de nouveaux paradigmes et technologies, le déploiement de solutions numériques et intelligentes basées sur le concept de l'industrie 4.0, ainsi que la généralisation du télétravail. Pour empêcher l'accès non autorisé aux actifs logiques ou physiques, plusieurs méthodes du CA sont mises en œuvre pour contrôler à quoi les utilisateurs peuvent accéder, quand et comment en appliquant les politiques organisationnelles définies.

Parallèlement à la progression technologique, divers travaux de recherche ont été menés en se concentrant sur le développement et l'amélioration des méthodes du CA en cinq étapes principales : (1) modèles du CA communs, (2) modèles hybrides, (3) modèles étendus et (4) modèles abstraits, et (5) métamodèles du CA. Les modèles courants mis en œuvre dans différents environnements informatiques sont le contrôle d'accès discrétionnaire (DAC), le contrôle d'accès obligatoire (MAC), le contrôle d'accès basé sur les rôles (RBAC) et le contrôle d'accès basé sur les attributs (ABAC). Pour trouver des fonctionnalités d'un CA plus avancées et définir un ensemble plus large de règles du CA, divers modèles hybrides avec des fonctionnalités combinées de deux modèles ou plus sont proposés (par exemple, le modèle hybride RBAC/ABAC). De plus, différents

modèles sont étendus en ajoutant de nouveaux composants en plus de ceux existants, pour améliorer leurs fonctionnalités. La réalité actuelle des environnements informatiques impose la nécessité de se concentrer sur le développement des méthodes du CA plus robustes et avancées, d'autant plus que les modèles CA communs, hybrides, étendus et abstraits ont atteint leurs limites et sont actuellement insuffisants pour répondre aux exigences du CA nécessaires. Ce qui rend cet aspect encore difficile, c'est l'hétérogénéité de tout - réseaux, applications, appareils, etc. - en plus de l'hétérogénéité des modèles du CA. Par conséquent, les métamodèles du CA proposés dans la littérature servent comme cadres unificateurs afin d'inclure la plupart des fonctionnalités et des composants des modèles du CA et permettre l'instanciation de divers modèles et la définition et l'application d'un ensemble plus large de politiques statiques et dynamiques.

Malheureusement, les métamodèles proposés ont des limites communes puisqu'ils ne sont : (1) pas assez génériques et n'incluent pas toutes les fonctionnalités des modèles CA, (2) pas assez dynamiques pour suivre les mises à jour technologiques et (3) pas extensibles. En outre, (4) ils ne prennent pas en charge la fonctionnalité de la hiérarchie pour tous les composants, (5) n'expliquent pas comment la collaboration et l'interopérabilité entre les modèles du CA peuvent être atteints et (6) n'abordent pas la question de la migration d'un modèle à un autre. Pour aborder les limitations existantes des métamodèles du CA, dans ce projet de recherche, nous abordons les limitations génériques, extensibles, dynamiques et hiérarchiques. Nous proposons un métamodèle du CA hiérarchique, extensible, avancé et dynamique (HEAD) pour les structures dynamiques et hétérogènes, capable d'englober l'hétérogénéité des modèles du CA où divers modèles CA peuvent être dérivés (modèles existants et non existants). Pour l'implémentation, nous utilisons Eclipse (xtext) pour définir le langage spécifique au domaine (DSL) du métamodèle HEAD. Nous illustrons notre approche avec plusieurs instanciations réussies de divers modèles pour montrer comment il prend en charge des fonctionnalités avancées par rapport à d'autres métamodèles. Pour l'évaluation et la validation, le métamodèle HEAD est utilisé pour spécifier les politiques du CA nécessaires pour deux études de cas inspirées de l'environnement informatique de l'Institut Technologique de Maintenance Industrielle (ITMI)-Sept-Îles, QC, Canada ; le premier est destiné à l'environnement local (non IdO) d'ITMI et le second à l'environnement IdO d'ITMI. Pour chaque étude de cas, le modèle du CA nécessaire est dérivé à l'aide du métamodèle DSL du HEAD, puis la notation xtend (un dialecte expressif de Java) est utilisée pour générer le code Java nécessaire qui représente l'instance concrète du modèle dérivé. Au niveau du système, pour obtenir les règles du CA nécessaires, des requêtes Cypher sont générées puis injectées dans la base de données Neo4j pour représenter la politique de contrôle d'accès de nouvelle génération (NGAC) sous forme graphique. Le cadre NGAC est utilisé comme point d'application pour les règles générées de chaque étude de cas. Les résultats montrent que le métamodèle HEAD peut être adapté et intégré à divers environnements locaux et distribués, capable de servir de cadre unificateur, de répondre aux exigences CA actuelles et de suivre les mises à niveau de politique nécessaires. De plus, nous implémentons un panneau d'administration pour le métamodèle HEAD, comme exemple supplémentaire, en utilisant VB.NET et SQL pour montrer que le métamodèle peut être implémenté pour générer des règles du CA à l'aide d'autres plates-formes.

iTMI
Institut technologique
de maintenance industrielle