Resumo

Um dos principais componentes de segurança em sistemas computacionais é o controle de acesso que busca garantir meios para proteção, confidencialidade e confiabilidade dos acessos dos usuários aos objetos dentro dos sistemas de uma organização. As políticas de controle de acesso descrevem, assim, as regras de acesso aplicadas aos usuários de um sistema. Em sistemas com múltiplos sujeitos, muitas ações e diversos objetos, eventualmente, ocorrerão conflitos entre políticas. Um conflito ocorre quando os objetivos de duas ou mais políticas não podem ser atendidos simultaneamente em um determinado contexto. Políticas conflitantes podem levar o sistema a estados inconsistentes, tais como, acessos não autorizados ou negações a acessos legítimos. Geralmente, a literatura especializada em detecção de conflitos se baseia em técnicas que analisam as políticas em pares e este tipo de análise pode gerar um problema NP-completo, considerado computacionalmente custoso. Já as abordagens que usam mineração de dados e aprendizagem de máquina, geralmente, não têm a detecção de conflitos entre políticas como foco principal. Este trabalho propõe que o problema da detecção de conflitos em políticas pode ser convertido em um problema de *data mining* (mineração de dados) resolvido pela tarefa da classificação além de modelar e sintetizar uma forma de detectar estes conflitos mediante o uso de diferentes algoritmos e técnicas da aprendizagem de máquina e fornecer modelos genéricos o suficiente que possam ser usados em outros contextos. O trabalho apresenta, portanto: (i) A mineração de dados associada a técnicas de aprendizagem de máquina para detectar os conflitos de modalidade entre políticas; (ii) A análise da inserção de novas regras no sistema utilizando o modelo de aprendizagem de máquina gerado; (iii) O comparativo entre algoritmos de mineração apresentando quais deles possibilitam modelar a melhor forma de detecção automática de conflitos entre políticas (com seus hiperparâmetros) e, finalmente, que (iv) o problema de detectar conflitos entre políticas de controle de acesso pode ser resolvido como um problema de classificação utilizando os algoritmos de mineração de dados e aprendizagem de máquina com boa acurácia e precisão. Para alcançar os objetivos propostos foram realizados diversos e múltiplos experimentos onde foram utilizados os principais algoritmos de classificação com diferentes datasets. Para as avaliações quantitativas e outras análises estatísticas diversas métricas foram empregadas e após os experimentos concluiu-se que as Redes Neurais, o SVM e o Random Forest são os melhores algoritmos para este fim sendo as redes neurais o modelo que apresentou as maiores acurácias médias.

Palavras-chave: Controle de Acesso. Mineração de dados. Aprendizagem de máquina. Conflitos diretos. Detecção de conflitos.