|  |  |  |  |
| --- | --- | --- | --- |
| Grifo UA preto | **University of Aveiro**  **2015.** | Department of Electronics, Telecommunications and Informatics | |
| Vedran  Semenski | An ABAC framework for IoT applications, utilizing the OASIS XACML standard | | |
|  | This thesis is submitted to the University of Aveiro and Faculty of Electrical Engineering and Computing, University of Zagreb for compliance with the requirements for the degree of Master of Science in Computing, performed under the supervision of prof. dr. sc. Óscar Pereira, Professor on the Department of Electronics, Telecommunications and Informatics of the University of Aveiro and Mr. Sc. Ricardo Azevedo, from PT – Inovação e Sistemas | | |
|  |  | |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
| palavras-chave | Access Control, ABAC, XACML, IoT, Big Data, NoSQL, XML, JSON, SMARTIE, Smart City, M2M, Security |
| resumo | IoT (*Internet of Things*) é uma área com futuro promissor, que apesar dos seus problemas já terem soluções satisfatórias, a segurança permaneceu de certa forma esquecida, continuando a ser um grande problema. Controlo de acesso é uma forma de reforçar segurança que envolve avaliar pedidos de acesso a recursos e negar o acesso caso este não seja autorizado, providenciando assim segurança para recursos vulneráveis. Controlo de Acesso é um termo lato e que consiste em diversas metodologias, das quais as mais significantes são: IBAC (*Identity Based Access Control*), RBAC (*Role Based Access Control*) and ABAC (*Attribute Based Access Control*). Neste trabalho vai ser usado ABAC, já que oferece uma maior flexibilidade comparativamente a IBAC e RBAC, requerendo menos requisitos de manutenção e longevidade pela sua natureza adaptativa. OASIS (*Organization for the Advancement of Structured Information Standards*) desenvolveu XACML (*eXtensible Access Control Markup Language*), um padrão para escrita/definição de pedidos/políticas e de avaliação de pedidos sobre conjuntos de políticas com o propósito de reforçar o controlo de acesso sobre recursos. XACML foi definido com o propósito de que os pedidos e as políticas fossem fáceis de ler por humanos, retendo uma estrutura bem definida que permita uma avaliação precisa. O padrão usa ABAC. Este trabalho tem o objetivo de criar uma estrutura de segurança que utilize os padrões ABAC e XACML para que possa ser usado por outros sistemas e reforce o controlo de acesso sobre recursos que careçam de proteção, garantindo acesso apenas a pessoas autorizadas. Vai também permitir uma definição pormenorizada de regras e de pedidos para permitir uma avaliação de maior precisão e com um maior nível de segurança. Os casos de uso principais são aplicações IoT, como aplicações Smart City, que inclui monitorização de trafego inteligente, energia e consumo de utilidades, monitorização pessoal de saúde, etc. Estas aplicações lidam com grandes quantidades de informação (*Big Data*) confidencial e/ou pessoal. Existe um número significativo de soluções NoSQL para resolver o problema, mas a segurança é ainda uma questão por resolver. Este trabalho vai usar duas bases de dados NoSQL. Uma base de dados *key-value* (Redis) para armazenamento de políticas e uma base de dados *wide-column* (Cassandra) para armazenamento de informação de sensores e informação de atributos adicionais durante os testes. |
|  |  |
|  |  |
| keywords | Access Control, ABAC, XACML, IoT, Big Data, NoSQL, XML, JSON, SMARTIE, Smart City, M2M, Security |
| abstract | IoT (Internet of Things) is an area which offers great promise and although a lot of core problems already have satisfactory solutions, security has remained somewhat unaddressed and remains to be a big issue. Access Control is a way of enforcing security that involves evaluating requests for accessing resources and denies access if it is unauthorised, therefore providing security for vulnerable resources. Access Control is a broad term that consists of several methodologies of which the most significant are: IBAC (Identity Based Access Control), RBAC (Role Based Access Control) and ABAC (Attribute Based Access Control). In this work, ABAC will be used as it offers the most flexibility compared to IBAC and RBAC and because of ABAC's adaptive nature it also offers lower maintenance requirements and longevity. OASIS (Organization for the Advancement of Structured Information Standards) developed the XACML (eXtensible Access Control Markup Language) standard for writing/defining requests and policies and the evaluation of the requests over sets of policies for the purpose of enforcing access control over resources. It is defined so the requests and policies are readable by humans but also have a well defined structure allowing for precise evaluation. The standard uses ABAC. This work aims to create a security framework that utilizes ABAC and the XACML standard so that it can be used by other systems and enforce access control over resources that need to be protected by allowing access only to authorised subjects. It will also allow for fine grained defining of rules and requests for more precise evaluation and therefore a greater level of security. The primary use-case scenarios are large IoT applications such as Smart City applications, including smart traffic monitoring, energy and utility consumption, personal healthcare monitoring, etc. These applications deal with large quantities (Big Data) of confidential and/or personal data. A number of NoSQL (Not Only SQL) solutions exist for solving the problem of volume but security is still an issue. This work will use two NoSQL databases. A key-value database (Redis) for the storing of policies and a wide-column database (Cassandra) for storing sensor data and additional attribute data during testing. |