Uma Infraestrutura de Autenticação e de Autorização para a Web das Coisas baseada nos padrões SAML e XACML*

Marlon Cordeiro Domenech, †, Michelle Silva Wangham ‡

[1]Laboratório de Sistemas Embarcados e Distribuídos (LSED)
e 4Vision Lab – Universidade do Vale do Itajaí (UNIVALI) – SC – Brasil

marloncdomenech@edu.univali.br, wangham@univali.br

Abstract. *Distributed feature and heterogeneity of the Web of Things (WoT) leads to the necessity of authentication in collaborative environments, composed of different security domains. This work presents an authentication and authorization infrastructure (AAI) for WoT, capable of providing device and user Single Sign-On facing different authentication mechanisms, besides allowing the use of different access control models. Through a case study, the impact of the integration of the AAI in a WoT industrial application was evaluated, considering devices' computational resources usage.*

Resumo. *A característica distribuída e a heterogeneidade da Web das Coisas (WoT) levam à necessidade de autenticação em ambientes colaborativos, compostos por diferentes domínios administrativos de segurança. Este trabalho apresenta uma infraestrutura de autenticação e de autorização (IAA) para a WoT, capaz de prover a autenticação única de dispositivos e de usuários por meio de diferentes mecanismos de autenticação, além de permitir o uso de diferentes modelos de controle de acesso. Por meio de um estudo de caso, foi avaliado o impacto da integração da IAA em uma aplicação industrial de WoT, em termos do uso de recursos computacionais dos dispositivos.*

1. Introdução

O atual salto no crescimento da Internet é decorrente da interconexão de objetos físicos do dia a dia à rede de computadores, paradigma conhecido como Internet das Coisas (*Internet of Things* – IoT). A ideia básica da IoT consiste na presença de uma diversidade de coisas que interagem e cooperam entre si afim de atingir um objetivo comum, por exemplo, o compartilhamento de informações, utilizando métodos de endereçamento único e protocolos de comunicação padronizados [Atzori et al. 2010].

A IoT integra dispositivos heterogêneos (coisas) que interagem entre si, com seres humanos e com sistemas na Internet, o que demanda uma preocupação sobre a interoperabilidade entre estes [Atzori et al. 2010, Matharu et al. 2014]. A Web das Coisas (*Web of Things* - WoT) é uma das abordagens para prover essa interoperabilidade, por meio da reutilização e adaptação de tecnologias e padrões Web que são comumente utilizados em aplicações Web tradicionais. Um dos aspectos que favorece a WoT é a possibilidade de

*Projeto financiado pelo CNPq (RHAE 459623/2013-3) e pela Microsoft Research ("PaaS for smart machines monitoring and control").

†Bolsista CAPES.

‡Bolsista CNPq.

abstrair os dispositivos inteligentes como Serviços Web e integrá-los de maneira transparente à Web atual em uma arquitetura orientada à recursos (ROA). Os Serviços Web *RESTful* tem sido adotados nas abordagens de WoT, em detrimento do uso de Serviços Web arbitrários (WS-*) [Zeng et al. 2011].

Apesar da Web permitir que dispositivos heterogêneos comuniquem-se entre si e com sistemas na Internet, esta heterogeneidade e as restrições computacionais dos dispositivos desafiam as soluções de segurança atuais e requerem soluções diferenciadas para prover segurança na Web das Coisas [Matharu et al. 2014] . Uma Infraestrutura de Autenticação e de Autorização (IAA) é conhecida como o elemento central para prover a segurança em aplicações distribuídas [Lopez et al. 2004]. Com esta infraestrutura, é possível implantar a gestão de identidades de forma a impedir que usuários ou dispositivos não autorizados tenham acesso aos recursos, impedir que usuários ou dispositivos legítimos acessem recursos que estes não estão autorizados e permite que os usuários ou dispositivos legítimos tenham acesso aos recursos a estes autorizados [Liu et al. 2012].

Assim como na Web atual, na WoT, um usuário ou um dispositivo pode requerer acesso a um recurso que esteja em outro domínio administrativo, o que vai demandar que este se autentique e que seu acesso seja autorizado neste outro domínio de segurança [Gardel et al. 2013, Liu et al. 2012] . Uma das maneiras de prover a gestão de identidades em um ambiente colaborativo com múltiplos domínios de segurança é por meio de uma IAA que segue o modelo de gestão de identidades federadas, o qual se baseia no conceito de federação [Bhargav-Spantzel et al. 2007].

Uma federação é composta por provedores de identidades (*Identity Provider* - IdP), responsáveis pela autenticação e gerenciamento das informações dos usuários de um domínio, e provedores de serviços (*Service Provider* - SP). IdPs e SPs estabelecem relações de confiança entre si suficientes para permitir a troca de informações de identidades e o compartilhamento de serviços. Tais acordos de confiança garantem que usuários autenticados no IdP do domínio de origem possam acessar recursos protegidos disponibilizados em SPs de outros domínios da federação [Bhargav-Spantzel et al. 2007]. Se o mesmo evento de autenticação puder ser utilizado para acesso a diversos serviços da federação, tem-se a autenticação única (*Single Sign-On – SSO*).

Na literatura, a autenticação de dispositivos e de usuários em uma mesma infraestrutura é abordada para os modelos de gestão de identidades centralizado e tradicional, contudo não é tratada para o modelo federado. As IAAs para IoT que seguem o modelo federado [Akram e Hoffmann 2008, Gardel et al. 2013, Liu et al. 2012] apresentam soluções para a autenticação única apenas de usuários, não de dispositivos. Assim, a gestão de identidades federadas de dispositivos ainda é um desafio de pesquisa.

Sobre a autorização, as IAAs utilizadas na IoT se baseiam em modelos de controle de acesso já empregados na Internet clássica. Alguns trabalhos relacionados que tratam da autorização na IoT [Liu et al. 2012, Graf et al. 2011] se limitam a tratar apenas um modelo de controle de acesso, o que impõe restrições às aplicações (SPs).

O objetivo deste artigo é descrever uma IAA para a WoT, baseada no modelo de gestão de identidades federadas, que permite a autenticação única de usuários e de dispositivos e que provê um mecanismo de autorização flexível. De forma a avaliar a aplicabilidade e o impacto do uso desta IAA, um protótipo foi desenvolvido e integrado

em um estudo de caso (controle e monitoramento remoto de máquinas industriais).

O restante do trabalho está dividido da seguinte forma. A Seção 2 introduz conceitos e padrões de gestão de identidades. A IAA proposta é descrita na Seção 3. A implementação de um protótipo e sua integração a uma aplicação industrial de WoT é apresentada na Seção 4 e a avaliação dos resultados obtidos é descrita na Seção 5. A Seção 5 analisa e compara os trabalhos relacionados e, por fim, as conclusões e os trabalhos futuros são apresentados na Seção 7.

2. Gestão de Identidades

A gestão de identidades (*Identity Management* – IdM) pode ser entendida como o conjunto de processos e tecnologias usados para garantir a identidade de uma entidade ou de um objeto, garantir a qualidade das informações de uma identidade (identificadores, credenciais e atributos) e para prover procedimentos de autenticação, autorização, contabilização e auditoria [ITU 2009].

Dentre os modelos de IdM, destaca-se o federado, em que a tarefa de autenticação é descentralizada entre vários IdPs, localizados em domínios administrativos diferentes. Um domínio administrativo é composto por usuários, SPs e um IdP [Bhargav-Spantzel et al. 2007]. No contexto de gestão de identidades federadas (FIdM), destaca-se o conjunto de especificações SAML (*Security Assertion Markup Language*). O SAML é um padrão baseado em XML (*eXtensible Markup Language*) para a descrição e troca de asserções de segurança entre parceiros de negócio na Internet. O SAML define protocolos para troca de mensagens e a sintaxe destas e permite a autenticação única entre domínios de segurança. Além disso, o SAML provê perfis de uso que permitem descrever eventos de autenticação para diferentes mecanismos de autenticação, além de prover pontos de extensão, que permitem a representação dos mecanismos de autenticação não descritos na especificação [OASIS 2008].

Para a autorização, um padrão reconhecido no cenário de sistemas distribuídos é o XACML (*eXtensible Access Control Markup Language*). O XACML é uma linguagem baseada em XML para descrição de políticas de autorização e para requisição/resposta de decisões de controle de acesso. Com o XACML, é possível basear a decisão de autorização em atributos do ambiente, do sujeito, do recurso que será acessado e na ação que será realizada. É possível estender a especificação para suportar novos atributos. Assim, o XACML permite construir mecanismos de autorização flexíveis [OASIS 2013].

3. Infraestrutura de Autenticação e de Autorização para a Web das Coisas

A IAA proposta neste trabalho está baseada do padrão SAML e é capaz de prover, na mesma infraestrutura, a autenticação única de dispositivos e de usuários por meio de diferentes mecanismos de autenticação. Na IAA, os IdPs podem ser oferecidos como um serviço IdPaaS (*Identity Provider as a Service*) na nuvem ou *on premise*.

Em relação a autorização, a IAA proposta adota o padrão XACML, o que permite o uso de diferentes modelos de controle de acesso e possibilita a tomada de decisão de acesso dentro do ambiente computacional do dispositivo (SP) ou fora deste (*outsourcing model*) . Na solução *outsourcing*, a tomada de decisão pode ser oferecida como um serviço (PDPaaS - *Policy Decison Point as a Service*) na nuvem ou *on premise*.

Em cada domínio de segurança, a IAA possui os seguintes componentes:

- Provedor de Identidade (IdP): responsável por autenticar usuários e dispositivos, gerar asserções de atributos e validar asserções SAML assinadas por outros IdPs;
- *Policy Enforcement Point* (PEP): responsável por requisitar decisões de controle de acesso ao PDP e aplicar tais decisões;
- *Policy Decision Point* (PDP): toma uma decisão de autorização com base nas políticas aplicáveis (fornecidas pelo PAP) e nas informações disponíveis do ambiente (fornecidas pelo PIP);
- *Policy Administration Point* (PAP): permite a criação e gerenciamento das políticas de autorização;
- *Policy Information Point* (PIP): possui informações que podem ser necessárias para tomada de decisão de autorização feita pelo PDP;
- Cliente Ativo SAML: um componente de software que implementa o protocolo SAML e que pode ser acessado via API pelos desenvolvedores do software embarcado do dispositivo. O Cliente Ativo SAML usa apenas o protocolo HTTP e auxilia na troca de mensagens SAML do cliente com o IdP e do cliente com o SP.

Para que a AAI possa ser utilizada, os seguintes processos de registro e estabelecimento de relações de confiança precisam ser executados: (i) registro dos domínios de segurança, (ii) estabelecimento das relações de confiança entre os IdPs dos domínios da federação e (iii) registro dos clientes (usuários e dispositivos) e dos dispositivos SPs no IdP do domínio correspondente.

O registro do domínio de segurança deve ser executado pelos domínios que farão parte da federação. Este processo consiste no registro do domínio na estrutura DNS da Internet e no registro dos componentes da IAA na estrutura DNS do domínio local. Em seguida, deve ser executado o estabelecimento das relações de confiança entre os IdPs dos domínios de segurança da federação. Este processo é realizado por meio da troca de metadados entre os IdPs, feita sobre um canal TLS mutuamente autenticado.

O terceiro processo consiste no registro dos clientes e SPs no IdP do domínio do qual fazem parte. Três tipos de entidades podem registrar-se: um dispositivo SP, um dispositivo cliente ou um usuário cliente. O registro de um dispositivo SP provê ao dispositivo um identificador único na federação e o registro no DNS local. O registro de um dispositivo cliente permite que este receba material criptográfico gerado pelo IdP, bem como um identificador único para o dispositivo. Por fim, o registro de um usuário cliente é realizado por meio do navegador Web pelo administrador do IdP, utilizando um certificado digital do usuário. Ao final desse processo, o identificador e os atributos dos usuários e dispositivos são armazenados em um serviço de diretório.

Após os processos descritos terem sido executados, os processos de autenticação e de autorização podem ser providos pela IAA. A infraestrutura possui dois modos de operação, que existem em função das possíveis diferenças em relação à capacidade computacional do SP:

1. Modo de Operação SP Restrito: SP com restrição computacional o que torna custosa a tomada de decisão de autorização no próprio dispositivo. Utiliza o modelo de controle de políticas *outsourcing*; e
2. Modo de Operação SP sem Restrição: SP com recursos computacionais suficientes para executar todos os componentes de autorização, sendo capaz de tomar a

decisão de autorização no próprio dispositivo. Utiliza o modelo de controle de políticas *provisioning*.

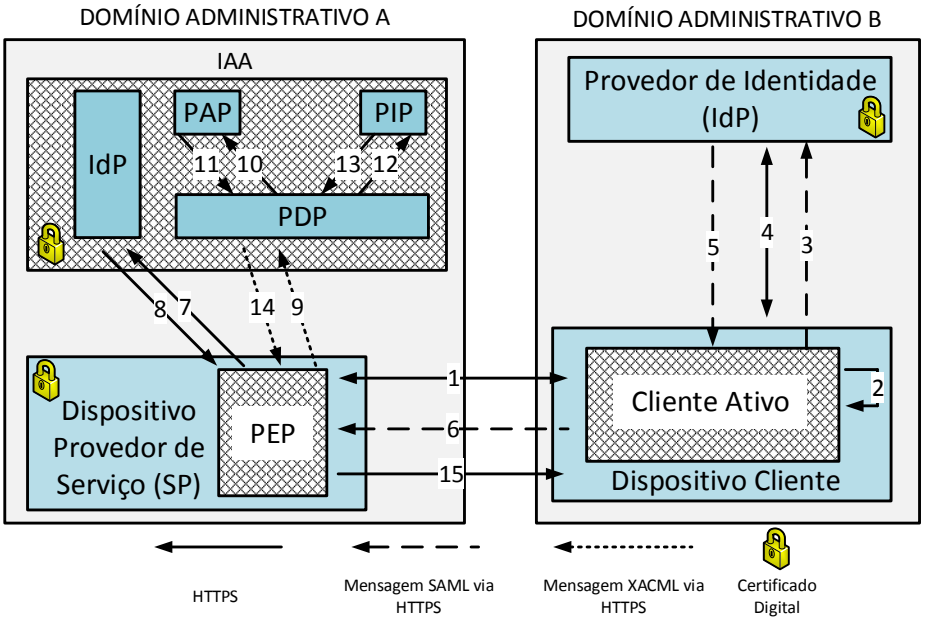

Figura 1. Troca de mensagens entre os componentes da IAA

A Figura 1 ilustra a troca de mensagens entre os componentes da IAA para o Modo de Operação SP Restrito. Todas as mensagens são enviadas sobre um canal seguro TLS. Inicialmente, o Cliente Ativo SAML obtém a política de qualidade de proteção (em formato WS-Policy) do SP (passo 1). Com base nesta política, o Cliente Ativo monta uma requisição de autenticação no formato SAML (passo 2) e a envia ao IdP (passo 3). O IdP e o Cliente Ativo trocam mensagens para autenticação do dispositivo cliente (passo 4) e, caso a autenticação seja bem sucedida, o Cliente Ativo recebe do IdP uma asserção SAML assinada (passo 5). Em seguida, o Cliente Ativo requisita ao SP o serviço desejado pelo dispositivo cliente e anexa à requisição a asserção SAML recebida (passo 6). O PEP intercepta a requisição e solicita ao IdP de seu domínio que valide a asserção SAML recebida (passo 7). O IdP informa ao PEP se a asserção é confiável ou não (passo 8), tendo como base a assinatura digital da asserção SAML. Em caso positivo, o PEP utiliza a asserção SAML para criar uma requisição de decisão de autorização no formato XACML, que é enviada ao PDP que está fora do dispositivo (passo 9). O PDP obtém do PAP a política de autorização aplicável ao dispositivo (passos 10 e 11) e, caso necessário, solicita ao PIP informações adicionais para a tomada de decisão (p.e. informações do recurso que será acessado) (passos 12 e 13). Com base nestas informações e nas regras de acesso, o PDP emite uma decisão de autorização em formato XACML e a envia ao PEP (passo 14). Por fim, o PEP aplica a decisão de autorização (passo 15) e envia ao cliente o recurso desejado ou um erro HTTP.

4. Implementação da IAA e Integração a um Estudo de Caso

Para avaliar a IAA, um protótipo foi desenvolvido. Esta seção descreve este protótipo e a aplicação industrial de WoT utilizada no estudo de caso e que faz uso da IAA.

4.1. Protótipo da IAA

No protótipo da IAA, foi desenvolvida uma Aplicação de Registro de usuários e de dispositivos para que o administrador do IdP cadastre e gerencie as identidades dos usuários e dos dispositivos[1] que poderão se autenticar no IdP. A aplicação foi desenvolvida em PHP, sendo as identidades armazenadas em um serviço de diretório LDAP. Foram definidos ainda os metadados para as identidades de usuários e de dispositivos. Os atributos de uma identidade de usuário inclui os atributos: nome, sobrenome, e-mail, organização, unidade organizacional, função, cpf (identificador único) e certificado digital X.509. Os atributos que compõe a identidade de um dispositivo são: o número de série (identificador único), nome de exibição, contato do administrador, organização, unidade organizacional, descrição, tipo de dispositivo, referência de localização física, latitude, longitude, altitude, disposição (fixo ou móvel), exposição (*indoor* ou *outdoor*) e status (*online* ou *offline*).

Os usuários se autenticam no IdP utilizando um certificado digital[2]. Os dispositivos se autenticam no IdP por meio de um protocolo de acordo de chaves autenticado não-interativo Sakai-Ohgishi-Kasahara [Sakai et al. 2000]. Pelo fato deste criptosistema ser baseado em identidades, a chave pública do dispositivo é baseada em um parâmetro público de sua identidade, neste caso, o número de série. Para isso, foi utilizada a implementação do acordo de chaves Sakai-Ohgishi-Kasahara disponível na biblioteca RELIC [Aranha e Gouvêa 2014].

Dois cenários fazem parte da implementação da etapa de autenticação e consumo de um recurso no SP: (i) o dispositivo cliente é embarcado em um BeagleBone Black) e consome recursos de um SP na *Cloud*; e (ii) o cliente é uma aplicação desktop executada em um notebook e o dispositivo SP é um software embarcado em um BeagleBone Black. Em ambos os casos, utilizou-se o modo SP restrito no qual o IdP e o PDP são oferecidos como um serviço na nuvem (IdPaaS e PDPaaS).

Nos experimentos com o protótipo, assume-se que o Cliente Ativo já buscou a política de qualidade de proteção e extraiu as informações necessárias [3]. No protótipo, o Cliente Ativo, que é uma aplicação Java 7, monta uma requisição de autenticação SAML (passo 2 da Figura 1) por meio da biblioteca OpenSAML 2.6.1, e a envia via HTTPS.

O IdPaaS desenvolvido foi baseado no framework SimpleSAMLphp, que implementa a versão 2.0 do SAML. Os dois mecanismos de autenticação foram ativados no IdP, por meio do módulo *multiauth* do SimpleSAMLphp. Ao receber a requisição, o IdP solicita que seja feita a escolha do mecanismo de autenticação, o qual é indicado pelo Cliente Ativo via *Query String* em um HTTP GET. Em seguida, ocorre a troca de mensagens para autenticação do cliente. Caso o cliente esteja autenticado, o IdP envia ao Cliente Ativo uma mensagem SAMLResponse digitalmente assinada, a qual contém uma Asserção SAML que indica o momento da autenticação, o mecanismo utilizado e os atributos do cliente.

O Cliente Ativo estabelece com o SP um canal seguro TLS (SP é autenticado pelo Cliente Ativo por meio de certificado SSL) e envia a solicitação para o recurso do SP utilizando o método HTTP GET. A mensagem SAML Response é enviada em um

[1] Com esta aplicação é possível gerenciar o ciclo de vida das identidades de usuários e dispositivos (inserção, consulta, exclusão e alteração de atributos de identidades)

[2] Foi utilizada a implementação do SimpleSAMLphp da *Authentication Context Class Public Key - X509*.

[3] Passo 1 da Figura 1 não foi implementado.

cabeçalho (*HTTP Header*) chamado *SAMLResponse*. Na implementação do cliente de Serviço Web *RESTful* Java foi utilizado o framework Jersey.

Ao receber a mensagem HTTP GET, o PEP verifica se a assinatura digital da mensagem SAMLResponse e da Asserção SAML são de algum dos IdPs que fazem parte do círculo de confiança do SP. Se sim, o SP gera uma requisição de decisão de autorização no formato XACML e a envia ao PDP via HTTP POST, por meio de um canal seguro TLS mutuamente autenticado. De posse da requisição, o PDP consulta as políticas locais e toma a decisão de autorização (os passos 10 a 13 da Figura 1 não foram implementados). Em seguida, uma decisão de autorização no formato XACML é gerada pelo PDP e enviada ao PEP do SP, que a aplica e fornece ou não o recurso ao cliente.

Nos experimentos, após estes passos, o Cliente Ativo possui uma Asserção SAML que serve apenas para um SP. Para usufruir da autenticação única e consumir recursos de outros SPs, o cliente deverá submeter uma nova requisição de autenticação SAML ao IdP enviando junto os *cookies* recebidos durante a autenticação. Se o contexto de autenticação ainda for válido, não há necessidade de uma nova autenticação e o IdP gerará a nova asserção SAML destinada ao outro SP. Após receber a Asserção SAML, o fluxo entre o cliente e o SP mantém-se o mesmo já descrito.

4.2. Aplicação de WoT para Controle e Monitoramento de Máquinas Industriais

A aplicação de WoT de monitoramento e controle de máquinas industriais, descrita em [Silva et al. 2015], visa obter os dados de monitoramento de uma máquina industrial, ou de um conjunto de máquinas, tratá-los e disponibilizá-los de duas maneiras: (i) para uma aplicação na Nuvem, que faz a persistência dos dados recebidos e os disponibiliza para uma aplicação de controle e monitoramento remoto; e (ii) para o acesso em tempo real de dados sobre a máquina monitorada, feito por dispositivos. O estudo de caso considerou uma das máquinas industriais produzida pela Empresa XYZ [4].

A máquina industrial possui um sistema SCADA (*Supervisory Control and Data Acquisition*) instalado no notebook que a acompanha, conforme ilustrado na Figura 2. O sistema SCADA registra em um arquivo de log todas as atividades realizadas pela máquina. Visando não alterar esse fluxo funcionamento, uma aplicação chamada Monitor foi criada para intermediar a comunicação entre o SCADA e o *Smart Gateway* (papel similar ao do *Device Driver*)[Silva et al. 2015]. A cada registro de log criado pelo sistema SCADA, a aplicação Monitor recebe um aviso do sistema operacional informando que o arquivo do log foi alterado. A aplicação Monitor lê o novo registro de log e o envia ao *Smart Gateway*, por meio de uma mensagem HTTP POST para um Serviço Web de recebimento de mensagens de log (chamado *Message*). Ao receber esta mensagem, este serviço a interpreta e monta a representação virtual da máquina.

Por meio dos Serviços Web RESTful, o *Smart Gateway* permite a consulta aos recursos da máquina em tempo real (por meio de requisições HTTP GET) e a atuação sobre a máquina por meio de requisições HTTP POST de um recurso. No protótipo desenvolvido, para cada alteração na representação virtual da máquina, é gerado um registro, que é armazenado em memória e, a cada 20 segundos, este registro é enviado para o Serviço Web de persistência de dados na Nuvem, conforme mostra a Figura 2.

[4]Produtora de máquinas industriais para a indústria têxtil que prefere manter o anonimato.

Como prova de conceito, foram desenvolvidas duas aplicações clientes em Java que consomem recursos do *Smart Gateway*: o Cliente Desktop (para usuários) e o Dispositivo Cliente Embarcado em um BeagleBone Black - aplicação autônoma. As aplicações realizam requisições do tipo HTTP GET ao recurso monitorado no *Smart Gateway*.

A Figura 2 apresenta a integração da aplicação de monitoramento de máquinas industriais com a IAA proposta. Esta integração deu-se por meio da inclusão do Cliente Ativo no *Smart Gateway* e no Cliente Desktop e no Dispositivo Cliente, os quais autenticam-se no IdPaaS. O PEP foi incluso no *Smart Gateway* e no Serviço de Recebimento de Dados da aplicação de nuvem, os quais solicitam decisões de autorização para um PDP oferecido como um serviço na nuvem (PDPaaS).

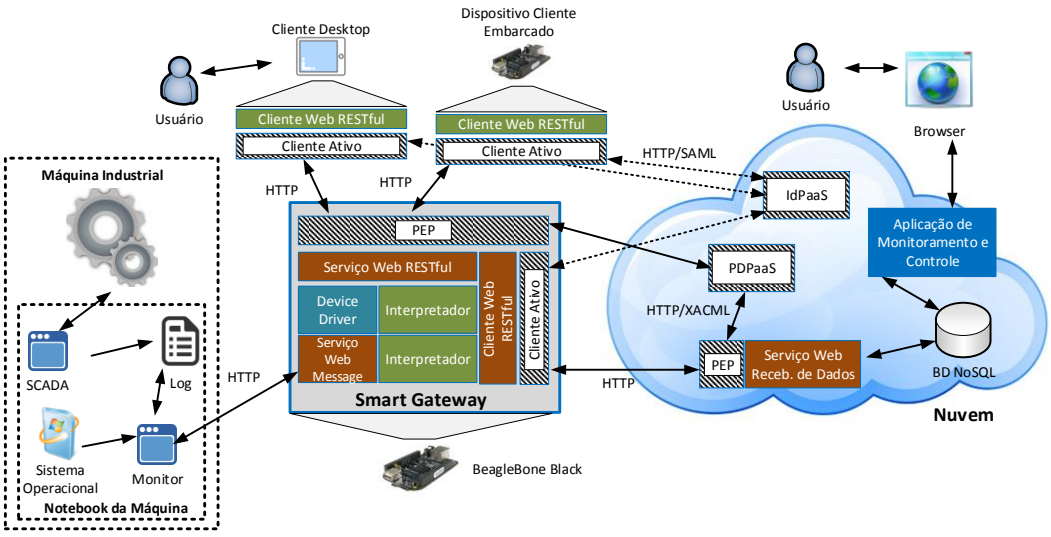

Figura 2. Integração da Aplicação de WoT com a IAA proposta

5. Avaliação

Os experimentos avaliaram o impacto do uso da IAA na Aplicação de WoT no uso de recursos computacionais dos dispositivos. A Aplicação de WoT sem a IAA foi comparada com a Aplicação de WoT integrada à IAA. Cada experimento foi executado 50 vezes. Dos dados obtidos, foram calculados a média e o desvio padrão.

Tabela 1. Uso de CPU - Experimento do Processo de Autenticação

	SSO	**Uso Máximo de CPU (%)**	
		Média	Desvio Padrão
Cliente *Smart Gateway*	-	90.38	15.91
Cliente *Smart Gateway*	X	45.42	22.61
Cliente Desktop	-	62.16	12.5
Cliente Desktop	X	64.95	13.71

O primeiro experimento avaliou o processo de autenticação de um dispositivo cliente (cliente *Smart Gateway*) e de um cliente desktop no IdPaaS, desde a montagem da requisição de autenticação até o recebimento da asserção SAML pelo Cliente Ativo. Foram avaliados o caso em que o cliente executa todo o processo de autenticação e o caso

no qual o cliente já está autenticado e apenas a nova asserção SAML é provida (coluna SSO da Tabela 1). Este processo de autenticação ocorre quando o dispositivo *Smart Gateway* envia os dados monitorados da máquina industrial para a aplicação hospedada na Nuvem ou quando o Cliente Desktop, executado em um notebook, envia requisições para um recurso de monitoramento do *Smart Gateway*.

A Tabela 1 mostra a média e desvio padrão dos valores obtidos para a métrica de custo de CPU. É possível perceber que para o caso do cliente *Smart Gateway*, a média do valor máximo no caso do uso da autenticação SSO é menor quando comparado ao caso em que o dispositivo precisa passar por todo o processo de autenticação.

A Tabela 2 apresenta os dados de consumo de potência elétrica para o Experimento do Processo de Autenticação do Cliente *Smart Gateway*. São apresentados dados de consumo mínimo, máximo e a faixa de valores obtidos. Ao comparar os cenários com a autenticação completa e com autenticação SSO, há um aumento de 53,57% quando não se tem a autenticação completa.

Tabela 2. Consumo de Potência - Experimento do Processo de Autenticação

	SSO	**Menor Consumo (W)**			**Maior Consumo (W)**		
		Média	D. Padrão	Faixa	Média	D. Padrão	Faixa
Cliente SG	-	1,05	0	1,05	1,72	0,03	1,65-1,75
Cliente SG	X	1,05	0	1,05	1,12	0,02	1,1-1,15

O experimento de Processo de Autorização compreende desde o momento em que o Cliente Ativo SAML monta a requisição até receber o recurso desejado (após a autorização de acesso ao recurso). A Tabela 3 mostra os dados de tamanho das mensagens trocadas entre cliente e SP com e sem a IAA (foi considerado todo o segmento TCP). Observa-se um aumento expressivo no tamanho da solicitação enviada do cliente para o SP, devido à inclusão da Asserção SAML no cabeçalho da requisição HTTP.

Tabela 3. Tamanho das Mensagens - Experimento de Requisição ao Provedor de Serviço

	IAA	**Tamanho das Mensagens (bytes)**	
		Média	Desvio Padrão
Cliente *Smart Gateway*	-	423,34	9,19
Cliente *Smart Gateway*	X	13.193,22	16,97
Cliente Desktop	-	211	0
Cliente Desktop	X	11.644,22	37,38

O Processo Completo de obtenção do recurso pelo cliente também foi avaliado e os dados obtidos são mostrados na Tabela 4. Percebe-se em todos os clientes que, ao utilizar a IAA, há um aumento do uso de recursos computacionais e do tempo de processamento. Também percebe-se que, ao utilizar a autenticação única, o impacto no uso de recursos computacionais é atenuado o que comprova os benefícios desta.

6. Trabalhos Relacionados

O framework de IdM apresentado em [Akram e Hoffmann 2008] tem como objetivo abstrair dos desenvolvedores os mecanismos de IdM utilizados em suas aplicações em ambientes federados. O *middleware* provê interoperabilidade de mecanismos de autenticação

Tabela 4. Experimento do Processo Completo para Obtenção de um Recurso

	IAA	SSO	**Memória RAM (MiB)**		**Tempo de Proc. (ms)**	
			Média	D. Padrão	Média	D. Padrão
Cli. SG	-	-	195,08	1,29	4.558,92	2.446,84
Cli. SG	X	-	305,7	13,01	15.106,66	1.713,77
Cli. SG	X	X	285,38	2,17	9.802,76	1.346,4
Cli. Desktop	-	-	18,43-22,6	0,18-0,14	49,08	103
Cli. Desktop	X	-	59,22-97,65	10,37-18,78	5.045,12	652,11
Cli. Desktop	X	X	66,99-109,83	21,72-23,45	4.426,06	576,9

única de usuários. Contudo, a autenticação de dispositivos não é tratada e só é possível o uso de um modelo de controle de acesso.

Em [Alam et al. 2011], objetiva-se prover o acesso seguro a serviços na IoT e a interoperabilidade de diferentes modelos de controle de acesso. Entretanto, a infraestrutura não trata a autenticação de usuários e de dispositivos. Em [Conzon et al. 2012], é apresentado o VIRTUS, um *middleware* para comunicação segura na IoT baseado nos protocolos TLS e SASL, o que permite o uso de diferentes mecanismos de autenticação. Contudo, a autenticação única de usuários e a autenticação de dispositivos não é abordada e há suporte a apenas um modelo de controle de acesso.

Em [Liu et al. 2012], é proposta uma arquitetura para IoT baseada no OpenID, que trata da autenticação e do controle de acesso em um ambiente federado. Dispositivos e usuários registram-se em uma terceira parte confiável de seu domínio administrativo, a qual auxilia no processo de autenticação de usuários. Contudo, a autenticação de dispositivos não é tratada e só é possível utilizar o modelo RBAC para controle de acesso.

Em [Gardel et al. 2013], um barramento de serviços é utilizado para publicação e descoberta de recursos de dispositivos da WoT, por meio de Serviços Web *RESTful*. No barramento de serviços são aplicadas as políticas de controle de acesso utilizando o framework OpenID Connect, o qual permite a autenticação única de usuários em um ambiente federado. Não é abordada a interoperabilidade entre diferentes mecanismos de autenticação nem a autenticação de dispositivos, e apenas um modelo de controle de acesso é possível. Em [Seitz et al. 2013], é apresentado um framework de controle de acesso baseado no padrão XACML e SAML. Entretanto, o mecanismo não trata de autenticação e não aborda autorização em um contexto M2M.

A Tabela 5[5] compara os trabalhos relacionados, os quais são caracterizados com base no (i) foco (autenticação ou autorização); (ii) se tratou da interoperabilidade entre diferentes mecanismos de autenticação de usuários e de dispositivos; (iii) o modelo de IdM e (iv) os modelos de controle de acesso utilizados; (v) se foi abordada a autenticação única (SSO) de usuários ou de dispositivos; (vi) se foi abordada a autenticação de usuários e (vii) de dispositivos; (viii) se foi implementado; (ix) se foi abordado um cenário M2M; e (x) se apresentou uma abordagem para a WoT.

Dos trabalhos descritos, apenas [Akram e Hoffmann 2008] e [Conzon et al. 2012]

[5]T1 = [Akram e Hoffmann 2008]. T2 = [Alam et al. 2011]. T3 = [Conzon et al. 2012]. T4 = [Liu et al. 2012]. T5 = [Gardel et al. 2013]. T6 = [Seitz et al. 2013]. N/A = Não se aplica. N/D = Não definido.

trataram da interoperabilidade entre diferentes mecanismos de autenticação, mas apenas para autenticação de usuários e fora de um contexto M2M. A autenticação única também é tratada em [Akram e Hoffmann 2008] e [Gardel et al. 2013], mas apenas para usuários, não para dispositivos. Apenas [Alam et al. 2011] é independente do modelo de controle de acesso, contudo, este não trata a autenticação. Por fim, nota-se que a autenticação de usuários na WoT é bem abordada, mas há uma lacuna para abordagens que tratem também, na mesma infraestrutura, a autenticação de dispositivos.

Tabela 5. Comparação entre os trabalhos relacionados e este trabalho

	T1	T2	T3	T4	T5	T6	Este Trab.
Aut./Autz.	Sim/Sim	-/Sim	Sim/Sim	Sim/Sim	Sim/Sim	-/Sim	Sim/Sim
Interop. Aut.	Usuários	N/A	Usuários	-	-	N/A	Sim
Modelo IdM	Fed	Fed.	Trad.	Fed.	Fed.	Cent.	Fed.
Modelo AC	CBAC	Indep.	ACL	RBAC	CapBAC	N/D	Indep.
SSO	Usuários	N/A	-	-	Usuários	N/A	Sim
Aut. Usuários	Sim	N/A	Sim	Sim	Sim	N/A	Sim
Aut. Dispos.	-	N/A	-	-	-	N/A	Sim
Implement.	Sim	Sim	Sim	-	Sim	Sim	Sim
M2M	-	Sim	-	-	-	-	Sim
WoT	Sim	Sim	-	Sim	Sim	Sim	Sim

7. Conclusão e Trabalhos Futuros

Este trabalho apresentou uma IAA para a WoT, a qual foi integrada a uma aplicação de WoT de monitoramento e controle remoto de máquinas industriais. Os resultados obtidos permitiram mensurar o impacto do uso da IAA em termos do uso de recursos computacionais dos dispositivos. Percebe-se que, apesar da IAA ser viável para esta aplicação de WoT, existem impactos claros no uso de recursos dos dispositivos. Assim, testes com outras aplicações de WoT são necessários para que se possa melhor avaliar a IAA proposta. Por outro lado, os resultados permitem afirmar que a autenticação única trouxe benefícios para o cenário dos experimentos, uma vez que foram utilizados menos recursos computacionais do que nos casos da autenticação completa.

Como trabalhos futuros, pretende-se aprimorar o protótipo implementado visando diminuir o custo computacional utilizando, por exemplo, JSON ao invés de XML e mecanismos de compressão. Pretende-se estender o IdPaaS para que este suporte outros mecanismos de autenticação de usuários e de dispositivos. Por fim, pretende-se também avaliar a aplicabilidade da IAA em outros cenários, como por exemplo os de Saúde Eletrônica e Cidades Inteligentes.

Agradecimentos

Os autores agradecem à CAPES e ao CNPq pelo apoio financeiro e à Microsoft Research pelo ambiente de *Cloud Computing* utilizado neste trabalho.

Referências

Akram, H. e Hoffmann, M. (2008). Supports for identity management in ambient environments-the hydra approach. In *Proceedings...*, pages 371–377. 3rd International Conference on Systems and Networks Communications, 2008. ICSNC'08.

Alam, S., Chowdhury, M. M., e Noll, J. (2011). Interoperability of security-enabled internet of things. *Wireless Personal Communications*, 61(3):567–586.

Aranha, D. F. e Gouvêa, C. P. L. (2014). RELIC is an Efficient LIbrary for Cryptography. `https://github.com/relic-toolkit/relic`.

Atzori, L., Iera, A., e Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15):2787–2805.

Bhargav-Spantzel, A., Camenisch, J., Gross, T., e Sommer, D. (2007). User centricity: a taxonomy and open issues. *Journal of Computer Security*, 15(5):493–527.

Conzon, D., Bolognesi, T., Brizzi, P., Lotito, A., Tomasi, R., e Spirito, M. A. (2012). The virtus middleware: An xmpp based architecture for secure iot communications. In *Proceedings...*, pages 1–6. 21st International Conference on Computer Communications and Networks (ICCCN), 2012.

Gardel, T., Andrade, N., Farias, F., e Prazeres, C. (2013). Autenticação e autorização para acesso a aplicações em um barramento de serviços para a web das coisas. In *Anais do*. 13 Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2013, SBC.

Graf, S., Zholudev, V., Lewandowski, L., e Waldvogel, M. (2011). Hecate, managing authorization with restful xml. In *Proceedings of*, pages 51–58. Second International Workshop on RESTful Design, ACM.

ITU (2009). Ngn identity management framework. Recommendation Y.2720.

Liu, J., Xiao, Y., e Chen, C. P. (2012). Authentication and access control in the internet of things. In *Proceedings...*, pages 588–592. 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), 2012.

Lopez, J., Oppliger, R., e Pernul, G. (2004). Authentication and authorization infrastructures (aais): a comparative survey. *Computers & Security*, 23(7):578–590.

Matharu, G., Upadhyay, P., e Chaudhary, L. (2014). The internet of things: Challenges amp; security issues. In *Emerging Technologies (ICET), 2014 International Conference on*, pages 54–59.

OASIS (2008). Security assertion markup language (saml) v2.0 - technical overview.

OASIS (2013). extensible access control markup language (xacml) version 3.0.

Sakai, R., Ohgishi, K., e Kasahara, M. (2000). Cryptosystems based on pairing. In *The 2000 Symposium on Cryptography and Information Security*, pages 135–148.

Seitz, L., Selander, G., e Gehrmann, C. (2013). Authorization framework for the internet-of-things. In *Proceedings...*, pages 1–6. IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM).

Silva, P. H. d., Domenech, M. C., Rauta, L. R. P., Silva, R. C. d., e Wangham, M. S. (2015). Controle e monitoramento remoto de máquinas industriais por meio de smart gateways na web das coisas. In *Anais do Computer on the Beach*, pages 298–307.

Zeng, D., Guo, S., e Cheng, Z. (2011). The web of things: A survey. *Journal of Communications*, 6(6).