Gerenciamento Descentralizado de Identidades para Cidades Inteligentes Baseado na Tecnologia Blockchain

André Luiz Almeida Cardoso[1], Bruno Maciel Rotondaro[2], Luiz Gonzaga Penha[1], Markus Endler[3], Arlindo Flávio da Conceição[2], Francisco José da Silva e Silva[1]

[1]Laboratórios de Sistemas Distribuídos Inteligentes (LSDi)
Universidade Federal do Maranhão (UFMA)
São Luís–MA, Brasil

[2]Instituto de Ciência em Tecnologia (ICT)
Universidade Federal de São Paulo (UNIFESP)
São José do Campos–SP, Brasil

[3]Laboratory for Advanced Collaboration (LAC)
Pontifícia Universidade Católica (PUC)
Rio de Janeiro–RJ, Brasil

{andre.cardoso,luiz.penha,fssilva}@lsdi.ufma.br,
{bruno.rotondaro,arlindo.conceicao}@unifesp.br, endler@inf.puc-rio.br

Abstract. *Smart City is a paradigm capable of mitigating the problems caused by urbanization, transforming the city environment into something more sustainable. For the adoption of this paradigm, a relevant issue is the identity management of the various actors involved, which involves administrative units of municipal power, IoT devices, service providers and users. This work presents a model for decentralized identity management based on blockchain, specifically focused on the context of smart cities. Additionally, the model was explored to develop a security infrastructure integrated to a middleware platform for smart cities. This article describes the proposed model, its implementation, validation and evaluation, thus demonstrating its feasibility.*

Resumo. *Cidade Inteligente é um paradigma capaz de atenuar os problemas causados pela urbanização, transformando o ambiente da cidade em algo mais sustentável. Para a adoção deste paradigma, uma questão relevante é a gestão de identidade dos diversos atores envolvidos, que envolve unidades administrativas do poder municipal, dispositivos de IoT, provedores de serviços e usuários. Este trabalho apresenta um modelo para gestão descentralizada de identidades baseado em blockchain, especificamente voltado para o contexto das cidades inteligentes. Adicionalmente, explorou-se o modelo para desenvolver uma infraestrutura de segurança integrada a uma plataforma de middleware para cidades inteligentes. Este artigo descreve o modelo proposto, sua implementação, validação e avaliação demonstrando, assim, sua viabilidade.*

1. Introdução

Cidade Inteligente (CI) é o termo utilizado para representar o conceito de redução dos problemas causados pela urbanização por meio da utilização de novas tecnologias, tornando o ambiente da cidade com mais sustentável e eficiente [Xie et al. 2019]. Dentre as

características de uma CI, podemos citar o uso pervasivo de Tecnologias da Informação e Comunicação (TIC) em diversos domínios urbanos para aumentar a eficiência na utilização de seus recursos [Neirotti et al. 2014]. A Internet das Coisas é uma das tecnologias-chave para implementação do conceito de cidades inteligentes.

Um dos grandes desafios envolvendo Cidades Inteligentes é a cibersegurança, que aborda problemas relacionados a proteção de dados, assim como do software e da infraestrutura utilizada para processar e armazenar os dados [Alamer and Almaiah 2021]. Ameaças de segurança como negação de serviço, invenção e modificação de dados ou acesso não autorizado a serviços e dados tem potencial para causar danos em uma CI que variam de prejuízos financeiros até a morte de residentes. Requisitos básicos de segurança como confidencialidade, integridade, irretratabilidade, disponibilidade, controle de acesso e privacidade também se aplicam às Cidades Inteligentes e devem estar presentes no mundo físico (i.e., no sensoriamento), na comunicação e nas informações [Zhang et al. 2017].

As identidades digitais já ocupam um importante papel em nossa sociedade, elas são geridas por sistemas de gerenciamento de identidade e são exploradas por provedores de serviços para oferecer segurança em suas operações [Liu et al. 2020]. Em um ambiente de uma Cidade Inteligente, onde podem existir milhões de dispositivos IoT consumindo e produzindo dados, a gestão de identidades se apresenta como forma de aprimorar o ambiente da cidade em relação à segurança computacional. Dados produzidos por dispositivos em uma CI são utilizados para tomar decisões ou atuar sobre o ambiente da cidade, e isto se reflete diretamente nos recursos da cidade. A autenticação dos geradores de informação (i.e., sensores ou dispositivos IoT) é fundamental para a IoT, pois decisões não podem ser tomadas considerando dispositivos desconhecidos ou não confiáveis.

O ecossistema de uma CI envolve diversos atores que se comunicam entre si, consumindo e produzindo dados. Como exemplo, podemos citar órgãos públicos tais como prefeituras, sub-prefeituras, secretarias ou similares, que atual como gestores da cidade. Outros atores ainda compõem este ambiente, tais como pessoas, sensores e atuadores, dispositivos IoT em geral, serviços e aplicações. Para melhor entendimento sobre a solução proposta neste artigo, considera-se o cenário de uma CI administrada por órgãos públicos, no qual a administração deseja implantar dispositivos IoT (e.g., sensores, atuadores, câmeras de segurança) para monitorar o ambiente da cidade e fornecer dados para serem consumidos pelo cidadão através de serviços e aplicações. Sem a garantia de que são íntegros os dados provenientes do sensoriamento de uma cidade inteligente, torna-se inviável para administração tomar decisões estratégicas, atuar sobre o ambiente da cidade ou disponibilizar tais dados para serviços e aplicações.

O objetivo deste trabalho é (i) propor um modelo para gestão descentralizada de identidades voltado para o domínio de Cidades Inteligentes, (ii) implementação dos mecanismos, baseado na tecnologia *blockchain*, que implementam o modelo proposto, e (iii) utilizar os mecanismos desenvolvidos para prover uma infraestrutura de segurança, voltada para a coleta, distribuição e acesso a dados, integrada a plataforma InterSCity. O InterSCity[1] é uma plataforma de *middleware* desenvolvida com o objetivo de facilitar o desenvolvimento de aplicações voltadas para CI. Neste cenário típico de uma CI, com

[1]https://interscity.org/software/interscity-platform/

muitos emissores de informação (i.e., sensores, dispositivos IoT) gerenciados por diferentes entidades administrativas (e.g., prefeituras, secretarias, etc.), o gerenciamento de identidades deve ser naturalmente descentralizado, e, portanto, pode-se explorar o uso de tecnologias distribuídas como *Blockchain*.

O restante do artigo está organizado da seguinte forma. A Seção 2 introduz conceitos importantes para o melhor entendimento deste artigo. A Seção 3 apresenta, e discute os trabalhos relacionados a gestão de identidades. A Seção 4 aborda o modelo proposto, sua implementação e aplicação para prover uma infraestrutura de segurança para uma plataforma de Cidades Inteligentes. A Seção 5 apresenta um caso de uso e, a partir dele, avalia a adoção da solução proposta em termos de consumo de memória de processamento. Por fim, a Seção 6 conclui o trabalho discutindo os resultados obtidos, resumindo as principais as contribuições e apresentando as perspectivas futuras.

2. Fundamentação

Esta seção apresenta alguns conceitos importantes para melhor entendimento deste trabalho. Serão apresentados conceitos de Identidade, Identidade Digital e Gerenciamento de Identidades. Além disso, será introduzida a tecnologia *blockchain* e sua relação com o gerenciamento de identidades.

2.1. Identidades e Gerenciamento de Identidades

Identidades são popularmente conhecidas como "algo que identifica" e são utilizadas no cotidiano, ao, por exemplo: apresentar a habilitação com intuito de identificar-se e provar o direito de conduzir veículos. O conceito de identidade pode ser formalmente definido como informação sobre uma entidade que é suficiente para identificar aquela entidade em um contexto específico [ITU 2009]. Além do conceito geral de identidades, também é definido o conceito de identidade digital. Segundo [El Haddouti and El Kettani 2019], uma identidade digital refere-se a um conjunto de informações que identificam exclusivamente um indivíduo usando informações digitais para garantir o mesmo nível de confiança que uma transação presencial geraria.

A Gestão de Identidades (*Identity Management* - IdM), ou Gestão de Identidade e Acesso (IAM), é uma importante linha de pesquisa pertencente à segurança computacional. Diversos autores definem a gestão de identidades de forma semelhante. Segundo [Bertino and Takahashi 2010], a gestão de identidades pode ser definida como manter a integridade de identidades ao longo de seu ciclo de vida com objetivo de disponibilizar as identidades e seus dados relacionados para serviços de forma segura. Segundo a União Internacional de Telecomunicações (ITU) [ITU 2009], a gestão de identidade se refere a gestão das informações contidas nas identidades através de operações como emissão, revogação, atualização e obtenção de identidades. Em [Manohar and Briggs 2018], a gestão de identidades é uma diretriz de segurança que permite que os indivíduos certos acessem os recursos certos, no momento certo e por razões corretas. Segundo [Liu et al. 2020], a gestão de identidades se refere a um arcabouço (i.e., framework) de políticas e tecnologias para garantir que apenas indivíduos autorizados acessem os recursos pertencentes a uma determinada organização.

Os conceitos apresentados reforçam que a gestão de identidades não envolve somente a manutenção (i.e., emissão, atualização, revogação, etc) de identidades, mas

também autenticação e controle de acesso. Sistemas que efetuam a gestão de identidades, também chamados de *Identity Management Systems* (IdMS), implementam diferentes tipos de arquiteturas a fim de oferecer seus serviços de identidade.

2.2. Blockchain

Uma *blockchain* é essencialmente um livro-razão descentralizado, distribuído, compartilhado e imutável que armazena registros de ativos e transações através de uma rede peer-to-peer [Khan and Salah 2018]. Na *blockchain*, todas as transações são armazenadas permanentemente e qualquer participante da rede pode acessar, enviar e verificar transações [Xie et al. 2019]. As características intrínsecas a tecnologia *blockchain* podem ser exploradas no contexto da gestão de identidades, segundo [da Conceição and Rocha 2020], a tecnologia *blockchain* oferece algumas características no desenvolvimento de aplicações, tais como: descentralização da informação, disponibilidade, privacidade, integridade, imutabilidade e auditabilidade. Tais características são benéficas considerando também o contexto de Cidades Inteligentes e, portanto, a tecnologia é cada vez mais explorada neste domínio.

Na literatura, diversos autores exploram a tecnologia *blockchain* para aplicá-la no gerenciamento de identidade [Ghaffari et al. 2022]. De acordo com [Dunphy and Petitcolas 2018], as tecnologias de ledger distribuído (e.g., *blockchains*) são adequadas para garantir consenso, transparência e integridade de transações efetuadas, de forma que existem diversos benefícios no uso de DLT (*Distributed Ledger Technology*) aplicado a gestão de identidades, tais como: descentralização, imutabilidade, eficiência de custo e disponibilidade.

3. Trabalhos Relacionados

O gerenciamento de identidades é uma área bastante explorada, [Tracy 2008] apresenta uma visão geral sobre a arquitetura de sistemas de gerenciamento de identidades tradicionais. Recentemente o uso de *blockchain* é explorado para aprimorar tais sistemas. Uma revisão sistemática conduzida por [Liu et al. 2020] explora diversos trabalhos sobre sistemas de gerenciamento de identidade baseados em *blockchain* [Santos 2018, Mikula and Jacobsen 2018, Kikitamara et al. 2017]. A seguir, serão resumidos apenas os trabalhos recentes envolvendo gestão de identidades baseados em *blockchain* e voltados para IoT.

Em [Venkatraman and Parvin 2022], os autores propõem um sistema de gerenciamento de identidades que utiliza uma plataforma de *blockchain* federada e contratos inteligentes para dar suporte a armazenamento seguro de dados e autenticação segura de recursos de IoT. Como prova de conceito do modelo proposto, foi desenvolvido um protótipo considerando um cenário de caso de negócios de uma organização que já gerencia identidades de recursos IoT, onde a solução atual de gerenciamento de identidades não suporta o crescimento do número de dispositivos IoT conectados, nem monitora transações de dispositivos automaticamente. Para o gerenciamento de identidades, classificam-se os recursos de IoT em quatro tipos: recursos computacionais (i.e., dispositivos IoT), recursos de software, usuários e recursos de dados (i.e., operações realizadas). Apesar de demonstrado a praticidade do modelo proposto através do protótipo, este se limita ao cenário do caso de negócios, perspectivas futuras pretendem avaliar o modelo em cenários mais amplos.

Em [Wang et al. 2022], os autores utilizam a tecnologia de *ledger* distribuído IOTA para desenvolver um mecanismo leve e escalável para efetuar o gerenciamento de identidades de dispositivos IoT e controle de acesso a grandes volumes de dados de IoT. Através da tecnologia IOTA, são efetuadas as operações de registro, atualização, revogação e recuperação de identidades de dispositivos IoT, eliminando assim os problemas causados por um gerenciamento centralizado. Devido às limitações computacionais de dispositivos IoT, o registro de identidades ocorre através de um componente chamado `Fog Node` que atua próximo ao sistema onde dispositivos atuam. Através deste mecanismo para gerenciamento de identidades de dispositivos IoT e controle de acesso dados de IoT resolve-se problemas de ponto único de falha e escalabilidade presentes em soluções já existentes.

Em [Rahat et al. 2022], foi proposto um sistema de gerenciamento de identidades para uso geral, asseguradas através da tecnologia *blockchain*. Neste modelo, ao invés de diversos documentos de identificação, usuários possuem uma única identidade que pode ser utilizada para provar sua identidade em diversas aplicações ou serviços. A *blockchain* é utilizada para armazenar de forma íntegra as identidades, que podem ser auditadas pelo governo. Utiliza-se o conceito de identidades autossoberanas [Preukschat and Reed 2021], no qual o usuário possui total controle sobre sua identidade.

Diversos trabalhos da literatura são focados na gestão de identidade em geral e alguns abordam especificamente a IoT, mas os trabalhos que consideram as especificidades do domínio das cidades inteligentes são ainda incipientes. Uma Cidade Inteligente é um ambiente heterogêneo onde atores se comunicam através de diferentes tecnologias de redes e protocolos de comunicação, assim como dispositivos podem diferir em termos de poder de processamento, armazenamento ou conectividade. Considerando esta lacuna, este trabalho tem como foco apresentar um modelo para gestão distribuída de identidades, baseado na tecnologia *blockchain* voltado especificamente para o domínio de CI.

4. Solução Proposta: Gerenciamento de Identidades Utilizando a Tecnologia *Blockchain*

Esta seção aborda a visão geral da solução, sua implementação e integração com a plataforma de *middleware* InterSCity.

4.1. Modelo de Gestão de Identidades

Nosso modelo para gestão de identidades considera que o processo de controle de uma CI deve ser feito de forma descentralizada, por órgãos públicos que possuem interesse em manter o ambiente da cidade seguro. Para isso, classificam-se os atores de uma CI em dois tipos: entidades administrativas e demais entidades. Como entidades administrativas, temos prefeituras, sub-prefeituras, secretarias e até empresas privadas parceiras do estado, no modelo proposto estas entidades tem como responsabilidade manter a infraestrutura necessária (i.e., rede *blockchain*), assim como a emissão de identidades das demais entidades. Dentre as demais entidades, podemos citar dispositivos IoT, coisas, funcionários, serviços, aplicações, componentes de software, e qualquer outro ator que exista no ambiente de uma CI. A rede *blockchain* a ser utilizada neste este modelo, deve ser permissionada por um consórcio de entidades administrativas. Cada entidade administrativa, atuando como provedor de identidade, tem direito de emitir sua própria identidade

e utilizá-la para gerar identidades das demais entidades. Dessa forma, existe uma hierarquia onde cada identidade armazenada na rede *blockchain* foi emitida por uma entidade administrativa. A administração de uma CI pode utilizar este modelo de gestão de identidades para identificar, autenticar e controlar acesso a seus recursos de forma distribuída.

O registro de identidades na rede *blockchain* é regido por meio da execução de contratos inteligentes escritos em JAVA. A Figura 1 exibe o diagrama de classes implementado pelos contratos inteligentes.

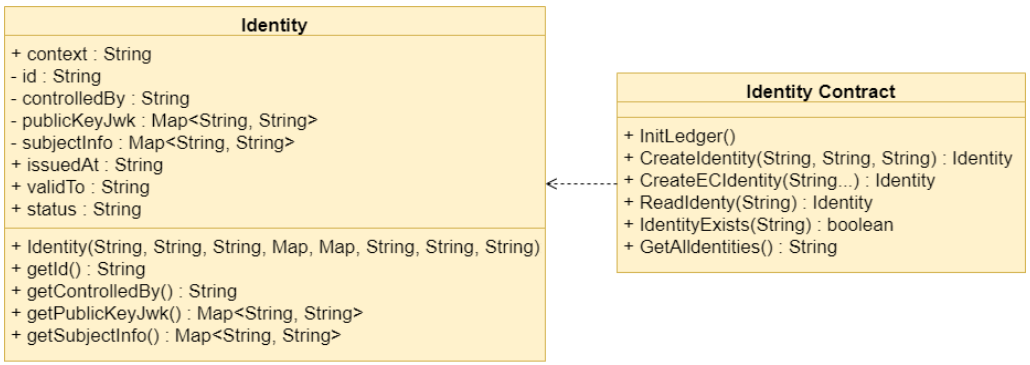

Figura 1. Diagrama de classe referente ao modelo de identidade.

Uma identidade é basicamente composta pelos seguintes campos: identificador único, identificador único do emissor, chave pública. O atributo `subjectInfo` consiste em um conjunto de pares chave e valor que podem ser preenchidos com informações correspondentes ao sujeito de cada identidade. Considerando a eventual restrição de recursos computacionais de dispositivos IoT, adotou-se por padrão a criptografia de curva elíptica (ECC) para geração de chaves criptográficas, pois estas garantem o mesmo nível de segurança que as do tipo RSA, porém utilizando tamanhos de chave menores [Mektoubi et al. 2016]. O armazenamento das chaves é feito segundo o formato *JSON Web Key* (JWK — RFC7517) [Jones 2015]. Apenas dispositivos IoT capazes de realizar requisições HTTP e gerar assinaturas digitais conseguem utilizar as identidades propostas pelo modelo, caso contrário, é possível utilizar *gateways* para gerenciar os dispositivos.

4.2. Implementação: *Entity Manager*

Para implementar este modelo proposto, utilizando a tecnologia *blockchain* para armazenamento distribuído das identidades, implementou-se um componente de *software* chamado `Entity Manager`. Este componente representa as entidades administrativas do modelo proposto, sendo capaz de enviar transações a *blockchain* para executar os contratos inteligentes responsáveis pela emissão de identidades das demais entidades. A complexidade dos conceitos envolvendo *blockchain* e contratos inteligentes justifica o desenvolvimento deste componente, que atua para facilitar a emissão e recuperação de identidades. As funcionalidades deste componente para registro de identidades são disponibilizadas através de uma API Rest. Cada identidade emitida por uma entidade administrativa, através do `Entity Manager`, traz uma referência apontando para o emissor da identidade. Assim, todas a identidades registradas na rede *blockchain* podem ser verificadas para determinar seu originador (i.e., a entidade administrativa de origem). Antes de emitir identidades, o *Entity Manager* gera seu par de chaves, emite e registra sua

própria identidade da *blockchain*. Como a rede *blockchain* é mantida por um consórcio de órgãos públicos, cabe aos administradores da rede conceder a permissão de escrita na *blockchain* ao *Entity Manager*. Dessa forma, cada participante da rede pode possuir instâncias independentes do *Entity Manager*, que emitem identidades. Por exemplo, uma prefeitura pode manter uma instância do componente para uma secretaria de transporte emitir identidades para seus ônibus, enquanto outra instância representando a secretaria de segurança pública emite as identidades de suas câmeras de segurança. Como cada identidade deve estar associada a um par de chaves criptográficas, convencionou-se que as chaves utilizadas por um dispositivo IoT devem ser geradas localmente no dispositivo, de forma a evitar a transmissão de chave privada via Internet. Uma vez que o dispositivo é implantado, cabe ao administrador do *Entity Manager* registrar a identidade do dispositivo associada a respectiva chave pública. Cada portador de identidade deve manter de forma segura sua chave privada enquanto a chave pública é registrada em sua identidade na *blockchain*. Através de assinaturas digitais, é possível utilizar as identidades digitais para identificação, autenticação mútua, controlar acesso, etc.

4.3. Integração com a Plataforma InterSCity

Após a implementação do modelo, desenvolveu-se uma infraestrutura de segurança voltada para coleta, distribuição e acesso aos dados na plataforma InterSCity. Esta infraestrutura de segurança utiliza o modelo proposto para assegurar canais seguros de comunicação, com autenticação e controle de acesso de escrita de dados na plataforma.

O InterSCity é um projeto colaborativo de pesquisa que abrange nove instituições nacionais e parceiros internacionais. A plataforma InterSCity [Del Esposte et al. 2017] foi criada para dar suporte ao desenvolvimento de projetos e aplicações de IoT, Big Data e Computação em Nuvem. Através da plataforma, pode-se registrar dados de sensoriamento de uma CI em termos de recursos de capacidades. Um ônibus inteligente é um exemplo de recurso, que pode ser modelado de forma a possuir capacidades de temperatura, intensidade de ruído e coordenadas geográficas. Uma vez que algum dispositivo efetue essas leituras de sensoriamento e registre os dados na plataforma, uma aplicação de mobilidade urbana pode consultar a plataforma para obter o valor da temperatura ou quaisquer outras capacidades daquele recurso específico (*i.e.*, ônibus inteligente).

A plataforma InterSCity não contava com mecanismos de autenticação e controle de acesso, de forma que uma instância do InterSCity não conseguia diferenciar produtores de dados ou impedir que algum produtor se passe por outro. Utilizando o modelo proposto para gerenciamento de identidades baseado em *blockchain*, desenvolveu-se uma infraestrutura de segurança para garantir mecanismos de autenticação e controle de acesso na escrita de dados. Para isto, desenvolveu-se dois componentes de *software* denominados *Secure Resource Adaptor* e *IoT Cataloguer*. O componente *Secure Resource Adaptor* atua como uma extensão de um componente pré-existente no InterSCity (i.e., Resource Adaptor), anteriormente na plataforma o *Resource Adaptor* apenas recebia o dado e o inseria na plataforma sem qualquer tipo de verificação. Estendeu-se o conceito de recursos de capacidades do InterSCity introduzindo o conceito do dispositivo IoT, que deve possuir uma identidade e publicar dados sobre as capacidades de um determinado recurso. O componente *IoT Cataloguer*, é responsável por manter um mapeamento relacionando o dispositivo IoT, sua identidade na *blockchain*, o recurso e as capacidades associadas a este dispositivo. A entidade administrativa, através do *Entity Manager*, tem direito de registrar

estes relacionamentos no *IoT Cataloguer* e assinaturas digitais são utilizadas para garantir que apenas o *Entity Manager* emissor da identidade do dispositivo pode adicionar as permissões de escrita. Estas permissões de escrita, ou seja, quais dispositivos podem publicar sobre quais recursos e capacidades, são consultadas pelo *Secure Resource Adaptor* que tem agora a responsabilidade de receber os dados e garantir a autenticação e controle de acesso. Cada dispositivo que deseje enviar dados a plataforma deve antes se autenticar com o *Secure Resource Adaptor* para obtenção de um *token de acesso*. O processo de autenticação consiste em verificar uma assinatura digital para confirmar a identidade do dispositivo, verificar uma lista de *Entity Managers* válidos e obter as permissões de acesso do dispositivo autenticado. Essas informações são codificadas em um *token* JWT, com validade parametrizável, que é retornado ao dispositivo. Em posse do *token*, o dispositivo pode enviar os dados de forma a ser identificado pelo *Secure Resource Adaptor* onde são garantidas as políticas de acesso à escrita do dado. Assim, pode-se distribuir de forma segura os dados de dispositivos para armazenamento na plataforma InterSCity, através canal seguro de comunicação, com autenticação e controle de acesso. Também impede-se que um dispositivo não cadastrado possa enviar dados, ou até se passar por outro dispositivo. Para garantir a confidencialidade no canal de comunicação utilizou-se o TLS [2].

A Figura 2 ilustra a arquitetura geral da solução proposta, onde dispositivos podem inserir dados na plataforma InterSCity, através do componente `Secure Resource Adaptor`, de forma segura utilizando o modelo de gestão de identidades proposto e a infraestrutura de segurança desenvolvida.

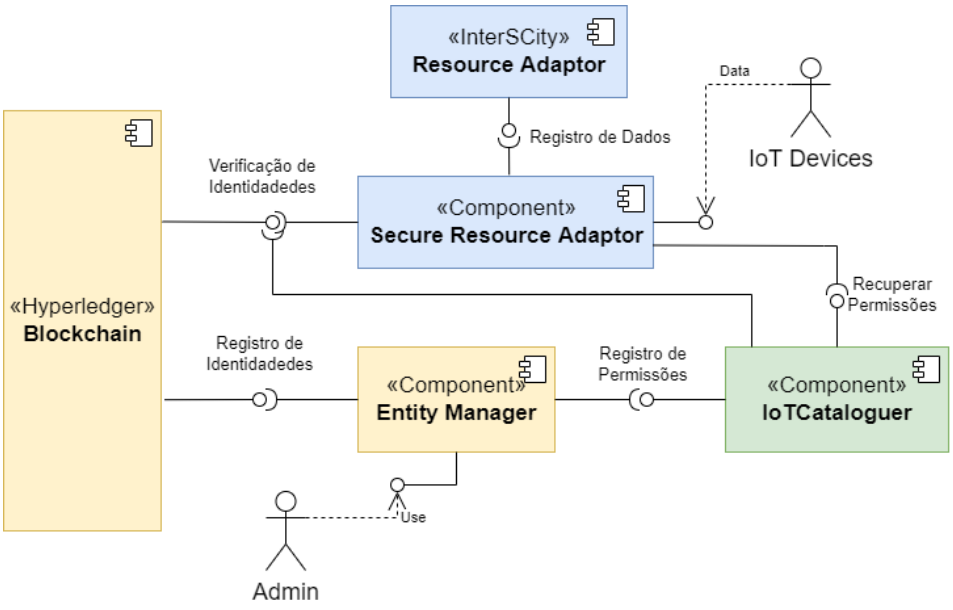

Figura 2. Arquitetura geral da solução proposta.

A Figura 3 apresenta o diagrama de sequência que descreve todo o processo de implantação de um dispositivo até a publicação do dado na plataforma InterSCity. Primeiramente as chaves são geradas no dispositivo, e então, através do *Entity Manager*, sua

[2]https://www.internetsociety.org/deploy360/tls/basics/

identidade é registrada na *blockchain* pelo administrador. Após isso o dispositivo deve autenticar-se ao *Secure Resource Adaptor* para obtenção do *token* e em posse do *token* o dado pode ser inserido de forma segura.

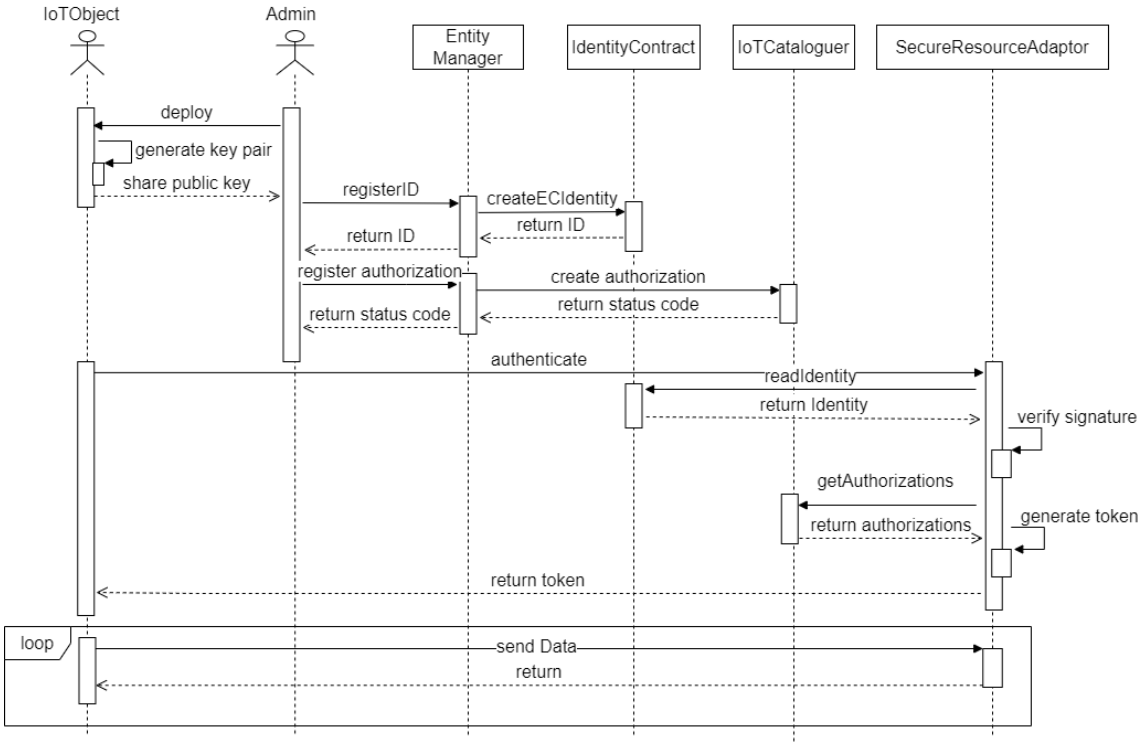

Figura 3. Diagrama de sequência correspondente ao processo de registro de dispositivos, autenticação e envio de dados a plataforma InterSCity.

5. Estudo de Caso e Avaliação

5.1. Estudo de Caso

Para validar a solução proposta, desenvolveu-se um estudo de caso voltado para gestão de energia elétrica em um campus universitário. Este estudo de caso utiliza o modelo proposto de gestão de identidades para simular um *smart meter* instalado em um campus universitário. O *smart meter* faz medições periódicas de corrente, potência e energia consumida e as transmite para a plataforma InterSCity. Neste cenário, por meio do componente `Entity Manager`, as universidades geram identidades para os *smart meters* instalados ao longo do campus.

Desenvolveu-se uma aplicação JAVA que simula o comportamento do *smart meter*. A aplicação gera suas chaves criptográficas, que posteriormente são registradas na *blockchain*. Antes de enviar os dados para a plataforma InterSCity, a aplicação simulada gera uma assinatura digital e então autentica-se junto ao `Secure Resource Adaptor` para a obtenção do *token*. Após autenticada, a aplicação envia os dados para a plataforma InterSCity. Os dados simulados são provenientes do *dataset* COMBED [Batra et al. 2014], que traz leituras de corrente, energia e potência de 200 *smart meters* instalados em um campus universitário. Através deste estudo de caso, mostra-se que é possível desenvolver aplicações seguras para CI utilizando o modelo proposto. Os

dados são inseridos na plataforma InterSCity através de um canal seguro de comunicação com os mecanismos de autenticação e controle de acesso propostos.

Por meio de estudos de caso como este, pode-se identificar os padrões de consumo de energia, picos de corrente elétrica e até equipamentos defeituosos. Torna-se possível também gerar alertas que indicam consumo excessivo. Tais informações podem ajudar a gerir melhor o consumo de energia levando a maior economia de recursos públicos.

5.2. Avaliação

Aproveitou-se o cenário do estudo de caso para avaliar a infraestrutura de segurança implementada a partir do modelo proposto para gestão de identidade. Optou-se por avaliar a aplicação que simula um dispositivo IoT, enviando dados para plataforma InterSCity. Esta escolha se deve ao fato de que dispositivos IoT geralmente apresentam restrições em seus recursos computacionais, assim, mecanismos de segurança adequados para IoT não devem ser muito custosos. O objetivo desta avaliação é determinar o custo adicional, em termos de consumo de memória e processamento, para um dispositivo IoT, que utiliza a infraestrutura de segurança recém-adicionada ao InterSCity. Além disso, também deseja-se avaliar o tempo de resposta médio para obtenção do *token* de acesso, necessário para publicação segura de dados a partir do `Secure Resource Adaptor`. Os três experimentos foram executados em um computador *Desktop* com 16G de memória RAM, e processador AMD Ryzen 5 2600.

O primeiro experimento avalia o consumo máximo de memória por parte da aplicação Java que simula um disposto IoT, assim, o experimento prosseguiu conforme roteiro a seguir. Inicialmente, sem utilizar a infraestrutura de segurança, a aplicação faz a leitura dos dados provenientes do *dataset* e os envia ao InterSCity durante 10 minutos. O envio de dados ocorre à uma frequência de meio segundo. Através da ferramenta de *profiling* `JProfiler` [3] foi medido o consumo de memória instantâneo a cada segundo pela aplicação. Após os 10 minutos, registrou-se apenas o consumo máximo de memória durante esse intervalo. Da mesma forma, o procedimento foi repetido, desta vez utilizando a infraestrutura de segurança com os mecanismos de autenticação e controle de acesso, e o protocolo TLS para garantir confidencialidade no envio das mensagens. Novamente o consumo máximo de memória ao longo dos 10 minutos foi coletado.

Duração	Segurança Habilitada	Consumo Máximo de Memória
10 min	Não	28,19 MB
10 min	Sim	31,64 MB

Tabela 1. Resultado do consumo máximo de memória utilizada (em MB), por parte da aplicação que simula o dispositivo IoT, ao longo de 10 minutos, com e sem a utilização da infraestrutura de segurança.

Conforme ilustra a Tabela 1, houve diferença no consumo máximo de memória ao longo dos 10 minutos. Houve um aumento no consumo máximo de memória de 12,32%.

O segundo experimento avalia o tempo de processamento gasto pela aplicação, assim, o experimento prosseguiu conforme roteiro a seguir. Inicialmente, sem utilizar a infraestrutura de segurança, o dispositivo faz a leitura dos dados provenientes do *dataset*

[3]https://www.ej-technologies.com/products/jprofiler/overview.html

e os envia ao InterSCity durante 5 minutos. Neste experimento, os dados são enviados a uma frequência alta, ou seja, as requisições são feitas imediatamente uma após a outra. Utilizou-se a ferramenta `VisualVM` para obter o tempo efetivo de processamento (CPU Time) que foi utilizado pela aplicação ao final dos 5 minutos de execução. Estes mesmos passos foram repetidos utilizando a infraestrutura de segurança.

Duração	Segurança Habilitada	Tempo Efetivo de Processamento
5 min	Não	1625,00 ms
5 min	Sim	1687,50 ms

Tabela 2. Tempo efetivo de processamento em milissegundos utilizado pela aplicação que simula o dispositivo IoT, ao final de 5 minutos de execução, com e sem a utilização da infraestrutura de segurança.

Conforme ilustra a Tabela 2, o tempo efetivo de processamento gasto pela aplicação ao se utilizar a infraestrutura de segurança apresentou valores maiores em relação ao não uso da infraestrutura. A diferença percentual entre os valores indica um acréscimo de 3,846% no custo de processamento ao se utilizar a infraestrutura de segurança.

Por fim, o último experimento tem o objetivo de avaliar o tempo de resposta para obtenção do *token* na aplicação que simula o dispositivo IoT. Neste experimento, o processo de autenticação é efetuado 1000 vezes e ao final de cada autenticação armazena-se o tempo decorrido. O processo de autenticação consiste nos seguintes passos: leitura de sua chave privada, geração de uma assinatura digital, envio da assinatura para o *Secure Resource Adaptor*, recebimento do *token* por parte do *Secure Resource Adaptor*. Este processo foi repetido 1000 vezes e foi calculado a média, moda, mediana e desvio padrão relativo ao tempo de resposta para obtenção do *token*.

Requisições	Média	Desvio Padrão	Min	Max	Mediana	Moda
1000	52,77 ms	17,96 ms	41,0 ms	525,0 ms	50,0 ms	47,0 ms

Tabela 3. Avaliação do tempo de resposta, em milisegundos, para obtenção do token: média, desvio padrão, moda, mediana, valores mínimo e máximo obtidos.

A Tabela 3 exibe as estatísticas básicas em relação ao tempo de resposta para obtenção do *token*, foram efetuadas 1000 requisições de autenticação (i.e., solicitação de token). Conforme podemos observar, o tempo máximo para requisições foi de 525 ms, enquanto o valor médio foi de 52,77 ms. O desvio padrão apresenta um valor alto em relação a média, o que pode indicar que existe grandes variações entre os valores, apesar disso, percebe-se que a média esta relativamente distante do valor máximo, o que indica que existem poucas ocorrências de valores próximos ao valor máximo de tempo de resposta. Precisamente, apenas a primeira requisição ocupou o tempo de resposta na ordem de 500 ms, todas as outras apresentaram valores menores. Isto ocorre pois em cada requisição ao *Secure Resource Adaptor*, este deve consultar a *blockchain* para validar a identidade do dispositivo antes de emitir o *token*. A primeira requisição apresenta valores altos pois a conexão com a *blockchain* ainda não esta aberta, e uma vez que a conexão é aberta e mantida as outras requisições acontecem em tempo menor.

6. Discussão e Conclusão

Conforme podemos observar a partir dos resultados obtidos, determinado custo em uso de memória e processamento é adicionado a um dispositivo de IoT que faz uso do modelo proposto e implementado neste trabalho. Precisamente, há um aumento de 12,32% em relação ao uso máximo de memória e um acréscimo de 3,846% de tempo efetivo de processamento. Apesar deste custo, o uso do modelo proposto para assegurar a inserção de dados na plataforma InterSCity é opcional, ficando a critério dos responsáveis pela plataforma em trocar desempenho por segurança. Para tentar reduzir os custos dos processos de autenticação e controle de acesso, a solução proposta faz o uso de *tokens* que são válidos por período de tempo parametrizável, não sendo necessário o dispositivo se autenticar toda vez que envia dados. O uso de um mesmo *token*, por um período de tempo, reduz os custos relativos ao processo de autenticação do dispositivo, mas também do processo de verificação de integridade do dispositivo por meio do *Secure Resource Adaptor*, uma vez que este componente apenas *tokens* verificados emitidos por si. O modelo mostra-se adequado, uma vez que em um ambiente de IoT existem dispositivos com restrições de recursos computacionais.

O modelo proposto para gerenciamento distribuído de identidades, baseado na tecnologia *blockchain*, mostrou-se eficiente e capaz de servir de base para o desenvolvimento de infraestruturas de segurança, considerando o ambiente de uma cidade inteligente onde podem existir diversos produtores de dados, e entidades independentes que administram a cidade em conjunto. Além de identificar as entidades gerais (i.e., dispositivos IoT, etc) que são controladas por entidades administrativas (i.e., secretarias, prefeituras, etc), foi possível desenvolver uma infraestrutura com um mecanismos para garantir um canal seguro de comunicação com confidencialidade (TLS), autenticação e controle de escrita de dados de dispositivos.

Além disso, impede-se que dispositivos se passem por outros ao publicar dados na plataforma InterSCity. Através do modelo proposto e da infraestrutura implementada, pode-se identificar e gerenciar os dispositivos implantados na cidade, assim como garantir que os dados produzidos são inseridos de forma segura na plataforma, possibilitando-se assim o desenvolvimento de aplicações de cidades inteligentes que exigem requisitos básicos de segurança. Além disso, a emissão de identidades para atores de uma CI, de forma descentralizada, estimula a descentralização do processo de controle de uma CI. Isto tem impactos positivos para governança da cidade, pois descentraliza o poder, e também para a disponibilidade dos serviços ofertados pela cidade pois as informações de identidade estão armazenados de forma distribuída.

As identidades que compõe o modelo são flexíveis e podem ser utilizadas para identificar quaisquer atores que existam em uma cidade inteligente, apesar disso não foram abordadas questões de privacidade. Desta forma, apesar de possível, não é adequado utilizar estas identidades para armazenar informações pessoais de cidadãos. Como perspectivas futuras deste trabalho, pretende-se explorar conceitos como Identidades Autosoberanas, onde o controle da identidade é feito inteiramente pelo portador. De forma que além de dispositivos, serviços ou componentes de *software*, usuários também possam ter identidades de forma a resguardar sua privacidade. No futuro, espera-se explorar as identidades de usuários para desenvolver mecanismos de sensoriamento participativo e oportunístico com o auxílio dos residentes da cidade.

7. Agradecimentos

Esta pesquisa é parte do INCT da Internet do Futuro para Cidades Inteligentes, financiado por CNPq (proc. 465446/2014-0), Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001 e FAPESP (procs. 14/50937-1 e 15/24485-9). O autor Bruno Rotondaro também recebeu apoio do programa PROCAD, CAPES, processo 88887.200532/2018-00. Arlindo F. da Conceição foi parcialmente apoiado pelo projeto SmartMed, Research Council of Norway, projeto 288106.

Referências

Alamer, M. and Almaiah, M. A. (2021). Cybersecurity in smart city: A systematic mapping study. In *2021 International Conference on Information Technology (ICIT)*, pages 719–724. IEEE.

Batra, N., Parson, O., Berges, M., Singh, A., and Rogers, A. (2014). A comparison of non-intrusive load monitoring methods for commercial and residential buildings. *arXiv:1408.6595*.

Bertino, E. and Takahashi, K. (2010). *Identity management: Concepts, technologies, and systems*. Artech House.

da Conceição, A. F. and Rocha, V. E. M. (2020). *Blockchain: conceitos básicos*. Amazon Kindle.

Del Esposte, A. M., Kon, F., Costa, F. M., and Lago, N. (2017). Interscity: A scalable microservice-based open source platform for smart cities. In *SMARTGREENS*, volume 1, pages 35–46.

Dunphy, P. and Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. *IEEE security & privacy*, 16(4):20–29.

El Haddouti, S. and El Kettani, M. D. E.-C. (2019). Analysis of identity management systems using blockchain technology. In *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, pages 1–7. IEEE.

Ghaffari, F., Gilani, K., Bertin, E., and Crespi, N. (2022). Identity and access management using distributed ledger technology: A survey. *International Journal of Network Management*, 32(2):e2180.

ITU, I. T. U. (2009). *NGN identity management framework*. International Telecomunication Union, itu-t y2720 edition.

Jones, M. (2015). Json web key (jwk). Technical report, Internet Engineering Task Force (IETF).

Khan, M. A. and Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395–411.

Kikitamara, S., van Eekelen, M., and Doomernik, D. I. J.-P. (2017). Digital identity management on blockchain for open model energy system. *Unpublished Masters thesis–Information Science*.

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., and Choo, K.-K. R. (2020). Blockchain-based identity management systems: A review. *Journal of network and computer applications*, 166:102731.

Manohar, A. and Briggs, J. (2018). Identity management in the age of blockchain 3.0. *Workshop HCI for Blockchain*.

Mektoubi, A., Hassani, H. L., Belhadaoui, H., Rifi, M., and Zakari, A. (2016). New approach for securing communication over mqtt protocol a comparaison between rsa and elliptic curve. In *2016 Third International Conference on Systems of Collaboration (SysCo)*, pages 1–6. IEEE.

Mikula, T. and Jacobsen, R. H. (2018). Identity and access management with blockchain in electronic healthcare records. In *2018 21st Euromicro conference on digital system design (DSD)*, pages 699–706. IEEE.

Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., and Scorrano, F. (2014). Current trends in smart city initiatives: Some stylised facts. *Cities*, 38:25–36.

Preukschat, A. and Reed, D. (2021). *Self-sovereign identity*. Manning Publications.

Rahat, A. H., Rumon, M. R., Joti, T. J., Tasnin, H., Akter, T., Shakil, A., and Hossain, M. I. (2022). Blockchain based secured multipurpose identity (smid) management system for smart cities. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0737–0744.

Santos, J. P. N. d. (2018). Identity management in healthcare using blockchain technology. Master's thesis, Universidade de Évora.

Tracy, K. (2008). Identity management systems. *IEEE Potentials*, 27(6):34–37.

Venkatraman, S. and Parvin, S. (2022). Developing an IoT identity management system using blockchain. *Systems*, 10(2):39.

Wang, S., Li, H., Chen, J., Wang, J., and Deng, Y. (2022). DAG blockchain-based lightweight authentication and authorization scheme for IoT devices. *Journal of Information Security and Applications*, 66:103134.

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., and Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(3):2794–2830.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., and Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine*, 55(1):122–129.