Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Proposta de Um Método de Controle de Acesso Baseado em Atributo em Redes Dispositivo a Dispositivo

Fernando Luis Alfeld

JUIZ DE FORA
DEZEMBRO, 2023

Proposta de Um Método de Controle de Acesso Baseado em Atributo em Redes Dispositivo a Dispositivo

Fernando Luis Alfeld

Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Bacharelado em Ciência da Computação

Orientador: Edelberto Franco Silva

JUIZ DE FORA

DEZEMBRO, 2023

Proposta de Um Método de Controle de Acesso Baseado em Atributo em Redes Dispositivo a Dispositivo

Fernando Luis Alfeld

MONOGRAFIA SUBMETIDA AO CORPO DOCENTE DO INSTITUTO DE CIÊNCIAS EXATAS DA UNIVERSIDADE FEDERAL DE JUIZ DE FORA, COMO PARTE INTEGRANTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE BACHAREL EM CIÊNCIA DA COMPUTAÇÃO.

Aprovada por:

Edelberto Franco Silva
Doutor em Ciência da Computação

Alex Borges Vieira
Doutor em Ciência da Computação

Luciano Jerez Chaves
Doutor em Ciência da Computação

Leonardo Vieira dos Santos Reis
Doutor em Ciência da Computação

JUIZ DE FORA

11 DE DEZEMBRO, 2023

Resumo

As comunicações dispositivo a dispositivo (D2D) referem-se a uma tecnologia que permite ligações diretas entre dispositivos, sem o envolvimento de infraestruturas de rede fixa, como pontos de acesso ou estações rádio base. Sua aplicação permite que dispositivos da Internet das Coisas (IoT) se comuniquem via Wi-Fi em modo *ad hoc*, ou por tecnologias ponto a ponto, como o Bluetooth. Para construir conexões D2D sustentáveis, é necessário possuir um controle de acesso dinâmico que trate adequadamente de questões de segurança e privacidade na troca de mensagens pela rede. O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos e condições ambientais, como hora do dia e local, atribuídos a usuários e aos recursos. Desta forma, este trabalho estuda o ABAC, para, através de validações, avaliar quais atributos são mais relevantes no ambiente D2D.

Palavras-chave: Dispositivo a Dispositivo, Controle de Acesso Baseado em Atributos, IoT, Cibersegurança.

Abstract

Device-to-device (D2D) communications is a technology that allows direct connections between devices without involving fixed network infrastructures, such as access points or radio base stations. Its application allows Internet of Things (IoT) devices to communicate via Wi-Fi in *ad hoc* mode or via peer-to-peer technologies, such as Bluetooth. Building sustainable D2D connections requires dynamic access control that adequately addresses security and privacy issues when exchanging messages over the network. Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes and environmental conditions, such as time of day and location, assigned to users and resources. Therefore, this work seeks to study ABAC and other access control models to, through validations, evaluate which attributes are most relevant in the D2D environment.

Keywords: Device to Device, Attribute-based Access Control, IoT, Cybersecurity.

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Abreviações

D2D	*Device to device* - Dispositivo a dispositivo
ABAC	Controle de acesso baseado em atributo
RBAC	Controle de acesso baseado em função
IoT	*Internet of things* - Internet das coisas
UA	Unidade Certificadora
PIP	*Policy Information Point* - Ponto de Informação de Política
PAP	*Policy Administration Point* - Ponto de Administração de Política
PEP	*Policy Enforcement Point* - Ponto de Execução de Política
PDP	*Policy Decision Point* - Ponto de Decisão de Política
SpEL	*Spring Expression Language* - Linguagem de expressão spring

1 Introdução

1.1 Apresentação do tema

Atualmente, cada vez mais pessoas e empresas estão aderindo seus equipamentos e processos a dispositivos com diversos tipos de conexões e funcionalidades. Isso se dá por conta do desenvolvimento rápido que as comunicações sem fio e móvel têm promovido, além da popularização de dispositivos ligados à IoT (Internet das Coisas - *Internet of Things*). Uma das maiores motivações, nesses casos, visa melhorar o desempenho dos dispositivos, funcionalidades, monitoramento, troca de mensagens e consumo de energia (YAN et al., 2018).

Porém, um ponto relevante nesse contexto é a segurança e privacidade. Com o passar do tempo, os cenários, soluções e dispositivos foram evoluindo, surgindo novas formas de controlar o acesso ao ambiente - os chamados controles de acesso - que tentam refletir melhor as novas demandas (BHATT; SANDHU, 2020). Uma das maiores demandas relacionadas às comunicações dispositivo a dispositivo (D2D - *Device-to-Device*), que referem-se a uma tecnologia de interconexão na qual é possível a ligação direta entre dispositivos, sem envolvimento direto de infraestruturas de rede fixa (BHATT; SANDHU, 2020). Da mesma forma que a comunicação direta entre dispositivos pode facilitar a criação da rede, a falta de um ponto central gera um desafio frente à gestão e à segurança (ASADI; WANG; MANCUSO, 2014).

Dispositivos autônomos e uma grande quantidade de dados associados a eles têm alimentado pesquisas significativas em controle de acesso D2D e privacidade na academia e na indústria (YAN et al., 2018). Para construir uma rede D2D com crescimento sustentável, é totalmente necessário possuir um controle de acesso dinâmico e controle de comunicação estruturado que trate adequadamente de questões de segurança e privacidade na rede.

Existem diversos métodos de controle de acesso associados à autorização, como baseados em papéis (RBAC - *Role-based Access Control*), listas de controle de acesso

(ACL - *Access Control List*), baseados em risco (RbAC - *Risk-based Access Control* e o controle de acesso baseado em atributos (ABAC - *Attribute-based Access Control*) (SILVA; MUCHALUAT-SAADE; FERNANDES, 2018). Resumidamente, o ABAC é uma estratégia de autorização que define permissões com base em atributos e condições ambientais. Esses atributos podem corresponder à hora do dia, localização, atributos de usuários ou recursos, e assim criar uma única política de ABAC ou um pequeno conjunto de políticas para seus dispositivos (HU et al., 2015).

Desta forma, visando melhorar a segurança das redes D2D em IoT, é necessário o estudo aprofundado das várias implementações de controle de acesso no ambiente. Validar ou propor a aplicação do métodos ABAC no contexto, além de realizar avaliações por simulação detalhada, a fim de definir qual a melhor implementação de controle de acesso para o ambiente D2D.

Cada controle de acesso possui um fator de atrito, no qual o termo atrito em relação a uma conexão, em ambientes tecnológicos, refere-se à resistência ou dificuldade encontrada durante o estabelecimento ou manutenção da conexão entre dois dispositivos, sistemas ou entidades. O atrito pode ser causado por uma variedade de fatores que influenciam a eficiência, velocidade e confiabilidade da comunicação entre as partes envolvidas. Em nossa proposta o termo atrito está relacionado à usabilidade e experiência do usuário, como interfaces complexas ou procedimentos complicados, podem adicionar atrito à conexão. Ou seja, quanto maior a quantidade de interação do usuário para que a conexão ocorra maior será o atrito, e quanto menor a quantidade e dificuldade da interação menor será o atrito.

1.2 Motivação

Os dispositivos e aplicativos atualmente já possuem suporte a diversos tipos de controles de acesso em suas configurações. Porém, é necessário para cada ambiente investigar e definir o modelo de controle de acesso que melhor se aplica. Por exemplo, em um cenário de recursos computacionais, talvez o melhor acesso seja somente baseado em papéis, RBAC, porém em um ambiente hospitalar, o modelo baseado em risco pode ser mais interessante. Em ambientes de larga escala e que necessitam de maior autonomia, o modelo ABAC é

um dos mais recomendados. Assim, percebemos como o tema cresce a cada dia com a motivação dos novos dispositivos e as demandas de uso (HSU; FAN; WANG, 2021).

O estudo e os testes das diferentes combinações de parâmetros/atributos e dados usados para o ABAC está em evolução (BHATT; SANDHU, 2020), porém ainda é difícil definir quais os melhores atributos devem ser utilizados para garantir uma segurança e a redução de falsos positivos (acesso permitido de forma equivocada) e falsos negativos (acesso negado de forma equivocada).

Atualmente o uso do ABAC e suas derivações em redes D2D pode ser vista no trabalho sobre dispositivos IoT produzido por Smriti Bhatt (BHATT; SANDHU, 2020), e também seu uso em empresas de IAM (Gestão de Identidade e Acesso - *Identity and Access Management*) como a Incognia[1] que funciona da seguinte forma, segundo a própria empresa:

> *Funciona como um fingerprint de localização, que está em constante atualização e que não requer captura ou processamento de nenhum dado pessoal adicional do usuário. A tecnologia de Incognia atua na prevenção de fraude através da verificação da localização do usuário no momento do login, confrontando com o padrão de localização histórico e utiliza a biometria comportamental por localização para entregar um score de risco ultra preciso nesta verificação, para uma autenticação segura e sem fricção para usuários legítimos.* (INCOGNIA, 2021).

1.3 Objetivos

O objetivo deste trabalho é reduzir os problemas atuais em relação à conexão segura e acesso a dados de dispositivos IoT. Ao realizar um estudo aprofundado e selecionar cuidadosamente os atributos mais adequados, propo uma implementação do Controle de Acesso Baseado em Atributos (ABAC) no ambiente Dispositivo a Dispositivo (D2D) de IoT.

Podemos destacar os seguintes objetivos específicos:

- Estudar o protocolo ABAC, assim como suas variantes.
- Categorizar os parâmetros/atributos por objetivos.
- Criação de uma autoridade certificadora que controle chaves para autenticação dos

[1] ⟨https://www.incognia.com/pt/⟩

dispositivos.

- Concluir quais os melhores atributos para utilizar, observando também o impacto que cada um pode trazer em relação ao tempo/atrito.

- Proposta e validação do controle de acesso ABAC para o ambiente D2D.

2 Fundamentação Teórica

2.1 IoT

A Internet possibilitou uma verdadeira transformação na maneira que a sociedade se relaciona. A sua ampliação, aumento da velocidade e diminuição dos aparelhos telefônicos, transformando-os em *smartphones* que conseguem alterar a percepção de realidade, cria novos modelos de interações humanas, ampliando espaços e cultura (ALVES; CAMPOS; BRITO, 1999). De acordo com o site (Convergência Digital, 2023) são ao todo 8,4 bilhões de *smartphones* ativos no mundo. Grande parte dessa penetração de usuários se dá pelo uso da "Internet das coisas".

IoT(*Internet of Things*) que em uma tradução direta significa a internet das coisas, na qual essas "coisas" podem ser diversos tipos de dispositivos, como por exemplo: sensores de alertas, biochips em pessoas, tratores e sensores para áreas agrícolas, sensores em veículos, dispositivos empresariais e outras infinidades de dispositivos que aumenta a cada dia e com diversas funcionalidades e objetivos. "Não se trata apenas de uma tecnologia, mas da nova fronteira em que a internet está se aprofundando" (FACCIONI, 2016).

Um dispositivo IoT de maneira geral possui um ambiente preparado para sistemas web, assim como processador, sensores, antenas e placas de rede (comunicação) para que possam coletar, enviar e receber informações, que se conecta a um gateway ou outra ponte de conexão para enviar e receber dados para a nuvem e também para se comunicarem diretamente entre si sem precisar de um intermediário que pode ser chamada de conexão *device to device* (dispositivo a dispositivo). Isso permite que os dispositivos conversem entre si e também recebam e enviem dados e/ou comandos a outros dispositivos e pessoas.

A conexão, rede e protocolos de comunicação podem variar dependendo das especificações do próprio dispositivo IoT e ambiente, além de poderem possuir conexões com motores de movimentos o que torna o uso abrangente em indústrias nas quais as máquinas coletam e compartilham dados com outros dispositivos conectados repassando

apenas dados mais relevantes.

2.2 Benefícios e importância dos dispositivos IoT

Os dispositivos permitem que as pessoas vivam e trabalhem de maneira mais inteligente através de automações residenciais e industriais, permitindo monitoramento em tempo real e acompanhamento de processos. Se usado de maneira correta e inteligente isso o faz capaz de economizar custos em tempo de diversos processos, interações, aumentar a produtividade e ajudar a tomar melhores decisões com base nos dados.

Há muitas aplicações possíveis também na área da saúde permitindo assim salvar mais vidas, na área agrícola monitorando as plantações e uso de máquinas, também nos setores de construção nas quais as máquinas podem ser controladas de forma contínua e remota. Em empresas, um dispositivo pode ser usado para controle de estoque, otimizando o tempo de contato com os clientes e ajudando a tomar melhores decisões de acordo com a experiência gerada pelo usuário. Em carros elétricos, os dispositivos e sensores são capazes de detectar problemas do veículo coletando seus dados. Nas "*smart homes*"(casas inteligentes/tecnológicas) trancas, janelas e alarmes são controladas por IoT. Muitos setores estão passando por uma série de transformações digitais, cada vez maiores, mais rápidas e eficientes. (MANCINI, 2018) resume a usabilidade

> *A Internet das Coisas proporciona aos objetos do dia a dia, com capacidade computacional e de comunicação, se conectarem à internet. Essa conexão viabilizará controlar remotamente os objetos, e acessá-los como provedores de serviços, e se tornarão objetos inteligentes ou smart objects. Os objetos inteligentes possuem capacidade de comunicação e processamento aliados a sensores.* (MANCINI, 2018).

Em todos os casos, o que um dispositivo IoT gera, na prática, é a redução de custos com infraestruturas e pessoas envolvidas nos processos, aumentando a fluidez em atendimentos, a segurança e a rapidez na coleta de dados pertinentes a cada processo. Possibilitando assim a tomada de decisão em cada caso é mais assertiva e fluida.

2.3 Desafios e Dificuldades de Segurança

Com o crescente uso, abrangência e variedades de dispositivos as dificuldades e pontos de desafios também crescem, como por exemplo conectividade e principalmente a parte de segurança e privacidade dos dispositivos e redes.

Cada dispositivo e rede tem suas particularidades relacionadas à segurança. Por exemplo, dispositivos que se conectam pela nuvem correm o risco de receberem ataques *hackers* pela internet; dispositivos que não possuem a conexão com a internet também podem ser vulneráveis a ataques se estiverem próximos fisicamente ou integrando o mesmo perímetro de uma rede local.

Se o número de benefícios e vantagens de se usá-los é grande, os riscos de uma invasão maliciosa é tão grande quanto. Por exemplo, se uma casa com diversos dispositivos é invadida e consegue-se controlá-los e monitorá-los, grandes danos podem ser gerados. O mesmo vale para empresas, fábricas, veículos e tudo que tenha um meio de conexão estão passíveis de ataques, por isso um ponto muito importante é a parte de segurança, tanto em conexão na nuvem quanto em conexões dispositivo a dispositivo.

Assim, como o número de dispositivos IoT crescem conforme as necessidades de automação de cada setor, a atualização das formas de invadi-los são rapidamente feitas. Por isso, é importante que ao automatizar cada processo seja incluído como prioridade um modelo de segurança capaz de prever e barrar esses hackers. Para cada forma de IoT há um modelo de segurança que se apresenta como mais adequado na mitigação ou prevenção de tais vulnerabilidades.

Um dos desafios de se garantir tal segurança nos dispositivos é por ter que lidar com diversos dispositivos diferentes que acabam por se integrarem. Dessa forma, é preciso criar camadas de segurança em cada um para que os ataques fossem dificultados.

Há algumas maneiras básicas de se prevenir ataques aos dispositivos IoT: i) limitando em cada dispositivo o acesso do usuário de acordo com a função que ele precisará exercer; ii) personalizando senhas e monitorando os dispositivos em tempo real, identificando assim atividades suspeitas (fora do perfil esperado); iii) mantendo atualizadas as versões dos sistemas e suas bibliotecas.

2.4 Modelos de Segurança e Estratégias

Por ser tão importante manter acessos aos dispositivos seguros, a indústria e o meio acadêmico vem fazendo diversos estudos, melhorias e atualizações nesta área a fim de tornar as IoT menos vulneráveis aos ataques hackers.

A implementação de padrões de segurança que já estão disponíveis no mercado dificulta os ataques cibernéticos, e consegue-se identificar diversos desses modelos que já são utilizados nos dispositivos. Dentre esses modelos, encontram-se os métodos de autenticação e de autorização e controle de acesso. Apresentaremos os principais métodos resumidamente e mais a frente o método de control de acesso baseado em atributos com mais detalhes.

Um dos mais tradicionais métodos de controle de acesso é o RBAC (*Role-based access control*). Este é um método que restringe o acesso a rede baseando-se em regras para cada usuário dentro da organização, que podem ser definidas usando diferentes fatores como nível de responsabilidade de cada usuário, ou competência (DIAS, 2018). E assim conceder ou limitar o acesso de cada usuário aos recursos.

Já o PBAC (*Policy-based access control*) determina os direitos de acesso avaliando as políticas que regem as ações do usuário no recurso baseando em atributos e regras. Por exemplo, o usuário 'aluno' só pode acessar ao sistema 'SIGA' no horário compreendido entre '00:00 de Segunda às 23:59 de Sexta'. A ideia central desse modelo é conceder acesso mediante o entendimento prévio em que um dado pode ser coletado ou acessado" (OLIVEIRA et al., 2023). Porém, em geral, seu código de políticas está presente diretamente no controlador do acesso ao recurso, o que pode ser um limitador para a escalabilidade.

Por fim, temos modelos de autenticação, como o SSO (*Single sign-on*), na qual através de login único se permite que o usuário tenha acesso a múltiplas aplicações e dispositivos. Também o OAuth e OAuth2 (OIDC - *OpenID Connect*), qué é um modelo que funciona de maneira que um recurso se autentique a outro, sendo muito utilizado para comunicação entre serviços distintos e logins em múltiplos serviços.

Além destes, temos o método de controle de acesso baseado em atributos, que será foco deste estudo.

2.5 ABAC

O ABAC (*Attribute-based access control*) é de um modelo de autorização que usa os atributos e características, ao invés de um conjunto de regras com a intenção de proteger tanto dados, redes de dispositivos, recursos de ti de usuários não autorizados mas também definir quais características e parâmetros são necessários e o nível de relevância de cada um ou seja, com o ABAC é possível definir as políticas de acesso e tomar decisões baseadas em atributos, ações, variáveis de ambiente em um determinado acesso o que pode ser muito útil se tratando de acesso a cada dispositivo em específico.

O PEP (*Policy Enforcement Point* - Ponto de Execução de Política) está localizado na fronteira do sistema e é responsável por aplicar as políticas de acesso definidas. Ele atua como a primeira linha de defesa, interceptando as tentativas de acesso a recursos. O PEP consulta o PDP para obter decisões sobre o acesso e, com base nessas decisões, faz cumprir as políticas.

O PDP (*Policy Decision Point* - Ponto de Decisão de Política) é o cérebro da arquitetura. Este é o componente que avalia solicitações de acesso recebidas em relação a políticas e retorna uma decisão de Permitir ou Negar. O PDP também pode usar o PIP para recuperar valores de atributos ausentes durante a avaliação de políticas.

O PIP (*Policy Information Point* - Ponto de Informação de Política) é responsável por fornecer informações de atributos necessárias para tomar decisões de acesso. Ele consulta repositórios e conecta o PDP a fontes externas de valores de atributos, como LDAP ou bancos de dados.

O PAP (*Policy Administration Point* - Ponto de Administração de Política) é quem gerencia a criação, atualização e exclusão de políticas avaliadas pelo PDP.

Alguns dos parâmetros que podem compor o ABAC são:

- Sujeito: Quem está fazendo o acesso que irá incluir os dados do usuário como id, nome, organização, departamento e outros.

- Recurso: O recurso ao qual se deseja acessar, pode ser uma rede, um dispositivo, uma pasta de arquivos em determinado servidor, e também podem ser usadas características e atributos baseado do ambiente como qual a data de criação, onde está

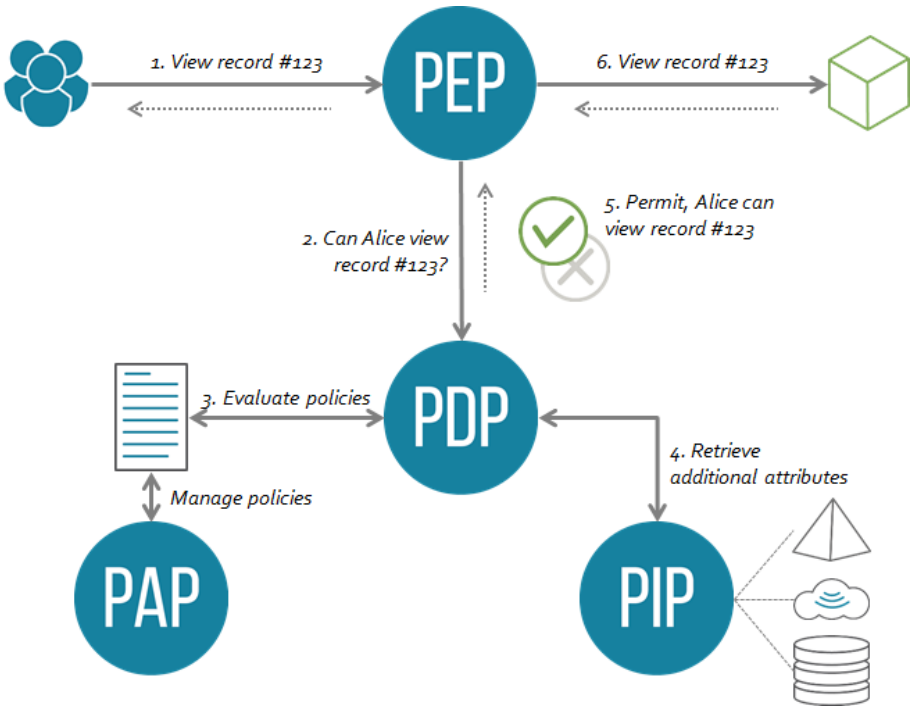

Figura 2.1: Diagrama clássico da arquitetura ABAC[1].

localizado, quem é o dono.

- Ação: O que deseja fazer com aquele recurso, como consultar alguma informação, inserir dados, deletar algo, realizar alguma ação.

- Ambiente: É o contexto mais amplo dos tópicos, pode ser usado atributos como a localização, o protocolo de comunicação, encriptação, a força de um sinal/antena.

Com base nessas informações o protocolo usa os dados contidos em cada um dos tópicos acima e cruza as informações com as regras de acesso definidas, nas quais as regras podem ser definidas de várias maneiras usando lacuna dos parâmetros ou a combinação entre eles assim como o nível de cada acesso, para assim definir quem é permitido ou e quem não.

Sempre que uma requisição de acesso é efetuada, o sistema ABAC analisa os atributos e as políticas estabelecidas para determinar se o acesso deve ser concedido. Neste contexto, a introdução mais aprofundada dos elementos responsáveis pelo controle de acesso, como PEP, PDP, PIP e PAP, será apresentado mais detalhadamente ao longo desta proposta, oferecendo uma compreensão do ambiente D2D e da aplicação do ABAC para

[1]Fonte: ⟨https://py-abac.readthedocs.io/en/latest/concepts.html⟩

mitigar problemas de segurança, como a falsificação de parâmetros e dados decorrentes de acessos indevidos.

3 Trabalhos Relacionados

Em 2016 Zhang *et al.*, propôs um protocolo de compartilhamento seguro de dados para comunicações D2D em LTE-Advanced (LTE-A), que realiza confidencialidade, integridade e não repúdio. No entanto, para compartilhamento de dados, um servidor de fornecimento de conteúdo deve ser instalado na rede celular e todos os dispositivos móveis precisam se registrar nele. Embora o servidor de fornecimento de conteúdo seja totalmente seguro, ele está exposto a ataques (ZHANG et al., 2016).

Em 2018 Zheng Yan propôs um controle de acesso para as redes D2D provendo flexibilidade e segurança, com um modelo no qual exista uma unidade para certificar os devices na rede e a comunicação acontece de forma criptografada (YAN et al., 2018). Em 2020 Smriti Bhatt propôs um controle de IoT chamado de ABAC-CC Framework, que possui como base o ABAC (BHATT; SANDHU, 2020). Estas duas propostas são as de maior relevância no momento.

Atualmente, a maioria dos modelos de controle de acesso para D2D e IoT foram desenvolvida com base em alguns modelos populares na indústria, como o controle de acesso baseado em função (RBAC) e o controle de acesso baseado em atributos (ABAC), na qual as permissões são determinadas com base em atributos (propriedades) de usuários (ou assuntos) e objetos. Apesar do desenvolvimento de vários modelos de controle de acesso, não há consenso em um modelo de controle de acesso formal padrão.

Em 2019 Aliane e Adda (ALIANE; ADDA, 2019) escreveram sobre um modelo denominado HoBAC (*Higher-order Attribute-Based Access Control*) que se trata de uma variação do método ABAC para redes de IoT, no qual este modelo se baseia que os dispositivos não precisam ser iguais para se conectarem, ou seja, eles podem possuir atributos e parâmetros diferentes (ALIANE; ADDA, 2019).

Em 2022 Amit Biswas (BISWAS; BARANWAL; Kumar Tripathi, 2022) propôs um modelo ABAC comparando alternativa por alternativa baseando-se em critérios de decisão múltiplos, a ideia é formar uma matriz de peso para cada parâmetro e assim aplicar um método MCDM (*Multi-Criteria Decision Making*) sobre a mesma, e assim

após as comparações das alternativas seria formada uma matriz de decisão. (BISWAS; BARANWAL; Kumar Tripathi, 2022)

Nossa abordagem será focada em redes D2D com a utilização do método ABAC como controle de segurança, fornecendo autorização e autenticação buscando uma maneira de proporcionar menor atrito nas conexões. O ABAC se mostra um adequado para esta finalidade, tendo em vista que quando um novo usuário se cadastra na rede ele não precisa de uma ação manual para obter os acessos, basta possuir os atributos necessários para a conexão e automaticamente já será autorizado.

O principal diferencial deste trabalho em relação ao estado da arte apresentado é o estudo do impacto dos parâmetros para cada meio-fim, visando sempre garantir o menor atrito possível e sem reduzir o nível de segurança e integridade de acordo com a criticidade de cada dispositivo. Também inserimos na arquitetura do modelo uma unidade centralizada, na qual uma vez realizada a conexão do dispositivo com a mesma, é possivel se conectar em todos os demais dispositivos da rede de modo par a par. Esta unidade é um elo de segurança entre os dispositivos da rede, sendo também responsável por notificar novos dispositivos e por algumas ações relacionadas ao gerenciamento que serão apresentadas mais a frente.

4 Desenvolvimento

4.1 Metodologia

O desenvolvimento do iniciou com o estudo referenciado a comunicação de redes D2D e sobre o controle de acesso ABAC visando identificar os melhores e mais eficientes atributos/parâmetros. A identificação dos atributos mais adequados visa ajudar a compreensão de seu funcionamento e de como o mesmo é implementado. Esse ponto é uma das contribuições do trabalho, uma vez que esses dados são a base para o controle de acesso na rede D2D e garante a confiança dele.

Ao término do estudo, diferentes parâmetros relevantes desse ambiente foram coletados através de uma pesquisa e dedução lógica, organizadas por relevância e impacto no método. Ou seja, classificados por características específicas dos possíveis parâmetros. Também foram estudados algoritmos de criptografia para uma unidade certificadora que, fora a autenticação inicial de um novo usuário/dispositivo da rede, será responsável pela distribuição de chaves para comunicação segura entre os dispositivos.

Com a organização dos parâmetros, foi mais fácil o estudo aprofundado da utilização e impacto de cada um deles. Coletamos informações teóricas, para que fossem avaliadas no testes. Com a limitação de acesso para avaliação de um grande número de dispositivos, esses testes serão realizados por meio de um *software* para simulação de redes D2D e uma unidade certificadora. Esse ambiente nos permite testar os diferentes parâmetros e funcionamentos. Posteriormente, serão geradas tabelas e gráficos de comparação dos resultados para uma melhor compreensão e análise.

Após análise dos resultados gerados pelas diferentes combinações de parâmetros, a melhor solução será destacada junto à uma conclusão, além de publicado o protótipo que pode ser consultado no *GitHub* [2] e simulador utilizado para avaliação.

[2] ⟨https://github.com/Feralfeld/TCC_PROTOTIPO/tree/master/src/main/java/projeto/tcc⟩

4.2 Visão Geral

De maneira resumida o funcionamento da nossa proposta para redes D2D se dará conforme demonstrado na Figura 4.1, e será explicado em mais detalhes nas seções a seguir.

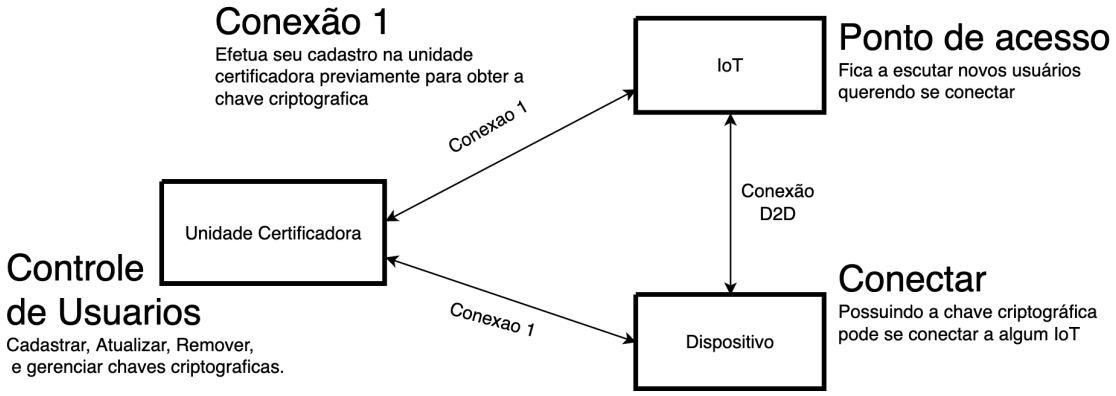

Figura 4.1: Diagrama de funcionamento da proposta.

A atribuição da unidade certificadora abrange a gestão dos dispositivos, demandando que um novo dispositivo, para interconectar-se com outros, proceda a um prévio registro junto à referida unidade certificadora, pois essa comunicação aos pares será criptografada e é papel da Unidade Certificadora gerenciar a chave de criptografia. A Unidade Certificadora também se encarrega de transmitir aos dispositivos previamente cadastrados os dados pertinentes ao novo aparelho conectado, bem como os parâmetros cadastrados para fins de verificação. A discussão a respeito dos parâmetros e de segurança será aprofundada em seções subsequentes.

Após efetuar o registro, o dispositivo recém-cadastrado recebe uma chave criptográfica, idêntica àquela distribuída aos demais dispositivos pela unidade certificadora. Essa medida proporciona a certeza de que, no momento em que uma conexão D2D é estabelecida, o dispositivo já está devidamente registrado na unidade certificadora e possui a chave correta, caso contrário a criptografia não combinaria entre os dois dispositivos, gerando um erro e falha na conexão.

O algoritmo de criptografia que utilizamos foi o AES (Advanced Encryption Standard) no qual é um algoritmo de chave simétrica amplamente utilizado para proteger informações sensíveis. Criado para substituir o DES (Data Encryption Standard), o AES

é considerado um padrão de criptografia robusto e seguro. O AES é um algoritmo de criptografia simétrica, o que significa que a mesma chave é usada tanto para criptografar quanto para descriptografar os dados. As partes que trocam informações precisam ter a mesma chave secreta. O AES suporta diferentes tamanhos de chave, incluindo 128 bits, 192 bits e 256 bits, sendo que chaves maiores geralmente oferecem um nível mais alto de segurança.

O AES é amplamente adotado em todo o mundo e é considerado seguro para uso em uma variedade de contextos, incluindo comunicações seguras pela internet e criptografia de dados armazenados. A escolha do tamanho da chave deve ser cuidadosamente considerada, equilibrando a necessidade de segurança com a eficiência operacional.

A partir desse estágio, as conexões D2D não mais demandam a intervenção da unidade certificadora e podem ser estabelecidas de modo autônomo, conforme o nível de acesso atribuído a cada dispositivo e a natureza da conexão permitida. Tais tecnologias de acesso, como dito anteriormente, podem ser Wi-Fi Direct, Wi-Fi em modo *ad hoc*, Bluetooth e até mesmo cabeado entre os pares.

Um exemplo de como uma conexão ocorre podemos considerar dois dispositivos: um celular e uma geladeira IoT. Inicialmente, ambos os dispositivos precisam ser previamente cadastrados na Unidade Certificadora para adquirirem suas respectivas chaves criptográficas. A geladeira permanece em modo de espera, aguardando por qualquer dispositivo que deseje estabelecer uma conexão, a qual pode ser realizada por meio de wi-fi, bluetooth, ou, embora menos comum neste caso específico, até mesmo uma conexão cabeada.

No momento em que o dispositivo desejado, como o celular em nosso exemplo, está dentro da distância permitida pela antena, ele tenta estabelecer uma conexão via bluetooth com a geladeira. A partir desse ponto, desencadeia-se o processo de autenticação e autorização. Inicialmente, os dispositivos verificam as chaves criptográficas um do outro para autenticar a validade do cadastro na Unidade Certificadora. Uma vez validadas as chaves, inicia-se o processo de autorização, utilizando o modelo ABAC. Detalhes sobre o fluxo de autorização e explicação de cada etapa serão discutidos mais adiante.

4.3 Unidade Certificadora

A função da Unidade Certificadora (UA) consiste na administração das conexões por meio da chave criptográfica, e também um CRUD (*Create, Read, Update and Delete*) dos dispositivos. Quando um novo dispositivo é registrado, a UA encarrega-se de transmitir por broadcast aos demais dispositivos as informações pertinentes ao recém-conectado, considerando o nível de confiabilidade associado aos parâmetros previamente cadastrados para fins de verificação.

A UA também detém a responsabilidade de gerenciar as chaves criptográficas dos grupos, estabelecendo um mecanismo assegurador de que a comunicação originada pelo novo dispositivo também foi submetida à UA, facultando a este dispositivo o conhecimento acerca do grupo ao qual está vinculado. Cabe destacar que as chaves criptográficas podem ostentar uma data de validade, conforme a configuração específica, a UA tem a capacidade de gerar novas chaves quando demandada.

As chaves criptográficas usadas na hora de enviar e receber as informações entre os dispositivos utilizada é a AES (*Advanced Encription Standard*), como já dito a administração dessa chave é de responsabilidade da UA.

Para desempenhar efetivamente o seu papel, a UA incorpora diversas funcionalidades relacionadas aos dispositivos, as quais serão abordadas de maneira detalhada a seguir com diagramas e explicações.

- Cadastrar (Figura 4.2)
- Remover (Figura 4.3)
- Atualizar (Figura 4.4)
- Consultar (Figura 4.5)

O cadastro de um novo dispositivo assim como mostra na figura 4.2 começa com o dispositivo interessado iniciando uma comunicação com a unidade certificadora e passando os atributos para que possam ser cadastrados juntos aos demais dados do dispositivo. A unidade certificadora então confere quais atributos o dispositivo forneceu, e após toda a verificação ela atualiza a base de dados com o novo dispositivo e envia as atualizações

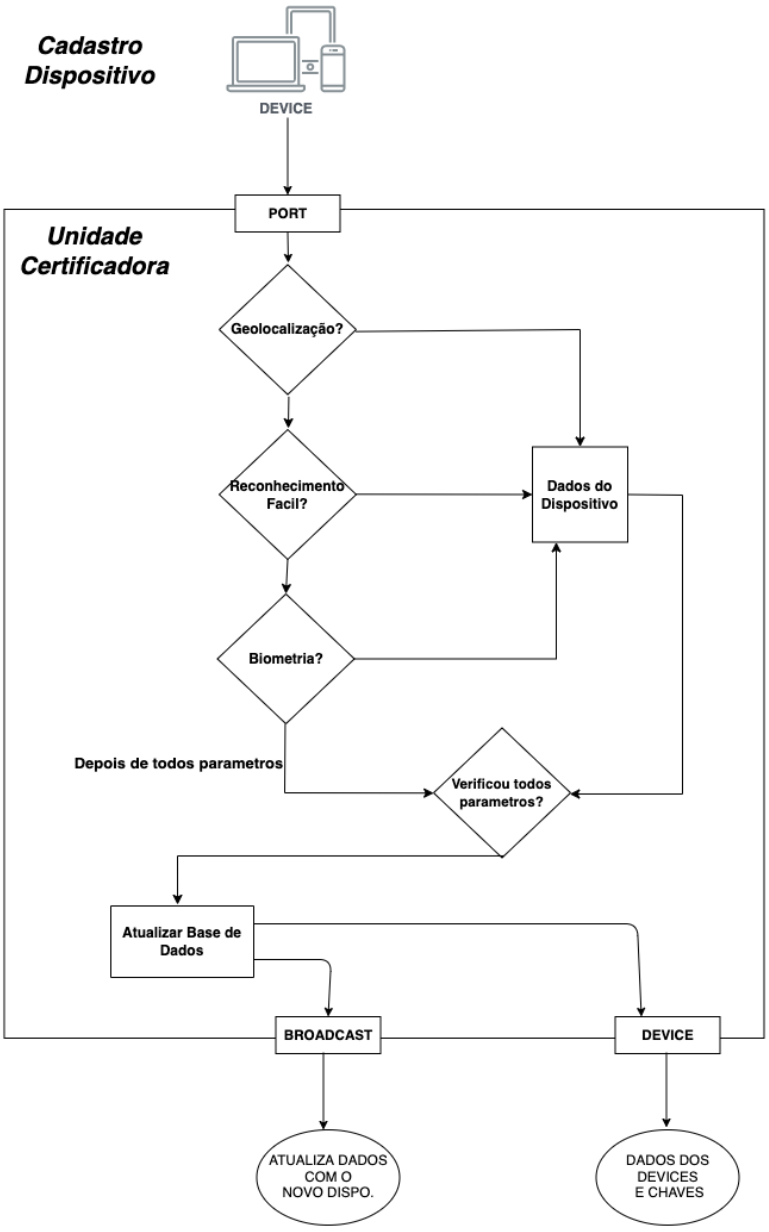

Figura 4.2: Diagrama de cadastro de novo dispositivo

informando que há um novo dispositivo para os demais que já estiverem previamente cadastrados.

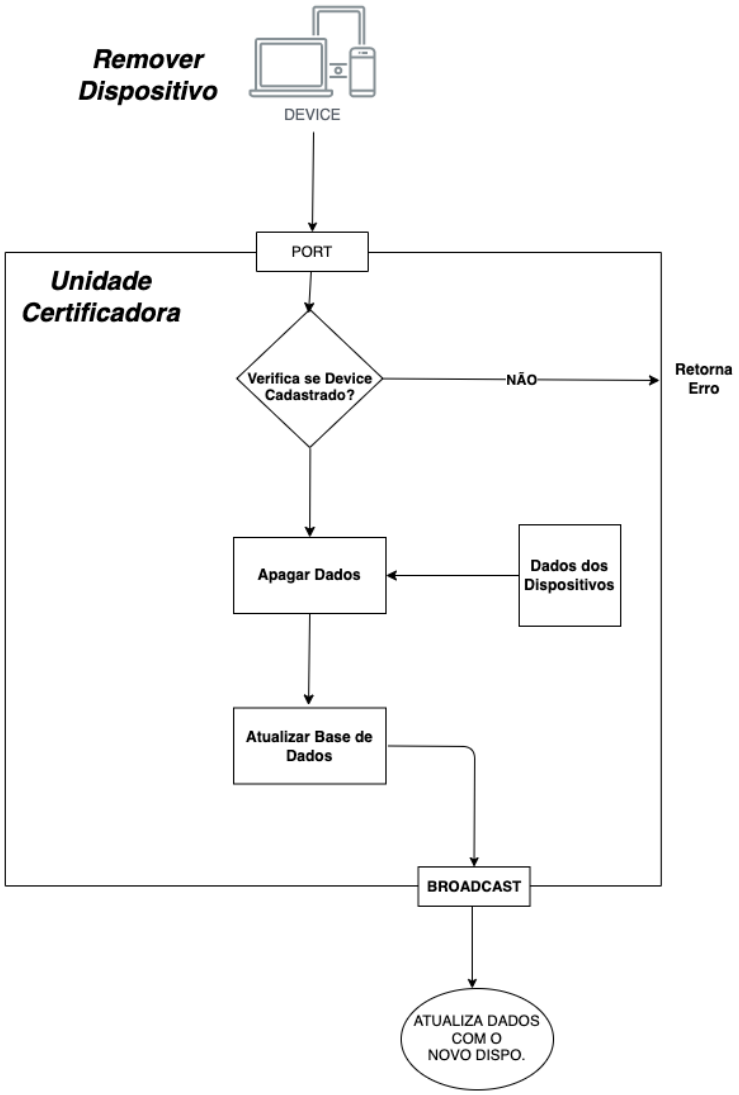

Figura 4.3: Diagrama de remover dispositivo

A remoção do dispositivo da unidade certificadora segue o diagrama 4.3, o processo se inicia com o dispositivo fazendo a solicitação de exclusão e então a unidade certificadora verifica se o dispositivo solicitante já está cadastrado. Caso não esteja a operação não é efetuada, mas se o dispositivo estiver cadastrado previamente os dados são removidos e a UA envia para os demais dispositivos cadastrados as atualizações, informando que um dispositivo foi excluído.

A atualização dos parâmetros de um dispositivo assim como mostra na figura 4.4 se inicia com o dispositivo interessado iniciando uma comunicação com a unidade certificadora, então a unidade certificadora verifica se o dispositivo solicitante já está cadastrado,

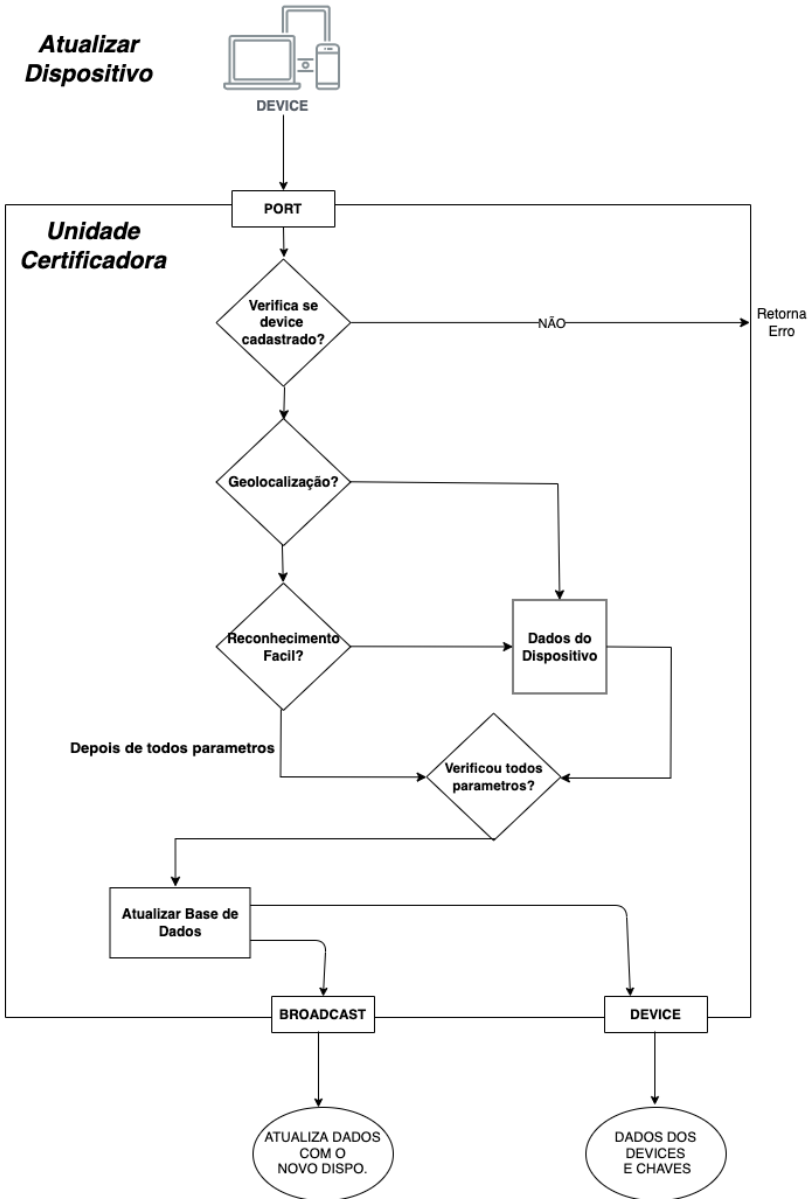

Figura 4.4: Diagrama de atualizar dados do dispositivo

caso não esteja ela não envia as informações, mas se o dispositivo estiver previamente cadastrado ela coleta novamente os atributos, fossem novos, antigos ou removidos. E após todos os parâmetros, ela atualiza a base de dados com os dados com esse dispositivo e envia atualizações para os demais dispositivos que já estiverem previamente cadastrados, informando que há um novo dispositivo.

A consulta de dados da unidade certificadora assim como mostrado na Figura 4.5 serve para que os dispositivos recebam os dados que nela estão, afim de se atualizem com os dados dos outros dispositivos que possam ter sido alterados ou dados de novos dispositivos que foram cadastrados desde a última atualização. O processo se inicia com

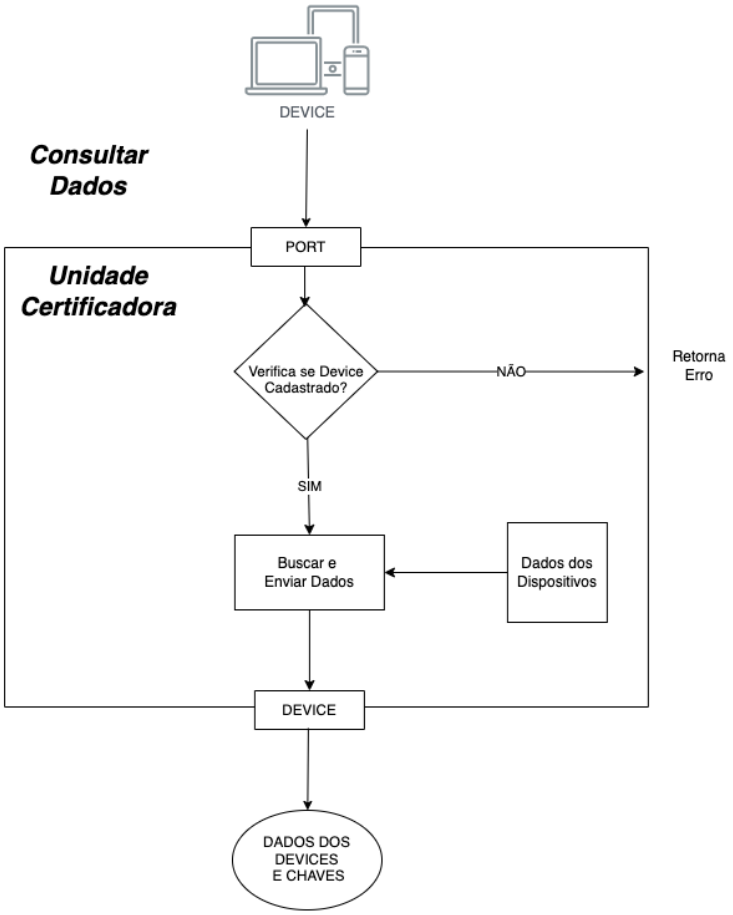

Figura 4.5: Diagrama de consultar dados

o dispositivo fazendo a solicitação dos dados e então a unidade certificadora verifica se o dispositivo solicitante já está cadastrado, caso não esteja ela não envia as informações, mas se o dispositivo estiver cadastrado previamente ela envia os dados de todos os dispositivos.

4.4 Controle de Acesso D2D

Após a conclusão do processo de registro na unidade certificadora e a aquisição da chave criptográfica, os dispositivos se encontram habilitados a estabelecer conexões entre si sem a necessidade de um intermediário. O procedimento de conexão segue a sequência descrita a seguir.

O dispositivo solicitante, com intuito de estabelecer uma conexão, submete uma requisição ao dispositivo alvo, o qual permanece em espera por uma conexão. A etapa inicial da verificação consiste na confrontação da chave criptográfica transmitida pela unidade certificadora, sendo esta verificação conduzida mediante a tentativa de descripto-

grafia da mensagem enviada/recebida. A congruência do conteúdo descriptografado com o esperado configura a verificação como bem-sucedida. A partir desse ponto, as demais fases de autenticação seguem um modelo baseado em controle de acesso por atributos (ABAC).

Consoante ao diagrama delineado na Figura 4.6, os componentes do protocolo operam de forma colaborativa para assegurar o controle de acesso em um contexto ABAC. Este artigo difere da arquitetura clássica como na Figura 2.1, a camada PIP não é utilizada pois não há necessidade de buscar informações extras em alguma base de dados. Uma análise mais aprofundada de cada um dos componentes revela suas funcionalidades distintas detalhadamente.

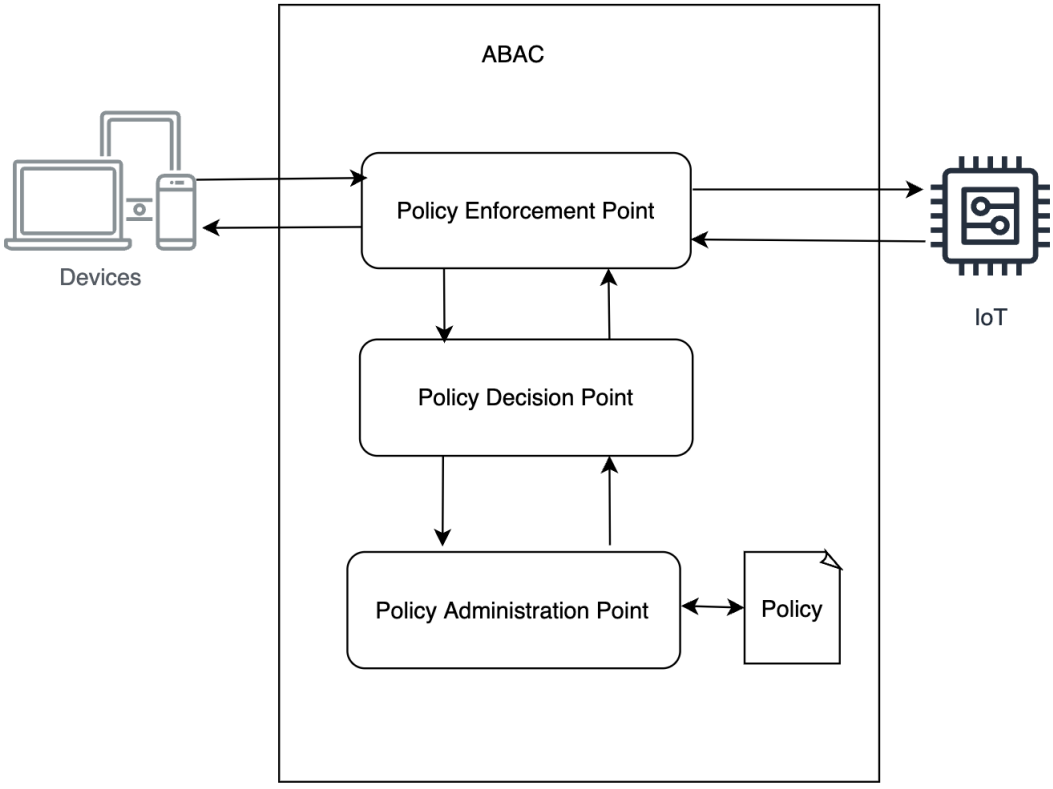

Figura 4.6: Diagrama de conexão ABAC

O PEP está localizado na fronteira do sistema e é responsável por fazer cumprir as políticas de acesso. Ele intercepta as tentativas de acesso a recursos e consulta o PDP para determinar se a solicitação deve ser permitida ou negada.

O diagrama representado na Figura 4.7 está numerado na ordem dos acontecimentos. Primeiro o dispositivo que deseja abrir a conexão chama o PEP, passando seus

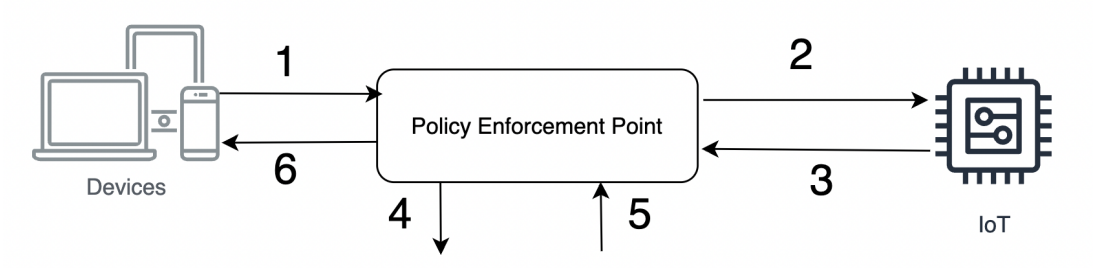

Figura 4.7: Diagrama PEP

atributos, como por exemplo sua geolocalização, biometria, nome do dispositivo entre outros. A partir deste ponto o PEP solicita os atributos do dispositivo IoT que podem ser atributos como: nível de bateria, geolocalização, data e hora. Na terceira etapa o dispositivo IoT envia os dados solicitados pelo PEP, este por sua vez encaminha a requisição com todos os dados coletados para a camada do PDP, e então é retornado um booleano dizendo se concede (*Access-Accept*/True) ou não (*Access-Deny*/False) o acesso ao dispositivo solicitante e este repassa a ação liberando ou não o dispositivo.

Como já dito, o PDP é o componente que toma as decisões de acesso com base nas políticas definidas. Ele recebe informações do PEP sobre a solicitação de acesso e do PIP sobre os atributos relevantes. O PDP avalia essas informações em relação às políticas de acesso e determina se a solicitação é permitida, negada ou se uma ação específica deve ser tomada.

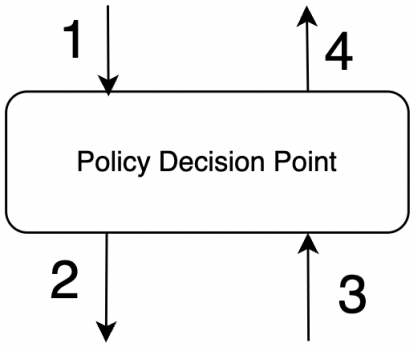

Figura 4.8: Diagrama PDP

A Figura 4.8 mostra o diagrama de funcionamento do PDP de maneira ordenada. É possível ver desde a etapa 1, na qual a requisição do PEP é recebida, e então solicitadas as informações administrativas sobre o acesso na camada PAP que retorna as informações.

Na etapa 4 o PDP faz uma análise interna com base nos parâmetros recebidos do PEP e decide se concede ou não o acesso. No capítulo 4.5 explica-se detalhadamente como o PDP realiza essa decisão na etapa 4, e a partir daí na etapa 5 ele responde ao PEP um booleano, dizendo se concede ou não o acesso ao dispositivo.

O PAP é responsável pela administração e definição das políticas de acesso. Ele permite que os administradores definam, modifiquem e removam políticas de acesso. O PAP é onde as políticas são configuradas e gerenciadas.

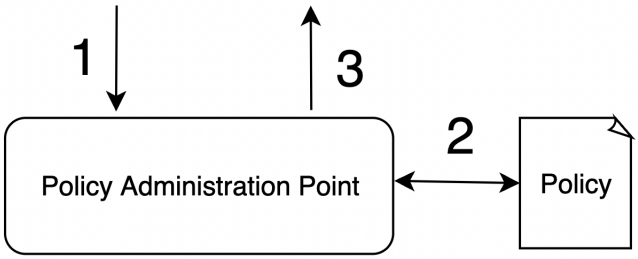

Figura 4.9: Diagrama PAP

No caso do PIP a arquitetura utilizada é um pouco modificada do ABAC clássico como na Figura 2.1. Então não há a camada PIP como pode ser visto na Figura 4.6.

4.5 PDP - *Policy Decision Point*

De maneira ainda mais detalhada sobre o PDP, que é como o cérebro da implementação, o ponto de decisão do modelo apresentado, tem como funcionamento interno o diagrama mostrado na Figura 4.10.

Para que o acesso seja concedido será necessário que o dispositivo atinja a pontuação básica para se comunicar com um dispositivo. Essa pontuação é definida na confiabilidade de segurança do parâmetro, os parâmetros e suas características serão abordados mais à frente no capitulo 4.6, por enquanto basta entender que o PDP funcionará somando os pontos dos parâmetros fornecidos e que para conseguir o acesso o dispositivo precisa atingir a pontuação mínima necessária de cada nível. Os níveis e pontos necessários para cada qual é abordado no capítulo 4.8.

O PDP pode receber uma variedade de parâmetros e variáveis, incluindo, por

exemplo, a hora do sistema e o nível de bateria do dispositivo, entre outros. As informações sobre quais parâmetros são considerados válidos e os detalhes associados a cada um são obtidas por meio das políticas, sendo que, no nosso contexto, utilizamos a SpEL (Spring Expression Language) que pode ser consultada no *website*[1]. Através então dessas políticas criadas como mostraremos na seção , o PDP é capaz de desempenhar sua função e chegar a uma conclusão.

Internamente, o PDP realiza uma ordenação dos parâmetros com base em uma pontuação total, sendo importante mencionar que discutiremos a pontuação mais adiante. Essa abordagem visa reduzir o atrito ao empregar o menor número possível de parâmetros, considerando que cada verificação demanda um determinado tempo. Assim, a cada parâmetro validado, os pontos de segurança acumulados aumentam, até que todos os parâmetros fossem verificados ou até que a pontuação mínima necessária seja alcançada.

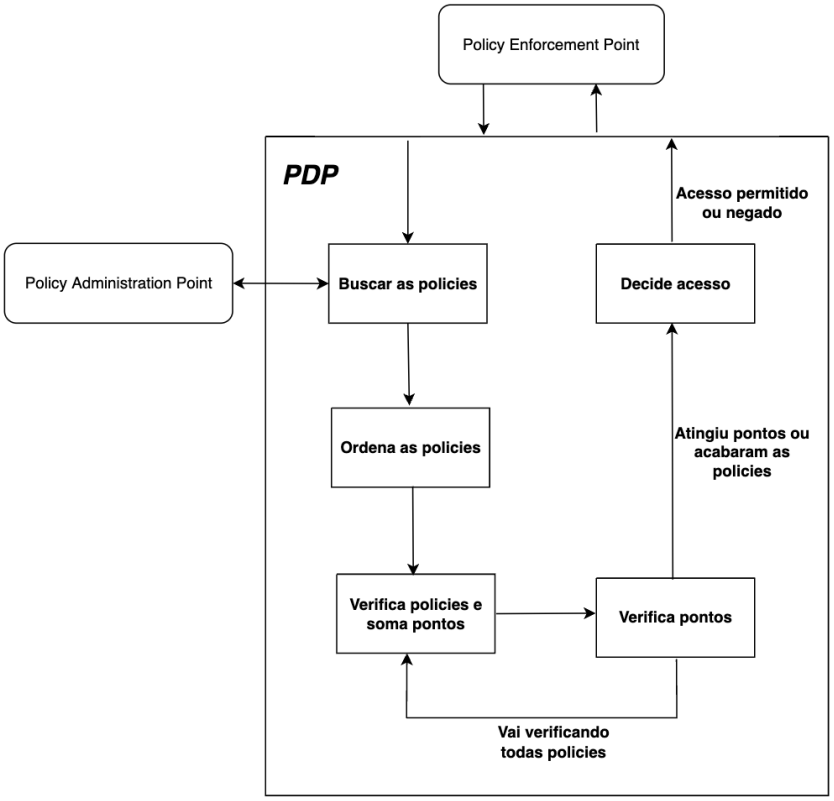

Figura 4.10: Diagrama Interno PDP

O PDP realiza uma seleção criteriosa das políticas que guardam pertinência com o dispositivo em consideração, conferindo a possibilidade de uma implementação adici-

[2]Website: ⟨https://docs.spring.io/spring-framework/reference/core/expressions.html⟩

onal que incorpore políticas exclusivas. Embora tal cenário não se configure na nossa atualidade, a estrutura da implementação proporciona essa adaptabilidade.

No que concerne à análise dos parâmetros e expressões utilizadas pelo PDP, optamos por adotar a Spring Expression Language ($SpEL$[1]) . Esta escolha propicia uma abordagem genérica para a verificação dos parâmetros, possibilitando a avaliação de atributos por meio de operadores aritméticos, relacionais, lógicos e condicionais.

As políticas ficam organizadas em um arquivo json contendo nome, descrição, ação, condição, valor da pontuação, valor de atrito, valor de segurança e tempo. Então o PAP usa desse arquivo json para buscar as informações relativas às políticas de acesso para que o PDP possa usá las, um exemplo de como o arquivo fica organizado é o seguinte:

```
[
    {
        "name": "Geolocalizacao",
        "description": "Geolocalizacao",
        "condition": "subject.geolocalizacao == resource.geolocalizacao",
        "value" : 14,
        "atrito" : 5,
        "seguranca" : 70,
        "tempo" : 1
    },
    {
        "name": "Senha",
        "condition": "subject.password == resource.password",
        "value" : 10,
        "atrito" : 7,
        "seguranca" : 70,
        "tempo" : 8
    },
    {
        "name": "Impressão Digital",
        "condition": "subject.fingerPrint == resource.fingerPrint",
        "value" : 19,
        "atrito" : 5,
        "seguranca" : 96,
        "tempo" : 3
    },
```

Figura 4.11: Exemplo policies

[2]Website: ⟨https://docs.spring.io/spring-framework/docs/3.2.x/spring-framework-reference/html/expressions.html⟩

4.6 Atributos e Parâmetros

Conforme pode ser consultado na Tabela 4.1, fizemos uma lista com diversos parâmetros e atributos que podem ser usados para o ABAC, logo em seguida nesta seção explicaremos melhor sobre cada um deles, listando pontos positivos e negativos que influenciarão em posterior análise quantitativa de geração de atrito, ao usarmos cada um deles, e também a fator de segurança que cada um prove.

Tabela 4.1: Tabela de parâmetros

Atributos/Parâmetros
Geolocalização
Rede Conectada
Impressão Digital
Reconhecimento Facial
Segundo Fator de Celular
Senha
Autenticação por Reconhecimento de Comportamento
Autenticação de Assinatura Digital
Autenticação de Retina ou Íris
Autenticação por Reconhecimento de Voz
Tokens de Hardware

- Geolocalização: A geolocalização envolve a identificação da localização física de um dispositivo ou usuário com base em informações como GPS, endereço IP ou torres de celular. Pontos Positivos: Pode ser usado para autenticação de dois fatores (2FA) baseada em localização. Útil para detectar atividades suspeitas ou não autorizadas com base em locais de acesso. Pontos Negativos: Pode ser impreciso em áreas com muitos dispositivos e torres de celular próximas. A geolocalização pode ser falsificada por meio de VPNs e proxies.

- Rede Conectada: A rede conectada se refere ao acesso a partir de uma rede específica, como uma rede corporativa ou doméstica. Pontos Positivos: Pode ser usada como um fator de autenticação. Acesso restrito a partir de redes específicas pode aumentar a segurança. Pontos Negativos: Limita a acessibilidade, tornando-se inconveniente quando o acesso é necessário de locais diferentes. Redes podem ser comprometidas, tornando essa abordagem menos segura.

- Impressão Digital: Este método utiliza da singularidade dos padrões de sulcos, cristas e pontos característicos presentes na impressão digital nos dedos de cada pessoa. Pontos Positivos: Muito difícil de falsificar, pois é baseado em características físicas exclusivas. Oferece alta segurança e conveniência para o usuário. Pontos Negativos: Não é facilmente recuperável em caso de falha do sistema ou perda de dados biométricos.

- Reconhecimento Facial: O reconhecimento facial envolve a identificação de uma pessoa com base em características faciais únicas. Pontos Positivos: É conveniente e amplamente utilizado em dispositivos móveis. Geralmente é difícil de falsificar. Pontos Negativos: Pode ser invadido por meio de fotos ou vídeos de alta qualidade. Preocupações com privacidade estão associadas ao armazenamento e uso de dados faciais.

- Segundo fator de e-mail: O segundo fator de e-mail envolve o envio de um código de autenticação para o endereço de e-mail registrado do usuário. Pontos Positivos: É uma camada adicional de segurança. Fácil de usar, pois a maioria das pessoas tem um endereço de e-mail. Pontos Negativos: Acesso ao e-mail principal pode ser o único obstáculo para invasores. Vulnerável a ataques de phishing se o e-mail for comprometido.

- Segundo fator de celular: O segundo fator de celular envolve o uso de um código enviado por SMS, um aplicativo de autenticação ou uma notificação push no celular do usuário. Pontos Positivos: A maioria das pessoas possui um celular. Oferece uma camada adicional de segurança. Pontos Negativos: Vulnerável a ataques de clonagem de SIM. Requer conectividade móvel e, portanto, pode não ser acessível em todas as situações.

- Senha: A senha é uma sequência de caracteres que o usuário digita para autenticar sua identidade, no nosso caso tomaremos como base uma senha de 8 caracteres contendo letras, números e caracteres especiais. Pontos Positivos: Amplamente utilizado e compreendido. Pode ser fortalecido com práticas de segurança, como senhas complexas e 2FA. Pontos Negativos: As senhas podem ser facilmente adivinhadas ou

roubadas. Os usuários podem esquecer senhas, resultando em problemas de acesso.

- Autenticação por Reconhecimento de Comportamento: Analisa os padrões de comportamento do usuário, como a forma como digita no teclado, para autenticá-lo. Pontos Positivos: Pode autenticar constantemente com base no comportamento, identifica comportamentos suspeito Pontos Negativos: Exige adaptação para mudanças no comportamento, pode sofrer influências por mudanças no ambiente ou estado emocional do usuário.

- Autenticação de Assinatura Digital: A pessoa realiza a assinatura em um dispositivo eletrônico, que digitaliza e captura os traços da caneta, convertendo-os em dados digitais, é então armazenada como uma representação digital, muitas vezes em um formato de imagem ou em dados vetoriais.Para autenticar a assinatura, os sistemas podem comparar a assinatura digitalizada com um modelo de assinatura armazenado anteriormente. Métodos mais avançados podem empregar técnicas biométricas para autenticação baseada em características únicas da assinatura. Pontos Positivos: A abordagem utiliza a assinatura manual, que é uma prática familiar e intuitiva para muitas pessoas, representação pessoal, aceitação legal, a tecnologia para capturar assinaturas manuais é relativamente acessível, exigindo dispositivos comuns, como tablets ou dispositivos sensíveis à pressão. Pontos Negativos: Comparada a métodos mais avançados, como assinaturas digitais baseadas em criptografia, a segurança da assinatura digital à mão pode ser considerada menos robusta, falsificação possível, dependência da tecnologia utilizada.

- Autenticação de Retina ou Íris: Usada em sistemas de alta segurança, envolvendo a digitalização da retina ou íris para autenticar o usuário. Pontos Positivos: Possui uma alta precisão, difícil de falsificar e rápida autenticação. Pontos Negativos: Alto custo de implementação, condições de saúde podem afetar a precisão.

- Autenticação por Reconhecimento de Voz: Baseada nas características únicas da voz de um usuário para fins de autenticação, pode ser usado com a pessoa lendo algumas palavras, falando algum comando entre outros objetos de fala. Pontos Positivos: Fácil de usar, pode se adaptar a mudanças na voz do indivíduo. Pontos

Negativos: Precisão pode ser afetada com ruídos externos, é vulnerável a imitação de voz.

- Tokens de Hardware: Dispositivos físicos, como chaves de segurança USB, que são usados para autenticação de dois fatores (2FA) e fornecem um alto nível de segurança.

4.7 Pontuação dos Atributos

Com o intuito de otimizar a utilização eficaz de cada parâmetro, bem como garantir a segurança apropriada para cada um dos níveis de acesso, concebemos a Tabela 4.2 que possui uma pontuação a cada atributo, ponderada pelo nível de segurança e o nível de atrito associados.

Este enfoque permite a avaliação conjunta do nível de atrito em concomitância com a segurança, através da formulação de uma relação proporcional. A pontuação final é derivada mediante o cálculo da divisão do fator de segurança pelo valor do atrito.

O valor de atrito pode variar de 5 a 8 para que a pontuação não oscilar demais e também não temos valores muito altos já que o atrito é um valor divisor no nosso cálculo da pontuação final, enquanto o valor do fator de segurança pode variar de 0 a 100, levando em conta esses parâmetros e como o cálculo é efetuado a pontuação final terá um valor máximo e mínimo como quando a segurança for 0 o cálculo final será 0, e quando for 100 e o atrito 5 que é o menor valor possível atingindo o valor de 20, sendo assim a pontuação final pode variar entre 0 e 20.

A avaliação da pontuação de atrito e segurança foi conduzida de maneira dedutiva, proporcionando uma aproximação sólida, embora não necessariamente represente a realidade de maneira precisa. Os parâmetros e atributos adotados são concebidos de forma mais genérica e explicativa, sendo vital uma avaliação específica para cada implementação. Os valores atribuídos a atrito e segurança são, portanto, uma abstração e poderiam variar entre diferentes parâmetros, sendo denominados genericamente como "parâmetro 1", "parâmetro 2"e assim por diante. No escopo deste trabalho, consideraremos que esses atributos específicos têm os valores indicados na Tabela 4.2.

Posteriormente, a pontuação final obtida será empregada para ordenar os atributos recebidos quando forem validados no PDP, proporcionando uma abordagem sistemática e equilibrada que considera tanto a segurança necessária quanto o impacto sobre a experiência do usuário durante o processo de conexão.

Tabela 4.2: Valor de atrito, segurança e pontuação final de cada atributo

Parâmetro/Atributo	**Atrito**	**Segurança**	**Pontuação Final**
Geolocalização	5	70	14
Reconhecimento Facial	8	80	10
Senha	7	80	10
Impressão Digital	5	96	19
Segundo fator sms	8	90	11
Assinatura Digital	6	90	15
Rede Conectada	5	90	18
Reconhecimento Comportamento	6	80	13
Reconhecimento Voz	6	75	13
Tokens de Hardware	5	70	14
Retina ou Íris	8	100	12

4.8 Estrutura de Níveis e Dispositivos IoT

Com o intuito de fornecer uma exposição mais minuciosa acerca da organização hierárquica e do funcionamento subjacente, utilizaremos como paradigma uma residência tecnologicamente equipada. Nesse contexto, a habitação em questão incorpora uma variedade de dispositivos, cada qual caracterizado por funcionalidades distintas e atributos diversos de níveis de acesso, além de contar com a presença de uma unidade certificadora.

- Impressora: É um dispositivo que tem a função de produzir documentos, imagens ou gráficos em papel ou outros meios, geralmente a partir de um arquivo digital.
- Lâmpada Inteligente: É um tipo de lâmpada que pode ser controlada por meio de dispositivos eletrônicos, como smartphones, assistentes de voz ou dispositivos de

Tabela 4.3: Dispositivos e níveis de acesso

Dispositivos	
Dispositivo	Nível de acesso
Impressora	1
Lampada	1
Cafeteira	1
Geladeira	2
Porta	2
Portão Garagem	2
Cofre	3

automação residencial. Essas lâmpadas são geralmente equipadas com tecnologia de conectividade, como Wi-Fi ou Bluetooth, e podem ser ajustadas em termos de intensidade de luz, cor e programação por meio de aplicativos móveis ou comandos de voz.

- Cafeteira: É um eletrodoméstico que pode ser controlado e monitorado remotamente por meio de dispositivos eletrônicos, como smartphones, tablets ou assistentes de voz. Essas cafeteiras são projetadas para tornar a preparação do café mais conveniente e personalizada. Algumas das funcionalidades comuns de uma cafeteira conectada são Programação Remota, Monitoramento e Diagnóstico, Notificações, Controle por Aplicação.

- Geladeira: É um eletrodoméstico de refrigeração que incorpora tecnologia avançada para fornecer recursos adicionais e melhorar a experiência do usuário. Algumas das características de uma geladeira tecnológica incluem Câmera Interna, Conectividade com Internet, Dispensa Virtual, Automação Residencial,.

- Porta: Uma porta para o tráfego de pessoas, em que esta pode ser controlada remotamente através de um dispositivo celular, tablet ou outros. E tem como funcionalidades abertura e fechamento remoto, histórico de acessos, notificação em tempo real.

- Portão Garagem: Um portão para entrada e saída de veículos tecnológico, que pode ser controlado de maneira remota, possuir sensores de segurança, notificações,acesso compartilhado. No nosso caso em questão exploraremos a conexão de maneira peer

to peer.

- Cofre: Um cofre para guardar dinheiro e bens valiosos, que possui recursos tecnológicos como abertura pelo celular, câmeras integradas, registro de auditoria, sensores de movimento e vibração. Pensando em uma visão peer to peer podemos abri-lo a partir de um celular, assim como baixar dados de histórico por exemplo, visualizar seu interior sem abrir.

Os dispositivos em consideração foram categorizados em três níveis distintos de acesso. O primeiro nível engloba um conjunto de dispositivos caracterizados por uma demanda reduzida de segurança, associada a uma priorização significativa de facilidade de conexão e utilização. Estes dispositivos, por exemplo, poderiam ser destinados a convidados. No segundo nível, a exigência de segurança é incrementada para garantir o acesso exclusivamente a indivíduos autorizados, resultando em um nível de atrito ligeiramente mais pronunciado durante as conexões. No terceiro nível, reservado para dispositivos críticos, a restrição de acesso é máxima, acompanhada por um nível de atrito substancialmente elevado durante o processo de conexão. Em consonância com tais requisitos e configurações, procedeu-se à segregação dos dispositivos exemplificativos em três categorias distintas.

Os critérios subjacentes à determinação dos níveis encontram-se ancorados na relação inversa entre segurança e acessibilidade. Em outras palavras, quanto mais elevado o grau de segurança requerido, maior é a complexidade associada ao processo de acesso. Cada nível de acesso, por conseguinte, apresenta requisitos específicos e funcionalidades distintas, conforme detalhado na tabela subsequente.

Tabela 4.4: Tabela de níveis de acesso

Níveis de acesso		
Nível	Pontuação	Dispositivos
Nivel 1	200	Impressora, Lâmpada e Cafeteira
Nivel 2	350	Geladeira, Porta e Portão Garagem
Nivel 3	650	Cofre

Para estabelecer as pontuações, realizamos levantamentos para identificar os valores máximos, mínimos e médios alcançados por conjuntos de parâmetros. Essa abordagem é orientada pela intenção de determinar o quão restrito ou permissivo desejamos que um determinado dispositivo obtenha autorização para acessar os dispositivos em diferentes níveis. Esses valores podem ser ajustados conforme a necessidade e a preferência, visando manter um equilíbrio entre a segurança desejada e a minimização do atrito durante o processo.

5 Avaliação e Resultados

5.1 Infraestrutura para Avaliação

No desenvolvimento do presente estudo, foi criada uma estrutura na qual cada dispositivo foi concebido como um sistema Java independente, estabelecendo conexões por meio de *sockets*. Este arranjo simula os dispositivos e as conexões D2D. Todo o código Java utilizado está disposnivel *GitHub* [3].

A estrutura adotada resultou na criação de um menu na unidade certificadora, fomentando a comunicação eficaz com os dispositivos. Este menu oferece a opção de utilização das funcionalidades por parte dos dispositivos ou de manter-se inativo. Ao término da comunicação com a unidade certificadora, cada dispositivo apresenta a alternativa de permanecer disponível para novas conexões ou de estabelecer uma ligação com outro dispositivo.

No contexto da conexão entre dispositivos, ocorre uma interação na qual é desencadeada automaticamente a função de validação das identificações e protocolos de segurança. Este processo implica na mútua identificação entre os dispositivos, verificando-se tanto as informações no momento da conexão quanto aquelas previamente recebidas da unidade certificadora.

Uma vez estabelecida a conexão, viabilizamos a manutenção de um canal de comunicação aberto entre os pares. Este canal é versátil, permitindo a troca bidirecional de informações, abrindo perspectivas para uma variedade de possibilidades, e usada para exibir um menu com funcionalidades e seleção destas funções para cada dispositivo.

Para fins de simulação, foram criados dispositivos conforme listagem na Tabela 5.1, cada qual representado como um sistema Java independente. Estabelecemos conexões entre estes dispositivos e a unidade certificadora, seguindo uma lógica coerente de conexões, como, por exemplo, a vinculação entre o celular e a geladeira, ou o automóvel e o portão da garagem. Não obstante, evitamos configurações semânticas incoerentes, a

[3] ⟨https://github.com/Feralfeld/TCC_PROTOTIPO/tree/master/src/main/java/projeto/tcc⟩

exemplo da conexão entre a máquina de café e o portão da garagem.

No decorrer dos experimentos, foram testados os acessos permitidos para cada nível, assim como o comportamento em relação ao tempo de conexão e as garantias de segurança implementadas no sistema.

5.2 Simulação

Para a realização da simulação, foram concebidos e enumerados dispositivos conforme a Tabela 5.1. Cada dispositivo foi modelado como um sistema autônomo baseado em Java, viabilizando a criação de conexões tanto com a unidade certificadora quanto entre componentes cuja interação se justifica. A exemplificação dessa interação ocorreu de maneira pragmática, conectando, por exemplo, o dispositivo móvel à geladeira e o veículo ao portão da garagem, observando-se a relevância e coerência dessas conexões.

Tabela 5.1: Atributos em cada Dispositivo

Parâmetro/ Dispositivo	**Celular1**	**Celular2**	**Celular3**	**Computador1**	**Computador2**	**Computador3**	**Tablet**
Geolocalização	X	X	X	X		X	X
Reconhecimento Facial	X	X	X		X		X
Senha		X	X	X	X		X
Impressão Digital	X	X	X	X			X
Segundo fator sms	X	X	X				
Assinatura Digital	X		X	X			X
Rede Conectada	X	X	X	X	X		X
Reconhecimento Comportamento		X	X	X	X		
Reconhecimento Voz	X	X	X	X			X
Tokens de Hardware	X		X	X		X	
Retina ou Íris			X	X			

Ao longo do processo, conduzimos testes para avaliar os acessos permitidos em

cada nível, bem como o comportamento temporal das conexões e a garantia de segurança associada a cada cenário. Diversos dispositivos foram simulados, cada qual caracterizado por uma miríade de parâmetros, permitindo-nos derivar conclusões com base em uma análise dos méritos e deméritos de cada parâmetro e sua combinação. Este procedimento implicou a exploração de diversas combinações lógicas, contribuindo para a identificação de padrões e considerações relevantes acerca do desempenho e eficácia do sistema proposto.

O fluxo de conexão acontece como citado no Capítulo 4.4. Um exemplo de conexões e funcionalidades dos dispositivos são apresentados na Figura 5.3, também é mostrado quando um dispositivo não possui o acesso ao IoT e é bloqueado.

```
Encerrando comunicação U.A
Computador 2 iniciando comunicação D 2 D
Passando pelo controle de seguranca ABAC
Não possui acesso
Falha ao conectar! Encerrando!
```

Figura 5.1: Mensagem de erro quando não possui acesso

Primeiro o dispositivo ao ser ligado se conecta a UA e confere se existe alguma atualização a ser feita, e apos a correta inicialização o IoT está disponível para conexões D2D como pode ser visto na Figura 5.2.

Com algum IoT previamente em funcionamento,e um outro dispositivo para a conexão D2D ela pode acontecer, como pode ser visto na Figura 5.3, no qual foi inicializado o dispositivo Celular 2. Após a inicialização do Celular 2, que acontece da mesma forma que na Figura 5.2 o dispositivo então conecta na geladeira se passar pelo o processo de autorização e então o menu do IoT é exibido, como podemos ver na Figura 5.3. E a geladeira emite logs e relatórios durante a conexão como pode ser visto na Figura 5.4.

Pode acontecer o caso no qual o dispositivo não tem o acesso permitido aos IoT's e assim ao tentar se conectar têm seu acesso negado, como mostrado na Figura 5.1 na qual o Celular 1 tenta fazer a conexão com a Geladeira porém não tem permissão.

```
Iniciando comunicacao com a U.A
|-------------MENU------------|
| Opção 1 - Cadastro User     |
| Opção 2 - Update User       |
| Opção 3 - Delete User       |
| Opção 4 - Atualizar Dados   |
| Opção 5 - Exit              |
|------Digite uma opção: -----|
4
Dados dos grupos atualizados
|-------------MENU------------|
| Opção 1 - Cadastro User     |
| Opção 2 - Update User       |
| Opção 3 - Delete User       |
| Opção 4 - Atualizar Dados   |
| Opção 5 - Exit              |
|------Digite uma opção: -----|
5
Encerrando comunicação U.A
Geladeira devidamente inicializada
==================================================
Geladeira abrindo porta para comunicação D 2 D
```

Ce

Figura 5.2: Inicialização Geladeira

5.3 Avaliação

A avaliação se baseia nos seguintes critérios: quantidade de parâmetros necessários para cada nível, quantidade de atrito relacionada, também iremos avaliar com quais combinações de parâmetros os dispositivos se saíram melhor, na qual se sair melhor significa completar a conexão com sucesso possuindo o menor atrito e tempo possível.

Os dados serão coletados como mostrado na Figura 5.4, no qual o Iot que está sendo conectado emite métricas, ele exibe quais os atributos e seus respectivos valores de atrito, segurança e pontuação que foram usados para a autorização, também exibe a quantidade de atributos que foram usados e a somatória de seus valores, o tempo necessário para passar por todo o processo do ABAC é calculado e exibido juntos com as demais informações assim permitindo a coleta.

```
Encerrando comunicação U.A
Celular 2 iniciando comunicação D 2 D
Passando pelo controle de seguranca ABAC
Conexão com Geladeira estabelecida com sucesso!
|-------------MENU------------|
| Opção 0 - Encerrar conexao     |
| Opção 1 - Pegar agua gelada     |
| Opção 2 - Verificar estoque     |
| Opção 3 - Visualizar camera interna     |
|------Digite uma opção: -----|
1
Agua esta sendo preparado...
|-------------MENU------------|
| Opção 0 - Encerrar conexao     |
| Opção 1 - Pegar agua gelada     |
| Opção 2 - Verificar estoque     |
| Opção 3 - Visualizar camera interna     |
|------Digite uma opção: -----|
0
encerrando
```

Figura 5.3: Conexão entra o Celular2 e Geladeira

5.4 Resultados

Como citado no capítulo anterior 5.3, foram coletados dados de cada execução de dispositivo em todos os 3 níveis de acesso, e a partir desses dados foram geradas as tabelas para o nivel 1 5.2, tabela para o nível 2 5.3 e para o nível 3 5.4. Sendo assim as 3 tabelas são

```
================================================
Geladeira abrindo porta para comunicação D 2 D
Recebendo um novo dispositivo e iniciando o controle de seguranca ABAC
Dispositivo que está conectando -> Celular 2
Parametro = Biometria, seguranca = 96, somatorio seguranca = 96, atrito = 5, somatorio atrito = 5
Parametro = Rede Conectada, seguranca = 90, somatorio seguranca = 186, atrito = 5, somatorio atrito = 10
Parametro = Assinatura Digital, seguranca = 90, somatorio seguranca = 276, atrito = 6, somatorio atrito = 16
Parametro = Geolocalizacao, seguranca = 70, somatorio seguranca = 346, atrito = 5, somatorio atrito = 21
Parametro = Token Hardware, seguranca = 70, somatorio seguranca = 416, atrito = 5, somatorio atrito = 26
Foram necessarios 5 paremtros para atingir a pontuacao de 416 com o minimo do nivel sendo 350 o nivel de atrito foi de 26
O metodo executou em 6278 milis ou 6 segundos
Dispositivo autorizado, permitindo acesso...
Opcao Selecionada: Me envie o menu
Opcao Selecionada: 0
================================================
```

Figura 5.4: Informações emitadas pela Geladeira durante conexão

iguais, diferenciando apenas o nível que cada uma representa e os respectivos resultados.

Tabela 5.2: Tabela de dados Nivel 1

Nivel 1	**Celular1**	**Celular2**	**Celular3**	**Tablet**	**Computador1**	**Computador2**	**Computador3**
Acesso Permitido/ Negado	P	P	P	P	P	P	N
Tempo Total	4(s)	4(s)	4(s)	4(s)	4(s)	32(s)	1(s)
Quantidade de Parâmetros	3	3	3	3	3	3	1
Atrito Total	15	16	16	16	16	16	5
Pontuação Segurança Total	256	276	276	276	276	240	70

Tabela 5.3: Tabela de dados Nivel 2

Nivel 2	**Celular1**	**Celular2**	**Celular3**	**Tablet**	**Computador1**	**Computador2**	**Computador3**
Acesso Permitido/ Negado	P	P	P	P	P	N	N
Tempo Total	44(s)	6(s)	6(s)	15(s)	6(s)	39(s)	1(s)
Quantidade de Parâmetros	5	5	5	5	5	4	1
Atrito Total	27	26	26	27	26	26	5
Pontuação Segurança Total	411	416	416	421	416	310	70

A partir da compilação dos dados constantes nessas tabelas, procedeu-se à geração de gráficos, visando proporcionar uma visualização mais precisa dos dados coletados para posterior análise. Nesse contexto, foram elaborados três gráficos distintos. O primeiro destes representa a correlação entre a pontuação de segurança, posicionada no eixo x, e o valor global de atrito, disposto no eixo y. O segundo gráfico delineia o tempo despendido em segundos para a realização da conexão, com cada dispositivo individualizado ao longo do eixo x. O terceiro gráfico, por sua vez, ilustra a quantidade mínima de parâmetros exigidos para a obtenção do acesso em cada nível, tendo a pontuação de segurança ne-

Tabela 5.4: Tabela de dados Nivel 3

Nivel 3	**Celular1**	**Celular2**	**Celular3**	**Tablet**	**Computador1**	**Computador2**	**Computador3**
Acesso Permitido/ Negado	P	P	P	N	P	N	N
Tempo Total	91(s)	56(s)	66(s)	32(s)	66(s)	39(s)	1(s)
Quantidade de Parâmetros	8	8	8	7	8	4	1
Atrito Total	50	48	46	42	46	23	5
Pontuação Segurança Total	651	661	671	571	671	310	70

cessária ao acesso no eixo x e a quantidade total de parâmetros no eixo y. O tempo total não está completamente alinhado com a realidade mas possui uma dedução lógica para cada atributo e o tempo total da conexão é somado.

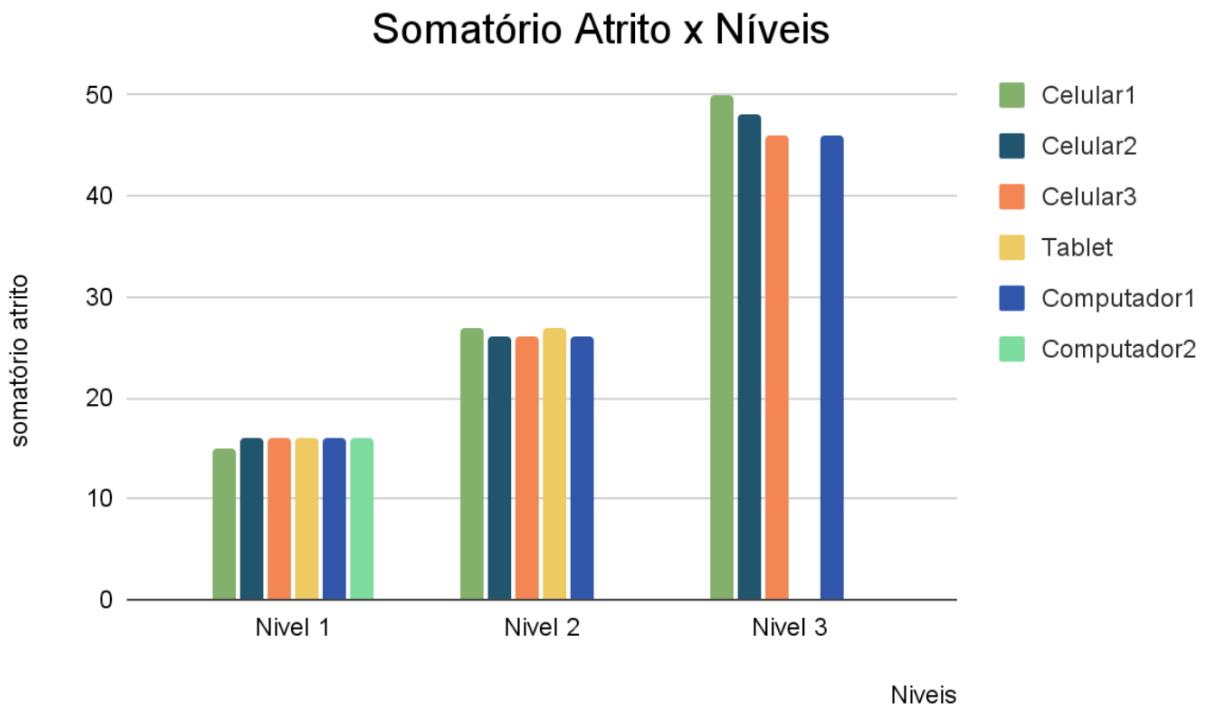

Figura 5.5: Quantidade de atrito por nível

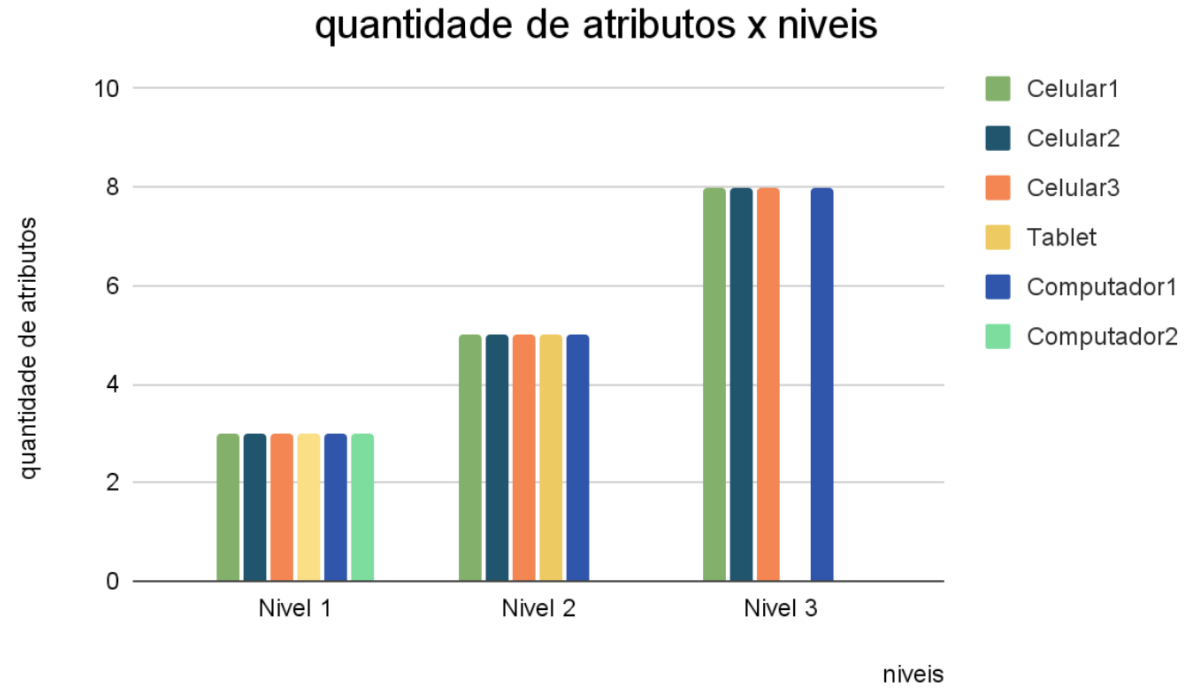

Figura 5.6: Quantidade de parâmetros por nível

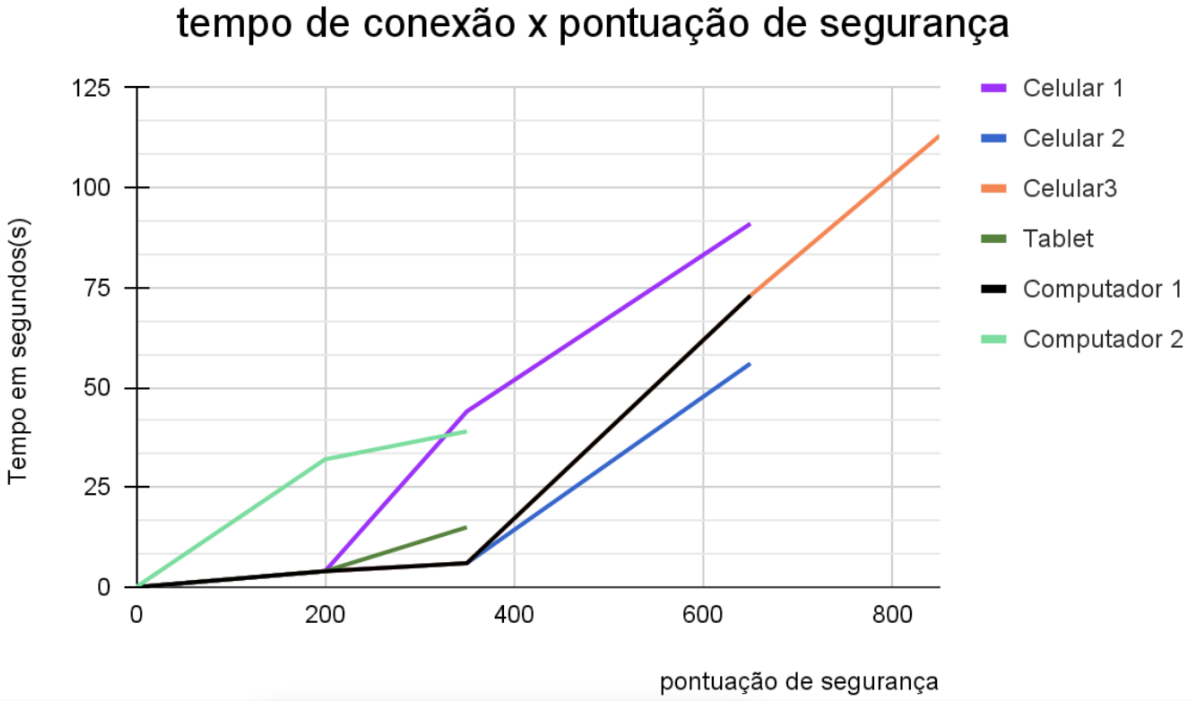

Figura 5.7: Tempo de conexão de acordo com os pontos

6 Conclusão

Com a análise realizada, os testes executados e a visualização dos gráficos, a conclusão que é possível chegar é que proposta atende às necessidades de segurança versus o atrito nos níveis de acesso. Observamos que há duas opções de parâmetros que se destacam na produção de atrito reduzida e tempo necessário para a conexão, sendo elas: ***Geolocalização*** e ***Impressão Digital***. A autenticação usando estes dois parâmetros se mostraram bem eficientes tendo em vista que Impressão Digital é um atributo confiável e com um bom custo de *hardware* e um atrito baixo, o movimento de colocar um dedo no sensor é bem rapido e fácil, sendo assim esta uma excelente opção a ser utilizada. A geolocalização pode ser considerada menos segura, porém em uma casa com mecanismos sem fio de acesso tem-se uma distância limitada, o que torna a falsificação mais difícil é assim o atributo se apresenta como uma excelente opção para ser usada, principalmente por conta do seu desempenho de tempo na hora da conexão.

Também é observado a crescente do tempo e atrito em relação ao níveis, à medida que eles vão subindo a quantidade de parâmetros cresce de maneira quase que linear, porém no tempo gasto o aumento é bem maior, numa proporção exponencial. Outro fator observado é a quantidade mínima de parâmetros necessários para cada nível, assim podemos previamente saber se o dispositivo terá acesso permitido ou não.

Levando em conta que a quantidade de atributos para cada nível sobe mais devagar que a quantidade de tempo necessária para a conexão em cada nível, concluímos que independentemente dos atributos usados o fator do tempo de conexão deve ser um dos fatores que mais pesam na hora da escolha dos atributos. Desta forma, fica evidenciado que os atributos que possuem menor tempo necessário são melhores e então ao se montar um sistema como este devemos dar preferência a equipamentos e dispositivos que possuam atributos de maior pontuação.

Concluímos também que um controle de acesso no modelo ABAC para o cenário de uma "casa inteligente" e com base em todos os testes, códigos, levantamentos e análises, se mostrou viável.

Como trabalhos futuros é possível avaliar a inserção de parâmetros exclusivos em cada dispositivo IoT. Por exemplo “a cafeteira entre 8:00 e 14:00 recebe pontos extras para facilitar o acesso” ou “verificar o nível de bateria como uma regra mandatória primária” e outras políticas que podem ser associadas à aos atributos de cada dispositivo. Outra possível avaliação é análise do impacto da expansão do cenário de uma casa tecnológica para uma cidade ou empresa inteligentes.

Bibliografia

ALIANE, L.; ADDA, M. Hobac: toward a higher-order attribute-based access control model. *Procedia Computer Science*, v. 155, p. 303–310, 2019. ISSN 1877-0509. The 16th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2019),The 14th International Conference on Future Networks and Communications (FNC-2019),The 9th International Conference on Sustainable Energy Information Technology. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S1877050919309585⟩.

ALVES, J. A.; CAMPOS, P.; BRITO, P. Q. *O futuro da Internet: estado da arte e tendências de evolução*. Centro Atlântico Lda., 1999. (Desafios). ISBN 972-8426-08-9. Disponível em: ⟨"https://books.google.com.br/books?id=ssCj-ag1lz8C&source=gbs_navlinks_s"⟩.

ASADI, A.; WANG, Q.; MANCUSO, V. A survey on device-to-device communication in cellular networks. *IEEE Communications Surveys Tutorials*, v. 16, n. 4, p. 1801–1819, 2014. Disponível em: ⟨"https://ieeexplore.ieee.org/document/6805125"⟩.

BHATT, S.; SANDHU, R. Abac-cc: Attribute-based access control and communication control for internet of things. In: *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*. New York, NY, USA: Association for Computing Machinery, 2020. (SACMAT '20), p. 203–212. ISBN 9781450375689. Disponível em: ⟨https://doi.org/10.1145/3381991.3395618⟩.

BISWAS, A.; BARANWAL, G.; Kumar Tripathi, A. Abac: Alternative by alternative comparison based multi-criteria decision making method. *Expert Systems with Applications*, v. 208, p. 118174, 2022. ISSN 0957-4174. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S0957417422013410⟩.

DIAS, P. H. *Desenvolvimento da Solução de Conectividade para a Rede de Sensores do Projeto VITASENIOR*. Dissertação (Mestrado em Engenharia Informática - Internet das Coisas) — Escola Superior de Tecnologia de Tomar, Novembro 2018. Disponível em: ⟨http://hdl.handle.net/10400.26/28597⟩.

FACCIONI, M. *Internet das Coisas*. 2016. Disponível em: ⟨"https://www.researchgate.net/profile/Mauro-Fazion-Filho/publication/319881659_Internet_das_Coisas_Internet_of_Things/links/59c038d5458515e9cfd54ff9/Internet-das-Coisas-Internet-of-Things.pdf"⟩.

HSU, R.-H.; FAN, H.-S.; WANG, L.-C. Sgd 2: Secure group-based device-to-device communications with fine-grained access control for iot in 5g. In: IEEE. *2021 IEEE Conference on Dependable and Secure Computing (DSC)*. [S.l.], 2021. p. 1–8.

HU, V. C. et al. Attribute-based access control. *Computer*, IEEE, v. 48, n. 2, p. 85–88, 2015.

INCOGNIA. *Autenticação baseada em risco*. 2021. Disponível em: ⟨"https://f.hubspotusercontent30.net/hubfs/5242234/Solutions%20Briefs/Incognia%20-%20Solution%20briefs%20-%20Autentica%C3%A7%C3%A3o%20baseada%20em%20risco.pdf"⟩.

MANCINI, M. Internet das coisas: História, conceitos, aplicações e desafios. 2018. Disponível em: ⟨"http://mmproject.com.br/wp-content/uploads/2020/02/artigo-iot-monicamancini-v1.pdf"⟩.

OLIVEIRA, N. R. de et al. Padrões e soluções para armazenamento, compartilhamento e estruturação de dados em saúde digital: Privacidade, integração e desafios. *XXIII Simpósio Brasileiro de Computação Aplicada à Saúde*, v. 23, p. 134, 2023. ISSN 978-85-7669-546-2. Disponível em: ⟨https://sol.sbc.org.br/livros/index.php/sbc/catalog/view/123/546/833-1⟩.

SILVA, E. F.; MUCHALUAT-SAADE, D. C.; FERNANDES, N. C. Across: A generic framework for attribute-based access control with distributed policies for virtual organizations. *Future Generation Computer Systems*, v. 78, p. 1–17, 2018. ISSN 0167-739X. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S0167739X17316060⟩.

YAN, Z. et al. Flexible data access control in d2d communications. *Future Generation Computer Systems*, v. 82, p. 738–751, 2018. ISSN 0167-739X. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S0167739X1730835X⟩.

ZHANG, A. et al. Seds: Secure data sharing strategy for d2d communication in lte-advanced networks. *IEEE Transactions on Vehicular Technology*, v. 65, n. 4, p. 2659–2672, 2016. Disponível em: ⟨https://ieeexplore.ieee.org/abstract/document/7065294⟩.