Controle de Acesso Sensível ao Contexto e *Zero Trust* para a Segurança em *E-Health*

Lucas Lino do C. Freitas[1], **Kristtopher K. Coelho**[2], **Michele Nogueira**[3], **Alex Borges Vieira**[1], **José Augusto M. Nacif**[2], **Edelberto Franco Silva**[1]

[1]Programa de Pós-Graduação em Ciência da Computação (PPGCC)
Universidade Federal de Juiz de Fora (UFJF)

[2]Instituto de Ciências Exatas e Tecnológicas
Universidade Federal de Viçosa (UFV - Campus Florestal)

[3]Departamento de Ciência da Computação (DCC)
Universidade Federal de Minas Gerais (UFMG)

{kristtopher.coelho,jnacif}@ufv.br, michele@dcc.ufmg.br

{edelberto,alex.borges,lucas.freitas}@ice.ufjf.br

Abstract. *In an increasingly connected world, ensuring security in e-health is a challenge. Traditional security models based on perimeter trust are insufficient to guarantee the protection of these systems. Since these models work by directly assigning trust to the user, the entire network becomes vulnerable if the user's credentials or device are compromised. Thus, this work proposes and evaluates a model based on Zero Trust to considerably increase security in e-health environments. The proposed model is based on privilege reduction and user confidence analysis to perform access control. The evaluation follows simulation in different scenarios, assessing their assertiveness in delegating access. The results show the effective detection of anomalies in accesses by the model.*

Resumo. *Em um mundo cada vez mais conectado, garantir a segurança em sistemas de saúde é um desafio. Os modelos de segurança tradicionais, baseados na confiança em perímetro, são insuficientes para garantir a proteção desses sistemas. Uma vez que esses modelos funcionam com a atribuição direta de confiança ao usuário, caso sejam comprometidas as credenciais ou o dispositivo do usuário, toda a rede se torna vulnerável. Assim, este trabalho propõe e avalia um modelo baseado em Zero Trust para o aumento considerável de segurança em ambientes e-health. O modelo proposto é baseado na redução de privilégios e na análise de confiança do usuário para realizar o controle de acesso. A avaliação de desempenho ocorreu por simulações, avaliando-se sua assertividade na delegação de acesso. Os resultados mostram a detecção eficaz de anomalias nos acessos pelo modelo.*

1. Introdução

A medicina incorpora cada vez mais tecnologias que ajudam a combater várias doenças. Essas tecnologias adicionam inovações nos sistemas de saúde e contribuem para aprimorar a qualidade de vida dos pacientes [Barra et al. 2006]. No entanto, a implementação de

novos recursos tecnológicos tem tornado os sistemas *e-health* alvos de invasores que buscam ter acesso aos recursos e seus dados. Segundo [Luh and Yen 2020], a área da saúde enfrenta uma "tempestade cibernética perfeita", onde cada vez mais são produzidos dados médicos, porém o investimento na segurança dos sistemas ainda se mantém insuficiente. Neste sentido, garantir um controle de acesso aos recursos de forma eficiente é vital.

De maneira geral, o modelo de segurança no controle de acesso comumente utilizado nas organizações é baseado em perímetro, onde sua infraestrutura de rede é dividida em duas ou mais áreas, diferenciando a rede interna e externa. A segurança aplicada se baseia na rede utilizada. Este modelo faz uso de confiança implícita, concedendo acesso aos recursos aos usuários considerados confiáveis, por meio de processos de autenticação e autorização. No entanto, esse modelo traz uma série de vulnerabilidades, pois, uma vez que um invasor consiga se autenticar, passa a ser considerado confiável e ter acesso aos sistemas disponíveis [Teerakanok et al. 2021].

Nestes modelos, para mitigar os riscos de acesso de usuários em perímetros não confiáveis, diversas ferramentas são comumente empregadas para compor o controle de acesso (e.g., *firewall*, *proxy*, IDS, IPS). Essas ferramentas validam o acesso do usuário antes que ele tenha acesso aos perímetros confiáveis, mas nem sempre sendo eficazes [Souza 2013]. Diante disso, o *Zero Trust* (ZT) surge como uma alternativa para proporcionar maior segurança ao controle de acesso, independentemente do perímetro de rede utilizado pelo usuário. Com sua arquitetura definida pelo *National Institute of Standards and Technology* (NIST) [Rose et al. 2020], o modelo ZT assume que ninguém é considerado totalmente confiável e que a autorização de acesso aos recursos deve ser revista continuamente.

Este trabalho apresenta um sistema de controle de acesso em ambientes *e-health* baseado no princípio do *Zero Trust*, reduzindo privilégios de acesso e eliminando a confiança implícita. Sua principal contribuição está na proposta de um modelo simples e sensível para cálculo de confiança e detecção de acessos anômalos. O sistema proposto avalia o nível de confiança do usuário para cada acesso, considerando atributos do ambiente, perfil do usuário e sensibilidade do recurso e, assim, permite ou nega o seu acesso à aplicação de *e-health*. Embora o tema *Zero Trust* ainda seja muito pouco explorado por outros autores, este trabalho busca, além de avaliar o controle de acesso, aproximar os experimentos de situações reais que podem serem exploradas em ambientes *e-health*, tais como uso normal, roubo de *token*, roubo de credenciais e ataque de força bruta. Os resultados mostram que o sistema determinou a confiança ao usuário de forma eficiente, identificando ações suspeitas e bloqueando acessos indevidos.

Este trabalho segue a estrutura descrita a seguir. A Seção 2 aborda a fundamentação teórica sobre os temas. A Seção 3 apresenta os trabalhos relacionados ao ZT. A Seção 4 detalha o processo de desenvolvimento do sistema. A Seção 5 descreve os testes e resultados obtidos. Por fim, a Seção 6 apresenta as conclusões.

2. Fundamentação Teórica

Esta seção aborda conceitos para a compreensão do trabalho. Os conceitos de gestão de identidade e de acesso e métodos de autorização são descritos. Em seguida, é apresentada uma visão do *Zero Trust* e sua arquitetura.

2.1. Gestão de Identidade e Acesso

A Gestão de Identidade e Acesso (IAM) pode ser definida como um conjunto de processos e métodos cujo objetivo é fornecer segurança adequada para a identidade, dados e recursos da organização, por meio de políticas e procedimentos empregados [Sharma et al. 2015]. A identidade no mundo digital representa uma série de informações do usuário, as quais podem ser utilizadas para diversos fins. O gerenciamento de identidade é uma metodologia de representação e reconhecimento de identidades no mundo digital, de forma a garantir a integridade das informações [Leandro et al. 2012].

Na gestão de identidade, além de todo processo de emissão, revogação e segurança da identidade do usuário, se faz muito presente também os processos de autenticação, autorização e auditoria (Protocolos AAA). O processo de autenticação é responsável por assegurar que determinado usuário ou dispositivo é quem realmente afirma ser. Já o processo de autorização garante que, uma vez autenticado, o usuário ou dispositivo só tenha à sua disposição os recursos aos quais está permitido usar. Por fim, a auditoria é o processo de análise das operações, onde através da coleta dos dados relacionados ao uso dos recursos pelos usuários, como quem acessou, quando acessou, o que acessou, entre outros, se possa aferir sua qualidade [Pace 2008]. Alguns métodos de autorização serão descritos na Seção 2.2.

2.2. Métodos de Autorização

Uma vez combinados com modelos de autenticação, os mecanismos de autorização garantem que usuários ou dispositivos, com identidades já verificadas, estejam permitidos a acessar recursos específicos. Ao serem liberados, os mecanismos de autorização asseguram que o usuário ou dispositivo tenha acesso aos recursos que lhes são correspondentes, de forma ágil e sem interrupções. Dentre os diversos modelos de autorização, podemos citar como principais, o controle de acesso baseado em atributos e risco.

No modelo de Controle de Acessos Baseado em Atributos (ABAC), o sistema utiliza de atributos em torno da operação para determinar a validade de determinada solicitação de acesso, utilizando esses atributos como base para a liberação ou não do acesso ao recurso. Os atributos considerados podem ser os mais diversos, mas geralmente trabalha-se com os três principais: atributos de sujeito, objeto e ambiente [Hu et al. 2015]. Para a liberação de acesso nesse modelo, em cada requisição realizada, os atributos correspondentes ao recurso devem ser atendidos pelos atributos do usuário. Após um conjunto de decisões baseadas nos atributos especificados, o usuário terá seu acesso permitido caso satisfaça a todas as condições [Cremonezi et al. 2021].

Já no modelo de Controle de Acessos Baseado em Riscos (RbAC), o sistema considera todas as variáveis envolvidas para promover uma análise e estudo dos riscos, e com base nas probabilidades e potenciais danos de uma ocorrência, determina-se a validação ou não da liberação de determinado acesso [Hany et al. 2017]. O processo de análise de risco para o controle de acessos pode se dar de duas formas: qualitativa ou quantitativa. No modelo qualitativo, é necessária a intervenção de um especialista para valorizar os riscos, permitindo a aplicação de diferentes escalas de graduação. No modelo quantitativo, procura-se atribuir números que representam o risco envolvido. O cálculo geralmente utilizado em métodos quantitativos para se definir o risco é dado por $R = P \cdot I$, onde o R é o risco, P a probabilidade da sua ocorrência e o I o impacto deste risco [Santos et al. 2013].

2.3. *Zero Trust*

Focada na proteção dos recursos, o *Zero Trust* (ZT) trabalha com a ideia de que a confiança no usuário não deve ser estabelecida de forma fixa ou determinada de acordo com sua localização no perímetro, mas sim analisada e atribuída continuamente. O ZT não é um produto em si, mas um conjunto de princípios que buscam proporcionar maior segurança aos recursos da organização, onde promove a proteção na transação de informações, a integralidade dos dados e a certificação/autorização dos usuários ou dispositivos que acessam os recursos [Rose et al. 2020]. Por não se basear no perímetro de rede, o ZT trata todos os usuários igualmente como não confiáveis. A metodologia oferece apenas o mínimo de privilégios necessários para realizar sua tarefa, ao contrário dos modelos baseados em perímetro, nos quais o usuário muitas vezes recebe privilégios além do necessário para sua atividade. Para mitigar os efeitos da incerteza associada a um usuário com "plenos poderes", o *Zero Trust* busca autenticar o usuário e analisar seu comportamento, contexto, histórico e demais informações, para assim atribuir um determinado nível de confiança que deve ser atendido para acessar o recurso desejado [Rose et al. 2020]. Através da análise e atribuição de confiança, uma única solução é capaz de lidar com ameaças, tanto internas quanto externas, da mesma maneira.

3. Trabalhos Relacionados

Muitas propostas de controle de acesso para ambientes *e-health* já foram discutidas na literatura, abordando diversas metodologias. A maioria dos trabalhos visa implementar soluções para atenuar o acesso indevido aos recursos, com baixo custo, sem que isso afete os acessos legítimos. Nesta seção são abordados trabalhos de controle de acesso na área da saúde, que utilizaram pelo menos uma das metodologias: RbAC, ABAC ou *Zero Trust*.

Um modelo de RbAC para ambientes *e-health* foi proposto em [Mazzocca et al. 2022], onde a premissa para determinar o acesso está no risco envolvido na operação. Seu objetivo principal foi propor um controle de acesso adaptável, de forma que, ao estimar o risco de acesso e avaliar o contexto, seja possível tomar sua decisão dinamicamente. Para isto, a estimativa do risco de cada acesso é classificada como estável, grave ou crítico, conforme a possível interferência em tratamentos médicos e a sensibilidade dos dados desejados. A avaliação do contexto, por sua vez, verifica principalmente as informações armazenadas e da requisição para construir políticas de controle de acesso.

Em [Pussewalage and Oleshchuk 2017], foi proposto um modelo de ABAC com delegação de acesso. No sistema apresentado, para conceder o acesso aos recursos, o modelo analisa os atributos da requisição, buscando correlações entre o usuário e os dados requeridos. Caso não haja correlações, é possível criar delegações de acesso, temporárias ou permanentes, através de *tokens* assinados. Desta forma, cria-se uma forma mais flexível para o compartilhamento de dados entre múltiplas bases de dados.

Em relação ao *Zero Trust*, ainda é um tema pouco explorado, especialmente na área da saúde. Em [Wang et al. 2023] foi realizada uma pesquisa e implementação de um modelo *Zero Trust* para propor maior segurança em ambientes médicos. Ele utiliza do modelo RBAC e dos princípios do ZT para determinar a confiança do usuário com base em seu comportamento. Para a determinação do acesso, é realizada uma análise abrangente entre o valor de risco e o grau de confiança. Como resultados, o modelo se mostrou

eficaz, melhorando a proteção dos recursos médicos. Entretanto, os autores destacam a necessidade de estudos futuros para melhoria de eficiência, autenticação e otimizar os resultados. Em [Chen et al. 2020] também foi proposto um modelo *Zero trust* para *e-health*, porém abordado no de uso de redes 5G. Para determinação do nível de confiança e risco em cada acesso, o sistema considerou quatro dimensões (compondo assunto, objeto, ambiente e comportamento) para realizar seu cálculo. Os testes mostraram que o sistema foi eficaz no controle de acesso, entretanto os autores apontam a necessidade de otimização de desempenho, devido a altos custos computacionais durante avaliação de confiança.

Embora os trabalhos mencionados tenham apresentado bons resultados em relação ao controle de acesso, os estudos que abordaram o Zero Trust (ZT) exploraram pouco testes em cenários e situações reais de uso, concentrando-se principalmente no controle entre recursos e usuários. Por outro lado, os trabalhos que não abordaram o ZT ainda são fundamentados em perímetros e operam com a confiança implícita. Neste sentido este trabalho busca implementar e testar um modelo com ZT em cenários distintos, mesclando diferentes metodologias, onde através da determinação da confiança do usuário (ZT), do risco envolvido (RbAC) e análise dos atributos (ABAC), visa-se estabelecer um controle de acesso sensível em ambientes de *e-health*, independentemente do perímetro de uso.

4. Sistema Proposto

O desenvolvimento deste trabalho baseou-se na definição da arquitetura base do ZT, definida em [Rose et al. 2020] e apresentada na Figura 1-a. O processo consiste em um conjunto de usuários ou dispositivos que buscam acessar determinados recursos, e entre essas duas partes, o sistema ZT analisa as requisições, determina o nível de confiança do usuário e a sensibilidade do recurso para tomar sua decisão. Como apresentado na figura, a implementação foi dividida em três partes: cliente, recursos e sistema de controle de acesso (ZT). Essas partes foram desenvolvidas na linguagem de programação Python[1], uma linguagem amplamente utilizada para análise de dados e desenvolvimento.

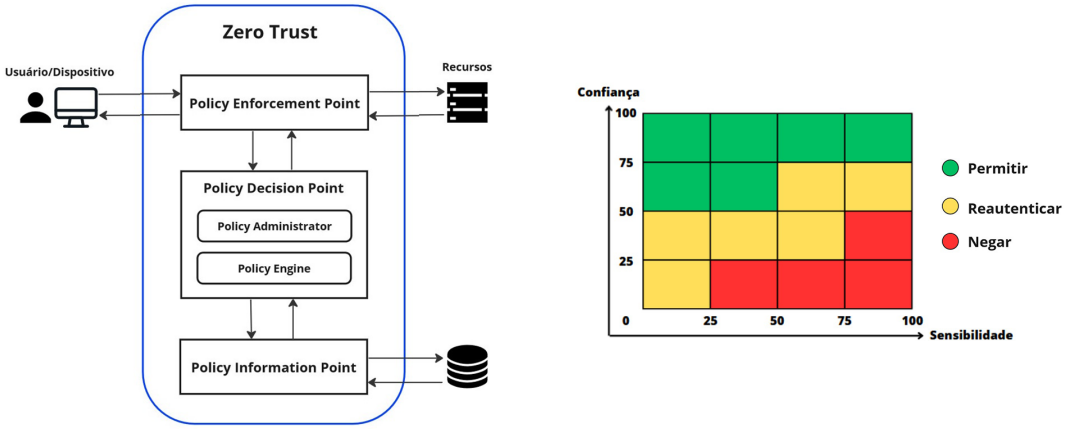
A arquitetura do ZT proposto é composta por três módulos principais: PEP (*Policy Enforcement Point*), PDP (*Policy Decision Point*) e PIP (*Policy Information Points*). O PEP é responsável por receber a requisição, fazer todo o controle de sessão, enviar o pedido ao PDP e aplicar a decisão tomada. O PDP é responsável por conduzir o controle de acesso com base nas políticas definidas. Por fim, o PIP é responsável por reunir todas as informações necessárias para que o PDP possa analisar o pedido. Para simulação da rede, cada um dos componentes (usuários, dispositivos, recursos e ZT) foram executados como um *processo*, onde a comunicação entre eles se deu através de *sockets*[2].

Para determinar o acesso aos recursos, o ZT proposto toma sua decisão através do cruzamento de duas informações, ambas definidas com valores em um intervalo de 0 a 100. Primeiro, é calculada a confiança do usuário, e em seguida, é definido o risco de acesso, ou seja, a sensibilidade em relação ao recurso desejado. O cálculo da confiança e a definição da sensibilidade são detalhados nas Seções 4.1 e 4.2, respectivamente.

Com a confiança e a sensibilidade definidas, o acesso pode ser permitido, negado ou solicitada uma reautenticação, de acordo com seus níveis. Conforme ilustrado na

[1] `https://www.python.org/`

[2] Socket: Um *endpoint* composto por uma quádrupla "IP:PORT" (origem/destino) utilizado para identificar um processo específico.



(a) Arquitetura ZT [Rose et al. 2020]

(b) Tabela de Permissões

Figura 1. Arquitetura *Zero Trust* e tabela de permissões.

Figura 1-b, caso o nível de confiança seja baixo, o usuário só poderá acessar recursos de menor sensibilidade e por meio de reautenticação. À medida que o nível de confiança aumenta, será permitido o acesso a recursos mais sensíveis. Desta forma, caso o sistema identifique alguma anormalidade de acesso, basta reduzir a confiança do usuário para proteger os recursos mais sensíveis. O fluxo de atividades realizado pelo sistema pode ser observado no diagrama da Figura 2, onde a sensibilidade e a confiança são detalhadas nas seções 4.1 e 4.2 respectivamente, e o resultado final definido conforme Figura 1-b.

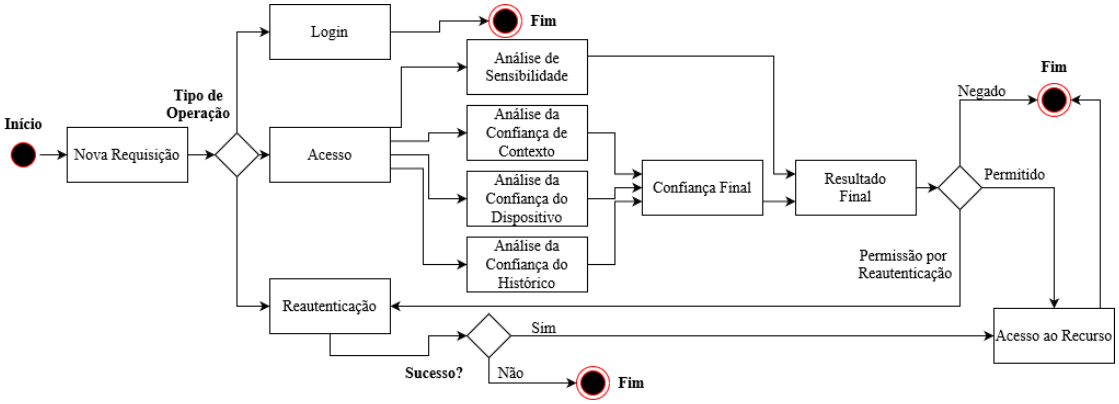


Figura 2. Diagrama de Atividades.

4.1. Recursos e Sensibilidade

Para explorar os ambientes *e-health* realistas, foram escolhidos cinco recursos, comumente utilizados na área da saúde, para compor os recursos disponíveis. Esses recursos foram modelados e são utilizados pelo ZT para o emprego do controle de acesso. São eles: Registro Eletrônico de Saúde (EHR); Sistema de Informação Hospitalar (HIS); Monitoramento Remoto do Paciente (RPM); Portal do Paciente (PP) e Telemedicina.

Além disso, para cada um desses recursos é necessário descrever sua sensibilidade, para compor o controle de acesso juntamente com a confiança atribuída ao usuário.

Classificar a sensibilidade dos recursos é normalmente um processo que requer a opinião de especialistas da área para que seja possível quantificar seu risco. No entanto, como o objetivo deste trabalho está na autorização de acesso, as sensibilidades dos recursos foram definidas de forma empírica. A análise da sensibilidade dos recursos foi realizada em relação aos seus sub-recursos, com base nos tipos de informações que contêm e no tipo de ação, ou seja, caso o tipo de ação e informação do sub-recursos possuir uma alta probabilidade de impacto na vida ou tratamento dos pacientes, vazamento de dados, etc, será classificado com uma sensibilidade maior. Para isso, cada sub-recurso foi classificado em um intervalo de 0 a 100, sendo 0 como não sensível e 100 como altamente sensível, conforme exemplo da Tabela 1.

Tabela 1. Exemplo de classificação de sensibilidade

Sensibilidade dos Sub-recursos				
Tipo de Informação	**Leitura**	**Escrita**	**Modificação**	**Exclusão**
Prescrições Médicas (EHR)	35	60	70	73
Notas Clinicas (PP)	53	80	88	88
Histórico Médico (EHR)	63	95	98	98

4.2. Análise de Confiança.

Os mecanismos de avaliação de confiança desempenham um papel fundamental no suporte à tomada de decisões em sistemas de controle de acesso. Eles são utilizados para avaliar o grau de confiança de usuários em potencial e determinar a probabilidade de que identidades possam estar comprometidas ou realizar ações não autorizadas. O cálculo de confiança do usuário pode ser realizado de diversas maneiras, tendo como principal fator de avaliação a análise com base no seu comportamento. Com base neste preceito, a proposta de avaliação de confiança foi realizada a partir de três perspectivas, cada uma tendo como resultado uma pontuação de 0 a 100:

• **Confiança ao usuário baseada no contexto**. Nesta fase, a confiança é determinada com base na forma como os usuários interagem com o sistema. Os seguintes fatores de penalização foram elaborados:

- P1: Múltiplos *logins* falhos consecutivos recentes
- P2: Alterações de senha recente
- P3: Mudanças considerável na localização com base nos acessos recentes
- P4: Acesso fora do horário estipulado (proporcional ao quanto)
- P5: Redução de privilégios recentes
- P6: Mudança da rede que utiliza para conectar ao sistema

• **Confiança ao dispositivo**. A avaliação do dispositivo utilizado para acesso pode indicar anomalias no acesso. Os seguintes fatores de penalização foram elaborados:

- P7: Dispositivo nunca utilizado anteriormente
- P8: Dispositivo compartilhado por outros usuários
- P9: Alteração nas características do dispositivo (*device fingerprint*)
- P10: Dispositivo com versões de sistema/softwares antigos

• **Confiança com base no histórico**. Refere-se ao nível de confiança do usuário, com base em seu comportamento passado. Os seguintes fatores foram levados em consideração:

- P11: Frequência de acesso à recursos altamente sensíveis
- P12: Múltiplas requisições negadas
- P13: Usuário recente

Ainda para análise da confiança no histórico, foi levada em consideração a média obtida da confiança do usuário em seus 3 últimos acessos. Após a análise dos dados mostrados anteriormente, o índice de confiança de cada perspectiva é calculado através da pontuação máxima que ele pode obter (100), subtraindo as penalidades encontradas:

$$C_p = 100 - \left(\sum_{n=1}^{N} A_n \right), \text{ onde } A_n \in [0, 100] \tag{1}$$

Onde N é o número de fatores avaliados, A_n é a avaliação de penalidade para o fator n e C_p é o resultado da confiança na perspectiva p (contexto, dispositivo e histórico), definida no intervalo $C_p \in [0, 100]$. Para calcular a confiança final, primeiramente é estabelecida uma média entre as confianças do contexto e dispositivo, para que por fim, possa-se levar em consideração a confiança do histórico. Desta forma, a confiança com base no histórico possui uma relevância alta no resultado final, o que contribui para um dos requisitos do *Zero Trust*, no qual um usuário recente recebe baixa confiança e privilégios mínimos. O cálculo da confiança final pode ser observado na Equação 2.

$$C_f = (\sqrt{C_c \cdot C_d})P, \text{ onde P } = \begin{cases} \frac{1}{100} C_h, C_h > 0 \\ 0.1, C_h = 0 \end{cases} \tag{2}$$

Onde C_h é a confiança com base no histórico, P é a normalização do valor de C_h em [0.01, 1], C_d é a confiança com base no dispositivo, C_c é a confiança com base no contexto e C_f é o resultado final da confiança do usuário. Para avaliações de confiança com base no histórico que obtiveram pontuação 0 (como no caso de usuários novos), é determinada uma pontuação mínima para evitar uma estagnação na confiança final.

5. Avaliação e Resultados

Para a realização dos testes, foram geradas instâncias que definem o comportamento do usuário. Em cada instância, um vetor determina uma sequência de operações que um usuário realiza, contendo os dados necessários para o acesso. Para realizar uma operação de acesso, por exemplo, o usuário deve enviar ao ZT o recurso desejado, o tipo de operação, seu *token* de acesso, o tipo de ação a realizar em cima do recurso, dentre outros, conforme exemplificado na Figura 3. Deste modo, foi possível simular todo um contexto de uso, com diversos atributos, compreendendo desde a rede até o horário de acesso.

Em sistemas normalmente classificados como sensíveis (*e.g.*, *e-Health*, financeiros), é comum que haja uma análise prévia do dispositivo, para coletar informações e garantir maior segurança. No caso deste trabalho, o mesmo foi simulado com o envio das informações como sistema operacional, versão e *Device Fingerprint*. Um ponto a ser destacado na estrutura da instância utilizada é a definição se o usuário poderá realizar a reautenticação ou não, caso solicitado (atributo da linha 3 na Figura 3). Isso é útil, pois possibilita testar cenários de acessos ilícitos onde um infiltrante possui, de alguma forma, acesso a um dispositivo autenticado ou *token* do usuário, porém não detém das credenciais para se identificar e portanto, não consegue se reautenticar.

```
[
    {
        "REAUTHENTICATE": true,
        "TYPE": "ACCESS",
        "RESOURCE": "Sistema de Informacao Hospitalar",
        "SUB_RESOURCE": "Registros Cadastrais da Enfermagem",
        "TYPE_ACTION": "Leitura",
        "IP_ADDRESS": "172.16.10.1/24",
        "LATITUDE": "-21.7866751",
        "LONGITUDE": "-43.3688584",
        "MAC": "CA-14-17-8G-9E-9F",
        "DFP": "29930a0e2ea9e88d47e59571862aaf2c01781cbef7dbac0615e9efe383c8235b",
        "OS": "Windows 10",
        "VERSION_OS": "21H2",
        "TIME": "2023-06-15 13:36:19.047062"
    }
]
```


Figura 3. Instância de exemplo de acesso do usuário

Para avaliar a proposta, foram gerados 4 cenários distintos nos quais foram analisadas métricas de taxa de erros e sucessos no controle de acesso, bem como se acessos legítimos foram negados indevidamente, ou se acessos ilegítimos foram permitidos erroneamente. Para cada cenário, foi calculado também o tempo para tomada de decisão em cada acesso, sendo este o intervalo entre a requisição e a resposta. As escolhas dos cenários testados ocorreram, principalmente, pelo fato de serem comuns em ambientes de saúde e por seu potencial dano.

5.1. Cenário 1: Uso Normal

Neste cenário, o objetivo é simular uma sequência de acesso semelhante a um uso normal do cotidiano. Determinar um uso normal pode não ser trivial, uma vez que o perfil de cada usuário pode variar. Assim, foi aplicada uma aproximação para classificação relacionada ao que consideramos como uso normal.

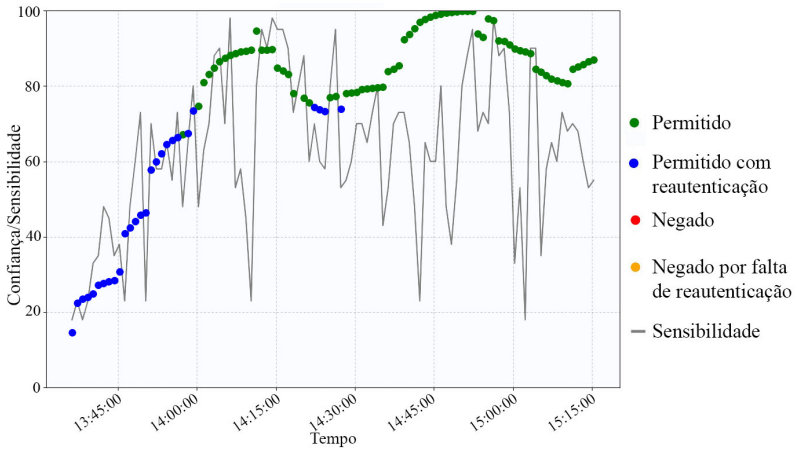


Figura 4. Teste cenário 1: Uso Normal.

O gráfico da Figura 4 mostra a simulação realizada com 100 acessos consecutivos, com intervalo de 1 minuto, onde no eixo Y temos a confiança/sensibilidade do acesso e no eixo X o tempo. A linha cinza mostra a sensibilidade do recurso acessado em cada requisição, e cada ponto representa um acesso. Os pontos verdes, azuis, vermelhos e laranjas representam os acessos permitidos, permitidos por meio da reautenticação, negados e negados por falta de reautenticação, respectivamente.

É possível observar neste primeiro cenário que, nas primeiras requisições, o nível de confiança do usuário foi baixo, visto que não foi possível coletar informações necessárias para creditar mais confiança. Portanto, nas requisições iniciais o usuário só conseguirá ter acesso aos recursos com sensibilidade mais baixa e por meio de reautenticação. O que está em concordância com a premissa do ZT de definir sempre privilégios mínimos ao usuário. Podemos observar também que, à medida em que o usuário continua a realizar os acessos, sua confiança aumenta gradativamente, até permitir acesso aos recursos com sensibilidade altíssima e não necessitar mais de reautenticação. Outro ponto interessante a observar é que ao realizar uma sequência de acessos a recursos altamente sensíveis, ocorreu um efeito de "onda", que reduziu sua confiança, forçando-o até a se reautenticar para continuar o acesso. Isto se deve à penalização P11 da avaliação da confiança com base no histórico, que diz respeito à frequência a recursos altamente sensíveis. Desta forma, esta regra garante uma certa proteção a estes recursos em casos de acessos indevidos. Neste cenário, 73% dos acessos foram permitidos e 27% permitidos por meio de reautenticação. O tempo médio para tomada de decisão neste cenário foi de 36 milissegundos. Para realização dos demais cenários, os mesmos funcionarão como uma extensão deste cenário, com a adição de 20 novos acessos, cada um com suas especificações.

5.2. Cenário 2: Roubo de *Token*

O cenário 2 avalia casos em que ocorre a captura do *token* de um usuário legítimo por um usuário malicioso. Testar esse caso se faz necessário, visto que, com o *token* em mãos, um usuário ilegítimo pode se identificar e acessar a conta, sem necessariamente possuir as credenciais de acesso do usuário, serviços e recursos protegidos, além de realizar ações em nome do usuário sem sua permissão. Assim, é imprescindível que o sistema de controle de acesso detecte mudanças no uso para identificar e indeferir acessos ilegítimos.

Existem diversas formas pelas quais um ataque de roubo de *token* pode ocorrer. Entre as mais conhecidas, uma das formas de obtenção de token é através da interceptação do tráfego de rede, como forma de capturar pacotes na rede (*sniffing*) ou interceptar e intermediar a comunicação entre cliente e servidor (*Man-in-the-Middle*). Outros meios ainda podem ser empregados, como a utilização de *malware* para infectar e capturar *tokens* armazenados nos dispositivos de médicos e pacientes. Devido às diferentes formas pelas quais este roubo de *token* pode ocorrer, esse cenário foi dividido em duas partes: a primeira com acessos em regiões próximas à área de uso do usuário legítimo e a segunda em regiões mais distantes.

Para a realização do primeiro teste, foi considerado que o invasor está localizado em região próxima à de uso do usuário e não possui as credenciais para autenticação. O fator localização é importante, visto que um dos critérios de avaliação da confiança é a análise da localização de acesso atual em relação aos acessos anteriores. Isso permite detectar mudanças bruscas em um curto intervalo de tempo, ou mesmo avaliar acessos fora dos locais habituais. Neste teste, consideramos também que o invasor utilizou outra rede e seu próprio dispositivo para efetuar o acesso. Ao analisar o primeiro gráfico da Figura 5, podemos perceber que, a partir do momento da primeira requisição, foram detectadas mudanças no comportamento do usuário e por consequência, sua confiança foi reduzida para proteger os recursos. Neste caso, a penalização na confiança ocorreu tanto pela leve alteração na localização, quanto pela mudança repentina de rede e pelo uso de um dispositivo nunca antes utilizado. Podemos observar também que, de imediato, o sistema

exigiu reautenticação para que o usuário continuasse com o acesso. Como neste cenário o usuário não dispunha das credenciais necessárias, teve seu acesso negado. Como resultado, 15% dos acessos deste teste foram negados por falta de reautenticação e os demais foram diretamente negados, com sua confiança reduzida gradativamente. O tempo médio para tomada de decisão deste teste foi de 38 milissegundos.

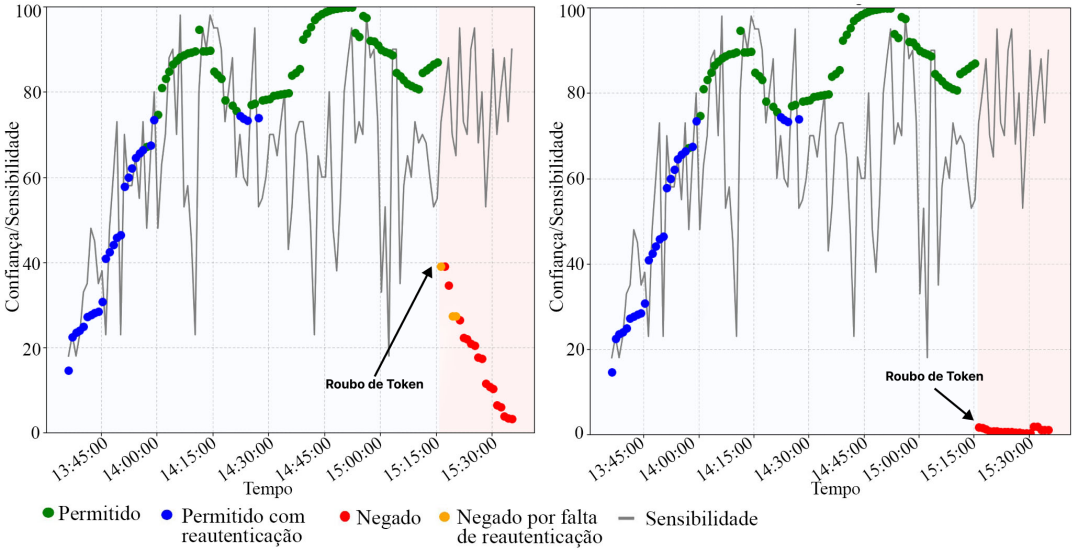


Figura 5. Teste cenário 2: Roubo de *token* em região próxima e distante.

De forma semelhante ao caso anterior, o segundo teste utilizou as mesmas configurações, porém realizado em uma região muito distante à habitual e em um intervalo de tempo muito pequeno. Como podemos observar no segundo gráfico da Figura 5, como forma de garantir a segurança de seus recursos, todas as requisições foram negadas, onde não permitiu nem ao menos a possibilidade de reautenticação. O tempo médio para tomada de decisão neste segundo teste foi de 38 milissegundos.

5.3. Cenário 3: Roubo de Credenciais

Neste terceiro cenário, o objetivo é avaliar situações relacionadas ao roubo de credenciais de acesso. Este tipo de caso é um desafio para o controle de acesso, visto que, como o invasor possui conhecimento das credenciais, o mesmo pode se reautenticar –caso seja exigido–, o que dificulta a diferenciação entre um usuário ilegítimo e um legítimo. Portanto, nestas circunstâncias, o comportamento do usuário se torna ainda mais relevante para determinar sua confiança.

Para obtenção das credenciais de acesso, um invasor pode utilizar diversos meios, tendo como principais a utilização de técnicas de engenharia social, onde se faz uso de estratégias para ludibriar o usuário (*e.g.*, *e-mails* falsos de resultados laboratoriais com exigência de *login* em site falso para visualizá-lo), ou até mesmo com o uso de *malwares* para captura das teclas digitadas em seu dispositivo (*e.g.*, *keylogger*). Neste sentido, este teste seguiu configurações semelhantes às realizadas no primeiro teste do cenário 2, com a diferença de que o invasor possui acesso à credencial e não ao *token*. Ainda assim, ao manter as tentativas de acesso em uma região próxima ao de acesso do usuário, mas utilizando outra rede e outro dispositivo.

Como podemos observar no gráfico da Figura 6, neste cenário o sistema proposto apresentou resultados interessantes, porém passíveis de aprimoramento. É possível perceber que o sistema reduziu a confiança ao detectar mudanças em seu comportamento e, conforme a sensibilidade do recurso requisitado, exigiu a reautenticação ou negou seu acesso. Como o infiltrante possui acesso às credenciais, ele conseguiu acessar alguns recursos de sensibilidade não tão alta (*i.e.*, média, baixa). Contudo, ainda assim, o acesso aos recursos altamente sensíveis foi protegido, tendo neste cenário uma eficácia de 50% do total de acessos. É possível compreender também neste cenário, que a utilização de um segundo fator de autenticação poderia contribuir para a redução dos acessos indevidos, de forma a reduzir a quantidade de informações de identificação que um invasor possa obter. O tempo médio para tomada de decisão deste cenário foi de 37 milissegundos.

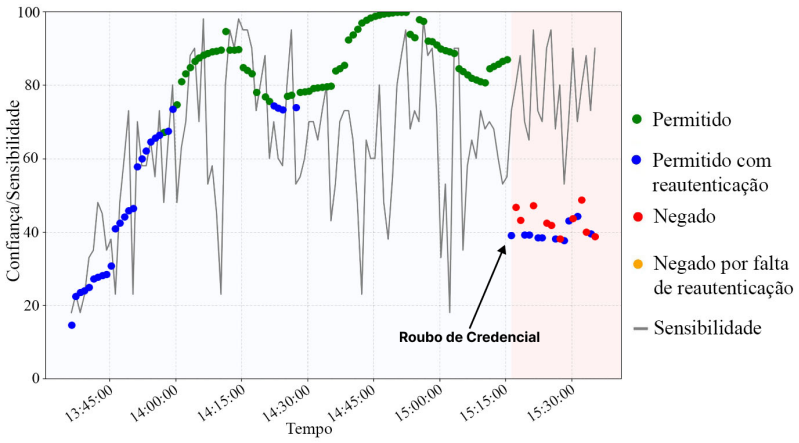


Figura 6. Teste cenário 3: Roubo de credencial.

5.4. Cenário 4: Ataque de Força Bruta

No quarto cenário, o objetivo foi analisar e testar uma situação de ataque de força bruta. Esse tipo de ataque é uma técnica usada por invasores para tentar quebrar a segurança de uma conta ou sistema ao testar várias combinações possíveis de login em um curto espaço de tempo. Geralmente, esse tipo de ataque visa explorar vulnerabilidades em senhas fracas ou previsíveis, na tentativa de encontrar a combinação correta para obter acesso não autorizado. Assim, é possível avaliar neste cenário principalmente como a penalização P1 impacta no controle de acesso. Para isto, este teste foi dividido em duas partes: a primeira sem o sucesso no ataque e o segundo com sucesso.

No primeiro teste, foi simulada uma condição onde ocorreu uma série de tentativas de autenticação falhas, enquanto um usuário legítimo realizava seus acessos normais. Testar esta circunstância é importante para mensurar o quanto uma sequência de tentativas pode influenciar no uso regular, visto que, a redução de confiança de funcionários hospitalares por exemplo (e possivelmente a negação de acesso aos recursos), podem interferir diretamente no tratamento de pacientes. Ao observar o primeiro gráfico da Figura 7, podemos concluir que este ataque influenciou diretamente no cálculo e queda da confiança do usuário, porém não impediu sua utilização. Como resultado, o sistema protegeu os recursos mais sensíveis exigindo sua reautenticação. É possível observar também que nos últimos acessos sua confiança voltou a crescer, visto que não houve nenhuma outra penalização. O tempo médio para tomada de decisão deste teste foi de 40 milissegundos.

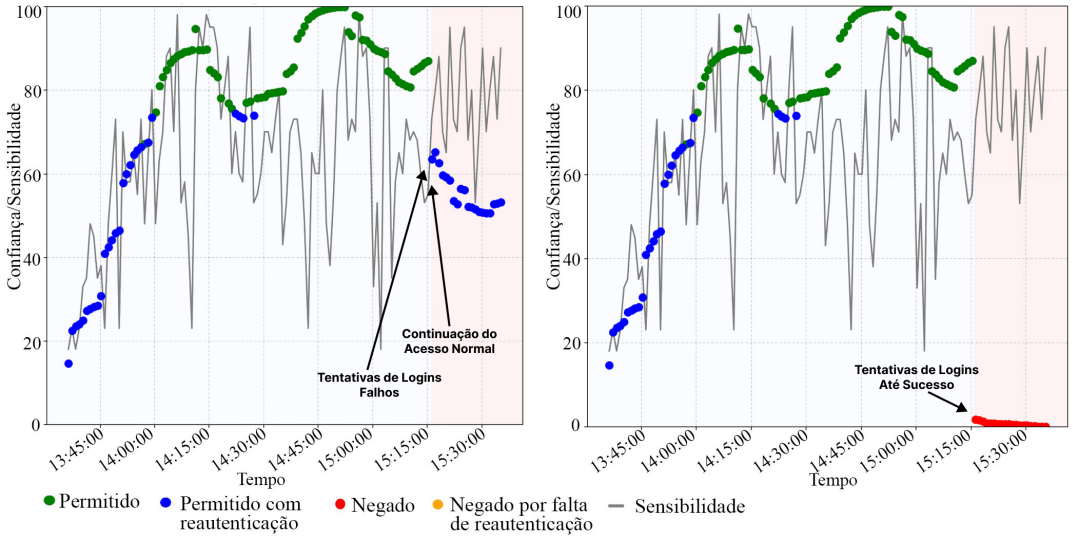


Figura 7. Teste cenário 4: Ataque de Força Bruta sem e com Sucesso.

Para o segundo teste, foi considerado que após uma sequência de tentativas de login, o invasor conseguiu se autenticar e tentou acessar os recursos. Neste caso foi considerado também que, após o sucesso no ataque, o invasor realizou trocas de senhas, uma prática comum para impedir que o usuário legítimo retome o acesso à sua conta. Além destes fatores, foi definido também que o invasor realizou seus acessos em rede e dispositivo diferente do usuário e em localidade próxima dos acessos anteriores. É possível perceber pelo segundo gráfico da Figura 7 que após conseguir se autenticar, devido às diversas tentativas falhas, e as demais configurações deste teste, de imediato a confiança foi drasticamente reduzida, o que impossibilitou a realização dos acessos seguintes e protegeu, em especial, os recursos de sensibilidade média ou superior. Para este teste, o tempo médio para tomada de decisão foi de 37 milissegundos.

6. Considerações Finais

Este trabalho propôs um modelo de confiança baseado em atributos e risco em conjunto à arquitetura *Zero Trust* como forma de acentuar a segurança em ambientes *e-health*. Foi possível observar que, através do cálculo de confiança nas perspectivas de contexto, dispositivo e histórico, e das classificações das sensibilidades dos recursos, revelou-se eficaz para mitigar ameaças tanto internas quanto externas no controle de acesso, mesmo em ambientes e soluções geograficamente distribuídas. Os resultados dos cenários indicam que a proposta proporcionou a detecção de anomalias de maneira ágil e um bom controle de acesso, em especial, aos recursos de sensibilidade mais elevada, o que por consequência, pode resultar na proteção da vida, tratamento e dados dos pacientes. Os *datasets* resultantes deste trabalho estão disponíveis publicamente em um repositório GitHub[3] para referência e colaboração. Como trabalhos futuros, propõe-se a utilização de técnicas de autenticação em segundo fator para reduzir os impactos causados pelo roubo de credenciais (cenário 3), de forma a melhorar a identificação na reautenticação e reduzir acessos indevidos. Adicionalmente, deseja-se melhorar o fator de usabilidade, de maneira a reduzir os números de reautenticações nos primeiros acessos, sem impactar na sua segurança.

[3] `https://github.com/LucaslcFreitas/Zero-Trust`

Referências

Barra, D. C. C., do Nascimento, E. R. P., de Jesus Martins, J., Albuquerque, G. L., and Erdmann, A. L. (2006). Evolução histórica e impacto da tecnologia na área da saúde e da enfermagem. *Revista Eletrônica de Enfermagem*, 8(3).

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., and Zhai, Y. (2020). A security awareness and protection system for 5g smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, 8(13):10248–10263.

Cremonezi, B., Vieira, A., Nacif, J., Silva, E. F., and Nogueira, M. (2021). Um método para extração e refinamento de políticas de acesso baseado em árvore de decisão e algoritmo genético. In *Anais do XXXIX SBRC*. SBC.

Hany, F. A., Alenezi, A., Walters, R., and Wills, G. (2017). An overview of risk estimation techniques in risk-based access control for the internet of things. In *2nd International Conference on Internet of Things, Big Data and Security*, pages 254–260. INSTICC.

Hu, V. C., Kuhn, D. R., Ferraiolo, D. F., and Voas, J. (2015). Attribute-based access control. *Computer*, 48(2):85–88.

Leandro, M. A. P. et al. (2012). Federação de identidades e computação em nuvem: estudo de caso usando shibboleth. Master's thesis, Universidade Federal de Santa Catarina.

Luh, F. and Yen, Y. (2020). Cybersecurity in science and medicine: Threats and challenges. *Trends in biotechnology*, 38(8):825–828.

Mazzocca, C., Romandini, N., Colajanni, M., and Montanari, R. (2022). Framh: A federated learning risk-based authorization middleware for healthcare. *IEEE Trans. Comput. Soc. Syst.*

Pace, A. (2008). Identity management. *Journal of Physics: Conference Series*, 119(1):012002.

Pussewalage, H. S. G. and Oleshchuk, V. A. (2017). Attribute based access control scheme with controlled access delegation for collaborative e-health environments. *Journal of information security and applications*, 37:50–64.

Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). Zero trust architecture. Technical report, National Institute of Standards and Technology.

Santos, D. R. d. et al. (2013). Uma arquitetura de controle de acesso dinâmico baseado em risco para computação em nuvem. Master's thesis, UFSC.

Sharma, A., Sharma, S., and Dave, M. (2015). Identity and access management-a comprehensive study. In *IEEE ICGCIoT*.

Souza, W. S. d. (2013). Superando os riscos da segurança baseada em perímetro-uma abordagem com identificação federada através de certificados digitais a3/icp-brasil e saml. Master's thesis, Universidade Federal do Rio Grande do Norte.

Teerakanok, S., Uehara, T., and Inomata, A. (2021). Migrating to zero trust architecture: reviews and challenges. *Security and Communication Networks*, 2021.

Wang, Z., Yu, X., Xue, P., Qu, Y., and Ju, L. (2023). Research on medical security system based on zero trust. *Sensors*, 23(7):3774.