DESAFIOS DA AUTENTICAÇÃO E AUTORIZAÇÃO NA COMUNICAÇÃO ENTRE SERVIÇOS EM ARQUITETURAS DE MICROSSERVIÇOS

Lis Araújo[1], **Edwin Marinho**[1]

[1]CESAR School
Recife – PE – Brazil

{lrva,ecrm}@cesar.school

Abstract. *In recent years, microservices have emerged as an alternative to monolithic architecture due to the many benefits this new approach offers. However, this transition has brought with it challenges related to security. This research aims to understand the main challenges faced and the solutions adopted in the context of authentication and authorization in microservices. Thus, we evaluated 21 studies, which revealed the main problems and various solutions to mitigate these problems, such as the use of JSON Web Tokens (JWT), OAuth 2.0, mTLS (Mutual Transport Layer Security) protocol, Role-based Access Control Model (RBAC), OpenID Connect, Single Sign-On (SSO) and API Gateway.*

Resumo. *Nos últimos o uso de microsserviços surgiu como alternativa à arquitetura monolítica, devido aos vários benefícios que essa nova abordagem oferece. No entanto, essa transição trouxe consigo desafios relacionados à segurança. Esta pesquisa tem como objetivo compreender os principais desafios enfrentados e as soluções adotadas no contexto de autenticação e autorização em microsserviços. Sendo assim, foram avaliados 21 estudos, que revelaram os principais problemas e diversas soluções para mitigar tais problemas, como o uso de JSON Web Tokens (JWT), OAuth 2.0, protocolo mTLS (Mutual Transport Layer Security), Role-based Access Control Model (RBAC), OpenID Connect, Single Sign-On (SSO) e API Gateway.*

1. Introdução

A arquitetura monolítica, que consiste em ter funções encapsuladas em uma única aplicação, costumava ser a abordagem tradicional de desenvolvimento de software alguns anos atrás [De Lauretis 2019]. Porém, devido à demanda por sistemas mais complexos, essa abordagem começou a se tornar difícil de gerenciar. Nesse contexto, emergiu a arquitetura de microsserviços, alternativa ao modelo monolítico que divide o sistema em serviços menores [Alshuqayran et al. 2016].

No entanto, é necessário que cada serviço tenha suas próprias abordagens de segurança, aumentando a complexidade se comparado ao estilo monolítico, em que as estratégias são desenvolvidas em uma única aplicação [de Almeida and Canedo 2022]. Nesse contexto, falhas relacionadas a autenticação e autorização podem afetar todo o sistema [ShuLin and JiePing 2020].

Esse estudo tem como objetivo identificar os principais desafios e eventuais soluções de autenticação e autorização na comunicação entre os serviços em arquiteturas de microsserviços mapeados na academia. Foram definidas duas questões para guiar

a pesquisa, sendo elas: ”Quais são os principais problemas de segurança mapeados na academia com relação a autenticação e autorização na comunicação entre os serviços em arquiteturas de microsserviços?”e ”Quais as soluções mais abordadas na literatura no contexto da autenticação e autorização na comunicação entre os serviços em arquitetura de microsserviços?”. O trabalho consistiu em uma *Rapid Review* para identificar os desafios e soluções mais citados na literatura.

O artigo é estruturado em seções. A seção 2 descreve brevemente os principais conceitos necessários para a compreensão da pesquisa. A seção 3 discute trabalhos relacionados ao tema. Em seguida, são descritas as etapas e os procedimentos adotados. Na seção 5, são apresentados os resultados. Já a seção 6 traz as discussões e análises baseadas nos resultados obtidos. Por fim, são apresentadas as eventuais ameaças à validade do estudo, seguidas pela conclusão e sugestões para os trabalhos futuros.

2. Fundamentação teórica

A arquitetura de microsserviços vem ganhando popularidade associada ao aumento da demanda por sistemas mais complexos [De Lauretis 2019]. O principal objetivo desse modelo arquitetural é que os serviços sejam independentes entre si, possibilitando projetar, desenvolver, testar e liberar cada um deles isoladamente em relação ao resto do sistema [Dragoni et al. 2017].

Entretanto, essa característica também resulta em alguns desafios. A independência dos serviços cria a necessidade de estabelecer uma comunicação robusta, pois o acesso não autorizado a um serviço pode comprometer todo um sistema. Assim, falhas na validação de entradas fornecidas pelos usuários podem agravar o impacto de problemas como o SSRF (*Server Side Request Forgery*), pois uma requisição maliciosa a um serviço público pode afetar um serviço projetado para acesso apenas por outros serviços, permitindo ao atacante realizar ações não autorizadas [Greyhats 2021].

É necessário verificar se os usuários estão devidamente autenticados e autorizados ao realizar cada uma das requisições. A autenticação verifica se o usuário é quem realmente diz ser, enquanto a autorização verifica se o usuário possui acesso a determinados recursos do sistema. Tais mecanismos são essenciais no controle da comunicação entre os serviços, protegendo os recursos da aplicação [He and Yang 2017].

2.1. Desafios de autenticação e autorização em microsserviços

Um dos desafios, o controle de acesso, refere-se à limitação das ações que podem ser executadas em uma aplicação, tanto as ações diretas do usuário quanto as ações de outros programas [Sandhu and Samarati 1994]. Falhas nesse controle podem expor, alterar ou destruir informações sem autorização e permitir ações além dos limites necessários. Exemplos de vulnerabilidades nesse contexto incluem acesso indiscriminado, manipulação de *tokens* para aumentar privilégios e acesso não autorizado a páginas protegidas.

Outro desafio diz respeito à contenção de ataques *man-in-the-middle* (MITM), que ocorrem quando um terceiro malicioso se posiciona no canal de comunicação entre duas partes que estão trocando mensagens, interceptando as informações trafegadas. Esse tipo de ataque pode comprometer a confidencialidade, integridade e disponibilidade do sistema, uma vez que o invasor consegue interceptar, modificar ou apagar as informações em trânsito [Conti et al. 2016].

Modelos fracos de autenticação possibilitam que invasores se passem por usuários legítimos. Isso pode ocorrer especialmente em aplicativos que permitem ataques de força

bruta, uso de senhas fracas ou processos ineficazes de recuperação de credenciais e esquecimento de senha. Por outro lado, o ataque de sequestro de sessão explora o mecanismo de controle de sessão da web, obtendo acesso não autorizado ao comprometer ou prever um *token* de sessão válido. A partir dessas vulnerabilidades, um invasor pode autenticar-se num sistema como um usuário legítimo, assumindo o controle de sua sessão e realizando ações em seu nome sem o devido consentimento [Yarygina and Bagge 2018].

2.2. Soluções de autenticação e autorização em microsserviços

Algumas soluções relacionadas a autenticação e autorização são apontadas na literatura para uso em arquiteturas de microsserviços. Como exemplo, o OAuth 2.0, que atua como um *framework* para garantir a segurança de cada microsserviço, permite que o cliente se autentique no servidor de autorização e obtenha um *token* de acesso, emitindo uma solicitação ao usuário para conceder uma sessão [Pasomsup and Limpiyakorn 2021]. O objetivo é permitir que os usuários autorizem aplicativos de terceiros a acessarem seus recursos protegidos sem compartilhar suas credenciais de login [Triartono et al. 2019]. Um outro método que oferece um logon único e provisionamento de identidade para usuários em diferentes aplicativos é o OpenID Connect, possibilitando que os usuários tenham apenas uma identidade digital. Ele é construído em cima do protocolo OAuth 2.0 e fornece uma camada adicional de autenticação para aumentar a segurança [PortSwigger 2023].

Outra solução abordada na literatura é o JSON Web Token (JWT), um formato de *token* que permite transmitir informações confiáveis e seguras entre as partes em um formato de objeto JSON [Ethelbert et al. 2017]. O JWT possui assinatura digital, garantindo a verificação da integridade do conteúdo e a certificação de que os remetentes são quem dizem ser. Também é mencionado o uso de SSO (Single Sign-On), um sistema de autenticação que permite aos usuários fazer *login* uma única vez em uma aplicação e, em seguida, acessar vários recursos ou serviços do sistema sem precisar fazer login novamente, o que simplifica o gerenciamento de identidade e acesso [Bánáti et al. 2018].

Outra solução explorada é o protocolo SSL (Security Socket Layer)/ TLS (Transport Layer Security), que são versões diferentes do mesmo protocolo, em que o segundo se trata de uma versão mais segura em relação ao primeiro [Satapathy et al. 2016]. Já o mTLS (Mutual Transport Layer Security) é uma extensão do TLS, que adiciona autenticação mútua entre o cliente e o servidor, assegurando a validação das partes envolvidas em uma conexão de rede [Namer 2022].

O RBAC (Role-Based Access control) é um modelo de controle de acesso - conjunto de operações que definem as ações permitidas para um usuário - baseado em função. Nesse modelo os privilégios são associados aos papéis ou grupos de papéis. Portanto, um usuário terá todas as permissões correspondentes ao papel ao qual ele pertence [Triartono et al. 2019]. Outra solução que atua como um nível intermediário, recebendo as solicitações dos clientes e as direcionando para o serviço adequado, é o API Gateway. Ele protege a arquitetura interna do sistema e seu objetivo é simplificar a comunicação entre clientes e serviços [Xiong and Li 2022].

3. Trabalhos relacionados

No estudo [Yarygina and Bagge 2018] são discutidos os desafios associados à complexidade da arquitetura de microsserviços, bem como cita algumas formas de mitigar esses problemas. Outro trabalho relevante nesse contexto é o apresentado em [Pereira-Vale et al. 2019], onde foi exposta uma análise sistemática dos mecanismos

de segurança mais utilizados em sistemas baseados em microsserviços, incluindo autenticação e autorização. Por outro lado, em [Billawa et al. 2022] é apresentada uma revisão de literatura cinza, focando nos desafios e melhores práticas de modo geral em arquiteturas de microsserviços.

Esta pesquisa difere dos trabalhos citados por possuir um foco específico na autenticação e autorização da comunicação entre serviços em arquiteturas de microsserviços, enquanto os artigos mencionados discutem microsserviços ou os desafios de segurança da arquitetura de forma geral.

4. Metodologia

Esta é uma pesquisa exploratória, com o intuito de proporcionar uma maior familiaridade com o problema [Gil 2002]. O método escolhido foi o *Rapid Review*, seguindo o protocolo apresentado por [Cartaxo et al. 2018]. Tal método visa fornecer informações relevantes baseadas em evidências dentro de um prazo adequado. Cada etapa foi documentada em uma planilha[1].

Foram utilizadas as bases IEEE e ACM na busca por estudos primários, devido às suas relevâncias na área da pesquisa. A primeira busca consistiu no uso da seguinte *string*:

(microservices OR microservice) AND (authorization OR authentication)

A *string* foi elaborada a partir das palavras-chaves a respeito do tema. Foram adotadas duas ordenações diferentes para a seleção dos estudos: por número de citações e por data de publicação mais recente. As ordenações foram aplicadas para garantir, respectivamente, uma seleção mais relevante e atualizada dos estudos avaliados. A segunda busca foi realizada em campos primordiais dos artigos, captando pesquisas onde o tema estava envolvido no contexto central dos trabalhos selecionados. Para tal, foi utilizada a seguinte *string*:

((”Publication Title”:microservices OR microservice) AND (”Publication Title”:authorization OR authentication)) OR ((”Abstract”:microservices OR microservice) AND (”Abstract”:authorization OR authentication))

Além disso, foi estipulado um critério de parada, que consistiu em interromper o processo ao analisar 20 artigos em sequência e nenhum deles apresentar relevância.

O processo de seleção foi baseado em alguns critérios. Os critérios de inclusão exigiam a presença de pelo menos um desafio relacionado a autenticação ou autorização em microsserviços, ou a menção de ao menos um mecanismo para lidar com tais problemas. Em contraste, os critérios de exclusão contemplavam estudos que não abordavam autenticação e autorização em arquiteturas de microsserviços, artigos duplicados, e estudos que não tratavam das questões relacionadas às perguntas de pesquisa. Caso o estudo atendesse a pelo menos um dos critérios de inclusão e não tivesse um critério de exclusão associado, tal estudo seria selecionado para a próxima etapa. Para aplicar os critérios de inclusão e exclusão foi feita a leitura do título, palavras-chaves e resumo de cada artigo.

Após a seleção, foram definidos dois critérios para avaliação de qualidade dos estudos. O primeiro critério consistiu em verificar se o estudo apontava algum problema

[1]https://shre.ink/auth-microservices

relacionado a autenticação e autorização em microsserviços, mesmo que não necessariamente apresentasse as respectivas soluções. O segundo critério consistiu em verificar se o estudo identificava mecanismos que mitigassem problemas ou desafios envolvendo autenticação e autorização na arquitetura de microsserviços. Foi feita a leitura completa de cada um dos artigos para realizar a avaliação de qualidade. Se o artigo respondia a pelo menos um dos critérios estabelecidos, cada informação relevante era extraída e utilizada para a avaliação final. Ao final do processo, os artigos que atenderam aos dois critérios foram considerados de alta qualidade e os que atenderam a apenas um dos critérios foram considerados de qualidade média.

Paralelamente à avaliação de qualidade dos artigos selecionados, foi realizada a codificação, um processo que envolveu a leitura, análise e organização dos dados, a fim de atribuir categorias às informações extraídas dos artigos. Essa etapa foi fundamental para extrair significado dos estudos e facilitar a posterior análise e interpretação dos resultados.

5. Resultados

Em relação aos resultados obtidos durante a pesquisa, a primeira *string* de busca utilizada retornou um total de 86 estudos na base IEEE e 1240 estudos na base ACM. Na IEEE, a partir da busca ordenada por número de citações, foram escolhidos 58 artigos. Na ordenação por data de publicação mais recente, foram escolhidos os primeiros 50 artigos. Já na base ACM, foram escolhidos 55 artigos na busca ordenada por número de citações e 45 ao ordenar por data de publicação. Em seguida, a pesquisa utilizando a segunda *string* de busca retornou um total de 65 estudos na base IEEE e 10 na base ACM. Ao avaliar os artigos de acordo com os critérios de inclusão e exclusão, 31 artigos atenderam aos critérios estabelecidos e foram selecionados para a etapa de avaliação de qualidade. No processo de avaliação de qualidade, 10 artigos foram descartados por não conter informações diretamente relacionadas ao tema da pesquisa, enquanto os 21 artigos restantes foram avaliados de acordo com os critérios estabelecidos. A Figura 1 representa a filtragem progressiva da quantidade de artigos em cada uma das etapas mencionadas.

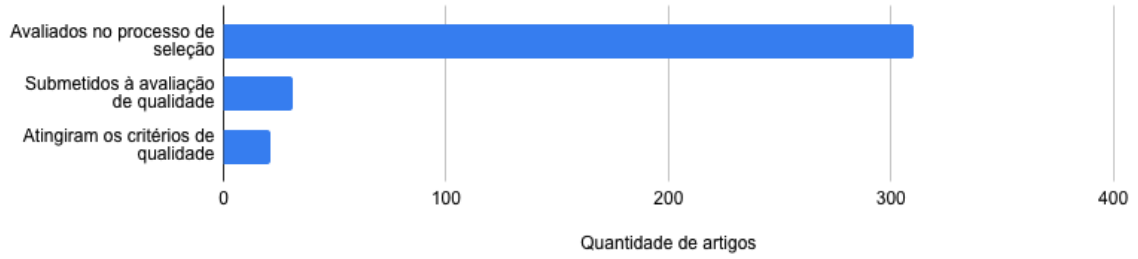

Figura 1. Quantidade de artigos em cada etapa da metodologia

5.1. Desafios

Em relação às dificuldades, a Tabela 1 estabelece uma relação entre cada estudo e os desafios abordados em cada um deles. Dessa forma, é possível notar que a maior quantidade de ocorrências esteve atrelada ao controle de acesso, seguido pelo risco de ataques *man-in-the-middle*, bem como a segurança na comunicação e confiança entre os serviços, que pode levar à vulnerabilidade da privacidade, integridade e disponibilidade de dados. Adicionalmente a esses desafios, outros problemas importantes foram citados, tais como a autenticação fraca em um aplicativo, que pode resultar em falsificação de identidade, além do risco de controle de sessão e a ocorrência de ataques em TLS.

Tabela 1. Desafios abordados em cada um dos artigos selecionados

Artigo	Controle de acesso	Man-in-the-middle	Segurança na comunicação e confiança entre os serviços	Falhas de autenticação	Controle de sessão	Ataques em TLS
01 - [Yarygina and Bagge 2018]	X	X		X	X	X
02 - [Pahl and Donini 2018]						
03 - [Pereira-Vale et al. 2019]		X	X			
04 - [Preuveneers and Joosen 2019]	X					
05 - [ShuLin and JiePing 2020]	X					
06 - [Bánáti et al. 2018]	X					
07 - [Triartono et al. 2019]	X					
08 - [Melton 2021]	X					
09 - [Catalfamo et al. 2021]		X				
10 - [Fu et al. 2018]	X		X			
11 - [Goel and Thangaraju 2022]		X				
12 - [Pasomsup and Limpiyakorn 2021]	X					
13 - [Dilshan et al. 2020]		X	X			
14 - [Yang et al. 2021]						
15 - [Kretarta and Kabetta 2022]	X					
16 - [Han et al. 2022]		X	X			
17 - [Xiong and Li 2022]	X					
18 - [Cerny et al. 2018]	X					
19 - [Zdun et al. 2023]		X				
20 - [Li et al. 2019]			X			
21 - [Walsh and Manferdelli 2017]			X			

5.2. Soluções

A Tabela 2 apresenta um panorama das soluções identificadas na literatura revisada. Tais soluções são utilizadas para lidar com os desafios relacionados à autenticação e autorização em arquiteturas de microsserviços.

Diversos estudos discutem a segurança do uso de JWT como método de autenticação em ambientes de microsserviços. Por exemplo, o estudo [Yang et al. 2021] menciona problemas de segurança associados ao JWT. No entanto, [Han et al. 2022] apresenta perspectivas positivas sobre a confiabilidade dessa ferramenta. Estudos como [Xiong and Li 2022] e [Pasomsup and Limpiyakorn 2021], abordaram o RBAC predominantemente de forma positiva, principalmente seu uso em sistemas complexos. O OAuth 2.0 foi considerado maduro e amplamente utilizado em uma variedade sistemas como uma solução altamente valorizada por [ShuLin and JiePing 2020].

6. Discussão

Ao analisar os dados, é possível observar que pelo menos um artigo sobre o tema foi publicado no mesmo ano em que esta pesquisa foi realizada, e outros oito artigos foram publicados nos dois anos anteriores. Esses números reforçam a atualidade do tema, que leva à seguinte proposição:

- ***Proposição 1:*** *Os desafios relacionados à autenticação e autorização em microsserviços são reconhecidos pela academia como uma questão atual e relevante.*

Um fator interessante é que, apesar de o foco ser em arquiteturas de microsserviços, os problemas apontados não parecem restritos a esse cenário. O "*Broken Access Control*"(do inglês, Controle de Acesso Quebrado) ficou em primeiro lugar no

Tabela 2. Soluções abordadas em cada um dos artigos selecionados

Artigo	JWT	OAuth 2.0	Protocolo TLS / / SSL / MTLS	RBAC	SSO	OpenID Connect	API Gateway	STS	JWS	JWE	ABE	Sessão distribuída	UMA 2.0	XACML 3.0	NGAC	OPA	Zuul	OTP
01	x	x	x	x	x			x	x	x								
02		x																
03	x	x			x							x						
04	x	x											x	x	x	x		
05	x	x															x	
06	x	x		x	x	x	x											
07		x		x														
08	x	x			x	x												
09																		x
10				x							x							
11	x		x															
12	x	x		x														
13			x															
14	x	x			x													
15	x					x												
16	x		x															
17				x			x											
18		x			x	x												
19	x	x	x			x	x											
20			x															
21			x															

ranking mais recente da OWASP[2] com os dez maiores riscos de segurança de aplicações web. Reforçando essa ideia, esse estudo revelou que o controle de acesso é o desafio mais abordado relacionado à autorização em microsserviços, com 11 citações. Essa questão representa um desafio significativo, uma vez que delegar o gerenciamento das decisões de controle de acesso é uma tarefa complexa, principalmente quando há várias partes envolvidas nessas decisões [Preuveneers and Joosen 2019]. Tal constatação direciona para a seguinte proposição:

- ***Proposição 2:*** *A academia reconhece que restringir o acesso a funcionalidades e recursos em uma arquitetura de microsserviços é um desafio que requer atenção das pessoas envolvidas na construção do software.*

O ataque *man-in-the-middle* (MITM) também é um problema preocupante, sendo o segundo problema mais citado nesta pesquisa. Além disso, a segurança na comunicação e confiança entre os serviços - terceiro desafio mais mencionado - é uma questão significativa. Diante disso, a próxima proposição é apontada:

- ***Proposição 3:*** *Os principais desafios de segurança na comunicação entre serviços em uma arquitetura de microsserviços estão relacionados a garantir os devidos controles de acesso, impedir ataques man-in-the-middle e garantir a identidade dos que estão realizando as ações.*

O OAuth 2.0 é a solução mais mencionada neste estudo, corroborando as conclusões do trabalho [Pahl and Donini 2018], que destaca sua predominância nos esquemas de autorização. Já o JWT, segunda solução mais mencionada nesse estudo, é considerado uma das estratégias mais adequadas para autenticação e autorização em

[2]https://owasp.org/www-project-top-ten/

microsserviços [Pereira-Vale et al. 2019]. No entanto, [Yang et al. 2021] ressalta que um usuário mal-intencionado, ao interceptar o *token* JWT, pode usá-lo para acessar e atacar os microsserviços até o seu tempo de expiração, já que o *token* não pode ser revogado imediatamente.

O RBAC (*Role Based Access Control*) é a terceira solução mais abordada nesse estudo, usada para evitar a divulgação indevida de informações [Pasomsup and Limpiyakorn 2021]. Os protocolos mTLS/TLS/SSL também são discutidos como soluções para mitigar problemas de comunicação entre serviços, como o ataque man-in-the-middle [Dilshan et al. 2020]. Já o SSO é citado como uma das estratégias mais adequadas para autenticação em microsserviços [Pereira-Vale et al. 2019]. Por fim, embora o uso de API Gateways apresente vantagens, [Yang et al. 2021] discutem os riscos associados, já que os serviços por trás do *gateway* podem ser explorados por um atacante que conseguir contorná-lo.

- ***Proposição 4:*** *As principais soluções para o desafio de autenticação e autorização em microsserviços são em sua maioria abordadas de forma positiva. No entanto, esse problema ainda é relevante, o que sugere a necessidade de um esforço contínuo de pesquisa para aprimorar e abordar de maneira abrangente essas soluções, visando alcançar uma resolução completa.*

A matriz de relacionamento apresentada na Tabela 3 foi desenvolvida a partir dos artigos selecionados, destacando as combinações entre as soluções mencionadas nesses estudos para enfrentar os desafios identificados.

Tabela 3. Possíveis combinações das soluções mais citadas

	JWT	OAuth 2.0	MTLS/TLS/SSL	RBAC	SSO	OpenID Connect	API Gateway
JWT		X		X	X	X	X
OAuth 2.0	X			X		X	X
MTLS/TLS/SSL							
RBAC	X	X					
SSO	X					X	
OpenID Connect		X			X		
API Gateway	X	X					

A análise dos resultados revela que a maioria das soluções identificadas podem ser implementadas de forma combinada a outras, proporcionando um aumento significativo na segurança do sistema de microsserviços.

A combinação mais citada é do OAuth 2.0 com o OpenID Connect, para conceder acesso a diversos sites utilizando uma identidade única [Yarygina and Bagge 2018]. Outra combinação é o OpenID Connect com o SSO e o JWT. Os *tokens* JWT são distribuídos usando o protocolo OpenID Connect, que por sua vez é hospedado por um provedor de SSO, permitindo que um único *login* acesse vários microsserviços [Melton 2021]. Já o uso de *frameworks* de autorização, como o OAuth 2.0, em conjunto com os *tokens* JWT, se tornaram o padrão da indústria para fornecer acesso seguro aos serviços por meio de API Gateways [Preuveneers and Joosen 2019]. Além disso, para simplificar o processo de autorização no lado do *backend* da arquitetura, é utilizado o RBAC em conjunto com o OAuth 2.0 [Triartono et al. 2019].

Esses resultados destacam a extrema importância da combinação de soluções no contexto abordado, revelando que a implementação não integrada de soluções pode não ser suficiente para lidar de forma eficaz com os desafios identificados. No entanto, vale

destacar que os resultados obtidos evidenciam que o protocolo mTLS não apresenta referências na literatura sobre formas específicas de combinação com outras soluções.

- ***Proposição 5:*** *A pesquisa em veículos de publicação acadêmicos não evidencia a experimentação prática para explorar possíveis estratégias de integração que otimizem a eficácia do mTLS em conjunto com outras soluções, a fim de aprimorar ainda mais a segurança dos sistemas de microsserviços.*

Para todas as demais soluções abordadas neste tópico, não foi possível identificar conflitos, indicando que poderiam ser utilizadas em conjunto. Esse tipo de combinação pode ser visto em soluções de gestão de identidade e acesso (IAM) [Indu and Anand 2015], abordagem que não ficou em evidência nos trabalhos avaliados. A construção de uma prova de conceito utilizando todas elas seria uma avaliação futura relevante. Diante disso, a seguinte proposição pode ser destacada:

- ***Proposição 6:*** *É possível combinar soluções diferentes relativas a autenticação e autorização em arquiteturas de microsserviços, de modo a construir aplicações mais resilientes a problemas como o controle de acesso na comunicação entre os serviços.*

A Figura 2 ilustra a relação entre os desafios mais discutidos e as soluções potenciais, com base na extração das informações abordadas nos artigos selecionados para esta pesquisa.

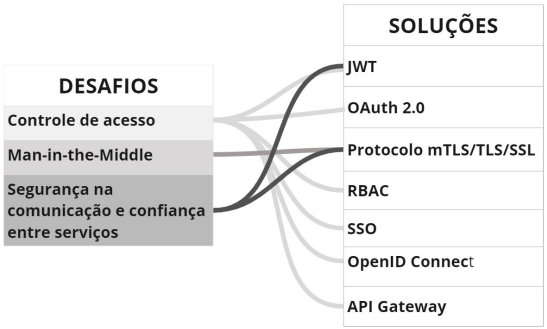

Figura 2. Soluções que ajudam a mitigar os principais desafios

Como é possível observar, fica evidente que a maioria das soluções apresentadas são abordadas como forma de mitigar os desafios relacionados ao controle de acesso em ambientes de microsserviços. No entanto, é interessante perceber que mesmo com essa variedade de soluções, o controle de acesso continua sendo o desafio mais citado. Isso sugere que apesar dos esforços atuais, ainda existem lacunas e dificuldades a serem superadas nessa área específica. Portanto, é crucial continuar investigando e desenvolvendo abordagens para enfrentar os desafios de controle de acesso em microsserviços.

7. Ameaças à validade

De acordo com [Cartaxo et al. 2018], *Rapid Reviews* geralmente apresentam mais ameaças à validade do que outros estudos secundários devido à sua metodologia simplificada. Nesse estudo, utilizou-se apenas duas bases de dados, mas para minimizar esse impacto, foram selecionadas bases relevantes, como IEEE e ACM. Além disso, todo o procedimento de seleção foi conduzido por uma única pesquisadora, o que pode introduzir um viés de seleção [Petersen et al. 2015]. Por fim, a inclusão da literatura cinza em trabalhos futuros visa contornar a restrição de publicações acadêmicas.

8. Conclusão

A *Rapid Review* realizada neste trabalho destaca a importância da segurança na comunicação entre os serviços em arquiteturas de microsserviços que, apesar de explorada, ainda apresenta desafios que exigem atenção durante o desenvolvimento das soluções. Foi identificado que o controle de acesso, ataques man-in-the-middle e problemas na comunicação entre os serviços são os principais desafios enfrentados nesse contexto. Diversas soluções também foram abordadas, como OAuth 2.0, JWT, RBAC, entre outras. No entanto, apesar das soluções serem abordadas de forma positiva na literatura, a quantidade de estudos dedicados aos desafios reforça a atualidade do tema. Além disso, é necessário explorar o potencial do protocolo mTLS para melhorar a segurança dos sistemas de microsserviços. Por fim, é essencial que os profissionais de tecnologia atentem-se aos problemas identificados e considerem a adoção das soluções citadas para garantir a segurança em arquiteturas de microsserviço.

Com o intuito de obter uma visão mais abrangente, a pesquisa será ampliada para englobar a literatura cinza [Garousi et al. 2019], com o propósito de investigar desafios e soluções conhecidas, porém não amplamente documentadas ou estudadas na academia. Além disso, também devem ser incluídas mais bases acadêmicas, como Elsevier e Springer, de modo a aumentar a cobertura e confrontar com os resultados obtidos. Por fim, experimentos devem ser realizados com a combinação de abordagens, de modo a avaliar a resiliência das propostas em cenários de ataques.

Referências

Alshuqayran, N., Ali, N., and Evans, R. (2016). A systematic mapping study in microservice architecture. In *2016 IEEE 9th International Conference on Service-Oriented Computing and Applications (SOCA)*, pages 44–51. IEEE.

Bánáti, A., Kail, E., Karóczkai, K., and Kozlovszky, M. (2018). Authentication and authorization orchestrator for microservice-based software architectures. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1180–1184. IEEE.

Billawa, P., Bambhore Tukaram, A., Díaz Ferreyra, N. E., Steghöfer, J.-P., Scandariato, R., and Simhandl, G. (2022). Sok: Security of microservice applications: A practitioners' perspective on challenges and best practices. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pages 1–10.

Cartaxo, B., Pinto, G., and Soares, S. (2018). The role of rapid reviews in supporting decision-making in software engineering practice. In *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018*, pages 24–34.

Catalfamo, A., Ruggeri, A., Celesti, A., Fazio, M., and Villari, M. (2021). A microservices and blockchain based one time password (mbb-otp) protocol for security-enhanced authentication. In *2021 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6. IEEE.

Cerny, T., Donahoo, M. J., and Trnka, M. (2018). Contextual understanding of microservice architecture: current and future directions. *ACM SIGAPP Applied Computing Review*, 17(4):29–45.

Conti, M., Dragoni, N., and Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE communications surveys & tutorials*, 18(3):2027–2051.

de Almeida, M. G. and Canedo, E. D. (2022). Authentication and authorization in microservices architecture: A systematic literature review. *Applied Sciences*, 12(6):3023.

De Lauretis, L. (2019). From monolithic architecture to microservices architecture. In *2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, pages 93–96. IEEE.

Dilshan, D., Piumika, S., Rupasinghe, C., Perera, I., and Siriwardena, P. (2020). Mschain: blockchain based decentralized certificate transparency for microservices. In *2020 Moratuwa Engineering Research Conference (MERCon)*, pages 1–6. IEEE.

Dragoni, N., Giallorenzo, S., Lafuente, A. L., Mazzara, M., Montesi, F., Mustafin, R., and Safina, L. (2017). Microservices: yesterday, today, and tomorrow. *Present and ulterior software engineering*, pages 195–216.

Ethelbert, O., Moghaddam, F. F., Wieder, P., and Yahyapour, R. (2017). A json token-based authentication and access management schema for cloud saas applications. In *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 47–53. IEEE.

Fu, G., Sun, J., and Zhao, J. (2018). An optimized control access mechanism based on micro-service architecture. In *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pages 1–5. IEEE.

Garousi, V., Felderer, M., and Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, 106:101–121.

Gil, A. C. (2002). *Como elaborar projetos de pesquisa*, volume 4. Atlas.

Goel, A. and Thangaraju, B. (2022). Authenticating distributed systems using spire over kubernetes cluster. In *2022 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pages 1–6. IEEE.

Greyhats, N. (2021). Server side request forgery. `https://nusgreyhats.org/posts/writeups/ssrf/`. [Online; acesso em 25-Maio-2023].

Han, J., Yun, I., Kim, S., Kim, T., Son, S., and Han, D. (2022). Scalable and secure virtualization of hsm with scaletrust. *IEEE/ACM Transactions on Networking*.

He, X. and Yang, X. (2017). Authentication and authorization of end user in microservice architecture. In *Journal of Physics: Conference Series*, volume 910, page 012060. IOP Publishing.

Indu, I. and Anand, P. R. (2015). Identity and access management for cloud web services. In *2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, pages 406–410. IEEE.

Kretarta, A. B. and Kabetta, H. (2022). Secure user management gateway for microservices architecture apis using keycloak on xyz. In *2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pages 7–13. IEEE.

Li, X., Chen, Y., and Lin, Z. (2019). Towards automated inter-service authorization for microservice applications. In *Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos*, pages 3–5.

Melton, R. (2021). Securing a cloud-native c2 architecture using sso and jwt. In *2021 IEEE Aerospace Conference (50100)*, pages 1–8. IEEE.

Namer, A. (2022). Multicast implementation over mutual transport layer security (mtls). `https://www.tdcommons.org/dpubs_series/5268`. Technical Disclosure Commons. [Online; acesso em 25-Maio-2023].

Pahl, M.-O. and Donini, L. (2018). Securing iot microservices with certificates. In *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, pages 1–5. IEEE.

Pasomsup, C. and Limpiyakorn, Y. (2021). Ht-rbac: A design of role-based access control model for microservice security manager. In *2021 International Conference on Big Data Engineering and Education (BDEE)*, pages 177–181. IEEE.

Pereira-Vale, A., Márquez, G., Astudillo, H., and Fernandez, E. B. (2019). Security mechanisms used in microservices-based systems: A systematic mapping. In *2019 XLV Latin American Computing Conference (CLEI)*, pages 01–10. IEEE.

Petersen, K., Vakkalanka, S., and Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and software technology*, 64:1–18.

PortSwigger (2023). Openid connect. `https://portswigger.net/web-security/oauth/openid`. [Online; acesso em 30-Maio-2023].

Preuveneers, D. and Joosen, W. (2019). Towards multi-party policy-based access control in federations of cloud and edge microservices. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 29–38. IEEE.

Sandhu, R. S. and Samarati, P. (1994). Access control: principle and practice. *IEEE communications magazine*, 32(9):40–48.

Satapathy, A., Livingston, J., et al. (2016). A comprehensive survey on ssl/tls and their vulnerabilities. *International Journal of Computer Applications*, 153(5):31–38.

ShuLin, Y. and JiePing, H. (2020). Research on unified authentication and authorization in microservice architecture. In *2020 IEEE 20th international conference on communication technology (ICCT)*, pages 1169–1173. IEEE.

Triartono, Z., Negara, R. M., and Sussi (2019). Implementation of role-based access control on oauth 2.0 as authentication and authorization system. In *2019 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, pages 259–263.

Walsh, K. and Manferdelli, J. (2017). Mechanisms for mutual attested microservice communication. In *Companion Proceedings of the10th International Conference on Utility and Cloud Computing*, pages 59–64.

Xiong, Q. and Li, W. (2022). Design and implementation of microservices gateway based on spring cloud zuul. In *CIBDA 2022; 3rd International Conference on Computer Information and Big Data Applications*, pages 1–5. VDE.

Yang, J., Hou, H., Li, H., and Zhu, Q. (2021). User fast authentication method based on microservices. In *2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA)*, pages 93–98. IEEE.

Yarygina, T. and Bagge, A. H. (2018). Overcoming security challenges in microservice architectures. In *2018 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, pages 11–20. IEEE.

Zdun, U., Queval, P.-J., Simhandl, G., Scandariato, R., Chakravarty, S., Jelic, M., and Jovanovic, A. (2023). Microservice security metrics for secure communication, identity management, and observability. *ACM Transactions on Software Engineering and Methodology*, 32(1):1–34.