Uma Análise Abrangente de Soluções de Autenticação para Microsserviços: Uma Revisão Sistemática

Rodrigo Cargnelutti[1], **Fábio Paulo Basso**[1], **Maicon Bernardino**[1]

[1]Laboratory of Empirical Studies in Software Engineering (LESSE)
Software Engineering – Federal University of Pampa (Unipampa)
97.546-550 – Alegrete – RS – Brazil

{rodrigocargnelutti.aluno,fabiobasso}@unipampa.edu.br,bernardino@acm.org

Abstract. *Systems migration currently focuses on modernizing legacy and monolithic systems to microservices architectures. The microservices architecture can bring benefits, however, it also brings challenges, especially regarding the security aspect for user authentication. To face these challenges, solutions such as API gateways and proxies are used to control user access to a set of applications that run under microservices. In this work, we seek to find studies that address aspects of solutions, tools and technologies for authenticating systems in microservices architecture. We identified 5 authentication tools most mentioned by the selected studies.*

Resumo. *A migração de sistemas atualmente se concentra na modernização de sistemas legados e monolíticos para arquiteturas de microsserviços. A arquitetura de microsserviços pode trazer benefícios, porém, também traz desafios, principalmente quanto ao aspecto de segurança para autenticação de usuários. Para enfrentar esses desafios, soluções como API gateways e proxies são utilizadas para fazer o controle de acesso do usuário a um conjunto de aplicações que rodam sob microsserviços. Neste trabalho buscamos encontrar estudos que abordam aspectos sobre soluções, ferramentas e tecnologias sobre autenticação de sistemas em arquitetura de microsserviços. Identificamos 5 ferramentas de autenticação mais mencionadas pelos estudos selecionados.*

1. Introdução

A abordagem arquitetural de microsserviços tornou-se cada vez mais popular, devido à sua flexibilidade e por ser composta por vários pequenos serviços independentes, cada um executando em seu próprio processo e se comunicando por meio de protocolos leves [de Almeida and Canedo 2022]. A arquitetura de microsserviços reduz o acoplamento entre os módulos do aplicativo e é benéfica para o desenvolvimento e manutenção dos sistemas. Ela fornece uma solução alternativa e flexível para escalabilidade de infraestrutura, diferentemente da arquitetura monolítica [Alshuqayran et al. 2016].

A medida que se começa a transição de um sistema monolítico para microsserviços, surge o problema de autenticação e autorização para arquitetura de microsserviços. Autenticação e autorização em um sistema monolítico é diferente da arquitetura de microsserviços. Na monolítica, a autenticação e a autorização são realizadas apenas uma vez, pois nesta arquitetura o processo de aplicação não é separado.

Já na de microsserviços, cada processo da aplicação pode ser tratado de forma independente de acordo com cada serviço, *e.g.* um microsserviço para tratar solicitações de autenticação e outro para autorização, e assim por diante [Triartono et al. 2019]. Já [Alshuqayran et al. 2016] define que o estilo arquitetônico de microsserviços enfatiza a divisão do sistema em vários serviços independentes, pequenos e leves.

Um API *gateway* é responsável por tarefas de autenticação e roteamento que atua como um único ponto de entrada para os clientes dos microsserviços do sistema. Em vez de chamar os microsserviços diretamente, os clientes chamam o API *gateway*, o qual recebe e redireciona a solicitação para o microsserviço apropriado. Quando o microsserviço responde à solicitação, o API *gateway* a retorna ao cliente [Raj et al. 2023]. A autenticação é um mecanismo no qual o usuário com credenciais validas pode ter acesso ao serviço. A autenticação responde a questão: Quem é você? A autorização, verifica se o usuário autenticado tem permissão para consumir ou não determinada informação ou serviço. Autorização responde à seguinte pergunta: Que permissões o usuário tem? Em resumo, a arquitetura de microsserviços enfrenta o desafio de segurança para autenticação e autorização do usuário de forma centralizada [Raj et al. 2023].

A pesquisa foi conduzida usando quatro bibliotecas digitais amplamente usadas. Aplicamos um protocolo rigoroso para extrair, classificar e organizar os estudos, resultando na remoção de 474 estudos duplicados e na rejeição de 2.806 estudos. Selecionamos cuidadosamente 19 estudos primários publicados de 2015 a janeiro de 2023, de um total de 3.299 estudos encontrados na literatura. Nesta Revisão Sistemática da Literatura (RSL) pretendemos encontrar recomendações abrangentes na literatura que abordem ferramentas, tecnologias e desafios relacionados a autenticação e autorização em arquitetura de microsserviços.

O restante do estudo está organizado da seguinte forma: Na Seção 2, fornecemos uma visão geral dos trabalhos relacionados à nossa pesquisa. A Seção 3 apresenta o protocolo da RSL. Além disso, a Seção 4 detalha como conduzimos o estudo. Na Seção 5 apresentamos a análise dos resultados das nossas questões de pesquisa. A Seção 6 discute as principais ameaças à validade. Ao final, na Seção 7, resumimos nossas conclusões.

2. Trabalhos Relacionados

Recentemente, [de Almeida and Canedo 2022] realizaram uma RSL selecionando 24 estudos publicados após o ano de 2010, para buscar identificar estudos que abordam autenticação e autorização em arquitetura de microsserviços, quais os mecanismos de segurança utilizados para lidar com os desafios e quais tecnologias de código aberto que implementam os mecanismos. Os autores relatam também uma grande carência quando o estudo é especifico para autenticação e autorização em arquiteturas de microsserviços, constataram também poucas indicações na literatura sobre soluções de código aberto.

[Pereira-Vale et al. 2019] descreve um projeto e os resultados de um mapeamento sistemático para identificar os mecanismos de segurança usados em sistemas baseados em microsserviços. Selecionaram 26 estudos primários de um total de 321 estudos encontrados entre o ano de 2015 e 2018. Eles observaram um incremento na quantidade de publicações em torno de 50% ao ano e os mecanismos de segurança mais relatados são Autorização, Autenticação e Credenciais.

[Alshuqayran et al. 2016] realizou um estudo de mapeamento sistemático sobre

os estilo de arquitetura para microsserviços que se concentra na identificação de desafios arquitetônicos relacionados a sistemas de microsserviços. A revisão foi conduzida da seguinte forma: primeiramente foi elaborada as questões de pesquisa. Na sequencia foi preparada a estratégia de busca, que restringiu a trabalhos publicados entre 2014 e 2016. Após a aplicação dos critérios de exclusão e inclusão, 33 estudos foram selecionados. Uma avaliação qualitativa foi realizada para criar um modelo de esboço para a qualidade do trabalho.

[Ponce et al. 2022] apresentou uma revisão multivocal da literatura que busca organizar conhecimento sobre segurança em aplicativos baseados em microsserviços. Analisaram 58 estudos primários, publicados de 2011 até o final de 2020. A pesquisa da literatura branca foi realizada combinando a *string* de pesquisa com o título e o resumo. A pesquisa na literatura cinza foi realizada pelos motores de busca: Google, Bing e DuckDuckGo. O estudo identificou dez maus cheiros para segurança de microsserviços e uma taxonomia que permite ajudar a mitigar seus efeitos.

[Hannousse and Yahiouche 2021] realizou um mapeamento sistemático para categorizar e apresentar um guia sobre ameaças conhecidas em microsserviços e como elas podem ser detectadas, mitigadas ou evitadas. A busca resultou 1.067 estudos, dos quais 46 foram selecionados como estudos primários entre o ano de 2011 e 2019. Para evitar a perda de estudos relevantes, foi conduzindo procedimento de *snowballing* [Wohlin et al. 2016] recursiva para trás e para frente. Por fim, na Tabela 1 apresentamos uma breve discussão e as soluções identificadas nos estudos relacionados.

Tabela 1. Resumo comparativo dos trabalhos relacionados.

Estudos	Período	#	Escopo	Soluções
Nosso Estudo	2015-2023	19	Identificar soluções, ferramentas e tecnologias que lidam com autenticação e autorização para arquitetura de microsserviços.	Keycloak, Zuul, Kong and Apache APISIX.
Alshuqayran (2016)	2014-2016	33	O estudo se concentra na identificação de desafios arquitetônicos relacionados a sistemas de microsserviços.	API Gateway, OAuth e Proxy.
Pereira-Vale (2019)	2015-2018	26	Descreve um projeto e seus resultados para identificar os mecanismos de segurança utilizados em sistemas baseados em microsserviços.	API Gateway, Distributed Session, SSO e JWT.
Hannousse (2021)	2011-2019	46	Fornece um guia sobre ameaças conhecidas em microsserviços e como elas podem ser detectadas, mitigadas ou evitadas.	API Gateway.
Ponce (2022)	2011-2020	58	Apresenta uma taxonomia referente à segurança em aplicações que utilizam a arquitetura de microsserviços.	API Gateway, OAuth e OpenID Connect.
de Almeida e Canedo (2022)	2010-2021	24	Aborda desafios, mecanismos e tecnologias relacionados à autenticação e autorização em microsserviços.	API Gateway, OAuth, OpenID Connect e JWT.

3. Protocolo da Revisão

Nesta seção, apresentamos o protocolo adotado para a realização desta RSL. Para atingir o objetivo da pesquisa, realizamos uma coleta sistemática na literatura e utilizamos para apoiar o processo de triagem e análise dos estudos encontrados a ferramenta Thoth[1].

3.1. Escopo e Objetivo

O objetivo principal desta RSL é identificar estudos publicados nas principais bibliotecas digitais da literatura entre 2015 e janeiro de 2023, que discorrem sobre soluções de autenticação e autorização para arquitetura de microsserviços.

[1]Thoth: `http://200.132.136.13/Thoth/`

```
(Microservice OR Microservices OR Container* OR ``Distributed
Application'') AND (Authentication OR Authenticate OR Authorization
OR ``API Gateway'' OR Access OR Proxy) AND (Management OR Identity
OR Control OR Permission OR Security) AND (Approach OR Mechanism*
OR Framework OR Architecture OR Strateg* OR Protocol* OR Solution*)
```

Figura 1. *String* de busca genérica

3.2. Questões de Pesquisa

Definimos as seguintes Questões de Pesquisa (QP): **QP1.** Quais são as ferramentas de gerenciamento de autenticação existentes para arquitetura de microsserviços na literatura? **QP2.** Quais são as tecnologias mais utilizadas pelas ferramentas de autenticação para arquitetura de microsserviços? **QP3.** Quais são os desafios relacionados aos aspectos de autenticação de sistemas na arquitetura de microsserviços?

3.3. Processo de Pesquisa

O método aplicado nesta pesquisa é o processo clássico de três etapas para a execução de estudos sistemáticos: Planejamento, Condução e Relatório proposto por [Kitchenham and Brereton 2013]. Para a realização da pesquisa foram utilizadas bibliotecas digitais que atendem aos seguintes critérios (1) possuem um mecanismo de pesquisa baseado na web; (2) tem um mecanismo de busca capaz de usar palavras-chave, e; (3) conter trabalhos da área de ciência da computação. Realizamos a busca nas principais bibliotecas digitais na área de Computação. As bibliotecas utilizadas foram IEEE Xplore, ACM Digital Library, Scopus e Engineering Village, todas acessadas em 12 de janeiro de 2023. Na Figura 1 apresentamos a *string* de busca utilizada, que foi definida de acordo com as palavras-chave que devem aparecer nos resultados da busca. Para formular a *string* de busca, utilizamos termos e sinônimos, as operações booleana "OR" para selecionar sinônimos alternativos para cada termo e "AND" para combinar os termos. Maiores detalhes sobre a execução da *string* em cada biblioteca digital pode ser encontrado em arquivos de imagens complementares disponibilizados no repositório Zenodo da RSL[2].

3.4. Critérios de Inclusão e Exclusão

Os critérios de seleção buscam identificar estudos que forneçam informações sobre as QPs. Definimos os seguintes **Critérios de Inclusão (CI)**: **CI1.** *Trabalhos publicados entre os anos de 2015 a 2023;* **CI2.** *Estudos sobre soluções de gerenciamento de autenticação em arquitetura de microsserviços;* **CI3.** *Publicações relacionadas a ferramentas de autenticação para arquitetura escalável.* **Critérios de Exclusão (CE)**: **CE1.** *Trabalhos que não estão escritos no idioma inglês;* **CE2.** *Arquivo PDF não disponível;* **CE3.** *Publicações que não atendam os critérios de inclusão.*

3.5. Critérios de Qualidade

O objetivo da avaliação de qualidade é avaliar os estudos, como forma de mensurar sua relevância em relação a outros. Os Critérios de Qualidade (CQ) foram baseados em [Dybå and Dingsøyr 2008]: relevância (CQ1, CQ2 e CQ3), relatório (CQ4), rigor (CQ5)

[2]Repositório Zenodo: `https://zenodo.org/records/10161123`

e credibilidade (CQ6). Cada um dos critérios de qualidade são avaliados de acordo com a seguinte nota: S (sim) = 100%; P (parcial) = 50%, N (não) = 0%. **CQ1.** *O estudo apresenta soluções de gerenciamento de autenticação para arquitetura de microsserviços? Avaliação*: **S**: Estudo apresenta pelo menos uma solução de autenticação; **P**: Estudo apresenta em partes uma solução de autenticação; **N**: Estudo não apresenta uma solução de autenticação; **CQ2.** *O estudo apresenta ferramentas de autenticação para se utilizar em uma arquitetura escalável? Avaliação*: **S**: O estudo apresenta pelo menos uma ferramentas autenticação; **P**: O estudo apresenta em partes uma ferramentas autenticação; **N**: Estudo não apresenta uma ferramenta de autenticação; **CQ3.** *O estudo identifica problemas e/ou desafios envolvendo autenticação na arquitetura de microsserviços? Avaliação*: **S**: O estudo identifica problemas e/ou desafios na autenticação em arquitetura de microsserviços; **P**: O estudo identifica em partes problemas e/ou desafios na autenticação em arquitetura de microsserviços; **N**: O estudo não identifica problemas e/ou desafios na autenticação em arquitetura de microsserviços; **CQ4.** *O objetivo da pesquisa realizada está claramente descrito? Avaliação*: **S**: O objetivo está claramente descrito; **P**: O objetivo está parcialmente descrito; **N**: O objetivo não está claramente descrito; **CQ5.** *A análise dos dados foi suficiente para abordar os objetivos da pesquisa? Avaliação*: **S**: A análise dos dados foi suficiente para abordar os objetivos da pesquisa; **P**: A análise dos dados foi parcialmente suficiente para abordar os objetivos da pesquisa; **N**: A análise dos dados não foi suficiente para abordar os objetivos da pesquisa; **CQ6.** *Existe uma declaração clara das conclusões? Avaliação*: **S**: Existe uma declaração clara das conclusões; **P**: Existe parcialmente uma declaração clara das conclusões; **N**: Não existe uma declaração clara das conclusões.

3.6. Processo de Seleção

Esta seção apresenta as etapas realizadas no processo de busca e seleção dos estudos: **(i)** Execução da *string* de busca nas bibliotecas digitais; **(ii)** Exportação dos arquivos no formato BibTeX com os estudos e importação dos mesmos na ferramenta Thoth; **(iii)** Remoção dos estudos primários duplicados; **(iv)** Aplicação dos critérios de inclusão e exclusão com base na leitura do título e o resumo; **(v)** Avaliação de qualidade e extração de dados com a leitura na íntegra dos estudos; **(vi)** Extração de dados dos estudos primários selecionados; **(vii)** Análise qualitativa com apoio da ferramenta QAnubis dos dados extraídos. O detalhamento do processo de seleção dos estudos, com os respectivos quantitativos está disponível no repositório Zenodo já mencionado.

4. Condução

Apresentamos uma análise da execução da *string* de busca em cada uma das bibliotecas digitais (BD). Limitamos a busca aos campos “Resumo” e “Título” em todas as BDs, excluindo o “Corpo” do estudo. As BDs IEEE Xplore e Engineering Village permitem refinar a busca, determinando o intervalo de ano da publicação direto na interface da aplicação. Já as BDs ACM Digital Library e Scopus o filtro foi incorporado como parte da *string* de busca. A aplicação da *string* em cada uma das BDs, totalizou 3299 estudos e 474 duplicados foram removidos. Isso reduziu a quantidade de estudos para 2825. Ao examinar o título e o resumo dos estudos restantes, 2806 foram rejeitados por sua irrelevância. Restando 19 estudos aprovados que tem alguma relevância com os critérios de inclusão. Disponibilizamos no repositório Zenodo uma planilha complementar com a relação completa de todos os estudos selecionados para nossa RSL.

Na etapa de avaliação de qualidade, aplicamos os CQs (Seção 3.5) para avaliar a confiabilidade e ranquear os melhores estudos. Como critério de exclusão na avaliação de qualidade, o estudo teria que ser pontuado como Fraco ou Médio, como nenhum dos estudos foi definido com essa classificação, manteve-se os 19 estudos para o andamento deste trabalho. Maiores detalhes sobre a avaliação de qualidade pode ser encontrados em planilha disponível no repositório Zenodo já previamente mencionado.

5. Análise dos Resultados

5.1. Respostas às Questões de Pesquisa

QP1. *Quais são as ferramentas de gerenciamento de autenticação para uma arquitetura de microsserviços existentes na literatura?* Entre os 19 estudos primários analisados, Keycloak é a ferramenta mais mencionada, seguida por Zuul, Kong, Okta e Apache APISIX. Na Tabela 2 apresentamos as ferramentas que implementam autenticação e autorização identificadas na literatura.

Tabela 2. Soluções encontradas nos estudos primários selecionados.

Soluções	Tipo	Link	Estudos
Apache APISIX	F	`apisix.apache.org`	[Raj et al. 2023]
Dubbo	F	`dubbo.apache.org`	[Yang et al. 2021]
Express Gateway	F	`www.express-gateway.io`	[Raj et al. 2023]
Gloo	F	`docs.solo.io/gloo-edge`	[Raj et al. 2023]
Goku	F	`www.gokuapi.com`	[Raj et al. 2023]
Keycloak	F	`www.keycloak.org`	[Ranawaka et al. 2020, Melton 2021, Preuveneers and Joosen 2019, Chatterjee and Prinz 2022, Das et al. 2021]
Kong	F	`konghq.com`	[Raj et al. 2023, Xu et al. 2019]
KrakenD	F	`www.krakend.io`	[Raj et al. 2023]
Ocelot	F	`ocelot.readthedocs.io`	[Raj et al. 2023]
Okta	F	`www.okta.com/`	[Snger and Abeck 2022]
Tyk	F	`tyk.io`	[Raj et al. 2023]
Zuul	F	`github.com/Netflix/zuul`	[ShuLin and JiePing 2020, Xiong and Li 2022]
OpenID Connect	P	`openid.net/connect`	[Bánáti et al. 2018, Melton 2021, Snger and Abeck 2022, Chatterjee and Prinz 2022, Yarygina and Bagge 2018]
OAuth	P	`oauth.net/2/`	[Triartono et al. 2019, Bánáti et al. 2018, ShuLin and JiePing 2020, Pasomsup and Limpiyakorn 2021, Snger and Abeck 2022, Chatterjee and Prinz 2022, Yarygina and Bagge 2018, Liu et al. 2020, Yang et al. 2021, Melton 2021]
JWT	S	`jwt.io`	[Pasomsup and Limpiyakorn 2021, Bánáti et al. 2018, ShuLin and JiePing 2020, Melton 2021, Snger and Abeck 2022, Xu et al. 2019, Yarygina and Bagge 2018, Bhutada and Jyothi 2019, He and Yang 2017, Pontarolli et al. 2021, Raj et al. 2023, Preuveneers and Joosen 2019, Yang et al. 2021]

Legenda: **F** = Ferramenta — **P** = Protocolo — **S** = *Standard*.

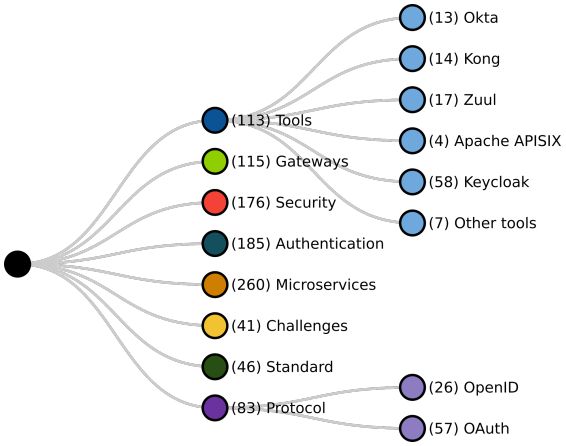
QP2. *Quais são as tecnologias mais utilizadas pelos mecanismos de autenticação para arquitetura de microsserviços?* Por outro lado, as principais tecnologias utilizadas para autenticação e autorização identificadas na literatura são apresentadas na Tabela 2, destacadas por **P**rotocolos e um padrão **S**tandard. Assim, destacamos os protocolos OAuth e OpenID Connect e o mecanismo JWT como as tecnologias mais citadas entre os estudos selecionados.

QP3. *Quais os principais desafios relacionados aos aspectos de autenticação de sistemas na arquitetura de microsserviços?* Os desafios mais relevantes identificados nos estudos sobre autenticação de sistemas na arquitetura de microsserviços foram citados 41

vezes nos estudos. Os desafios mais frequentemente mencionados na literatura foram: (i) Segurança/Privacidade (13 menções), (ii) Autenticação e Autorização/Controle de Acesso (9 menções), (iii) Arquitetura de Microsserviços (7 menções), e (iv) Aumento da superfície/grande número de microsserviços (4 menções). Entre os desafios, observamos a sua interligação direta, pois todos estão relacionados com mecanismos de segurança.

5.2. Análise Qualitativa

Para análise qualitativa, utilizamos a ferramenta QAnubis[3] desenvolvida pelo nosso grupo de pesquisa. Realizamos citações em forma de codificação em palavras, frases ou parágrafos que contém uma ideia clara que pode ser atribuída a um código específico. Durante a análise dos estudos, identificamos um total de 1019 citações codificadas em 8 temas. Dentre os temas, Microsserviços, Autenticação e Segurança se destacam como os de maior destaque, recebendo 260, 185 e 176 menções respectivamente, citados em todos os 19 estudos selecionados. A Figura 2a apresenta os códigos identificados e a árvore de temas. Por fim, apresentamos uma nuvem de palavras representando as mais citadas nos estudos analisadas. A nuvem de palavra exibida na Figura 2b incorpora uma Folksonomia [Xu et al. 2008], onde termos notáveis como “autenticação”, “segurança”, “microsserviço(s)”, “gateway”, “API”, entre outros, são exibidos.



(a) Árvore de códigos e temas.

(b) Folksonomy [Xu et al. 2008] - Citações Nuvem de Palavras.

Figura 2. Resultados da análise qualitativa.

6. Ameaças à Validade do Estudo

Nesta seção apresentamos as principais ameaças identificadas que poderiam comprometer a validade do estudo com base em [Ampatzoglou et al. 2019]:

Validade de Construção: Entre as ameaças identificadas nesta categoria está a possibilidade de que as questões de pesquisa ou os termos e sinônimos da *string* de pesquisa sejam inadequados, amplos ou incompletos e o fato da avaliação dos estudos não ser conduzida em pares. Para mitigar essas ameaças, buscamos orientação de pesquisadores experientes na área e utilizamos a ferramenta QAnubis.

Validade Interna: Este aspecto diz respeito ao exame das relações causais. Para mitigar estas ameaças, aplicamos um formulário para extração de dados levando em

[3]QAnubis: `http://168.138.132.249`

consideração as QPs. Também aplicamos uma estratégia de busca de trabalhos relacionados às palavras-chave definidas na *string* e excluímos a literatura cinza. Esse fator não teve impacto significativo, pois os estudos passaram por um rigoroso processo de seleção.

Validade Externa: A ameaça potencial diz respeito se os estudos selecionados realmente mencionam soluções de autenticação para arquitetura de microsserviços. Para mitigar a generalização dos resultados, aplicamos as melhores recomendações propostas por [Kitchenham and Brereton 2013].

Validade de Conclusão: O preconceito do pesquisador pode impactar significativamente as conclusões tiradas e pode ser considerado uma ameaça à validade da conclusão. Para mitigar essa questão, realizamos uma leitura criteriosa dos estudos e para mitigar o viés interpretativo, adotamos o uso de tabulação dos dados extraídos para obter respostas às QPs. Também seguimos as recomendações propostas por [Wohlin et al. 2012].

7. Considerações Finais

Realizamos uma RSL para identificar soluções de autenticação e autorização em arquitetura de microsserviços, obtendo 19 estudos primários. Observamos uma carência significativa de estudos relacionados a soluções de autenticação e autorização em arquiteturas de microsserviços. O modelo de arquitetura de microsserviços divide uma aplicação em serviços pequenos, independentes e escaláveis. Portanto, os aspectos de segurança devem ser cuidadosamente considerados para cada serviço individual, pois a arquitetura de microsserviços aumenta a superfície de ataque e a falta de atenção pode tornar a aplicação vulnerável. Um API *gateway* recebe solicitações de clientes e gerencia políticas de autenticação de usuário e controle de acesso para um conjunto de microsserviços.

Com base na análise realizada, os estudos revelam que a ferramenta Keycloak, os protocolos *OpenID Connect* e *OAuth*, e o padrão JWT estão entre os estudos selecionados sobre autenticação e autorização de sistemas para arquitetura de microsserviços (ver Tabela 2). Além disso, destaca-se os desafios de Segurança/Privacidade e Autenticação e Autorização/Controle de Acessos como os mecanismos mais mencionados nos estudos primários selecionados. Como trabalhos futuros pretende-se expandir este estudo usando os 19 estudos selecionados como sementes para um protocolo de *snowballing* [Wohlin et al. 2016] para identificar estudos semelhantes e expandir ainda mais as descobertas. Além disso, estas conclusões orientarão as decisões sobre a implementação de uma solução abrangente para autenticação e autorização em um ambiente universitário, onde existem atualmente múltiplas soluções independentes e desarticuladas de sistemas legados para autenticação e autorização. A partir dessas ferramentas, será realizada uma analise técnica para identificar a solução que melhor supre a demanda.

Agradecimentos

Os autores agradecem à FAPERGS (Projeto 22/2551-0000841-0) pelo apoio ao trabalho.

Referências

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

Ampatzoglou, A., Bibi, S., Avgeriou, P., Verbeek, M., and Chatzigeorgiou, A. (2019). Identifying, categorizing and mitigating threats to validity in software engineering secondary studies. *Applied Sciences*, 106(30).

Bhutada, S. and Jyothi, K. (2019). Enhancing security to the microservice (ms) architecture by implementing authentication and authorization (aa) service using docker and kubernetes. *International Journal of Innovative Technology and Exploring Engineering*, 8(6):401–407.

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

Chatterjee, A. and Prinz, A. (2022). Applying spring security framework with keycloak-based oauth2 to protect microservice architecture apis: A case study. *Sensors*, 22(5).

Das, D., Walker, A., Bushong, V., Svacina, J., Cerny, T., and Matyas, V. (2021). On automated rbac assessment by constructing a centralized perspective for microservice mesh. *PeerJ Computer Science*, 7:1–24.

de Almeida, M. G. and Canedo, E. D. (2022). Authentication and Authorization in Microservices Architecture: A Systematic Literature Review. *Applied Sciences*, 12(6).

Dybå, T. and Dingsøyr, T. (2008). Strength of evidence in systematic reviews in software engineering. In *2nd ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*, ESEM'08, pages 178—-187, New York, USA. ACM.

Hannousse, A. and Yahiouche, S. (2021). Securing microservices and microservice architectures: A systematic mapping study. *Computer Science Review*, 41.

He, X. and Yang, X. (2017). Authentication and authorization of end user in microservice architecture. *Journal of Physics: Conference Series*, 910(1).

Kitchenham, B. and Brereton, P. (2013). A Systematic Review of Systematic Review Process Research in Software Engineering. *Inf. and Softw. Tech.*, 55(12):2049–2075.

Liu, H., Wang, Z., Huang, L., and Wang, K. (2020). Building a private cloud based on microservices for computer science laboratory in universities. In *7th International Conference on Information Science and Control Engineering*, pages 379–384. IEEE.

Melton, R. (2021). Securing a Cloud-Native C2 Architecture Using SSO and JWT. In *2021 IEEE Aerospace Conference (50100)*, pages 1–8.

Pasomsup, C. and Limpiyakorn, Y. (2021). HT-RBAC: A Design of Role-based Access Control Model for Microservice Security Manager. In *International Conference on Big Data Engineering and Education*, BDEE'21, pages 177–181.

Pereira-Vale, A., Márquez, G., Astudillo, H., and Fernandez, E. B. (2019). Security Mechanisms Used in Microservices-Based Systems: A Systematic Mapping. In *XLV Latin American Computing Conference (CLEI)*, pages 1–10, Panamá. IEEE.

Ponce, F., Soldani, J., Astudillo, H., and Brogi, A. (2022). Smells and refactorings for microservices security: A multivocal literature review. *Systems and Software*, 192.

Pontarolli, R. P., Bigheti, J. A., de Sá, L. B. R., and Godoy, E. P. (2021). Towards Security Mechanisms for an Industrial Microservice-Oriented Architecture. In *14th IEEE International Conference on Industry Applications (INDUSCON)*, pages 679–685.

Preuveneers, D. and Joosen, W. (2019). Towards Multi-party Policy-based Access Control in Federations of Cloud and Edge Microservices. In *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 29–38.

Raj, P., Vanga, S., and Chaudhary, A. (2023). *Microservices Security: The Concerns and the Solution Approaches*, pages 289–298. Wiley-IEEE Press.

Ranawaka, I., Marru, S., Graham, J., Bisht, A., Basney, J., Fleury, T., Gaynor, J., Wannipurage, D., Christie, M., Mahmoud, A., Afgan, E., and Pierce, M. (2020). Custos: Security Middleware for Science Gateways. In *Practice and Experience in Advanced Research Computing*, PEARC'20, pages 278—-284, New York, USA. ACM.

ShuLin, Y. and JiePing, H. (2020). Research on Unified Authentication and Authorization in Microservice Architecture. In *20th International Conference on Communication Technology (ICCT)*, pages 1169–1173. IEEE.

Snger, N. and Abeck, S. (2022). Authentication and authorization in microservice-based applications. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, P-326:207–218.

Triartono, Z., Negara, R. M., and Sussi (2019). Implementation of Role-Based Access Control on OAuth 2.0 as Authentication and Authorization System. In *6th Int. Conf. on Electrical Engineering, Computer Science and Informatics (EECSI)*, pages 259–263.

Wohlin, C., Petersen, K., Runeson, P., Ohlsson, M. C., and Host, M. (2016). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *Empirical Software Engineering*, 21(3):797–829.

Wohlin, C., Runeson, P., Hst, M., Ohlsson, M. C., Regnell, B., and Wessln, A. (2012). *Experimentation in Software Engineering*. Springer Publishing Company, Inc.

Xiong, Q. and Li, W. (2022). Design and Implementation of Microservices Gateway Based on Spring Cloud Zuul. In *3rd International Conference on Computer Information and Big Data Applications (CIBDA)*, pages 1–5.

Xu, R., Jin, W., and Kim, D. (2019). Microservice security agent based on api gateway in edge computing. *Sensors (Switzerland)*, 19(22).

Xu, S., Bao, S., Fei, B., Su, Z., and Yu, Y. (2008). Exploring Folksonomy for Personalized Search. In *31st Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 155–162, New York, USA. ACM.

Yang, J., Hou, H., Li, H., and Zhu, Q. (2021). User Fast Authentication Method Based on Microservices. In *IEEE International Conference on Power Electronics, Computer Applications (ICPECA)*, pages 93–98.

Yarygina, T. and Bagge, A. (2018). Overcoming security challenges in microservice architectures. In *12th International Symposium on Service-Oriented System Engineering and 9th International Workshop on Joint Cloud Computing*, pages 11–20. IEEE.