MCIT Modeling, control & information technologies

Authentication and authorization in microservice oriented application design

https://doi.org/10.31713/MCIT.2024.035

Yurii Kovalov
Department of Computer Engineering Faculty of Radiophysics, Electronics and Computer Systems
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine,
yuk123@meta.ua

***Abstract* – In the past years microservice oriented design patterns obtained much popularity among the system architects and programmers. One of the obstacles in this design is authentication and authorization issues. This article presents one of the possible solutions for this problem. The essence of this methodology is a single point of authentication and many points of authorization spread across all the microservices.**

***Keywords* – microservice; authorization; authentication; monolith; application design;**

I. Introduction

Recently microservice oriented application design obtained much popularity among the software architectures and engineers. It introduces a lot of advantages compared to monolith application design but has drawbacks too. The main advantages are the possibility to break down business processes to parts that can be implemented by different teams and reducing the complexity of every part of application. One of the drawbacks is an increased complexity of authentication and authorization procedures.

The point is that with monolith design developers have to protect only the periphery of application while with microservices there are many peripheries to protect. Authorization in monolith applications is usually centralized, while with microservices design every microservice must authorize user's queries by itself.

Scientists tried different approaches in their studies. Two separate microservices for authentication and authorization were proposed, while investigating performance with SQL and No-SQL databases [1]. Another study investigated a common approach to access control authorization. Authorization rules were shared between different microservices [2]. In the next study an attribute based JSON access control policy language was proposed [3]. As concluded in the next study, there are not many studies in the subject and much less studies demonstrating practical implementation of authentication and authorization with microservice architecture [4].

II. Application Design

A. Interaction inside application

In this study some methodological recommendations in the authentication and authorization when dealing with microservice oriented application design were outlined. These recommendations are based on practical implementation of microservice systems for finance and accountancy.

As usual business processes in the realm of accountancy and finance are implemented very well with monolith application design. The benefits we would possibly receive from microservice design are easier support and maintenance. So let's try to implement microservice design including authentication and authorization to take advantage of both approaches simultaneously.

The idea is to implement a microservice application in such a way that it should look like a monolith for customers but behave like a microservice for programmers. In order to fulfill this the proposed methodology will construct a microservice application with one single entrance point – let's call it ApiGateway (Fig.1). All microservices are interacting with each other and users within a private secure network by sending events through EventBroker. ApiGateway authenticates users and passes out events to and from microservice applications and uses SSL (Secure Socket Layer) to communicate with end users.

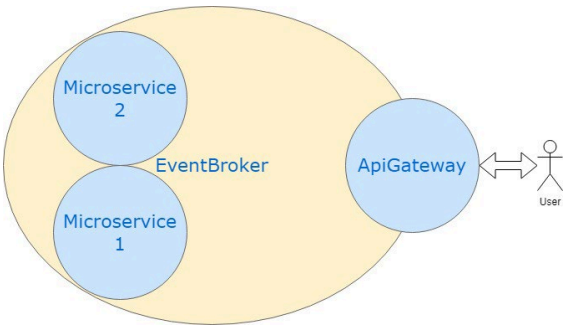


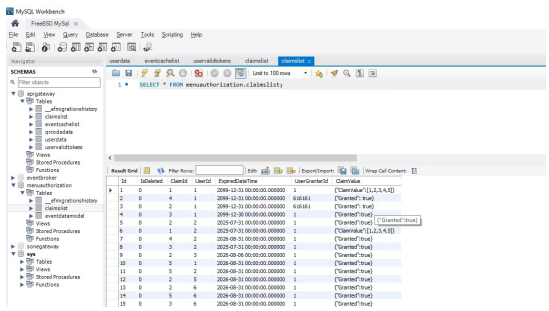
Figure 1. Authentication schema

It is crucial for systems to operate as quickly as possible inside the enclosed private network. One user's query may pass through multiple microservices before the answer is ready. In our methodology we don't recommend using encryption between microservices because it will inevitably slow down events flow. The private network is protected by firewalls and VPN (Virtual Private Network) gateways. The same mechanisms were used for monolith applications and they demonstrated effectiveness and robustness. Just like in monoliths we protect only the periphery and gates of microservice application.

B. Authorization

As already mentioned above one of the main advantages in microservice application design is the possibility of implementing microservice functions by different teams. Hence every microservice should be as independent from others in design as possible. The central part of any application is authorization. In this methodology every microservice is responsible to keep authorization information for every user in the system. Of course in this situation the default (no information about authorization) is denying access to resources.

The first authorization rule every microservice should implement is authorizing other authorization rules change. Let's look at the example with menu



microservice authorization rules (Fig. 2).

Figure 2. Authorization rules example.

The first authorization rule in the table sets access to users in giving authorization access for other people. Other rules are authorizing access to different parts of menu in microservice application.

All rules can be managed by authorized persons using a micro frontend interface that accumulates authorization rules from all microservices (Fig.3).

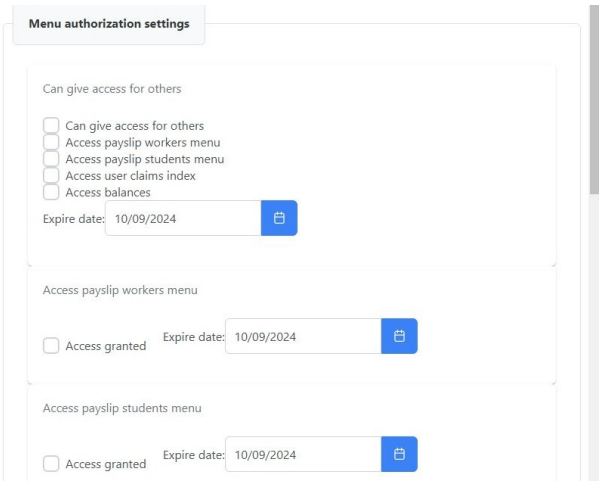


Figure 3. Authorization rules managing microservice.

It is essential to build this micro frontend interface with respect to possibility of changing it by every team independently, thus implementing microservice logic they would not intertwine with each other.

REFERENCES

[1] Randa Ahmad Al-Wadi and Adi A. Maaita (2023) "Authentication and Role-Based Microservice Architecture: A Generic Performance-Centric Design", Journal of Advances in Information Technology, Vol. 14, No. 4, November 2023, pp. 758-768 doi: 10.12720/jait.14.4.758-768.J. Clerk Maxwell, "A Treatise on Electricity and Magnetism," 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Algimantas Venčkauskas, Donatas Kukta , Šarūnas Grigaliūnas and Rasa Bruzgiene (2023) "Enhancing Microservices Security with Token-Based Access Control Method", Sensor, 23, 3363, pp. 1-21, doi: 10.3390/s23063363.

[3] Davy Preuveneers and Wouter Joosen (2017) "Access Control with Delegated Authorization Policy Evaluation for Data-Driven Microservice Workflows", Future Internet, 2017, 9, 58, doi: 10.3390/fi9040058.

[4] Murilo Góes de Almeida and Edna Dias Canedo (2022) "Authentication and Authorization in Microservices Architecture: A Systematic Literature Review", Applied Sciences, 2022, 12, 3023, pp. 1-20, doi: 10.3390/app12063023