Department of Computer Science

Distributed and Self-organizing Systems Group

<TODO: Art der Arbeit>

<TODO: Titel der Arbeit>

[Comments] mpc

Chemnitz, 30 January 2019

**Examiner:** <TODO: Prüfer>

**Supervisor:** <TODO: Betreuer>

**mpc,** [Comments]

<TODO: Titel der Arbeit>

<TODO: Art der Arbeit>, Department of Computer Science

Chemnitz University of Technology, 30 January 2019

Abstract

Many web applications grow over time to accommodate the new requirements of their users. With every newly added feature, the application becomes more interconnected and harder to scale and maintain. Microservices architecture was created to help developers scale their applications with ease without added complications for modifications or maintenance.

This new architecture suits both ends of the application, the Frontend and the Backend as well. Backend requirements will be handled by small tasks and each task will be performed by a microservice. On the other side, the Frontend will be divided into different parts and each part will be rendered by one micro frontend. As this implies communication between all micro parts, trust plays especially with parts of different parties a central role. The objective of this thesis is to research the workflow, tools and guidelines involved in creating a web application based on this architecture, while solving trust concerns via embedded content trust. To achieve this, a Blog will be developed out of micro frontends and microservices. The relationship among micro apps will be addressed regarding their content trust. A solution will be created to help the different parts of the application to establish a context-wise trust.

The objective of this master thesis is to find an approach or a combination of approaches to solve the previously mentioned problem in the context Microservices and Content Trust. This particularly includes the state of the art regarding microservices and trust in computer science with reference to Content Trust. The demonstration of feasibility with an implementation prototype of the concept is part of this thesis as well as a suitable evaluation with exemplary use case

Table of Contents

[List of Figures vii](#_Toc536558538)

[List of Tables ix](#_Toc536558539)

[List of Listings xi](#_Toc536558540)

[List of Abbreviations xiii](#_Toc536558541)

[1 Introduction 1](#_Toc536558542)

[1.1 Current Situation 2](#_Toc536558543)

[1.2 Motivation 3](#_Toc536558544)

[1.3 Problem 5](#_Toc536558545)

[1.4 Objective 7](#_Toc536558546)

[1.5 Outline 8](#_Toc536558547)

[2 State of The Art 11](#_Toc536558548)

[2.1 Requirements 11](#_Toc536558549)

[2.1.1 Requirements of Microservices and Micro frontends 12](#_Toc536558550)

[2.1.2 Requirements of Content trust 16](#_Toc536558551)

[2.1.3 Requirements of Developers and Users 19](#_Toc536558552)

[2.2 Literature Review 20](#_Toc536558553)

[2.2.1 Microservices and Micro frontends literature review 20](#_Toc536558554)

[2.2.2 Microservices vs monolithic 23](#_Toc536558555)

[2.2.3 Trust literature review 28](#_Toc536558556)

[2.3 Analysis 35](#_Toc536558557)

[2.3.1 Microservices analysis 36](#_Toc536558558)

[2.3.2 Content trust analysis 38](#_Toc536558559)

[3 Concept 41](#_Toc536558560)

[3.1 Concept of micro frontends 42](#_Toc536558561)

[3.2 Concept of microservices 43](#_Toc536558562)

[3.3 Concept of content trust 47](#_Toc536558563)

[3.3.1 Properties of the Content trust 48](#_Toc536558564)

[3.3.2 Context of Content trust 52](#_Toc536558565)

[3.4 Overall structure 53](#_Toc536558566)

[4 Implementation 57](#_Toc536558567)

[4.1 Implementation of microservices 57](#_Toc536558568)

[4.1.1 Microservices details 62](#_Toc536558569)

[4.2 Content trust implementation 67](#_Toc536558570)

[Bibliography 72](#_Toc536558571)

[Bezeichner für Anhang A 73](#_Toc536558572)

[Bezeichner für Anhang A.1 73](#_Toc536558573)

[Glossary LXXV](#_Toc536558574)

[Index LXXVII](#_Toc536558575)

# List of Figures

[Figure ‎2‑1 Scale Cube [35] 25](#_Toc536467436)

[Figure ‎3‑1 Overall structure 53](#_Toc536467437)

[Figure ‎4‑1: Overall interaction 58](#_Toc536467438)

# List of Tables

[Table ‎2.1: Comparing monolithic and microservices [34] 27](#_Toc536467687)

# List of Listings

[Listing ‎4.1: JSON format 59](#_Toc536467591)

[Listing ‎4.2 ContactUs API 61](#_Toc536467592)

[Listing ‎4.3: Structure of contact document 62](#_Toc536467593)

[Listing ‎4.4: Contact data example 63](#_Toc536467594)

[Listing ‎4.5: Installing jsonwebtoken using npm 64](#_Toc536467595)

[Listing ‎4.6: Generating a signed token 65](#_Toc536467596)

[Listing ‎4.7: Generated JWT [52] 65](#_Toc536467597)

[Listing ‎0.1 Mit Alt+ F9 bearbeiten (hängt von Heading 4 statt von 1 ab) 71](#_Toc536467598)

# List of Abbreviations

|  |  |
| --- | --- |
| **ABC** | Alphabet |
| **123** | Zahlenreihe |
| **HTML** | Hypertext Markup Language |
|  |  |

# Introduction

Traditional web applications are a software that comprises several parts, all those parts come together to form the final product. But at the end this product will look like as it is made out of one big unit. This unit is composed of few different layers on top of each other but each layer is tightly coupled with the other layers [46]. This architecture is sometimes called three-layered architecture that has presentation, business and data as its three layers.

The word “monolithic” is used in some of the literature to describe a three-layered architecture [2] [3] [34]. In this thesis both words, monolithic and three-layered will be used interchangeably to refer to a traditional web application that’s composed, mainly, of User interface, Logic layer, and a data access layer.

Once the application is ready to be deployed, developers will have to approach it as if it is, essentially, composed of two parts that can’t be divided into smaller units. Such division can be very useful when there’s a failure and the application is not running as it is supposed to. In this case, developers could isolate the malfunctioned parts. Hence the system will keep providing some of its services to the clients while also being maintained. Moreover, such possibility of parts isolation gives developers more flexibility and features when trying to find solutions for the problems.

Furthermore, updating a three-layered-based application and adding new features to it becomes harder the bigger the application is [34]. Application parts will be more interconnected and making changes to one part could result in needs to make changes to other parts. Hence developers might have to modify many parts of the system to allow for the new updates to take place.

Microservices architecture tries to overcome the challenges that are imposed when the application is created as a three-layered application. The idea of microservices is to have the system composed of many independent small parts that work together to form the final web application. This concept can also be projected into the frontend part of the application resulting into the micro frontends architecture. In essence, having the frontend as a combination of many small independent micro frontend apps.

## Current Situation

Microservices is still a new concept, although some companies have already migrated to the microservices architecture such as Amazon and Netflix [2]. There are companies facing many issues that could be solved by this new architecture. Yet those companies are hesitant in moving forward and migrating their application to the microservices architecture.

The idea of refactoring an existing application into a new one built using another architecture is not easy and brings with it many challenges [1]. Some of those challenges are still waiting to be addressed.

There are still many questions to be asked when thinking about the microservices architecture, for example: when thinking about the functional requirements of the application, developers should think about how their application can be divided into smaller parts. And whether following certain standards can be helpful in making a final better product. There can be other questions regarding the nature of the microservice itself. Such as the size of each microservice. Moreover, the communications between microservices are another challenge that deserves thoughtful consideration.

On the other hand, some concerns related to the frontend of the application can also be thought about. In principle, the frontend is what the user see and interact with. As an example for these concerns what if the frontend becomes also complex and needs to be divided into micro frontends. The concept of microservices can further be projected into the other side of the web application. Microservices is not just concerned with the backend side of the system, but it can be also applied to the frontend as well. When microservices concept is applied to the frontend it is called micro frontends [3].

Developers should find ways to help micro frontends exchange data between each other without violating the isolation and independence of each micro frontend. Since each micro frontend should be able to interact with other micro frontends while keeping the application loosely-coupled.

Furthermore, a mechanism should be in place to help microservices trust each other. Trust here doesn’t just mean believing each microservice to what it claims it is. But having a system that helps microservices to trust the behavior of each other.

There is still no standard definition of microservice architecture and there’s no clear guidelines of how an application based on microservices should be built [32]. Over the last few years some characteristics for a microservices-based application have been developed and some general basic outlines are now commonly used [1-2,31-34].

* Many small units: A microservices-based application should consist of more than one component: Unlike three-layered applications, a system built using microservices architecture should be composed of multiple components, each component is self-contained. This way the application can be changed, updated and modified whenever is needed. In this case, each change will be applied to only the concerned component itself and not the entire application.
* Simple Routing: Components in a microservice-based application will have a simple workflow. They will take an input, process it and then forwards the result.
* Decentralization vs centralization: An application based on microservice architecture is built out of many different components and each has its role. Sometimes there’s a central body that manages the interactions between the services. While other times, no one big unit moderating the communications between microservices.

Different technology stack: The development cycle of a microservices-based application involves having different teams working on different microservices. Each team can then choose development technologies and tools that are most suitable for their own microservice. With micro frontends, the frontend of the application is composed of many different small self-contained applications. Instead of having the frontend as a one unit written in one framework such as Angular or React JS. The frontend can be written and developed as a sum of smaller frontends. And then each micro frontend can be written in a different framework depending on its needs.

## Motivation

The current architecture that’s used heavily in building web applications is composed of layers built on top of each other. Each layer is responsible for a part of the application [34]. As mentioned in the first section of this chapter, it usually consists of three layers on top of each other’s [2] [46]. Moreover, some applications could end up having their logic layers divided further into more layers.

Although a three-layered web application is divided into layers, yet the application is still very tightly coupled [16]. There’s a great amount of connections between the layers. As a consequence, the system, of course, will be hard to maintain and update [34]. Each problem in the Backend could cause failure of the system, where no information could be processed or stored in the database. On the other hand, each problem in the User Interface could cascade to prevent data from flowing to the backend.

In some cases, fixing the issues could cost developers to make some modification. This leads to the problems of updating the system. Where Updating a traditional layered application is another big problem faces developers and business owners [34]. When needing new features or updates to fix the newly discovered issues, developers could find themselves facing two situations: Not being able to achieve the wanted updates and fixes as much as they’re supposed to. And on the other hand, having to perform huge system modifications and changes to accommodate the new desired features and changes.

These situations happen frequently and usually cost money, time and lots of efforts. Microservices architecture is developed to make applications more flexible. With microservice-based application, the system is now more accepting for changes. Developers don’t need to make great modification for the system to adapt a new feature. When a system failure happens or when a problem is discovered, developers have the ability to isolate the problem and fix it quickly.

Putting all the small parts together is not an easy task. Developers should think of the best way of having microservices interact with each other. Not just in the sense of sending and receiving information but also microservices should be able to exchange sensitive data. A mechanism of trust between microservices could help make the interaction more secure.

Such trust is very important, especially, when there is a need for using third-party microservices. In this case microservices might end up exchanging sensitive data such as user logins and passwords or maybe even bank details. In such scenario microservices should not start exchanging this type of data without verifying and knowing more details about the microservices on the receiving end. Here an implementation of content trust could mean a more secure system. It can insure that exchanging data between microservices only happens after having each microservice trusting the other one. Once it is known that no microservices have any harmful code, or bad intentions then data exchange should take place smoothly between microservices.

## Problem

Having microservices architecture in its early days means that not many resources are available. Moreover, not enough research is done yet to help developers find answers for their problems [32]. When dealing with microservices architecture two types of scenarios could be happening:

One case would be that; the Web application already exists based on three-layereds architecture. But there is a need to migrate it into microservices architecture. This thesis doesn’t try to find answers or better solutions for migrating from a traditional web application into a microservice-based application.

The other case would be that; developers want to develop the required system from the beginning based on the microservices architecture. One reason for this can be because the application is expected to grow. With microservices architecture, it is easier to scale the system as much as needed compared to three-layered architecture [34]. Another reason would be that the application has a complex nature and requires different technology stacks for its various parts. Such complex applications are not very common but they are mostly developed to provide solutions to big firms such as Amazon or Netflix [2]. Hence building such solutions using microservices architecture will help developers to use different tools and technologies for different parts as needed. This situation also applies for the frontend. In this case, the frontend could be complex and many special requirements are needed thus developers can divide it into smaller apps. With each app they can use different tools, frameworks and languages instead of having to use one toolset or one framework for developing the whole frontend.

Microservices architecture is basically one variant of Service Oriented Architecture (SOA) [32], but operations conditions are not quite the same as with traditional SOA [39]. With microservices architecture there are many small independent parts operating. Each part is providing or performing one small task. Sometimes microservices need to exchange data with each other and of course with the frontend.

Developers have to decide what kind of communication methods and protocols should be used among microservices. Representational State Transfer (REST) is one architecture that helps developers when creating web services. Another option is Simple Object Access Protocol (SOAP) which is a protocol for exchanging messages in a web services environment.

On the other hand, when developers decide to use micro frontends to render the frontend of the application. They should also think of how data is going to transfer between the different micro frontends and how communication between the many frontends and the microservices is happening.

In essence, micro frontends are autonomous independents parts [1]. These parts are not divided according to how they’re going to render on the screen. They’re divided according to their functionality or even the business they support. For example, in an online store, the distribution of micro frontends could be as follows: One micro frontend for the displaying of the products, another would be for the product details, a third micro frontend could be for adding items to the cart. And maybe a fourth for the check out and payment. Other micro frontend can be focused on other functionalities of the web site such as handling user data. For example, registration and creating a new account. This task can be assigned to a micro frontend, or updating user information. One micro frontend can also be created to handle security concerns such as when a user forgets his password.

A web application based on microservices could be composed of many microservices. At some point, these microservices may need to exchange sensitive information such as logins or bank details. Hence an implementation for content trust between services can help each service form an evaluation of trust before exchanging data with other microservices.

This situation would be more pressing if microservices were not all developed inside the same company. Such scenario could rise when small companies want to build their applications using microservices architecture. In this case, when having a small team of available developers, one could think of using ready-made solutions. Developers could use third-party microservices to save time and money. But doing this could expose the developed solution to more risks. Hence the need to establish a trust mechanism to help microservices evaluate how much each service trust the service on the other end, and if this trust is considered enough for each service to exchange data. Moreover, when adding new microservices to an already running system. Both the existing microservices as well as the newly added ones need to be able to have a way to assess how much they trust a service before deciding to exchange data or not. The kind of trust discussed here helps each microservice to form an opinion about microservices that are on the other side of the communication line before making the decision of whether to exchange data or not. After all, malicious or harmful microservices could hide their true intentions by expressing different behaviour while a harmful one is practiced behind the scenes.

There should be a way to help microservices trust each other without having a human intervention. When the application is getting bigger and embracing hundreds of microservices. Which in turn might also be depending on other microservices to run, then checking each one of them by the developers could end up being an endless task. Developers could start checking the microservices they adapted into their applications. But then shortly find themselves checking microservices that are used by the microservices they used. Hence keep moving backwards in the string of microservices.

Each microservice should be doing its own task of verifying its trust relationship with other microservices. When one microservice fails in doing so, and has no other options to fulfill the assigned task then developers should be alerted.

## Objective

The focus of this thesis will be on building a system out of microservices and micro frontends while providing a solution for content-trust among microservices.

Building a solution that’s ready to be deployed based on microservices and micro frontends architecture is still missing in the literature. Moreover, having a practical example of content trust between applications is also absent. Hence implementing a content trust mechanism between microservices will fill a gap in the literature. And could add to the work done in microservices as well as content trust.

While there are many questions and uncertainty to explore and research, this thesis will not try to find answers for every possible problem resulting from building microservices-based web applications. The workflow will be building of a Blog based on the microservices architecture, the development will involve using the latest technologies and tools to build the Blog. Solutions for faced challenges will be documented.

On the other hand, this thesis will not try to provide a full workflow and complete guidelines for building microservices-based web applications. Such attempts require years of research and will most likely be a never ending one. Since tools, frameworks and technologies are ever changing and developing and so are the ways of developing web applications. Moreover, it’ll not try to present a technology comparison of the possible ways to develop a solution based on microservices.

This thesis will also address the problems of content trust among microservices. A method will be created to help microservices trust each other context-wise. This trust is not just about verifying each microservice its identity to the other microservices, but it is also about having a mean or way of evaluating the trust between any two involved microservices.

## Outline

The next chapter of this thesis will be State-of-The-Art, in this part, discussion of requirements for microservices-based application and content trust will be presented. Moreover, a literature review and analysis of the requirements against the literature review will be provided.

Third chapter will focus on the concept of building microservices and establishing a content trust mechanism. This part of the thesis will try to weight the benefits as well as the negative sides of building applications based on the microservices architecture. It’ll investigate how a system with many moving parts can work and offer a stable and seamless experience to its users. At the same time have very clear division and separation of functionalities into small autonomous collaborating tasks. A method of content trust among microservices will be discussed and inspired from the content trust of the web. The discussion will also pay attention to the principles of micro frontends and the different methods, server-side as well as client-side, of combining micro frontends will be presented.

Chapter four will focus more on the practical side of the research. This chapter will discuss the development and building of a Blog based on the microservices architecture. The workflow will be presented and mistakes that have been done during the development will be discussed to help make other researches aware of them. The used tools will be explored and the reasons behind using such tools will be made clear. The developed method of content trust among microservices and micro frontends will be presented, how this method is developed will also be outlined and discussed.

Chapter five will be the evaluation, in this part of the thesis, an evaluation of the development and carried out research will be performed. This chapter will show the negative as well as the positive sides of the research and the implementation. It’ll also discuss the difference in the productivity when using specific tools or technologies. It’ll show the similarities and dissimilarities when selecting specific tools over others.

Last chapter is the conclusion; in this chapter a conclusion and a summary of the thesis will be presented.

# State of The Art

This chapter will be composed of three parts:

1. Requirements
2. Literature/State of the Art Review
3. Analysis

The first part will discuss and analyse the requirements for an application based on the microservices architecture. It will also discuss the requirements of content trust between microservices. Hence it will be composed of two sub sections. One for microservices and the other for content trust.

The second part will layout the literature review for microservices and also for content trust. As with the first section, this one will be mainly divided into two sections as well. One for microservices and the other for trust in general and content trust.

Last part of this chapter will be connecting the first two parts together. It will analyse the literature review against the requirements.

## Requirements

This part of the thesis will present requirements analysis for a microservices-based web application that uses a content trust mechanism between its microservices. The discussion will be split into three parts:

1. Requirements of Microservices and micro frontends
2. Requirements of Content trust between microservices
3. Requirements of Developers and Users

Microservices and micro frontends are architecture. Hence they have their own set of rules and requirements when it comes to building an application based on this new architecture.

On the other hand, when developing an application, developers should consider making the application as secure as possible. Yet, throughout the development of the proposed Blog, extra measures will not be taken in an effort to make the Blog more resistant to security threats. The focus will be on developing an implementation of content trust among different microservices, especially those coming from different sources/developers. Thus, this chapter will allocate a subsection in the requirements analysis to discuss the requirements of the content trust of the application.

### Requirements of Microservices and Micro frontends

A system based on microservices architecture consists of different small pieces of code. Each small piece is an application that can be deployed independently. It can also be updated and modified while keeping any modifications for the other small apps as minimum as possible. Such architecture, in theory, makes the system loosely coupled. Thus different system parts and components are easy to change, update, modify or even replace. As long as the interface of the new introduced microservices respects the old interface, or keeps using the same communications protocols, the system will continue to function.

Since micro frontends are basically microservices architecture applied to the frontend part of the application [50]. Some requirements should be respected when developing frontends as a group of small independent micro frontends.

Microservices, as described by Sam Newman in his book “Building Microservices” [1], are basically small independent services, that work together. From this definition, the basic requirements of microservices can be derived.

* Small
* Autonomous
* Has an Interface

Moreover, in [1,5,29] the description continues and more requirements can also be derived

* Replicable
* Respect Interface
* Reusable

Furthermore, respecting the five mentioned requirements results in the following features as described by [1, 5, 29]:

* Resilience
* Scalable
* Easy to deploy

The following pages will go in details about each one of the requirements. For each one, a discussion of the micro frontends requirements is presented when applicable.

**Small**

The idea of microservices architecture is that the application will be composed of small services. In order to get the most out of microservices, each service should be doing one task. Such focus is tied to the functional requirements of the business. With having each microservice handling only one task, developers can increase the chances of developing an application that respects other requirements of microservices, such as autonomous and reusable.

Each microservice is supposed to be small, the size of each service should be scaled down until it can’t be scaled anymore. Such approach will help to magnify the gains but also adds more overhead [1]. Once each service is very small then it can easily be replaced, isolated, updated or deleted while the rest of the system is still running. Moreover, the more services are divided, the more microservices the system will have. As a result, having many small dynamic parts in the system will make it harder to manage and could add extra complexity [1].

The size of each micro frontend is also supposed to be small, where the frontend will be decomposed into small apps and each app will handle a portion of it. For example, one micro frontend for the navigation bar, another for the footer, and more micro frontends will handle the body and other functionalities of the page.

**Autonomous**

Each service should have the possibility to get deployed independently. Such feature gives applications more flexibility. It’ll help to make the application more loosely coupled. Moreover, the isolation of each microservice is now easier and also important to make the whole system scalable [30].

Furthermore, each microservice is independent enough to allow developers to develop each microservice autonomously. This includes giving each team the freedom to choose which toolsets to be used for the development of this particular microservice. Such freedom helps developers to choose the most suitable tools based on the needs of each task.

This also applies to the micro frontends. Each micro frontend should be developed as an independent app. As a result, small teams of developers can be assigned small tasks instead of bigger teams. Which could lead into a faster development cycle for each app. While developers are free to choose the right tools for each task.

**Has an Interface**

Since the application consists of many small independent parts that work together. This means that each part of the system should provide some form of communication channels to other parts in order to be able to work with other parts and not to be isolated. Hence each microservice should provide an Application Programming Interface (API) that enables other microservices to talk to it and exchange data with it [33]. Such API will enable microservices to support the principle of encapsulation. Where each microservice will have the freedom to hide its internal implementation and expose only a channel of communication.

Furthermore, having each microservice offering an API will help to make the system adheres more to the principles of microservices. Hence allowing each microservice to be updated or changed without affecting the rest of the system as long as it keeps respecting the same style of the old API.

**Replicable**

When many modifications are required for one or more microservices, sometimes a redesign of the microservices or replacing them with new ones could be a better solution. The overall application must be designed in a way that gives developers the freedom to make changes for microservices. Each microservice must be developed in a way that makes replacing it with a new microservice a possibility anytime there is a need for such change. Furthermore, replacing one microservice with another microservice should be a seamless process where other microservices keep doing their usual routine when interacting with the new microservice.

**Respect Interface**

This requirement results from respecting the requirement of having each microservice as a replaceable entity. Since microservices only method of communication is through API then developers of the system should strive to keep each interface unchanged. After each update to the microservice or even after completely replacing an old microservice with a new one, the rest of the microservices should not be affected by changes concerning other microservices. When developers keep respecting the interface style of older or unmodified microservices then other microservices don’t have to change the way they make calls to those microservices. Hence, the application will keep functioning no matter what changes are made to the internals of each microservice.

In case a change of the interface is absolutely necessary, the influence of such change must be kept minimal [30].

**Reusable**

Each microservice should be designed to be as reusable as possible. Since each microservice is designed to handle one task in the application. And when the same task is needed in another application then reusing the microservice that handles this task in the second application should be possible [5].

Respecting this requirement leads to saving valuable resources such as time, money and efforts. While keeping the final application more loosely-coupled. Moreover, it could open the door to reusing the same microservices on different platforms. For example, after building a web application using microservices, the same services can be used to help power a mobile application. Since microservices will have an interface thus making it easy to communicate with each service as long as the communication respects the provided interface. Such feature will help developers release more combatable applications on different platform, faster than ever. As a result designing each microservice with reusability in mind helps in keeping the system more loosely-coupled where such microservices will not be dependent on other parts of the application.

Each micro frontend is an independent small application. hence, reusing micro frontends in different applications is possible. Developers should implement their micro frontend as reusable entities. Sometimes, few modifications to the styling are required to make the micro frontend more suitable with its new application.

### Requirements of Content trust

This section will discuss the requirements for a content trust mechanism that will be implemented to help microservices have an evaluation of trust among each other when making calls from one service to another.

Microservices themselves need to have clear rules about how to securely communicate with other microservices especially ones coming from different developers. This communication should allow microservices to make a judgment of whether to trust the other microservices or not.

Content trust has more dynamic nature than other types of trust such as authentication-based trust. While when performing an identity check the outcome could be one of two. Either the identity has been proven, or the identity failed to prove itself. But with content trust several characteristics, measures and aspects should be taken into account to come to a decision of trust or distrust. Those measures are inspired from content trust of web resources [17]. Moreover, this implementation is only concerned with having content trust between services in a microservice-based application.

Those measures differ in how hard it is to obtain the needed information. In order for microservices to be able to evaluate the content trust of one another, each microservice should be able to assess the following:

* The identity of a microservice
* Service sensitivity
* Number of interacting services
* Evaluation by other microservices
* Age of the microservice
* Last successful activity
* Deception

Content trust requirements of microservices are a combination of policy-based trust and reputation-based trust. Microservices have to make a decision of trusting other microservices based on evaluating several factors. There is a big margin of flexibility. Developers could implement a content trust mechanism based on their specific needs for a certain application.

**The identity of a microservice**

When an application starts using third-party microservices then there should be a need for verifying the identity of microservices. A system must be in place to help microservices verify each other and make sure that each microservice is what it claims to be.

A verification mechanism is implemented as a part of the content trust implementation. Each microservice must have the chance to verify the identity of any calling microservices. This verification helps in identifying each microservice and thus it helps microservice when evaluating the trust of each other.

**Service sensitivity**

The services provided by the different microservice will vary in nature. Hence the implementation of content trust should help microservices to know how sensitive the service of each microservice that makes a request to another microservice. Some services will offer simple service, while others will offer sensitive services. For example, some services could offer routing to help the user navigate from one page to another. while, other microservices would offer a login service to the user. The later service has a higher sensitivity than the other.

Microservices should be able to know how sensitive the service they are interacting with. This knowledge will help microservices to be more strict and demand a high level of trust when dealing with other microservices that handle important data. On the other hand, such knowledge will help microservices to be more tolerant in trusting other microservices that don’t have high trust but also don’t deal with important or sensitive data.

**Number of interacting services**

Each microservice should be able to know the following information about any microservice:

* Number of requests made to a specific microservice by other microservices
* Number of microservices that trusted a certain microservice enough to exchange data and handle a request successfully.
* Number of microservices that didn’t trust a certain microservice enough, and denied its requests.

All this information will help microservice when deciding to trust another microservice or not. Basically, a big number of successful interactions between any microservice and other microservice could play a role in increasing the trust in this microservice. On the other side, when there is a record of big number of denied requests from one microservice to other microservices then the trust of this microservice could be affected negatively.

**Evaluation by other microservices**

When a request is made from one microservice to another, both microservices should be able read the evaluation of trust given to each one of them by other microservices. This evaluation represents how much microservices trusted each one of the two involved microservices in their last interaction.

Such information helps the two involved microservices to evaluate their mutual trust. A good evaluation given to one microservice by other microservices will help in increasing the trust in this specific microservice, at this specific time. While, a negative evaluation by other microservices will harm the trust in this specific microservice at this specific time.

**Age of the microservice**

Microservice in the system might have different operation age, this difference come from the nature of the architecture of microservices itself. Microservices could be added gradually to the system. Hence some will be added in the early stages while other will be added at a later stage. Moreover, some microservices will be replaced by new microservices. And some new microservices will also be added to fulfill new requirements or fix a newly discovered bug. When making requests from one microservice to another, both microservices should be able to read the age of one another.

The age of microservices can play different roles depending on what the designers want. Some could consider the older a microservice is, the better, where the longer a microservice is operating the more trusted by the developers where it didn’t need to be replaced. On the other hand, some could consider the older a microservice is, the worse. Where newer microservice are more up-to-date and could be using better technologies.

**Last successful activity**

Each microservice should be able to show the last time it engaged successfully in a request. This information shows that the concerned microservice is active. A microservice that was not being used for long time raises more suspicious. As a result, such long period of inactivity from accomplishing a task would have a negative effect on the trust evaluation by other microservices.

**Deception**

Each microservice should be able to check if there are any records of deceptions attempts made by a certain microservice. For example, a microservice sending queries instead of the requested data in an attempt to, illegally, fetch data from a database. Such incident, if discovered, should be documented. The involved microservices should be identified.

When a microservice is trying to evaluate its trust of another microservice, it will also check to see if the concerned microservice has any deception record. In case such record exists then the trust would be affected negatively.

### Requirements of Developers and Users

Developers are the person or the group of people who are creating the application. From their point of view when trying to handle content trust between microservices, there can be two cases:

* All microservices are developed in-house
* Some microservices are developed by a third-party

When having all the microservices as an internal product, something developed by the same company, then trusting microservice is not as important. The reason for this is that when developers develop a microservice they’ll be able to trust it directly. They will be sure that no hidden intentions are implemented or any harmful script is intentionally in place. Furthermore, some concerns should be taken into consideration if in the future some microservices will be introduced from a third-party.

On the other hand, when some microservices are developed by a third-party, then developers must make sure that microservices of both sides will be able to communicate with each other to evaluate and build their trust. Developers should be able to adapt any third-party microservices. In such a way that makes it able to provide the requested information. Such information as identity verification, age of operation, the type of service provided, and so on. This information will help microservices to make a decision of whether they should trust a certain microservice or not. Failing to do so while having a content trust implementation could create many problems.

Furthermore, content trust requirements for the end-users of the application are outside the scope of this thesis, since the focus is on content trust between microservices. Hence content trust requirements for the end-users of a web application will not be discussed.

## Literature Review

This section presents a literature review for microservices as well as trust in computer system.

### Microservices and Micro frontends literature review

Micro frontends architecture is a new concept. Not many resources are available about it and not much discussion in the literature so far. Nevertheless, some re-sources online have discussed it and the following lines will present definitions and discussions about micro frontends.

Micro frontends are similar to microservices; the difference is that microservices are applied to the backend part of the system while micro frontends are applied to the frontend of the system. Many of the same concept of microservices can be applied to the frontend of an application and that would result in micro frontends. As explained in [42], micro frontends are independent components. It goes on to explain that the system can be split into parts and each part could have its micro frontend, a microservice, and maybe a database. [42].

While [44] argues that Instead of writing the application as a monolithic one, it can be divided into small parts. Moreover, [45] agrees with [42] [43] where it mentions that, micro frontends is the concept of microservices applied to the frontend. Furthermore, [45] presents an important feature of micro frontends which is developing each part using the right technology, where developers can use different toolsets for different micro frontends depending on the need of each frontend.

On the other hand, microservices architecture as defined in ([30], p. 4) is a way to develop an application that’s composed of a group of small independent services. Similar definition is given in [33] where it says: “Microservices is an architecture style, in which large complex software applications are composed of one or more services”. Furthermore, microservices are also referred to as small independent services that work together [1]. The definition given in ([5], p. 16) also agrees with the above mentioned definitions, it states: “Microservices are relatively small, autonomous services that work collaboratively together”. Writers in [32] go on explaining that microservices is a product of Service Oriented architecture (SOA). The same is also mentioned in [31]

The size of each microservice has also gained a considerable amount of attention when discussing microservices. Each microservice should get as small as possible [1]. While [5] mentions that each microservice must implement only one business requirement. And it’s been argued that no rules have been given to how small each service should be. [33] Also agrees with [5] where each microservice should try to represent one business functionality.

Moreover, how small each service is can be different from one system to another. [1] suggests that counting how many lines of code each service is, should give developers a good measure on how big each microservice is. Furthermore, counting the number of days each service takes to be developed is also another measure. In [1] it is advised that each microservice should not take more than two weeks to be developed. According to [29] services should be small, it uses the name of the architecture to indicate that each microservice should be small as the word “micro” suggests. Just like other researchers [32] describes applications built with microservices architecture as a composition of small services. While [33] Mentions that each microservice should only be concerned with implementing one task.

The literature also discuss how microservices should communicate between each other. At first it is mentioned in the definition of microservices architecture, that microservices collaborate with each other [1] [5]. This implies that microservices should find a method or mechanism to turn such collaboration into an actual exchange of data. Both [31] and [33] mention that each microservice should implement APIs where microservices can use these APIs to exchange data. It is also mentioned that microservices only communicate with each other using network calls [1]. Researchers in [30] agree that microservices should implement API that helps services to communicate with each other. However, [29] Doesn’t go in details about how each microservice can communicate with other microservices, it only mentions that communication between microservices is a distributed one.

The characteristics of microservices are also discussed by many writers. Many of them agree that each service should be small as in [1] [5] [29] [31] [32] [33]. The same agreement happens when talking about the independence of each microservice. For example, regarding the independence of each microservice [30] explains that each microservice operate in its own process. The same thought is mentioned in [1] and [31] where both of them mention the word autonomous to describe the independence of each microservice. In ([31], p. 3) “Each service is fully autonomous”. While ([1], p. 16) says: “Microservices are small, autonomous services”. Same with ([5], p. 16) where the word “autonomous” is also mentioned, it is stated: “Microservices are relatively small, autonomous services”. Also [33] agree that microservices should be independent from each other.

The relationships and the effects each microservice has on other microservices is also discussed. [31] Mentions that when changing the implementation of a microservice other microservices should not be affected. Researchers in [33] Agree that microservices should not affect each other, the term “loosely coupled” ([33], p. 4) is mentioned to describe the nature of the relationship between microservices. The word “isolation” is mentioned in ([1], p. 18) to describe how microservices should not affect each other when changes happen. On the other hand, such isolation could introduce “overhead” ([1], p. 18). The write goes on and describe that microservices should be able to change independently from each other. Researchers in ([5], p. 17) agree with the concept of having microservices independent from each other, they say: “Loose coupling is critical to a microservices-based system”.

Furthermore, [29] suggest that microservices are supposed to be easily-replaced components. The same is suggested in [1] where microservices should have the possibility of being isolated from the rest of the system or even getting re-placed completely. Such replacement and changes should not create complications for the system.

Moreover, the term “bounded context” has been mentioned in ([33], p. 4). It explains it as microservices doesn’t need to know anything about how each microservice was developed. A similar idea is also mentioned by other researchers. [30] Mentions that microservices can communicate using their API and the way each microservice is implemented should not have an impact on the communication. Furthermore, they explain that this property gives more freedom to developers to use different tools for different microservice. This same concept is explained in [1] where the write states that such freedom in choosing different tools for different microservices could help developers in choosing the right tool for the right task.

Many researchers also agree that if one service fails, the system should still be able to operate normally [1] [29] [32]. Moreover, since microservices support the promise of loosely coupling, at the times of failures, the failed service can be isolated and fixed while the rest of the system is still operating [1] [30].

### Microservices vs monolithic

This section will give a comparison overview of microservices vs monolithic architecture in literature. The comparison will focus on the following:

* Size
* Scalability
* Loose coupling
* Maintainability

**Size**

Microservices architecture is composed of different services each service is collaborating with the one or more other services. This whole dynamic will come together to form the final system. One of the key characteristics of microservices architecture is the size of each service. Almost every paper suggests that the size of the service should be relatively small [1][5] [29] [34]. Even some researchers suggested counting lines of code as a measure to decide on the size of the service [29]. While many other researchers suggested that each service should be concerned in handling one task [33]. This task should be derived from the business requirements.

Such small service size helps managers to assign a small team of developers to each service hence making the development faster and more efficient. Moreover, each team can decide to use different tools for different services, depending on which toolset is the best for each service.

On the other hand, monolithic applications are divided into three layers: Backend, logic layer and frontend [34]. Each layer is covering many functionalities of the system. Hence the size of each layer could end up getting bigger and bigger with more business requirements. Furthermore, assigning small team of developers will be harder and each team needs to collaborate with other teams during the development. Moreover, usually, teams don’t have the freedom of choosing their own toolsets for development. They are bounded to what other teams are using and whether their toolset is compatible with the rest or not.

**Scalability**

Applications based on microservices have the chance to grow when there is a need for new features in the application. Adding such new features means adding new services to the system. And adding new services to the system is usually an easy task.

On the other hand, at some point monolithic applications grow to the point where they are hard to scale. The codebase becomes very big and complicated and each additions of new features require a good amount of work to allow the application to accept the new features.

In the book The Art of Scalability [35] the scale cube is introduced. It can be seen in figure 2.1. The Scale Cube has 3 axes: X-axis, Y-axis, and Z-axis [35]

* Horizontal Duplication and Cloning (X-Axis)
* Functional Decomposition and Segmentation (Y-Axis)
* Horizontal Data Partitioning - Shards (Z-Axis)

Commonly, monolithic-based application can scale only on one axis, that’s (X-Axis). On the other hand, a microservice-based application has the ability to scale over all three axes [36].



Figure ‎2.1 Scale Cube [35]

**Loose coupling**

One of the important characteristics of microservices architecture is that services should be isolated from each other [33]. The connection between services is only achieved via a well-defined interface. And each service can be modified as long as it is still respecting its interface. Hence making the application components loosely coupled. On the other hand, monolithic applications developers have to take extra measures to make sure that the parts of their applications don’t overlap which costs them more time and work. The importance of loose coupling is stated clearly in [5] as “Loose coupling is critical to a microservices-based system”.

**Maintainability**

Since microservices are independent entities, then isolating each service in case of a failure is possible while the rest of the system continues operating [1]. However, the same can’t be true for monolithic-based applications and in worst cases one failure in the system could cascade to stop the whole system from operating [1].

In [34] researchers use different points to compare monolithic-based applications to microservices-based application. Table 2.1 presents the comparison. They conclude that both architecture styles have positive and negative points. In general, micro-service architecture is more suitable for projects with big codebase. But once the project is small building it with microservices architecture could bring an additional overhead [34].

|  |  |  |
| --- | --- | --- |
| **Category** | **Monolith** | **Microservices** |
| **Time to market** | Fast in the beginning, slower  Later as codebase grows. | Slower in the beginning because  of the technical challenges that microservices have. Faster later |
| **Refactoring** | Hard to do, as changes can affect multiple places. | Easier and safe because changes are contained inside the microservice. |
| **Deployment** | The whole monolith has to be deployed always. | Can be deployed in small parts, only one service at a time. |
| **Coding language** | Hard to change. As codebase is large. Requires big rewriting. | Language and tools can be selected per service. Services are small so changing is easy. |
| **Scaling** | Scaling means deploying the whole monolith. | Scaling can be done per service. |
| **DevOps skills** | Doesn’t require much as the number of technologies is limited. | Multiple different technologies a lot of DevOps skills required. |
| **Understandability** | Hard to understand as complexity is high. A lot of moving parts. | Easy to understand as codebase  is strictly modular and services use SRP. |
| **Performance** | No communicational overhead.  Technology stack might not support performance. | Communication adds overhead.  Possible performance gains because of technology choices |

Table ‎2.1: Comparing monolithic and microservices [34]

### Trust literature review

This part of the thesis tries to present a literature review of trust and the different approaches used when adopting trust in software development. First, a definition of trust is illustrated, to give the reader a broader understanding of trust and its use in the literature. The next step is presenting the different techniques of trust as used by researchers and software developers.

**Definition of trust**

The word trust has been a subject of many studies, many researchers tried to form a definition of trust and what it means. The reason for this is because trust plays an important part of people’s life and is involved in many scientific fields such as philosophy, psychology, economy and recently in computer science. In his famous PhD thesis Marsh [9] mentions that many efforts have been spent trying to discuss trust and putting a definition to it, especially in the second half of the last century. His research was an attempt to create a model that can offer a mathematical way to measure trust.

In ([6], p. 3) concludes that there’s no one agreed upon definition of trust, “little consensus has formed on what trust means”. In his research, he agrees with [9] that many discussions have been written about trust. Furthermore, he adds that different definitions of trust are used in the literature,” significantly diverse definitions of trust continue to be used in the interdisciplinary research literature. On the other hand, researchers in [18] try to give a definition or an explanation of how trust can be evaluated. Their idea is that the trust between two parties is a variable with many dependencies.

In [6] a distinguishes between six types of trust is made. While [18] makes a distinction between two types of trust, those are execution trust and code trust. Execution trust is explained as that the provider of the service will allocate the required resources for the execution correctly. On the other hand, code trust is where the side that is consuming the service will be making a request that is free from any harmful scripts.

Moreover [18] gives other distinctions for the trust, they explain this as trust could have other types. This extended distinction of trust types is composed of seven types of trust. Namely: Direct trust, indirect trust, full trust, partial trust, recommended trust, authentication trust and finally privacy trust.

The first type of trust defined in [6] is the Trusting Intention. This type of trust means that one is able to depend on others. [6] Argues that this type of trust is different from one situation to another. On the contrary to this definition, [10] thinks that this type of trust is not a situation specific.

The second type of trust is the “trusting behavior” [6]. The definition for trusting behavior is also given in [11] where it is explained as a voluntarily dependence from one person to another. This dependence is situation-specific where negative consequences could happen.

while [6] Goes further and tries to de-compose trusting behaviour into different sub construct forms. Namely are: cooperation, information sharing, informal agreements, decreasing controls, accepting influence, granting autonomy, and transacting business. Researchers in [12] studied the trusting behavior in their work, named: “Belief in others’ trustworthiness and trusing behavior”. They show that many factors play a role in the trusting behavior, and it is not just about gaining as much as possible.

The third type of trust in ([6], p. 33) is “trusting Beliefs”. The given explanation is “the extent to which one believes (and feels confident in believing) that the other person is trustworthy in the situation”. Other researches have also studied trusting beliefs, for example [13]. In their explanation they give an example of a vendor-consumer relationship.

Trusting beliefs is also used as one of the conceptual definitions of trust in [7]. Besides trusting beliefs, two more definitions are given: Disposition to Trust and Institution-based Trust.

In [37] a discussion about the importance of perceived information and its consequences. When low-quality information is provided but such information where not of a big importance then the consequences of such false information is relatively low. However, when the nature provided low-quality information has high importance then the negative consequences of trusting this information could be high.

Moving on to the fourth type of trust that was distinguished by ([6], p. 36), this type is called system trust. It is explained as “means the extent to which one believes that proper impersonal structures are in place to enable one to anticipate a successful future endeavour”. Researchers in ([14], p. 197) give an example of system trust, they use ecommerce system as such example. They concluded that system trust has an impact on the intentions of customers to decide whether to buy or not, “system trust plays an important role in the nomological network by directly affecting trust in vendors and indirectly affecting attitudes and intentions to purchase.”

Dispositional trust is the fifth type of trust in ([6], p. 38) explained as “if one believes that others are generally trustworthy (Belief-in-People), then one will have Trusting Beliefs (which in turn lead to Trusting Intention).” Dispositional trust is also noted in [15], in his research about situational uncertainty, he concludes that dispositional trust can foresee trusting phenomenon.

Lastly, the sixth type of trust according to ([6], p. 38) is the situational decision to trust. Explained as “the extent to which one intends to depend on a non-specific other party in a given situation “. Although it is recognized as a different type of trust, but it doesn’t exhibit much difference from the first type of trust which is Trusting Intention.

In his paper about the concept of trust, ([8], p. 55) defines trust as “Trust as a ‘leap of faith’ or willingness to be vulnerable”. He argues that trust is a tool learnt at as earl age as infancy. Where people use this tool to approach uncertain situations “trust is learned in infancy and enables the individual to deal with the unknowable in the social con-text”. In his explanation for the term ‘leap of faith’ he presents this term as an important part of the trust where it “involves the trustor experiencing a lack of expertise in a particular area of their life and acknowledging that the expertise they re-quire to address this lack is held by another individual or system. They either consciously “

However, another definition of trust is also presented in ([8], p. 57) trust is seen as a “social capital” writer argues about the role trust plays for individuals in society and hence the role each individual plays in the society.

Lastly ([8], p. 59) also presents trust as a part in the “power-knowledge” theory where knowledge leads to power and trust is an important component to acquire knowledge.

As can be seen that there’s no one definition of trust in the literature and many re-searchers have come to conclude different means and concepts of trust. Some have given examples from the real world such as [14] where he talks about trusting a sys-tem. The same concept of trust is agreed upon by [6] where he gives an example of trust in a system of doing a purchase via the credit card. Where both the buyer and the seller trust the system. In case the system rejects the credit card of the buyer, both parties will not have less trust of the system but the seller will only be suspecting the buyer and most likely never the system.

**Authentication and Authorization**

Authentication and authorization are important for the trust. When a service is able to identify itself to other services, it helps to add points to the overall evaluation of the trust. Authorization will help to have the requestor gains access to the resources such as data. In ([18], p. 85) a definition of authorization is given as “deals with issues like who can access which resources/services under which conditions”. Hence once a microservice is authorized, it will be able to make requests to other microservices and exchange data with them.

An explanation for an authorization system is given in ([18], p. 86) by describing it as a sys-tem that provides access rights. They explain “An authorization system can be defined as a system that grants specific type of access to specific requesters based on their authentication”

Furthermore, ([19], p. 33) Describe authentication as “allows identity verification of any entity.” Moreover, the authentication of users as “the basic feature of protecting data from computer system intruders”. Wallace ([20], p. 2) agrees to this definition, he states an authentication protocol as “its purpose is to authenticate entities wishing to communicate securely. “

Importance of authentication is described by ([21], p. 21) as a very important aspect of computer systems security, they mention “authentication in computer systems has been a cornerstone of computer security for decades” such statement shows without doubt the importance of authentication in computer system and applications and agrees with the rest of the researchers about its importance and role. Researcher in [20] continues to present the importance of authentication by stating that it is the very first step a requestor has to take before it is granted further access.

Furthermore, [21] tries to give a simple example of what an authentication process could look like. Their example uses the ID of a user for achieving an identity verification. They say: “In the basic authentication process, the entity desiring authentication presents credentials, usually an account ID and some additional information, to prove that the request is coming from a legitimate owner of the ID”. [19] Shows the importance of authentication as it is the proceeding step before authorization “Authentication is critical for sending our data over the internet, as well as for ensuring that authorizing is done properly allowing access to systems and services.” Writers in [21] agree with [19] to the importance of verification where “Identifying a user is essential for the application of security in the form of permissions to various objects, processes and access to resources”

In the book “Information Security: Principles and Practices” [22] enclose the goals of security in three point: “All information security measures try to address at least one of three goals” those points are stated to be “Protect the confidentiality of data, pre-serve the integrity of data, promote the availability of data for authorized use”. On the other l [19] states similar points as the task of authentication and authorization. They state that “Authentication and authorization is implemented to ensure confidentiality, integrity, availability, authenticity, and accountability.”

An indication to the importance of identity check in computer system is made in [20]. It explains that having identity verification helps in making the system more secure against attacks. “Validating users before allowing them access is an easy way to catch an intruder from stepping into boundaries that they shouldn't cross”.

Moving on, [19] continues to explain how authentication is achieved. Where they explain that “Authenticating users is carried out by the series of identification and verification stages. At the identification stage, access to a security system is defined, and the binding between an entity and an identifier is done during the verification step.”

From the definitions and explanations given by different researchers, it is clear that authentication is an important step in giving access rights to a requestor that’s trying to access one or more resources.

On the other hand, ([21], p. 1) tries to provide a more practical view on authentication by presenting a simple mechanism which uses a combination of a username and a password. They state “The concept of a user id and password is a cost effective and efficient method of maintaining a shared secret between a user and a computer sys-tem”. It moves on explaining that many computer systems use the simple known identification method. This method is composed of a username and a password, “Many modern systems have adopted a simple id/password method of achieving the goals associated with the identification and authentication function”. The same thing that [19] agree upon. It is also explained that despite all the advances that took place in both hardware and software, the combination of username and password is still the most dominant way of verification in computer systems. Saying: “Even with the adoption of new technologies in hardware and software, password authentication is still not completely replaced by the existing alternative authentication methods.” ([19], p. 33)

On the other hand, ([18], p. 86) gives more in depth definition of an authentication and authorization system. They define each entity in the process from the requestor to the requestee including the resources and the action to be taken upon these resources. They describe the requestor as “Subject is an entity that wants to access services/resources. It can be a user, a service or any other entity on behalf of user/service”. And then move on to describe the service by explaining that “Service is a piece of software that provides some functionality and can be accessed by Subjects or other Services”.

After that, [18] have described the requestor and the service they continue by giving a definition to the resource that’s being requested. They say: “Resource is an object that is accessed by Subjects. It can be a CPU, a storage device, software, data” ([18], p. 86).

Another interesting definition is about the requirements given by each service in order to be accessed. This is called Service Policy, explained as “Service Policy refers to the set of rules/requirements associated with the Service. A Subject must conform to Service Policy in order to Access that Service” ([18], p. 86). Furthermore, the access that’s granted to reach the requested service is also explained. Where “Access is an operation that a Subject performs on Service/Resource. The access is provided based on conformance to Service Policy that is associated with that Service/Resource. Hence it can be clearly seen by definitions in [18] that access to the service is not granted unless the service policy of the service is respected. While Policy itself is also described in [18] as “a set of rules/requirements” ([18], p. 86). Where this set of rules can be linked to the Subject, the Service or even the Domain according to [18].

**Reputation based trust**

Reputation based trust started as a review made by users for others, one of the earliest examples of it was adopted by eBay. As ([23], p. 1) refers “Reputation systems are already being used in successful commercial online applications”. A similar idea is referred to in [28], it says: “Reputation-based trust systems were mainly used in electronic markets, as a way of assessing the participants” ([28], p. 1).

However, trust has been divided into two distinctions one as “strong and crisp” while the other as “soft and social” according to [24]. The “soft and social” is concerned with reputation based trust. “reputation-based trust relies on a ‘soft computational’ approach “([24], p. 1). In this case, trust is computed from two sources: First based on own experience, second based on experiences of others as referred to by [24]. Moreover, trust depends on other factors such as the time and the settings [26].

The same concept for computing trust is used in [25], it agrees that reputation-based trust is computed from two sources. It says: “Reputation information is divided into two categories: First-hand experiences are gained from the trustor monitoring the outcomes of actions it has engaged in itself, and are generally considered to be error-free within the limits of observed- ability. External experiences are gained from third-party recommenders based on their own first-hand experiences” ([25], p. 2).

On the other hand, in [26] uses the term “behavioral trust” instead of “reputation trust”. It is defined as realizing the expectation of others. And it is classified into two categories: Direct trust and indirect trust. Where direct trust means the experiences gain from own direct interaction. While indirect trust means the experiences of other’s interactions. It is obvious that [26] agrees with [25] where it uses first-hand experiences and external-experiences instead of direct trust and indirect trust. In both definition, the resulted trust is variable and never constant, where its value changes after each interaction. While in policy-based trust the resulting decision is either positive or negative [24]. Where such trust depends on well-defined measures such as certificates and is referred to as “strong security” [24].

Also [27] agrees with the mentioned studies, it states that “reputation serves as the basis for trust”. Hence giving an important value for the experiences of other entities in the system.

A distinction between entity trust and content trust is given in [17]. Entity trust is given as an evaluation of an entity based on its ID and behavior. While content trust is defined as “A trust judgment on a particular piece of information in a given context “([17], p. 228). Both types of trust are related to each other’s.

Whether someone trusts some resource online is a personal matter that differs from one person to another. Where each person makes their judgment based on many influences that are affected by personal experiences. [17] mentions that some resources might be preferred to some people over other resources based on the context in which the resources are being judged. The context in which a resource is evaluated is argued more, an example of travel information is given where students may use different source for information than families. The date of which resources are consumed also has a value as stated in [17].

Moreover, [17] identifies 19 factors that influence content trust:

|  |  |
| --- | --- |
| * Topic | * Incentive |
| * Context and Criticality | * Limited resources |
| * Popularity | * Agreement |
| * Authority | * Specificity |
| * Direct experience | * Likelihood |
| * Recommendation | * Age |
| * Related resources | * Appearance |
| * Provenance | * Deception |
| * User expertise | * Recency |
| * Bias |  |

Furthermore, [17] explains that some of the factors are related. And some others can be grouped together such as Direct experience and Recommendation under reputation. In addition, [17] acknowledges that determining which of these factors can be used is not an easy task.

## Analysis

This section provides an analysis of the content trust as well as microservices architecture in regards to the requirements that were presented in the first section of this chapter. Those requirements will be analyzed against the presented literature review in the second section of this chapter. The analysis will be discussed under two titles:

* Microservices
* Content trust

Besides going through the previously presented literature review, the following pages will also compare the presented requirements against some well-known implementations of microservices as well as content trust.

### Microservices analysis

The following pages provide analysis for the literature review of microservices while comparing it to the requirements of microservices, mentioned in the first section of this chapter.

Microservice-based applications can be built using either one of two architecture styles, that’s is orchestration and choreography [41]. In orchestration, the work flow between services is managed centrally. One or more service is directing the calls to their intended destination. Hence, the application has a central part to manage the traffic and help services communicate with each other. On the other hand, services in an application based on the, choreography style should handle any calls by them-selves. They should identify the destination service whether its address or the type of service it offers. Unlike orchestration, choreography offers more loosely-coupled architecture since no centralization [41]. As a result, an application could benefit the most of microservice architecture.

According to the requirements, services are supposed to be small. When one tries to have an abstract understanding of the name microservices. The word micro reflects the size of the service. The size of the service was discussed heavily in the literature [1] [3] [5]. Some writers tried to introduce ways to measure how small each service should be. Others were pointing out that the decomposition of tasks should be ac-cording business requirements and each service should be handling only one task [5] [33].

Each microservice is supposed to be independent, can be deployed independently and can be changed without affecting other services. Such requirement was also dis-cussed in the literature. In the definition given in [1] it is clearly stated that micro-services should be autonomous. Writes in [31] [33] also emphasis that in order to get the most out of microservices architecture, services should be made as independent as possible. However, having services as independent entities, doesn’t mean that service can’t interact together. On the contrary as mentioned in the definition in [1] services are supposed to collaborate together. In order to keep services independent but at the same time having the chance to work together when needed, each micro-service should provide an interface. Writers in [1] [5] [29] [33] agree that micro-services should have interfaces to help other services interact with them. While at the same time giving each service a great deal of independence.

Since each microservice has a well-defined interface [1][5], then replacing one service with another is possible as long as the interface for the new service is the same as the old one. Moreover, reusing one or more microservices in other application is easier. One of the requirements of microservices is having the services as reusable entities. In [1] and [29] writers point out that microservices should be designed in a way that makes it easy to be used by more than one application. If the new application can adhere to the service interface then no changes are needed, and the service can be used easily.

The previous points bring the discussion to some of the features that can be gained from respecting the requirements of microservices architecture.

A microservice-based application will be more resilient than a traditional three-layered application. The system has a better ability to handle failures., in such a way that the rest of the system will keep working and only the failed parts will stop. Moreover, the failed parts can be isolated easily to be fixed or replaced. This was also mentioned in [1] [31]. Moreover, in [33] it is stated that each microservice should be encapsulated. Microservices don’t need to know anything about how each service is implemented. All what microservices need to know is how to communicate with the target microservice. This gives developers more freedom in how to implement each service, or even how to update or modify the implementation of an existing service. As long as the interface of the service is respected, other services will still be able to communicate with it. Hence the system will continue to function despite the updates and modifications.

Microservices architecture was developed to overcome the shortcoming of three-layered architecture. One of these shortcoming appears more clearly the more the project gets bigger. At some point adding more features to the application will be a difficult task [34]. An application could require huge modifications in order to accommodate new features. On the other hand, microservice-based applications are supposed to be scalable [5] [30]. where the system will be able to accommodate new services with ease.

Microservice-based applications have great flexibility in adding new features to the system. Developers can offer continuous delivery in a way that they can easily keep adding new services to the system without the need to release new versions with each newly added feature. In [1] as well as in [34], easy deployment of micro-services-based applications was discussed. In [34] a comparison was made between microservices and monolithic architecture where deployment was one of the com-pared points.

### Content trust analysis

Different definitions of trust were presented by different researchers. Where some of the definitions intersect with one or more of the provided requirements of content trust. One definition for trust distinguish between direct trust and indirect trust. Direct trust is established after own direct interaction with other entities. While indirect trust information is gathered from other entities experiences with the entity in concern. This definition can be seen in at least one of the requirements of content trust. Microservices will have their own evaluation of trust once they interact with a certain microservice. And also will be depending on the evaluation of other micro-services for the concerned microservice.

After each interaction, the trust they already have about the other microservice could be affected positively or negatively. Moreover, their new evaluation of trust could also play a role in how other microservices evaluate their trust with the concerned microservice. This is perceived from the indirect interaction, hence the indirect trust.

One of the widely cited study about trust [6] mentioned “trust leads to cooperation” this understanding is also exhibited in the requirements of content trust. The point of adopting content trust in microservices is to make collaborating microservices trust each other and exchange data safely. In such scenario, having high evolution of con-tent trust among microservices will lead to more exchanged data and cooperation.

Trusting the behavior of others was also mentioned by some researchers [6, 11]. One definition is presented as “Belief in others’ trustworthiness” this definition is reflected in the evaluation of trust each microservice will have. Believe is reflected as a dynamic value that can grow or shrink depending on the how positive or negative each interaction is.

The relationship among services is present in more than one requirement. On the other hand, the relationships among collaborating entities was mentioned by differ-ent researchers. Such collaboration between concerned entities is mentioned in the sixth definitions of trust presented in [6] as well as in [15].

The age of microservices is taken into account when deciding about the content trust of a microservice. It is mentioned as one of the requirements of the content trust implementation. However, the age doesn’t have much influence on any description provided for the trust or any of its contrasts or sub definitions. Yet the age is mentioned specifically in [17]. It is stated that the age of the content could play a role in helping the readers of the content on deciding whether the content is trustworthy or not.

The sensitivity of the service is also presented in the requirements of the content trust. In [37] the importance of the provided information is discussed. In the requirements of content trust, the sensitivity of the service can be projected into the importance of information presented in [37]. In such case when there’s a trust among microservices that are exchanging sensitive information, but the information where not of high degree of integrity. Then as indicated in [37] the consequences could be more serious, than if the exchanged information where of low importance.

The identity of a microservice has a weight in deciding of trusting a microservice or not. In the requirements of microservices, each microservice should be able to authenticate itself to other microservices. Failing to authenticate itself, could result in having a decreased evolution of the service by one or more other services. In [21] a model for verifying the identity of a requestor is presented as a combination of User ID and a Password. Such combination is also used by other researchers [19]. In the case of microservices, proving each service what it claims to be is important as it establish a first level of trust. Such ground could be used to move on and try to establish other forms of trust. Having the identity of the service verified will help in in-creasing the evaluation of it by one or more services positively.

Regarding the implementation of content trust. The most common one is used by Docker and it is called Docker content trust. Docker is basically a container for pro-cesses. One can think of it as a virtual machine but much lightweight and faster to boot. This lightweight virtual machine is called a container and one host can have more than one container running at the same time and sharing the host resources. Docker containers are actually used widely to deploy services for applications built on the microservice architecture. Docker content trust is used to help in trusting the images of the containers released by software providers. According to the official documentation [38], the point of Docker content trust is to ensure the integrity of Docker images and also verify the identity of the publishers of the image. This explanation only satisfies a portion of the requirements of content trust presented in the first section of this chapter. But it doesn’t go any further, for example: users of Docker images can’t provide an evaluation of their experience after using a specific image. Hence other users can’t use such information in helping them to decide of whether it is reasonable to put one’s trust in a specific image or not.

To conclude this chapter, an application based on microservices could be described as a big piece made of many small blocks, each block is an independent reusable entity. It can be reused to develop other applications. While content trust will add a trust layer between the small blocks. An implementation of content trust could be helpful once the blocks of the application is developed by different sources. Hence it will be a mechanism that helps each service to trust other services. This process is done automatically, without a human intervention.

Next chapter in this thesis will discuss the concept behind building the Blog. It will give an overview of how, micro frontends, microservices, and content trust implementation can all work together to produce a more secure, flexible and robust system.

# Concept

Microservices architecture helps developers create loosely-coupled applications. Although each small service is collaborating with other services but the collaboration happens under well-defined interfaces. Each service offers an interface that helps other services make a request to it and receives a response. So designing an application that’s loosely coupled is easier for developers and becomes more of a default behaviour.

Such loose coupling helps developers isolate any problems appear in the application after delivery. This isolation will only affect the service that host the problems and any other services that want to interact with this service. In other cases, the isolation of the problem could not affect the system at all when other services are providing the same functionality as the isolated ones. Developers could create more than one service to handle each task. When a service is isolated, the other services that perform the same task can handle the coming requests. In this case the system will continue to function as usual while the problem is being fixed.

Moreover, continuous deliver is much smoother under microservices architecture, developers don’t need to release a new version for each change they make. They can simply replace one service by a new one and the system will continue to run as usual.

This chapter will be composed of four sections. The first one will discuss the concept of micro frontends and how the frontend of a web application can be divided into small parts. The second section will focus on the concept of microservices and how services interact with each other. While the third section will discuss the content trust that will help microservices evaluate how much they trust each other before carrying on with their exchange of data. Finally, the last section will show how the three parts can work together in the final system.

## Concept of micro frontends

Micro frontends are a sum of small frontends that together form the final page that’s presented to the end-user. The concept behind micro frontends is derived from microservices [50]. Essentially, when applying the principles of microservices to the frontend of a web application the result would be micro frontends. As a result, micro frontends share many of the principles with microservices.

Nevertheless, micro frontends impose few more challenges that don’t exist in microservices. Such challenges include:

* Routing: frameworks such as ReactJS or Vue.js provide tools that help developers write applications that makes navigation from one page to another smooth and easy. When several applications are put together to form the final rendered page. The routing tools of each framework will not have access to the path of parent or overall page. Hence, navigating from one page to another from within a micro frontend is a challenge.
* Data exchanging: When micro frontends are delivered to the browser, they don’t have a default communication channel that help the apps to exchange data. The solution for this challenge depends on how micro frontends are stitched together, and what technologies are used to render the micro frontends in the browser.
* Styling: Micro frontends might face naming conflicts when each micro frontend has its own CSS files. If different micro frontends have the same set of HTML classes, then unwanted styling from one micro frontend might be applied to elements in another micro frontend.
* Events answering: micro frontends should be able to answer events that happens in other micro frontends. For instance, when the final application consists of a navigation micro frontend and some other micro frontends. If the user clicks on a link in the navigation app, a response should be delivered from another micro frontend where the user could be navigating from one page to another. In this case, other apps should be listening to events coming from the navigation app and act accordingly when they are meant to.

Next chapter in this thesis will try to find answers for the mentioned challenges and suggests alternative solutions when it is applicable. Moreover, a solution will be provided to putting all the micro frontends together and make them operate in harmony.

Two micro frontends will be rendered to the user at any given time. While the rest of the micro frontends will be rendered depending on the events happening in those two micro frontends. The idea is that, the functionalities of the frontend will be divided into tasks and each task will be handled by one micro frontend. For example, the navigation bar will be handled by one micro frontend, while the main area in the screen or the body of the frontend will be handled by another app. Yet, more than one app will be rendered to this area. The apps will be called to be rendered to the main area depending on the events coming from the end-user of the Blog. Those events will be applied to the navigation bar and the main area in the frontend.

## Concept of microservices

The Blog will have two parts, a frontend and a backend. The frontend will be composed of micro frontends, while the backend will include microservices. Some of the microservices will have access to one or more databases while others don’t need such access. Between the microservices a mechanism of content trust will resides.

The Blog will have microservices handling the following tasks.

* Creating users accounts
* Login operations
* Submitting emails to the admins
* Handling posts related requests
* Handling comments related requests.

There will also be services to handle other tasks such as:

* Protecting the Blog from invalid user’s input
* Protecting the Blog from Duplicated posts, comments or messages

Moreover, there will be microservices that will help other microservices by providing them with inputs. Such inputs could be reading certain values from the database, or processing data before submitting it to the responsible microservice.

The Blog will be simple in terms of functionality; it will offer the following services to its clients:

* Reading posts available in the Blog
* Commenting on posts
* Sending messages to the admins of the Blog
* Creating new user’s accounts
* Logging in with the created accounts
* Submitting new posts to the Blog
* Modifying, and deleting own submitted posts

Keeping the Blog simple, will help to focus on the implementation of the microservices, the content trust mechanism between the microservices, and the frontend. The frontend will be composed of many micro frontends. One could describe the Blog as a full-stack microservices application. Both, the frontend and the Backend uses the principles of microservices architecture to deliver the final product.

The services in the Blog will have certain features that make them suitable to be used in a microservice-based application. Such services adhere to the requirements mentioned in the second chapter. The services will be:

* Small
* Independent
* Has an interface
* Reusable

Each service in the Blog should have a small size where it handles one task. For example, one service would handle requests related to storing a new post, retrieve a post from the database or delete a post. Another service would handle clients logins, while a third service handles creating new accounts for new clients.

The reason for making services small is to be able to get the most possible benefits from using microservices architecture. When services are small, it becomes easy to replace them with new services, or isolate a service when it is not running correctly. Also it helps to make the system more scalable since adding new features means adding more small services to the Blog. This would be easier than adding a big service that handles many tasks and have to communicate with many other services.

Although microservices will be designed to be small but they will not be designed to be too small. For example, the Blog will have one or more microservices handling tasks related to posts such as making a new post, reading posts, deleting own posts...etc. Such microservice could be further divided where one microservice will handle creating a new post, another service handles reading a post, and so on. While such division makes each service handles only one specific task, it will also add overhead and unnecessary complexity to the Blog. As mentioned in [1], when the application has many small parts interacting together, there will be more overhead and complexity added to the application. A trade-off should be considered that helps in following the requirements of microservices while it keeps the complexity of the application as small as possible.

Furthermore, each service in the Blog is as independent as possible where it, generally, doesn’t rely on other services to perform its task. Services, of course, would need an input to start processing the data, but handling the data is something a service doesn’t need help with. The more independent each service is, the easier it is to form a loosely-coupled application.

When a service only needs the required input to operate then such service can easily be modified or updated without affecting other parts of the Blog. The only concern here is to keep the interface as it is so other services can still deliver data to it and receive the output.

For example, a microservice that creates new user’s accounts will be created. This microservice will have its own database where it stores the newly created accounts. Hence, this microservice and its database are completely independent entities. They can simply be used in any other application that requires user’s registration.

Additionally, services in the Blog should be independent but this doesn’t mean that services will act as isolated islands where no communication is happening among them. In fact, without such communication the overall functionality of the system can’t be achieved. Hence services in the Blog will offer an interface where other services can use it to communicate with them. It is important that all services that need to exchange data with other services be able to do it through a unified well-defined interfaces. Changes that happen to a services should not affect the interface that the service exhibit to the outer world.

Services will offer each other APIs that help them to make requests. Requests will be made over Hypertext Transfer Protocol (HTTP) using REST architecture. REST stands for Representational State Transfer. It is an architectural style that is composed of six constrains. REST helps in developing applications that are loosely-coupled [47]. More details about the constrains of REST will be provided in the next chapter.

Since each service is performing a small specific one task then there’s a high chance that the same functionality will be needed in other applications. For example, a service that’s responsible for registering new users in the Blog, could be reused in other applications where a user’s registration is required. Such concerns will be taken into account when designing each service. Because when most services are designed from the beginning as reusable entities, it would be easier than taking each service and adapting it to other applications.

As an example, at least one microservice will offer login services to the clients of the Blog. This service needs access to the database of the registered users so it compares the data it receives from the frontend with the data of the users in the database. This service can be reused in any other application that requires a microservice to handle login tasks. A small modification is required to help the microservice connects with the databases of different applications.

The Blog itself should also have few features that comes from using microservices architecture. After all, if those features are not met then the benefits of using such architecture are not reached to an acceptable level. On the contrary, microservices architecture brings its own challenges. Hence, using such architecture without getting the most of it adds overhead in the development. Where developers have to deal with many small apps and each app has its own development cycle, requirements and deadline. Development of many small apps to finally work together can get quiet complicated. The Blog will be:

* Scalable
* Resilient
* Loosely-coupled

Where new features can be added easily. The scalability of the Blog comes from the possibility of being able to add new services to the Blog. When there’s a need for new features, the existing services can’t be changed to accommodate the new features. Because it means that one or more of the existing services will be handling more than one task which in turns break one of the main characteristics of a microservice. That’s each service should be small and handles one task only. For this reason, services in the Blog should have the flexibility to accommodate new services and be able to communicate with them.

The Blog must be able to handle failures where they don’t cascade in a way that affects other services and stop the Blog from operating. The Blog must be flexible in a way that allow for failures isolation where the malfunction services are isolated from the rest of the Blog. Temporary replaced by other services until the failure is handled.

This is a very important feature of any microservices-based application. Such application should exhibit a better behavior when dealing with failures compared to a monolithic application.

Furthermore**,** The Blog should have its services as independent services that can operate without the need of other services. Each service in the Blog is a small application by itself. Some services might need an input or have an output but it is all performed via the interfaces of the services.

Such loosely-coupled structure of the application helps the Blog to be more flexible when facing problems. Or when some services should be replaced by others. It also helps when performing updates on the Blog.

In the future when new functionalities are needed in the Blog, for example, when categories are introduced to classify posts of the Blog into categories then the only changes that are required must happen in the Post microservice. Few changes will be needed to the micro frontends but most of the other microservices will stay the same, where there is no need to touch them.

## Concept of content trust

Content trust as defined in [17] is not an isolated judgment but it is related to the context in which the judgment is taking place. Hence the surrounding environment and the time of making the decision play a role in the final judgment.

Content trust and reputation trust are related but they are not the same. From the requirements provided in chapter 2, it can be seen that the reputation of the involved entities will play a role in the trust of each one of them. It is, however, not the only deciding factor. Many other factors influence the decision of trust. For example: Verifying the identity of each entity has also a negative or positive influence depending on the outcome of the verifying process. Such influence means that identity verification is also related to content trust.

In a microservices environment where many services are trying to work together, content trust will play a role in helping each service to make a judgment about trusting other services or not. On the other hand, such system of content trust must be designed with care, otherwise the system could behave in an unpredicted way. When such system is not given a thoughtful design and enough preparation and testing then sometimes services could end up making negative judgments about each other. Such negative judgment could happen while a positive judgment is the most probable decision to be made. In this case, services will reject the incoming requests and operations will not take place. Thus clients of the application will be denied the services for no valid reasons.

For example, in an online banking system, a user is trying to start a transaction from one account to another. The request goes from the frontend to the services responsible for handling such transactions. Before going any further, the involved services will try to evaluate the trust each one has about the other. If one of the services decides that it can’t trust at least one of the other services, then, theoretically, the transaction may not take place. The system eventually will refuse to complete the transaction leaving the client with unhandled request. Hence, clients could end up leaving such system and never using its services because of its unpredictable behavior.

The previous scenario, raises many design questions, one of them is whether a system should have more than one services providing the same service. In the previous example, if one service can’t trust another one, then the transaction can still take place if another microservice was available providing the same service as the untrusted one. Such duplication of services could be useful where each service has more than one option. On the other hand, such design can be redundant. It’ll take more time to design a system that has more than one service handling the same task.

### Properties of the Content trust

Content trust implementation will depend on one database to store the information about different microservices. This database will be accessible to all microservices and its data will change after each call made from one microservice to another.

**Unique Identification**

Each service will have unique identifications, this identification helps services to differentiate and identify each other. To challenge the mechanism of content trust, some services will be developed as an in-house development, while others will be developed as third-party microservices. Both types of microservices should be able to have unique identifications.

**Sensitivity classification**

Each microservice will have a sensitivity classification based on the services it provides. This classification will have different levels and each level belongs to a degree of sensitivity. When services are interacting with each other and evaluating their mutual trust, they will be able to see the sensitivity classification of each other. This classification will help services to decide what is the minimum value of trust required to trust one another.

When a service has a high level of sensitivity then the other service will only trust it until a high value of trust is acquired. On the other hand, if a service has a low sensitivity classification then a low trust would be sufficient to trust the service.

**Direct trust**

Microservices will look into their previous experiences and use it when deciding about trusting new interactions or not. For simplicity, each microservice will only be able to look into the last interaction that it had with any other microservice. When a request is sent from one microservice to another, each microservice will look into their last direct trust evaluation. If the evaluation recorded a good level of trust then the current evaluation will be affected positively. On the other hand, if the last direct interaction recorded a low level of trust then the current interaction will be affected negatively.

**Reputation-based trust**

Four Types of information will be used from the concept of reputation-based trust:

* The number of interacting microservices for a certain microservice
* The number of successful interactions with other microservices
* The number of failed interactions with other microservices.
* The evaluation of trust given by other microservices for a certain microservice

Each microservice will be able to see how many interactions a certain microservice has. This number will increase with every request this service receives as well as with every requests it initiates.

Each successful interaction with other microservices means that the service has reached a level of trust that was enough to the other service. At the same time, it has trusted the other service enough. When both cases happen then the successful interaction with other services will be increased.

In order of an operation to be successful, both microservices, the one who makes a request, and the one who receives a request will have to trust each other enough. If one of them could not trust the other microservice enough then the interaction will not continue and the microservice who made the request must look for another microservice to fulfil its request. In this case, the number of failed interactions for both microservices will be increased.

Whenever a microservice makes a request to another microservice or receive a request from it, both microservices will create an evaluation of trust about each other. Hence for any microservice, an evaluation of trust from other microservices might exist. When a microservice makes a call to another microservice, both microservices will be able to see the trust evaluation that’s made by other microservices. In case a microservice has never had any interactions with any other microservice then it will not have any evaluation of trust.

**Time factor**

Time will be used to give to types of information that will help microservices in evaluating the trust of each others:

* The operation age
* Last successful activity

Each microservice will have its operation time recorded. Hence when two microservices are interacting with each other, they will be able to see the age of each other. The age of any microservice could have an influence on the evaluation of trust by other microservices.

How the age affects the evaluation of trust depends on the context and how the designers want the system to behave. For the proposed Blog, the older the service the more trusted it is. The reason for this is, older services are still in the system because they have not exhibited any malfunctions that requires replacing them, moreover it is a sign that the microservice is handling its task well. Hence an older age means a better evaluation of trust.

It is worth noting that the same principle may not apply to other applications. Some system designers would prefer newer microservices over older ones since they might be more up-to-date. In such case, the evaluation of trust could be higher if the task is new. On the other hand, the evaluation of trust could be low if the microservice is old.

When two microservices are about to interact with each other and they are still evaluating the trust about one another, they will be able to see when was the last time each microservice has a successful interaction with other microservices. A successful interaction means when a certain microservice had a good evaluation of trust by another one while it also evaluated well how much it trusts the other service. Not having a recent successful interaction means the service has failed in trusting other services or was not trusted by other services for long time. Such information will have negative effects on the evaluation of trust.

**Number of services**

When an interaction between two microservices fails. Then a lack of trust from one or the two involved microservices happened. In this case, the microservice that made the request must make another request for another service that handles the same task. When there are no more microservices available that can handle the request, then the standers of trust of this microservice must be lowered and it must trust the service that has an evaluation of trust as close as possible to what it originally demands. Failing to do so could mean that the request will never be fulfil, hence the original request made by the client of the Blog would be rejected. This scenario must be avoided especially for important applications such as online banking. When a user is trying to make a transaction online then it is not acceptable that his request was rejected.

### Context of Content trust

Now the main points of content trust have been laid out, developers of an application will have to decide themselves on how to use such system. For example, the mentioned points above can all have the same evaluation level. Meaning that all parts of the system will have the same weight when deciding on trusting a service or not. For instance: Highly evaluated indirect trust, would have the same effect as highly evaluated direct trust.

On the other hand, a different team of developers developing another application, could think differently. The way they would use the content trust mechanism is similar but with different weighting. For example: A highly evaluated indirect trust doesn’t have the same effect as a highly evaluated direct trust. Developers could think that for this particular application that’s being developed, past experience should have more effect than the evaluation of indirect trust. And this will be applied to the rest of the points in the system. Each point could have a different weight from the other. This will cause different results if two systems used the exact system of trust but had different weighting systems. Hence the trust relationships between involved entities will be different.

## Overall structure

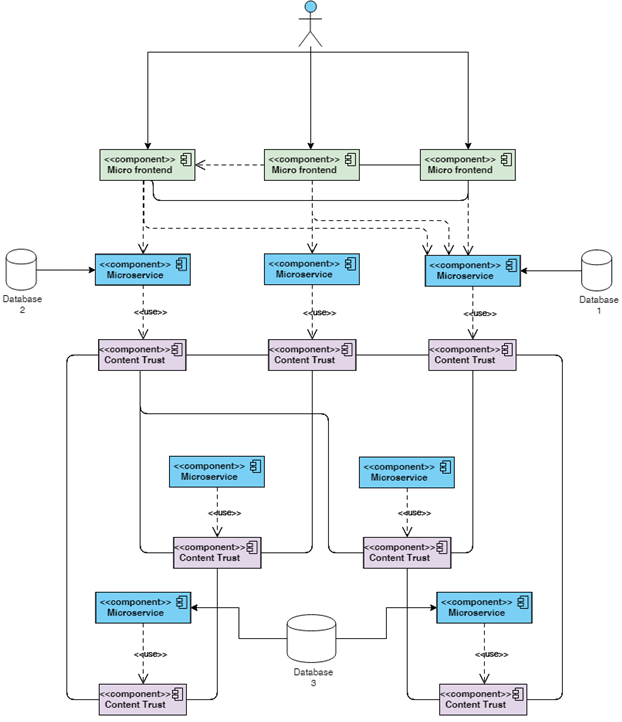


Figure ‎3.1: Overall structure

Figure 3.1 shows a possible structure of the proposed system. The system has the following parts:

* A frontend which consists of micro frontends
* Services
* One or more databases
* Content trust implementation
* Communication system between services

The Blog will have a frontend that helps users interact with it. The frontend will consist of more than one part. Each part is called a micro frontend. Each micro frontend is a small independent application that can be deployed independently and even reused in other applications. Each micro frontend can be developed using different technologies and frameworks.

The user that’s interacting with the frontend will not be able to notice any difference from interacting with a monolithic application. The frontend will appear to the user as if it is a one big frontend. Hence, it will be very hard for the user to tell where a micro frontend starts and where it ends.

Figure 3.1 shows some services that have a direct contact with a database. While other services don’t have a contact with a database. This simply explains that the system will have more than one database. The reason for this comes from the definition of a microservice that’s mentioned in the second chapter. Each microservice is an independent unit that can be deployed independently. As a result, some services will have their own small database. The microservice itself as well as the database can be reused in other applications.

It’s also worth noting that some services will not have their own database. Where for example the task of such services would be to validate some values or make a calculation. Such values will be provided by other services and the result will be sent back.

A content trust implementation is also proposed. This system will help microservices evaluate the trust of each other. In other words, the content trust mechanism will help services make sure that they interact with other microservices that score the highest trust evaluation. Content trust is also represented in figure 3.1 and has a label to indicate to it.

A communication system among services is proposed to make sure that the application operate as it is supposed to. Such communication is represented by links in figure 3.1. Each micro service in the Blog will have an interface. This interface helps microservice to interact with other microservices. Therefore, services will be communicating with each other to handle user’s requests. Yet, communication will only happen after having both microservices evaluating the trust about each other. If the desired trust level is not reached, then communication may not take place and the involved microservices may look for other microservices that satisfy their desired level of trust.

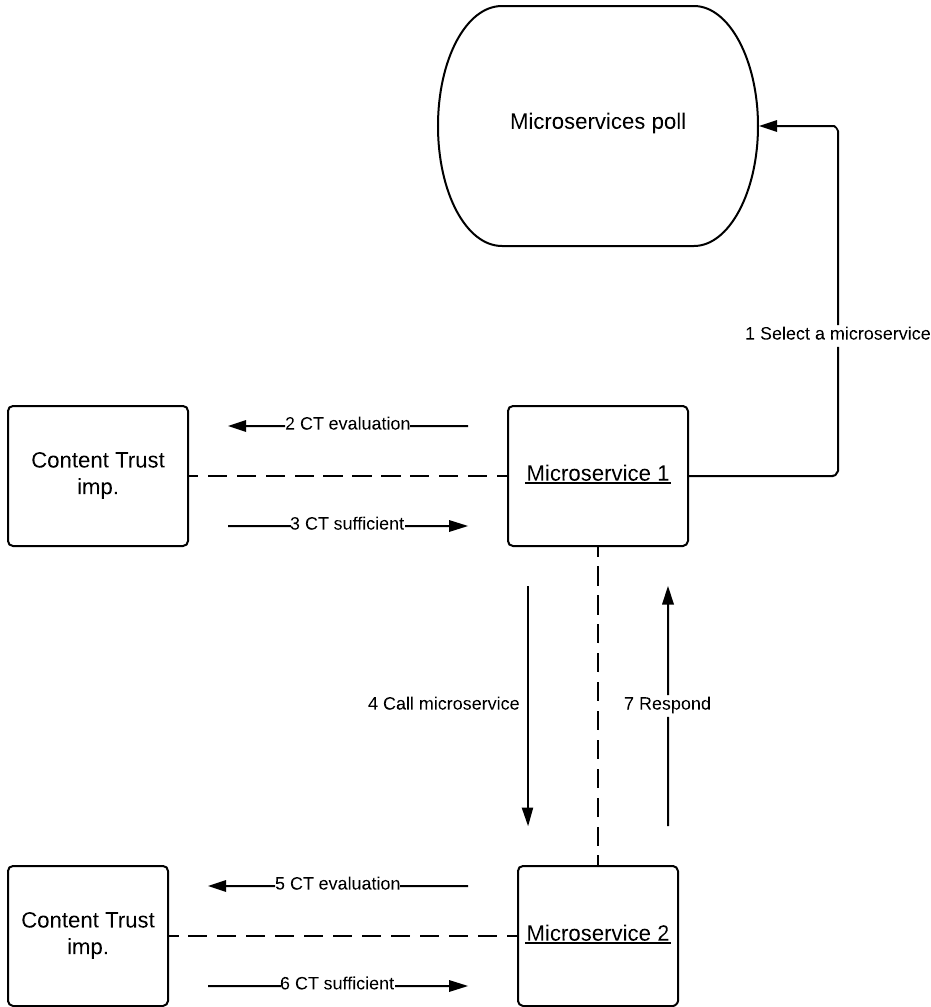


Figure ‎3.1: Microservices collaboration

Figure 3.1 shows an abstract interaction between two microservices. At first a microservice must choose what other microservices it needs to make a call to. Once a microservice is selected then content trust evaluation should be calculated. This evaluation estimates how much this microservice trusts the other microservice. Each microservice has the ability to calculate its evaluation of trust about any other microservice. Once the evaluation of trust has been calculated, it should be estimated if it is sufficient or not. If it is sufficient then this microservice will make its call to the target microservice. The target microservice will start its own evaluation of trust about the microservice that sent her a request. If its evaluation of trust is sufficient then it will respond to the request that it has received from the other microservice.

This diagram shows that at any given time, any involved microservices will have to make an evaluation of trust about each other. Communication between those two microservices will continue if both of them have a sufficient evaluation of trust about each other.

# Implementation

The following pages will present details of the implementation of the Blog. The Blog is developed to show a demonstration of a website based on microservices architecture. Where its frontend is developed based on the micro frontends. And an implementation of content trust to help microservices have an estimation of trust of each other before any exchange of data.

The first section will talk about the implementation of the microservices. It will give an overview of how microservices are implemented. Then detailed description of unique features and implementations that exist in microservices will be presented. The second section will discuss the implementation of Content trust. It will show what microservices uses to evaluate the trust of each other and how the evaluation process happens. Last section, will discuss the implementation of micro frontends and will provide a brief overview of alternative methods to implement micro frontends in a web application.

## Implementation of microservices

Just like many other websites, the Blog has a backend and a frontend. Both sides are implemented using the microservices architecture concept. The backend of the Blog is composed of many small services, and each service implements one task.

Furthermore, the communication between microservices passes through content trust. This approach helps microservices evaluate the trust about each other and enable them to exchange information with other microservices that achieve the highest trust evaluation each time.

The following services implements the functionality of the backend:

* Registration
* Userid
* Usercheck
* Login
* Islogged
* Search
* Post
* Contact us
* Comment
* Duplication
* Validation

Each service is responsible for serving one task once requested. There are services that serve the clients of the Blog. On the other hand, some services only serves other services and don’t have any interaction with the users or clients of the Blog.

Some of the services are replicated, where there will be more than one service handling the same task and has the same name. The reason for this is to distribute the load balance across more than one service. And also to make the content trust implementation more efficient. More discussion about the content trust implementation in the third section of this chapter.

The following pages will discuss in details the role of each service and the underlying implementation of each one.

These services are RESTful web services, meaning that they follow the standards of the Representational State Transfer (REST) architecture.

REST could simply be described in the following scenario where it involves a client and a server. On one side, the server is running a resource (files, database records…etc. stored in the server). On the other side, a client that requests these resource. REST stands for Representational State Transfer. The client asks for a representation of the resource, basically the data. In the case of the implemented Blog, the data mostly represents posts made by the users. The client doesn’t care about how the data is stored on the server side (what technologies are used…etc.). What it receives from the server is a representational state of the data. JavaScript Object Notation (JSON) is a common format for resource representation in REST architecture

C:\Users\Abid\Downloads\rest.png

Figure ‎4.1: Overall interaction

Figure 4-1 shows this scenario with the time line. The user interacts with the Blog via the micro frontends. Once the user requests to read a post on the Blog, the frontend sends this request to the backend. The backend is composed of many microservices. One of them is responsible for handling requests related to the posts. This microservice will receive the request, then initiate the connection with the database and request this specific post from it. The database will answer the request and sends the post. The post will be sent in the same format as it is stored in the database. The responsible microservice will receive the data, then transform it into JSON format and sends it back to the frontend. The frontend will show the post to the client.

This transferring of data between the client and the server is represented in the third word in the REST architecture which is transfer.

JSON format is commonly used in web services as well as other formats such as xml. JSON format has a key-value representation. For example, When the microservice sends the post back to the frontend, it could have the following format:

{

“title” : ”Lorem ipsum dolor sit amet, consetetur sadipscing elitr”,

“body” : ”Nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat“

}

Listing ‎4.1: JSON format

The above scenario doesn’t show the actual communication of the implemented Blog, it only shows how REST architecture is employed in the Blog.

In his famous PhD dissertation [47], Roy Thomas Fielding defines six constrains for REST architecture style. Those constrains are:

1. Client-Server
2. Stateless
3. Cache
4. Uniform Interface
5. Layered system
6. Code-On-Demand
7. Client-Server  
   As described in [47] “Separation of concerns is the principle behind the client-server constraints”. Such separation allows the client as well as the server to develop separately making the system loosely-coupled when it comes to the connection between the client and the server. Moreover, the client now has more portability where it can be a web application, a mobile application, or an application operating on any platform. As long as it respects the API offered by the server.
8. Stateless

The connection between the server and the client must be stateless as mentioned in [47]. The request made by the client must contains all the required information that helps the server to satisfies the request. Once the server replies to the request, no information will be stored on the server regarding this request. Any new request must contain all the relevant information, where the client doesn’t assume any knowledge the server could have from answering previous requests.

1. Cache

This constrain is added to improve network efficiency as described by [47]. When the server replies to a request and this reply contains data. This data should be noted as cacheable either explicitly or implicitly. The client cache could then use this data if it is cacheable for later requests.

1. Uniform Interface

Resources that are in the system and could be requested by the client must have one and only one Uniform Resource Identifier (URI). [47] defines four interface constrains, that are:

* Identification of resources
* Manipulation of resources through representations
* Self-descriptive messages
* Hypermedia as the engine of application state.

1. Layered system

This constrains means that the architecture is composed of hierarchal layers. Each component in a layer doesn’t have access to any layer beyond its adjacent layers [47]. This approach has a disadvantage as noted in [47] where it adds overhead and latency to the processing of data.

1. Code-On-Demand

This constrains allow the server to send a script or an applet to the client as part of the response [47]. This constrain improves system’s extensibility but reduces the visibility, hence it is considered optional by [47].

Each service is built using Node.js, Express.js, and other modules that are different from one service to another. Node.js is a JavaScript runtime environment that can execute JavaScript outside the browser [48]. When Node.js is installed, Node Package Manager (NPM) will be installed too. NPM helps in adding modules to the application. One can think of modules as packages that can be installed or added to the application. Each module can do one or more tasks that helps making the development faster. It is basically reusable units that the developer can use to achieve certain task without having to rewrite new code to implement the same functionality.

Based on the literature review given in the second chapter and the concept of microservices provided in the third chapter, microservices are small independent unit, that can be deployed and reused when needed. Each service in the Blog is developed based on the concepts presented in the third chapter. Hence many services have their own database. As a result, the Blog uses more than one database to provide its services to clients. There can be more than one services have access to the same database. While other services don’t need to access any database.

The following pages will provide a closer look at some of the services implemented in the Blog. Many services share similar characteristics and have a similar overall implementation. hence, in case of similarity between two or more services, only one example of the implementation will be discussed. And at the end of the thesis, a complete list of the services, with their inputs, outputs and a description will be provided.

### Microservices details

**ContactUs**

This service provides the users of the Blog with the possibility of contacting the admins of the Blog. Once the user submits a message to the admin, the message will then be stored in the database. This service has its own database. This service provides only one API. This API help the client to send a message to the service. The message must contain a name, an email, and the content of the message.

app.post('/contact', function(req,res)

Listing ‎4.2 ContactUs API

Listing 4.2 shows how the API is provided by the service. The API ends with ‘/contact‘ and starts with the address of the server and the number of the port where the service is deployed in. This service contacts other services to make sure that users are not submitting invalid information or to protect itself from spam attacks. To contact other services ‘ContactUs‘ uses Axios to make HTTP calls. Axios is Promise based HTTP client for the browser and node.js [49]. Promise simply means the final result of an asynchronous operation. While HTTP stands for Hypertext Transfer Protocol. The result could have one of three values: the request is fulfilled, the requested is denied or the request is still pending. A call-back function could be associated with Axios requests to handle the outcome of the request. In such case developers could check the result of the request in the call-back function and act accordingly.

Depending on the results received from the services that are called by ‘ContactUs‘ the service will either store the message in the database or inform the requestor of an error that happened via the result of the API call.

ContactUs, has its ow database where it stores the messages submitted to the admins. MongoDB is the selected database management system to help store data for services in the Blog.

According to [50] MongoDB is a cross-platform document database. It is also known as Not Only SQL (NoSQL) database [51]. MongoDB uses the concept of key-value, where each document has its own auto generated key. Documents are stored in collections. And a database can have one or more collections. Each collection has one document or more. The internal structure of documents inside collections can be different from one collection to another. In MongoDB, a JSON-like structure can be used where inside any given document, data can be stored in a key-value pair.

const Contact = mongoose.model('Contact',{

name :{

type: String,

required: true

},

email :{

type: String,

required: true

},

content :{

type: String,

required: true

}

});

Listing ‎4.3: Structure of contact document

Listing 4.3 shows the structure of a document that’ll be stored in the contact database. It has a JSON-like structure. It has attributes as well such as if a certain field is required or not or if it has a default value.

{

"name": "Lorem ipsum",

"email": [ipsum@gmail.com](mailto:ipsum@gmail.com),

“content”: “Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod...“

}

Listing ‎4.4: Contact data example

Listing 4.4 shows an example of how data can be stored in the Contact database. To retrieve the name, one show uses the key “name”. Same applies to the email and the content of the message.

**User Registration**

The microservice “Registration” is responsible for adding new users to the Blog. Any new user can simply submit their name, email and password and the “Registration” service will register the information and create a new user’s account if the provided information has no duplication of user’s email or any other errors.

Once the new user’s data has been submitted to the Registration service from the frontend, Registration service will validate the data to make sure that all inputs comply with the rules regarding the name, email and password. This is done by contacting another service to validate the inputs via a POST request. The next step is checking the input data against the data that’s already stored in the database. Service Registration will make a POST request to another service to check of whether the user’s data is unique or not. In case a negative response came as a result for the previous request then user can’t be registered. Otherwise, user’s data will be inserted into the database and Registration service will send a response to the frontend that helps it to recognize the result of the initial new user registration request.

Registration service has its own database. It uses MongoDB as its database management system. Other services that checks for the uniqueness of the entered data also have access to the same database. Registration interacts with other services such as Validation to check for the validity of the input values, and Usercheck to check if the entered data already exists in the database or not. Services interact with each other via HTTP requests.

**Login**

Login microservice helps users to login to the Blog after they have been registered successfully. Essentially, the Login microservice takes email and password as its inputs, and based on this data the user is either logged in or not. Once the email and the password are submitted to the Login microservice from the frontend. The Login microservice will take those inputs and validate them by passing them to another service for validation via a POST request. If the entered values by user are valid email and password, then the Login service will check this data against the database. If a match is found then user is logged in, otherwise and error message is sent as a response to the request. Which then will be forwarded to the frontend to show the error message.

Logging the user in is achieved via JSON Web Token (JWT). Since REST architecture is stateless where being stateless is one of its six constrains then session based authentication is not suitable for microservices application that uses REST architecture. The principle behind session based authentication is that once the user is logged in, the server will create a new session for the user/client, then it will send the session ID back to the user while keeping the session stored in the server. The client will then store the session ID in a cookie in the browser. With every request the user makes to the server, the cookie will be sent with the request. Once the server receives the request and the cookie, it’ll compare the session ID stored in the cookie with the session that the server has already stored internally. If both matches the user’s request is answered, otherwise, the request is declined.

In the Blog the chosen approach is JWT. Once the user sends a request to login, if the user’s data are valid and a match is found in the database, the Login microservice will create a JWT, sings it and sends it back to the client. JSW is created using a secret, that’s chosen by the server. Once the server sends the JWT to the client, no information is stored in the server about that token. Each token has a secret and expiry date.

Microservice Login uses “jsonwebtoken” package. This package can be installed with NPM using the command:

npm install jsonwebtoken

Listing ‎4.5: Installing jsonwebtoken using npm

Listing 4.5 shows how package “jsonwebtoken“ can be installed from the command line using Node.JS Package Manager. This package will do all the heavy lifting to generate and sign the JWT before sending it to the client using the microservice Login.

To sign the token, one piece of data regarding the requesting user is required, in this case, the ID of the user is fetched from the database when a match is found with the input data that’s sent from the frontend. A secret is required; the server is free to choose any secret that’s deemed valid by it. And finally an expiry date. This date will be associated with this specific token. Once this date is passed then the server will no longer accepts the token and user will be asked to login again.

jwt.sign({userID: doc.\_id, exp: expirationDate}, secret);

Listing ‎4.6: Generating a signed token

Listing 4.5 shows how a JWT is generated and signed using “jsonwebtoken” package. Once this token is ready, then it is sent back to the client as a result of the request made to login. A JWT could have the following shape:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.

eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.

TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ

Listing ‎4.7: Generated JWT [52]

Listing 4.7 shows an example of what JWT would look like after it has been generated.

**Comment**

This service allows the user to make a comment about a specific post. The user doesn’t need to be logged in, in order to submit a comment. The Comment service takes name and email as an input from the user. In addition to the ID of the post which is submitted by the responsible micro frontend to the microservice. Comment is also protected by many other microservices to help to respond to spam attacks, duplicated comments or bad input from the user. Moreover, Comment service has its own database, and all submitted comments will be stored in the database.

**Search**

This service helps the user to search the posts for a specific term. It also calls other microservices to validate the input that it receives from the frontend.

## Content trust implementation

In order for the content trust implementation to work, several properties and features must exist to help microservices evaluate the trust about each other. One database will exist to serve the implementation of content trust. This database is accessible to all the microservices of the Blog. This database will be using MongoDB as its Database management system. It will have two collections:

• Services

• Relations

The collection Services will store data about the different microservices that operate in the Blog, this data includes:

• ID of the microservice

• Name of the microservice

• Sensitivity of the microservice

• Development source

• Start date of operation

• Difference

Each microservice will be registered in the database and for each registered microservice there will be an ID associated with it. Each ID is generated by the application automatically for each registered microservice.

The name of the microservice will also be stored in the database. Microservices that offer the same type of services will have the same name. This name will help other microservices in choosing what microservices they want to call.

Sensitivity of the microservice will also be stored in the database. This sensitivity come from the nature of the task each microservice performs. For example, microservices that handles clients’ logins have a higher sensitivity than microservices that handles bringing comments from the database to the frontend. Essentially, sensitivity of the microservices has three classes:

• High

• Medium

• Low

This classification helps microservices in deciding the minimum requirements for trust evaluation. When two tasks are evaluating their mutual trust, if one of them has a sensitivity classification of low while the other has a classification of medium then their tolerance level will be different from each other. The one that has a classification of low could be trusted even if its evaluation was not considered high. On the other hand, the microservice with the medium sensitivity classification could not be trusted if its evaluation was considered low.

Development source refers to the developers of the microservice. In this case, for simplicity, it will have only two cases, either in-house, or a third-party. The source of the development will affect the trust evaluation based on the value it has. If the microservice has an in-house value, then the effect will be positive. Otherwise, this field will affect the evaluation of trust negatively. Source of the development could be extended to have more than two values. A classification could be given to the developers of each microservice. If the source can be trusted, then this will be reflected as a good value that will affect the trust evaluation positively. If the source is not well known, then it will be reflected as a value that will affect the trust evaluation negatively. This is flexible and depends on how specific the designers of the application want to be. In the Blog, only two values will exist for simplicity and because microservices are all developed by one source, yet some microservices registered as a third-party for testing and evaluation purposes.

The starting date of operation will also be stored in the database for each service. This will help to calculate the age of each microservice. The content trust implementation for the Blog will consider if a microservice has an old age then its trust evaluation will be more positive than if it has a young operation age. Basically, this is a design decision and depends on the context of where the content trust implementation is implemented. In other cases, a young operation age could be considered better than an old operation age.

The number of interactions with other microservices for any microservice can be stored also and can help in evaluating the trust. Moreover, the number of successful interactions that each microservice has can also help in evaluating the trust of a certain microservice. The bigger the number, the better the trust evaluation will be. On the other hand, the number of failed interactions can also play a role when evaluating the trust of a microservice. When the number of failed interactions is high then the trust evaluation will be affected negatively.

Services collection will only store one value. This value represents the difference between the successful interactions and the failed interactions. If this value was positive, then the number of successful interactions is higher than the number of failed interactions. While if this value was negative then the number of failed interactions is higher than the number of successful interactions. Depending if the value has negative or positive value, the trust evaluation will be affected accordingly.

On the other hand, the collection Relations stores the following information:

• The ID of the microservice

• The evaluation given by other microservices to this microservice

Relations will have an array of objects, and each object has a key-value pair. Each object will contain an ID of one microservice as a key and an evaluation of trust as a value. For any microservice, all other microservices will be mentioned in this array. So the IDs in the array each represents one microservice. While the values in the array each represents the trust evaluation given by the different microservices. So for each microservice there will be a document, in the relationships collection. Each document contains the ID of a microservice and evaluations of trust from other microservices to this microservice. Those trust evaluation represents the overall trust evaluation that this microservice gained from interacting with other microservices. If the value is null, then no previous interaction between those two microservices happened in the past.

When one microservice wants to make a request to another microservice, first, it must search the Services collection to find all the microservices that offer that services it is looking for. Once it gets a list containing microservices identifiers, it chooses one of them randomly. Once a microservice is chosen then both microservices, the calling one and the one that received the call, will start evaluating the trust of each other.

To evaluate the trust, all the information available about the two involved microservices will be used. At first each microservice will acquire the available data in the Services collection. The Development Source of the microservice will be interpreted as values between one and ten. The Development source in this case can either be in-house, or third-party. In-house will be evaluated to ten while third-party will be evaluated to five. On the other hand, The Difference will be evaluated as it is as long as it is in the range between ten and minus 5. Once it exceeds this range, it will be rounded, so it settles backs in the range between ten and minus 5. Sensitivity of the microservice and the Start date of operation will be used in later stages.

In the next step, each microservice will read the data available in the Relations collection about the other microservice. This data will be intersected with the data that was obtained from the Services collection to evaluate the trust.

Each microservice will read the direct trust it has about the other one. This value is generated in previous experiences that happened directly between these two microservices. Then each microservice will collect all the trust evaluations that other microservices generated about the two concerned microservices. **The median or the average** of these values will be created. This number will also be correlated with the direct trust each microservice obtained about the other one. The resulting value will be measured against the sensitivity of each microservice obtained from the Services collection.

The final evaluation of trust will be a value between zero and ten. If the value that’s obtained bigger than ten, it will be considered ten. And if the value is smaller than zero, it will be considered zero.

The required evaluation of trust for each microservice depends on the sensitivity level for each microservice and is as follows:

|  |  |
| --- | --- |
| Sensitivity | Sufficient Trust |
| Low | 1-3 |
| Medium | 4-7 |
| High | 8-10 |

Table ‎4.1: Sufficient trust evaluation for each sensitivity

Depending on the value each microservice has it will be decided if the other microservice will trust it or not.

When a microservice evaluate the trust of another microservice less than its suffiecient level then the connection between the two involved microservices will break. The calling microservice will look for another microservice to fulfil its request.

# Bibliography

[1] H. Gebhardt, “Dezentrale Autorisierung in,” 2010.

#### Bezeichner für Anhang A

##### Bezeichner für Anhang A.1

<xml>

<element id=”guid”>example</element>

</xml>

Listing ‎0.1 Mit Alt+ F9 bearbeiten (hängt von Heading 4 statt von 1 ab)

# Glossary

Glossarbegriff

Im Glossar können ausgewählte Begriffe genauer definiert werden…

HTML

Bei HTML (Hypertext Markup Language) handelt es sich um eine Auszeichnungssprache …

# Index

**No index entries found.**

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig angefertigt, nicht anderweitig zu Prüfungszwecken vorgelegt und keine anderen als die angegebenen Hilfsmittel verwendet habe. Sämtliche wissentlich verwendete Textausschnitte, Zitate oder Inhalte anderer Verfasser wurden ausdrücklich als solche gekennzeichnet.

Chemnitz, den 30. January 2019

[Comments] mpc

TODO: Es wird empfohlen die offizielle Selbständigkeitserklärung des ZPAs zu verwenden: [http://www.tu-chemnitz.de/verwaltung/studentenamt/zpa/formulare/ Allgemein/allgemein/selbststaendigkeitserklaerung.pdf](http://www.tu-chemnitz.de/verwaltung/studentenamt/zpa/formulare/%20Allgemein/allgemein/selbststaendigkeitserklaerung.pdf)

Für weitere Hinweise siehe Abschnitt ‎2.14 „Die Selbstständigkeitserklärung“