Decision Models for Selecting Patterns and Strategies in Microservices Systems and their Evaluation by Practitioners

Conference Paper · January 2022

DOI: 10.1109/ICSE-SEIP55303.2022.9793911

6 authors, including:

Muhammad Waseem
Wuhan University
24 PUBLICATIONS **89** CITATIONS
SEE PROFILE

Peng Liang
Wuhan University
197 PUBLICATIONS **2,500** CITATIONS
SEE PROFILE

Aakash Ahmad
University of Hail
51 PUBLICATIONS **123** CITATIONS
SEE PROFILE

Mojtaba Shahin
RMIT University
79 PUBLICATIONS **938** CITATIONS
SEE PROFILE

Decision Models for Selecting Patterns and Strategies in Microservices Systems and their Evaluation by Practitioners

Muhammad Waseem[1], Peng Liang[1*], Aakash Ahmad[2]
Mojtaba Shahin[3], Arif Ali Khan[4], Gastón Márquez[5]
[1]School of Computer Science, Wuhan University, Wuhan, China
[2]College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia
[3]Faculty of Information Technology, Monash University, Melbourne, Australia
[4]M3S Empirical Software Engineering Research Unit, University of Oulu, Oulu, Finland
[5]Department of Electronics and Informatics, Federico Santa María Technical University, Concepción, Chile

ABSTRACT

Researchers and practitioners have recently proposed many Microservices Architecture (MSA) patterns and strategies covering various aspects of microservices system life cycle, such as service design and security. However, selecting and implementing these patterns and strategies can entail various challenges for microservices practitioners. To this end, this study proposes decision models for selecting patterns and strategies covering four MSA design areas: application decomposition into microservices, microservices security, microservices communication, and service discovery. We used peer-reviewed and grey literature to identify the patterns, strategies, and quality attributes for creating these decision models. To evaluate the familiarity, understandability, completeness, and usefulness of the decision models, we conducted semi-structured interviews with 24 microservices practitioners from 12 countries across five continents. Our evaluation results show that the practitioners found the decision models as an effective guide to select microservices patterns and strategies.

CCS CONCEPTS

• **Software and its engineering → Designing software**; • **General and reference → Empirical studies**.

KEYWORDS

Microservices System, Software Architecture, Decision Model, Microservices Pattern, Quality Attribute

ACM Reference Format:
Muhammad Waseem[1], Peng Liang[1*], Aakash Ahmad[2], Mojtaba Shahin[3], Arif Ali Khan[4], Gastón Márquez[5]. 2021. Decision Models for Selecting Patterns and Strategies in Microservices Systems and their Evaluation by Practitioners. In *Software Engineering in Practice (ICSE-SEIP '22), May 8–27, 2022, Pittsburgh, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/xxxxxxx.xxxxxxx

ICSE-SEIP '22, May 8–27, 2022, Pittsburgh, PA, USA

ACM ISBN 978-1-4503-xxxx-x/xx/xx…$15.00
https://doi.org/10.1145/xxxxxxx.xxxxxxx

1 INTRODUCTION

Microservices Architecture (MSA), inspired by Service-Oriented Architecture (SOA), has gained immense popularity as an architectural style for service computing in the past few years [2]. With MSAs, an application is designed as a set of business-driven microservices that can be developed, deployed, tested, and scaled independently [25]. Organizations adopt MSA due to better availability, scalability, productivity, performance, fault-tolerance, and cloud support compared with SOA or monolithic applications. It is argued that MSA can also help build autonomous development teams for rapid development and delivery of software services [25].

Microservices systems entail a significant degree of complexity at the design phase and runtime configurations from an architectural perspective. Haselböck et al. [6–8] have identified several design areas for microservices systems, such as application decomposition, microservices security, microservices communication, and services discovery. On the other hand, literature reviews (e.g., [28, 29]), existing practices (e.g., [31]), and exploratory studies (e.g., [30]) indicate several challenges related to the design areas mentioned in [6–8]. Such issues vary from clearly defining the boundaries of microservices to security, communication, discovery, and composition aspects of MSAs.

Both academia and industry (see the identified literature in the Replication Package [27]) have presented reusable solutions for microservices systems in the form of patterns and strategies that can help address the above mentioned challenges. These patterns and strategies are currently distributed across different publications (e.g., scientific and grey literature). The practitioners need to navigate between several patterns and strategies till a suitable combination of patterns (and strategies) is found that can address the microservices development challenge. Moreover, the practitioners cannot find a holistic view of available patterns and find themselves underprepared to select patterns and strategies and oversee their impact on Quality Attributes (QAs). According to some recent studies (e.g., [28–31]), most of the design, development, monitoring and testing challenges are rooted in the design cycle of MSAs covering a multitude of aspects, including service design, deployment and discovery, (de-)composition, delivery, and security.

To assist practitioners in selecting appropriate patterns and strategies for microservices systems, we proposed the **decision models** that cover four MSA design areas: application decomposition into microservices, microservices security, microservices communication, and service discovery. Decision models are a structured

way of exploring the problem and solution space to achieve the design goal(s) [14]. In this work, the proposed models have been (1) developed by reviewing the scientific and grey literature and (2) evaluated through semi-structured interviews with microservices practitioners, which sought the practitioners' perspective on the familiarity, understandability, completeness, and usefulness of the models. The decision model for decomposing applications into microservices was proposed in our previous work [32]. This study proposed three more decision models and evaluated all the four decision models with microservices practitioners through semi-structured interviews.

The **core contributions** of this research are: (1) four decision models that exploit patterns and strategies to accommodate quality attributes (architecturally significant requirements) for microservices systems, and (2) empirical evaluations of the decision models (accommodating practitioners perspective).

Paper organization: Section 2 describes the research methodology; Section 3 presents the details of the decision models; Section 4 describes the evaluation of the decision models; Section 5 discusses the threats to validity; Section 6 presents related work; Section 7 concludes this work with future research directions.

2 METHODOLOGY

The decision models in software architecture are used to map elements of the problem space to elements of the solution space [14]. The problem space represents functional and non-functional requirements, whereas the solution space represents design elements [14]. To create decision models for microservices systems, we represent the problem space as a set of QAs and the solution space as a set of microservices patterns and strategies. We developed the decision models for four microservices design areas, i.e., application decomposition, microservices security, microservices communication, and services discovery, because most of the design, development, and testing challenges are rooted in these areas ([29–31]). The research method to conduct this study comprises three phases, each detailed below and illustrated in Figure 1.

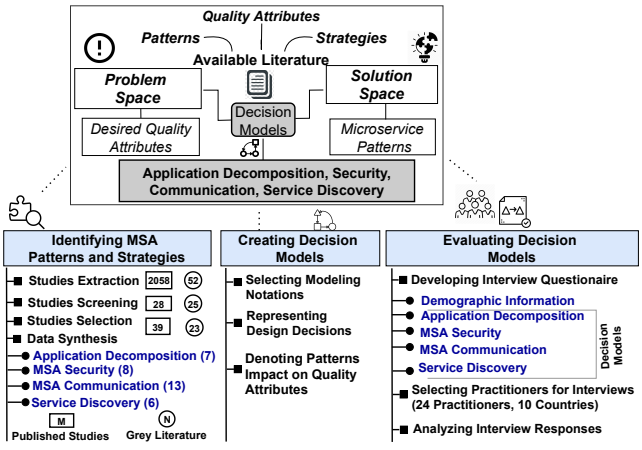

Figure 1: Overview of the research methodology

Table 1: Selected databases, search engines, and search string

Search string	
((microservice OR micro service* OR micro-service* OR microservices architect* OR microservices design) AND (pattern OR tactic OR quality attribute))*	
Database	**Targeted search area**
ACM Digital Library	Paper title, abstract
IEEE Explore	Paper title, keywords, abstract
Springer Link	Paper title, abstract
Science Direct	Paper title, keywords, abstract
Wiley Online	Paper title, abstract
Engineering Village	Paper title, abstract
Web of Science	Paper title, keywords, abstract
Google Scholar	General search
Google	General search

2.1 Identifying MSA Patterns and Strategies

We collected required patterns, strategies, QAs, and impact of patterns on QAs for creating decision models by reviewing scientific (e.g., journals and conference papers) and grey literature (e.g., blog posts and white papers) (see the Selected Studies sheet in the Replication Package [27]). The following four steps [3] are used to extract the relevant studies and required data from both scientific and grey literature.

Step 1 - *Initial search*: We extracted the related studies by executing a search string on eight major databases and Google (see Table 1). The search yielded 2058 scientific and 52 grey literature.

Step 2 - *Title and keywords based studies selection*: The extracted studies in scientific and grey literature were divided into two parts, and two authors (i.e., the first and sixth) further screened the literature independently by reading their titles and keywords. Both researchers excluded several hundred irrelevant scientific and grey literature that were not related to our study goal. Any uncertain literature during this screening process was discussed among all the authors to get a consensus. The title and keywords-based screening finally got 228 scientific and 25 grey literature.

Step 3 – *Abstract and topic based studies selection*: During this step, the first author read the abstracts of the 228 scientific studies and labelled each study as "relevant", "irrelevant", or "doubtful". The doubtful studies were discussed among all the authors for getting consensus about the relevance to our research context. On the other hand, the sixth author read the topics of the 25 grey literature and followed the same selection process. We finally selected 38 scientific and 22 grey literature based on their abstracts and topics (see the Selected Studies sheet in the Replication Package [27]).

Step 4 - *Data extraction and analysis*: We initially identified 211 patterns (strategies) from 39 scientific and 174 patterns (strategies) from 23 grey literature related to the four design areas, i.e., microservices decomposition, security, communication, and discovery. We found that studies use different names for the same pattern (strategy). We tried to understand each pattern (strategy) and identified the common naming for them. We also found that the terms "pattern" and "strategy" were used interchangeably. For instance, API rate limiting is a security pattern, but it is also discussed in the literature as a strategy (e.g., slow down attackers). After removing duplicate patterns and using common naming for several patterns, we finally got 7 patterns and strategies for application

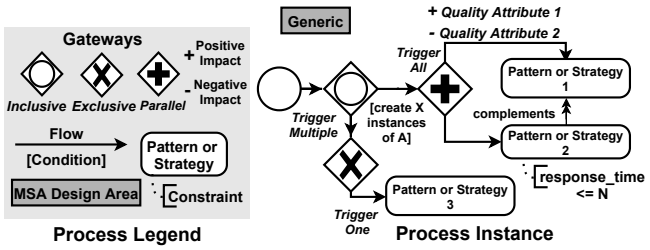

Figure 2: Notations used in the decision models

decomposition into microservices, 8 patterns and strategies for microservices security, 15 patterns and strategies for microservices communication, and 6 patterns and strategies for service discovery. Moreover, a particular pattern or strategy may have a positive or negative effect on QAs. During the data extraction and analysis, we also identified and analyzed the positive and negative impact of patterns and strategies on QAs (see the Patterns Impact sheet in the Replication Package [27]).

2.2 Modeling Decision Models

Figure 2 presents the notations used in the decision models presented in this paper. We used *Inclusive*, *Exclusive*, and *Parallel* gateways of Business Process Model and Notation (BPMN) for indicating the decision flow. Each MSA design area is represented through *grey box*. A *circle* is used to denote the start of a decision process. An *Inclusive gateway* is used to trigger more than one outgoing paths within a decision process. An *Exclusive gateway* is used to trigger one of the outgoing paths. In contrast, A *Parallel gateway* triggers all of the outgoing connected paths. We used *rounded rectangle* to represent the patterns and strategies belong to an MSA design area. A *double-headed* arrow shows a "complements" relationship between two patterns or strategies. An *octagon and dashed* arrow is used to represent the constraints of each pattern or strategy. Finally, plus (+) and minus (-) signs indicate the negative impact of each pattern or strategy on the QAs.

2.3 Evaluating Decision Models

To evaluate and refine the decision models, we conducted 24 semi-structured interviews with microservices practitioners from 24 medium and large companies from 12 countries. The interviewees were recruited through personal contacts, publicly available email addresses of microservices project contributors on GitHub, and social and professional platforms (e.g., microservices groups on LinkedIn, Facebook, and Google). We adapted the interview questions used in previous studies (e.g., [33], [14]) to evaluate the decision models (see the Questionnaire sheet in the Replication Package [27]). The interviews were conducted with a questionnaire which consists of five sections, including the questions about i) participant demographic information (5 questions), ii) decision model for application decomposition (8 questions), iii) decision model for microservices security (8 questions), iv) decision model for microservices communication (8 questions), and v) decision model for service discovery (8 questions). The interview questionnaire has both closed and open-ended questions.Participating in the interviews was voluntary with no compensation. The proposed models and interview questionnaire were shared with the interviewees 6 to 7 days before the interview.

3 DECISION MODELS

3.1 Application Decomposition Decision Model

Monolithic applications need to be decomposed into small, independent, and loosely coupled microservices to achieve the benefits (e.g., improved scalability, independent deployment). Table 2 lists the patterns and strategies covered by the application decomposition decision model (see Figure 3). The decision process for application decomposition into microservices is based on the team size and impact of patterns and strategies on QAs. If the application needs to be decomposed into microservices for the team of 5-9 people to increase *Availability*, *Scalability*, *Cohesion*, *Deployment*, *Performance*, and *Maintainability*, we can use one among seven illustrated patterns (see Figure 3). In the following, we further explain the other conditions, impact on QAs, and constraints for each pattern.

To increase *Flexibility*, *Granularity*, *Reliability*, *Reusability*, *Security*, *Functional suitability*, and *Portability*, **Decomposed by subdomains** pattern can be used. This pattern guides practitioners in defining each microservice responsibility, boundaries, and relationships with other microservices. To successfully implement this pattern, practitioners need to understand the overall business (see Figure 3). In contrast, if microservices need to be defined with respect to business capabilities, **Decomposed by business capabilities** pattern can be used. Normally, business capabilities are organized into a multi-level hierarchy and generate business value. This pattern improves the *Granularity*, *Performance*, and *Security* of microservices if the business capabilities are identified by understanding the client organization's structure, purposes, and business processes. However, this pattern reduces *Flexibility* because the application design is tightly coupled with the business model. Another option that we can use for decomposing applications is **Service per team** pattern. This pattern enables practitioners to break applications into microservices that individual teams can manage. It also complements **Decomposed by subdomains** and **Decomposed by business capabilities** patterns. A constraint of **Service per team** pattern is that only one small team (e.g., 5-9 people) owns one microservice, meaning that each team independently develops, tests, deploys, and scales individual microservice. The teams also interact with other teams to negotiate APIs. **Service per team** pattern increases *Availability*, *Scalability*, *Cohesion*, *Deployment*, and *Performance*, and *Maintainability*. If the project is large and needs to hire more people, **Service per team** pattern negatively impacts the development cost of microservices.

Another exclusive pattern option in decomposition patterns is **Decompose by transactions**, in which applications are decomposed based on business transactions. Each business transaction carries one task, and each microservice has the functionalities for several business transactions (e.g., sales, marketing). This pattern allows grouping multiple microservices to avoid latency issues. **Decompose by transactions** pattern can help to improve *Response time*, *Data consistency*, and *Availability* of microservices. Meanwhile,

Table 2: Application decomposition patterns and strategies

Name	Summary
Decomposed by subdomains [21] [4]	Define services corresponding to Domain-Driven Design (DDD) subdomains.
Decomposed by business capabilities [21] [4]	Define services corresponding to business capabilities.
Service per team [21] [4]	Break down the application into microservices that individual teams can manage.
Decomposed by transactions [4]	An application typically needs to call multiple microservices to complete one business transaction. To avoid latency issues, services can be defined based on business transactions.
Scenario analysis [26]	Identify the business capabilities by analyzing the nouns and verbs from given business scenarios.
Graph-based approach [11]	Identify microservices from the source code of existing monolithic applications by graph clustering and visualization techniques.
Data Flow-Driven (DFD) approach [15]	Follow a top-down approach in which data flow diagrams contain the business requirements that are later partitioned through a formal algebra algorithm for identifying microservices.

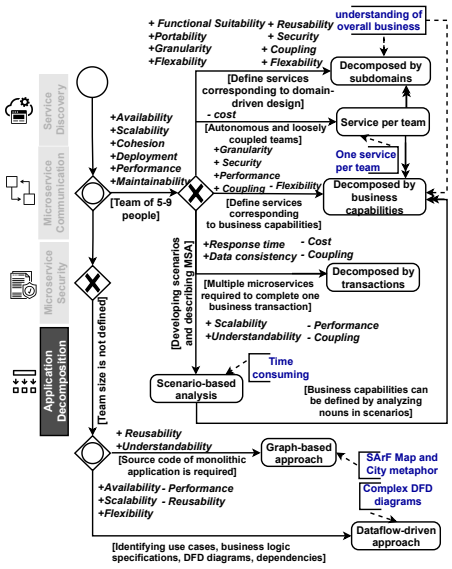

Figure 3: Decision model for application decomposition

decomposing applications based on transactions also increases *Execution cost* and *Coupling* of microservices due to multiple functionalities being implemented in one microservice. Another option to decompose an application is **Scenario-based analysis** which consists of several steps, such as developing scenarios, describing MSA, and evaluating scenarios. During the evaluation process of scenarios, practitioners identify the microservices and interactions between them. This pattern is appropriate if practitioners have enough time to develop and describe the scenarios and MSA, respectively. This strategy can also be used to identify the business capabilities of systems by analyzing the nouns and verbs from given business scenarios. The identified nouns represent the microservices, and the verbs describe the relationship among them. While this strategy increases *Scalability*, *Performance* and *Coupling* could be compromised due to the imprecise boundaries of microservices.

Suppose that the team size is not defined for designing and developing microservices, and we need to identify the microservices from the code of legacy applications. In that case, we can choose **Graph-based approach**, which uses the SArF clustering algorithm to decompose the system for comprehension [13] and the city metaphor techniques for visualizing the system structure [11]. The use of this approach increases the *Reusability* of the existing code. **Graph-based approach** also visualizes the extracted microservices and their relationships along with the structure of the whole system. Hence, it also increases the *Understandability* of the MSA design. Finally, if the team size is not defined and applications need to be decomposed by using DFDs, in that case, **Data flow-driven** approach can be used, which consists of several steps, such as eliciting and analyzing the business requirements for identifying use cases and business logic specifications, creating fine-grained DFDs, identifying the dependencies between processes and datastores, and identifying microservices by clustering processes and related data stores. **Data flow-driven** approach increases *Availability*, *Scalability*, and *Flexibility*. In contrast, it decreases *Performance* and *Reusability* mainly due to complex DFDs.

3.2 Microservices Security Decision Model

The distributed nature of microservices systems makes them a potential target for cyber-attacks. Practitioners need to secure microservices systems at the application, communication, and code levels. Table 3 lists the patterns and strategies covered by the microservices security decision model (see Figure 4). If microservices need to be secured at the application level to improve *Confidentiality*, *Integrity*, *Accountability*, *Authenticity*, and *Recoverability*, **Access and identity tokens** pattern can be used, which encapsulates the security credentials of users (e.g., user identity, user group, user privilege) for accessing microservices through API gateways. It can be implemented by following several access-based and token-based standards, such as OAuth, OAuth2, OpenID, HTTP Basic Auth, and JSON Web Token (JWT), which enable microservices to verify that the requester is authorized to perform specific or all operations according to the given privilege. Similarly, **Layered defense** pattern could be used to secure microservices at the application level. **Layered defense** pattern provides the layered defense-in-depth for microservices systems, and it can be implemented by following the "API-led architecture" in which the whole application is converted into different APIs layers according to the functionality domain. Every API layer has a separate API gateway containing authentication and authorization policies specific to the API layer. This pattern increases *Security*, *Confidentiality*, and *Integrity* because API gateways make it difficult for an intruder to penetrate deep into the system, while in the meantime, it increases *Complexity* of microservices systems.

If practitioners need to secure microservices at the communication level, they can use **Service-level authorization** pattern, **Edge-level authorization** pattern, and **HTTPS enforcement** strategy. The **Service-level authorization** pattern gives more freedom to each microservice to control and enforce the access control policies for communication, which consist of several API policies, i.e., Policy Administration Point (PAP), Policy Decision Point (PDP), Policy Enforcement Point (PEP), and Policy Information Point (PIP).

These access control policies are implemented through Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC) languages and notions. These API policies are mainly implemented in three ways [10]: i) directly implementing PDP and PEP at the microservices code level, ii) introducing a centralized policy repository containing a single policy decision point and implementing PDP and PEP at the microservices code level, and iii) introducing a centralized policy repository containing multiple policy decision points and implementing PDP and PEP at the microservices code level. This pattern improves *Security*, *Availability*, and *Resilience*. However, it has a negative impact on *Latency* because of additional network calls of the remote PDP endpoint. **Edge-level authorization** can also be used to secure microservices communication. This pattern enables the authorization at the edge level (API gateway). API gateway can consolidate authorization for all downstream microservices. Authorization at the edge level is hard to be implemented in a complex ecosystem due to many roles and access control policies. Moreover, because this pattern only secures API gateway, it violates the defense-in-depth policy. However, this pattern increases *Security* and *Integrity* of microservices systems. **Edge-level authorization** pattern can complement with **HTTPs enforcement** strategy that suggests the use of HTTPS connections instead of HTTP, and HTTPS implements a Secure Sockets Layer (SSL) protocol for establishing an encrypted link to secure the communication between microservices.

The code of microservices can be secured by using **API rate limiting**, **Encrypt and protect secrets**, and **Scan dependencies** strategies. **API rate limiting** strategy is used to slow down the attacks from intruders. The intruders use hundreds of gigs of the username and password combinations to breach security. This strategy can be implemented in microservices code or with an API gateway. This pattern not only increases the *Security* and *Authenticity* of microservices, but also protects microservices systems from abusive actions, including excessive API calls and rapidly updating configurations. **Encrypt and protect secrets** strategy is used to secure the microservices secretes (e.g., API key, user credentials). The secrets related to microservices can be stored using various key management services, such as Azure KeyVault, HashiCorp Vault, Spring Vault, and Amazon KMS. Finally, with **Scan dependencies** strategy, scanning programs (e.g., Dependabot) are used to scan the deployment pipeline, the primary line of code, the released code, and new code contribution from developers to detect security vulnerabilities.

3.3 Microservices Communication Decision Model

Microservices systems consist of several independent services running on multiple servers or hosts. Each service or service instance communicates with other services using several patterns. Table 4 lists the patterns and strategies covered by the microservices communication decision model (see Figure 5).

The decision process for microservices communication begins with deciding how the application clients (mobile browsers, desktop browsers) interact with microservices. Usually, a single client needs to fetch data from multiple microservices to complete one transaction. The interaction between the application clients and microservices becomes possible by implementing **API gateway** and **Backend for frontend (BFF)** patterns. **API gateway** provides a single entry point for application clients to access microservices underneath. API gateway also improves *Security*, *Availability*, and *Portability*. However, this pattern also increases *Response time* because of the additional network hop and *Complexity* due to the development, deployment, and management of API gateway. A variant of **API gateway** is **BFF** pattern. **BFF** pattern defines a separate API gateway (e.g., Web app API gateway, mobile API gateway, public API gateway) for each type of application clients (e.g., Web apps, mobile apps, 3rd party apps). This pattern is not appropriate for single interface (e.g., only Web interface) microservices systems. Similar to API gateway, **BFF** also improves *Security*, *Availability*, and *Portability* in microservices systems. This pattern decreases *Response time* due to dedicated API gateways for each type of application clients. We identified two other communication patterns that exclusively complement **API gateway** and **BFF** patterns. The first pattern is **Aggregator microservice** pattern that collects related items of data by invoking multiple microservices and returns

Table 3: Microservices security patterns and strategies

Name	Summary
Access and identity tokens [16, 21, 24]	Verifies that a user is authorized to perform specific operations or not
Layered defence [24]	Protect microservices systems by introducing multiple gateways and API-lead architecture
Service-level authorization [10]	Give freedom to each microservice to control and enforce the access control policies for communication
Edge-level authorization [10]	Secure the edge points (API gateway) of microservices
HTTPS enforcement [10, 16, 24]	Suggests using HTTPS instead of HTTP to secure communication between microservices.
API rate limiting [16, 24]	Slow down the attacks from intruders
Encrypt and protect secrets [9, 16, 24]	Use tools (e.g., HashiCorp Vault, Microsoft Azure Key Vault, Amazon KMS) to secure the API key, user credentials, and other credentials related to microservices.
Scan dependencies [16, 24]	Scanning programs are used to detect the security vulnerabilities that may occurs because of dependency issues

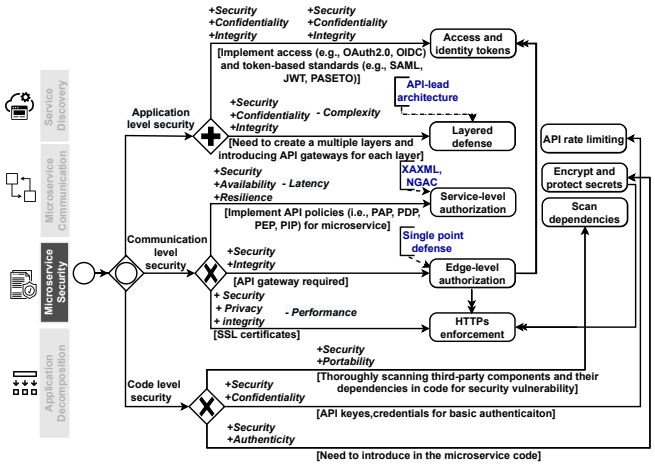

Figure 4: Decision model for microservices security

Table 4: Microservices Communication patterns and strategies

Name	Summary
API gateway [21]	Provide a single entry point to clients for accessing microservices
Backend for frontend [21]	Define a separate API gateway according to type of application client
Aggregator microservice [19]	Collect related items of data from multiple microservices
Proxy microservices [19]	Collect related items of data from multiple microservices through dumb and smart proxies
Remote procedure invocation [21]	Establish inter-service communication via a request/reply-based protocol
Asynchronous messaging [20]	Message sender does not wait for response of corresponding recipient microservices
Publish-subscribe messaging [19, 20]	Allow sender microservice to broadcast the message to zero or more recipient microservices
Publish-asynchronous messaging [19, 20]	Allow sender microservice to broadcast the message to one or more recipient microservices and get the response from some recipient microservices
Asynchronous request-reply [19, 20]	Allow sender microservice to directly send a request message to a recipient microservice and get the immediate response
Synchronous messaging[19]	Message sender waits for response of corresponding recipient microservices
Idempotent consumer [21]	Detect and discard duplicate messages from sender microservices
Anti-corruption layer [23]	Used to communicate the polyglot microservices

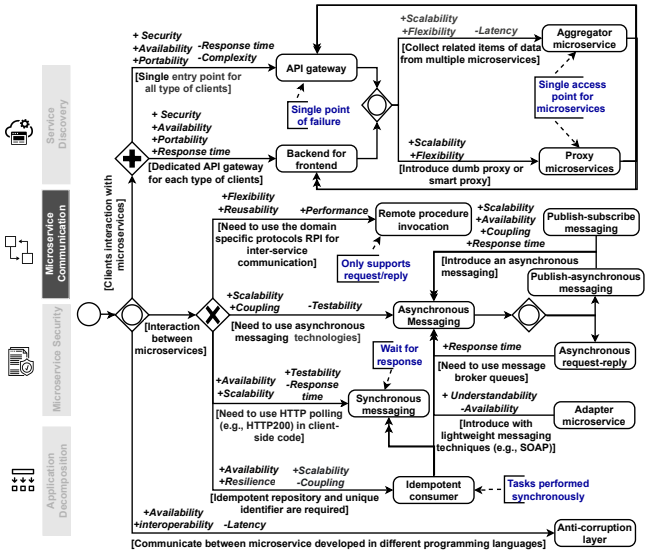

Figure 5: Decision model for microservices communication

them to the application clients via API gateway or BFF gateways (e.g., Web BFF API gateway, mobile BFF API gateway). **Aggregator microservice** pattern increases *Scalability* and *Flexibility*. However, it has a negative impact on *Latency*. A variant of **Aggregator microservice** pattern is **Proxy microservices** pattern, in which different microservices can be invoked according to business needs. However, this pattern uses dumb and smart proxies. The dumb proxy only delegates the request to targeted microservices and returns the data to application clients without any data transformation. In contrast, a smart proxy applies data transformation before sending back the response to application clients [19].

Inter-service communication often happens between microservices to complete business transactions. We identified several patterns that can be used for inter-service communication. **Remote Procedure Invocation (RPI)** enables inter-service communication between microservices through a request/reply-based domain-specific protocols (e.g., SMTP, IMAP, RTMP). Technologies like REST, gRPC, and Apache thrift can be used to implement **RPI** pattern. This pattern increases *Flexibility*, *Reusability*, and *Performance*. The alternative patterns for inter-service communication are **Asynchronous messaging** and **Synchronous messaging**. Typically, **Asynchronous messaging** adopts a choreography style for inter-service communication, whereas **Synchronous messaging** adopts an orchestration style [12]. In **Asynchronous messaging** pattern, sender microservice does not wait for the response of corresponding recipient microservices. This pattern can be implemented by using several asynchronous messaging technologies, including Apache Kafka and RabbitMQ. **Asynchronous messaging** pattern has a positive impact on *Scalability* and *Coupling*. However, *Testability* (debugging) for asynchronous messaging is difficult [18]. There are several patterns that are complemented with **Asynchronous messaging**, including **Publish-subscribe messaging**, **Publish-asynchronous messaging**, **Asynchronous request-reply**, and **Adapter microservice**. The conditions, QAs, and complements relations of these asynchronous messaging patterns are shown in Figure 5. On the other hand, inter-service communication can also be possible through **Synchronous messaging** in which sender microservice waits for the response of corresponding recipient microservices. This pattern implements through HTTP calls. **Synchronous messaging** increases *Availability*, *Scalability*, *Maintainability*, *Testability*, and *Coupling*. The *Response time* of this pattern is relatively lower than *Response time* of **Asynchronous messaging**. Furthermore, our decision model also contains **Idempotent consumer** pattern, which can be used with both **Asynchronous messaging** and **Synchronous messaging** patterns to handle duplicate messages for consumer services. This pattern detects and discards duplicates messages from sender microservices. Finally, **Anti-corruption layer** pattern can be used to communicate polyglot microservices. It increases *Availability* and *Interoperability*. However, *Latency* is compromised due to an extra layer between microservices. **Anti-corruption layer** can also be used between legacy and new microservices systems for migration purposes.

3.4 Service Discovery Decision Model

Microservices runs in a virtualized or containerized environment where the number of instances of a service and their locations dynamically change. A service's client needs to discovery the latest location of the service instances for communication purpose. Table 5 lists the patterns and strategies covered by the service discovery decision model (see Figure 6). The patterns included in this model are integrated through a parallel gateway, meaning that all patterns can be implemented together. The central pattern of this decision model is **Services registry**, which is necessary for the implementation of all other service discovery patterns. Typically, each

service has several instances which are hosted on virtual machines or containers with dynamic IP addresses. The number of instances increases or decreases according to the workload of the system, and IP addresses of instances change dynamically. For example, Amazon EC2 auto-scaling adjusts the number of instances according to the workload. **Service registry** pattern acts as a database of service instances and their locations.

At the first stage of the service discovery process, the service instances and their locations must be registered with service registry. The registration can be performed in two different ways, i.e., **Self registration** and **3rd party registration**. **Self registration** pattern enables service instances to register their hosts and IP addresses in service registry and makes themselves available for service discovery. Each service instance also needs to renew its registration with service registry periodically. This pattern improves the *Scalability*, *Maintainability*, and *Reusability* of microservices. However, it also increases *Coupling* because each service and its instances need to be registered with service registry. The alternative of **Self registration** is **3rd party registration pattern** that also registers service instances along with hosts and IP addresses in service registry when the services start and are unregistered when services shut down. This pattern increases *Scalability*, whereas it decreases *Coupling* between microservices.

If the clients of a service (e.g., API gateway) need to discover a service instance's current location, we can use **Client-side service discovery**, **Microservice chassis**, and **Server-side service discovery** patterns. **Client-side services discovery** pattern enables clients to directly request service registry for the location of the required service instances, and get a response. This pattern increases *Scalability*. However, it also increases *Coupling* due to direct calls between clients and service registry. To implement this pattern, we also need to implement separate service registration patterns according to the programming languages used to develop microservices. **Client-side service discovery** pattern complements **Self registration** and **Microservice chassis** patterns. **Client-side service discovery** is usually implemented with the help of **Microservice chassis** pattern. In **Microservice chassis** pattern, microservices are developed using different frameworks, such as Spring Boot, Spring Cloud, and Gizmo. **Microservice chassis** pattern also improves the *Availability* and *Resiliency* of microservices. Another alternative for service discovery is **Server-side service discovery** pattern, in which clients make a request via a router (i.e., load balancer) to service registry for the location of the required service instances, and get a response through the router. The implementation of **Server-side service discovery** is simpler than **Client-side service discovery** because it only makes the request to a router and the router requests service registry for the location of the service instances.

4 EVALUATION

To evaluate the decision models, we conducted 24 semi-structured interviews with a questionnaire [27]. The key results of the evaluation are presented below:

Demographics of interviewees: The 24 interviewees (P1 to P24) come from 24 IT companies from 12 countries (see Figure 7-a). The roles of the participants are mainly related to the design and development of microservices systems (see Figure 7-a), such as application developer (9 interviewees), architect (9 interviewees), architect and application developer (4 interviewees), and software engineer (2 interviewees). 11 interviewees have 2-3 years of experience, 8 interviewees have 4-5 years of experience, 4 interviewee has 0-1 year of experience, and only one interviewee has more than 6 years of experience working with microservices systems (see Figure 7-c). The domains of the participants' organizations are mainly related to E-commerce, healthcare, financial services, and tourism (see Figure 7-d).

Table 5: Service discovery patterns and strategies

Service registry [21, 22]	Hold the dynamic IP addresses of all service instances
Client-side service discovery [21, 22]	Directly access the dynamic addresses of service instances from service registry
Server-side service discovery [21, 22]	Access the dynamic addresses of service instances via routers from service registry
Microservice chassis [21, 22]	Enable the implementation of client-side service pattern via Microservices chassis frameworks
Self registration [21, 22]	Enables microservices to register their instances with service registry on service startup and update service status periodically
3rd party registration [21, 22]	3rd party registration pattern is an alternative solution of Self registration pattern

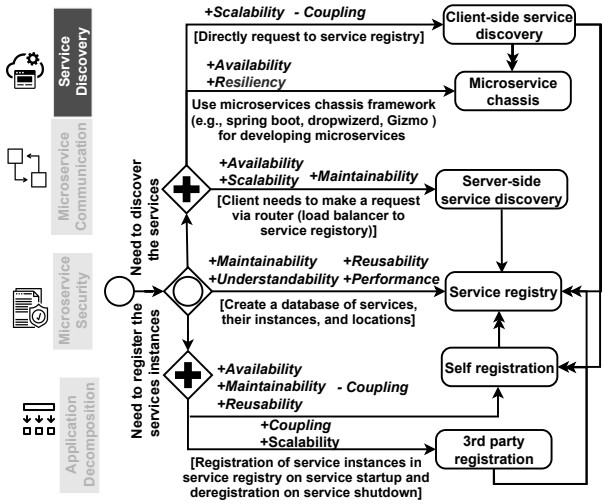

Figure 6: Decision model for service discovery

Familiarity with patterns and strategies: We asked the interviewees, "*Are you familiar with the patterns and strategies used to propose the decision models?*". The majority of the interviewees mentioned that they are familiar with most of the patterns and strategies used to propose the decision models (see Figure 8). For instance, 11 (45.8%) out of 24 interviewees mentioned that they are "familiar to most" of the application decomposition patterns and strategies, and 14 (58.3%) interviewees mentioned that they are "familiar to most" of the security patterns and strategies. Only two (8.3%) interviewees mentioned that they are not familiar with security patterns and strategies.

Understandability and correctness of decision models: Regarding the understandability of each decision model, we asked the

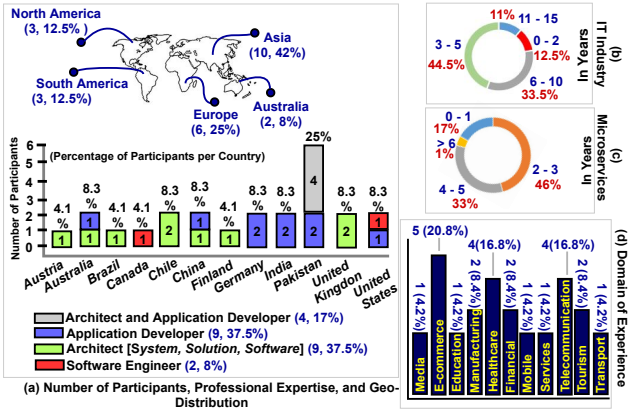

Figure 7: Demography details of interviewed practitioners

interviewees, "*To what extent decision models are easy to understand and use?*". The interviews show that most of the models are easy to understand and easy to follow because of the self-explanatory flow (see Figure 8). For example, 17 (70.8%) interviewees responded that the security decision model is easy to understand and use. Regarding completeness of the decision models, we asked the interviewees, "*Does the information in this decision model sufficiently support making decisions about application decomposition, security, communication, and service discovery?*". The interviews responded that most of the models are complete and sufficiently support decisions making (see Figure 8). For example, 17 (70.8%) interviewees responded that the application decomposition into the microservices decision model sufficiently supports decision making. We also asked the interviewees, "*Are these decision models correct? If not correct, please indicate the problem(s)*". In response to this question, the interviewees indicated several minor issues, such as missing conditions, unclear complements relation, duplicate patterns and strategies, and incorrect impact of patterns on QAs. We fixed these issues in the updated version of the models.

Usefulness for MSA design and development: Regarding usefulness we asked, "*Are the decision models useful to support making decisions in the design and development of microservices systems? Why?*". All the interviewees mentioned that every decision model sufficiently supports the corresponding MSA design area. Following is a representative answer about the usefulness of the microservices communication decision model.

"*This decision model illustrates several patterns and strategies for different kinds of communication styles, and each decision point also reflects the positive and negative impact of the patterns on QAs. Practitioners can easily decide which pattern or strategy they can apply to achieve the communication goal*" ***Architect and Application Developer (P6)***.

Usefulness for MSA evaluation: We also asked the interviewees, "*Are the decision models useful in the architecture evaluation of microservices systems? Why?*". Most interviewees thought that the proposed decision models are useful in microservices architecture evaluation due to the availability of the constraints on patterns, conditions that need to be met by the patterns, trade-off on QAs, and impact of patterns and strategies on QAs. Following is a representative answer about the usefulness of the decision models in microservices architecture evaluation.

"*This set of decision models is helpful in evaluating different aspects of the microservices architecture. Each model proposes a number of design choices for the respective design area along with QAs that can be used for MSA evaluation*" ***Architect and Application Developer (P4)***.

Suggestions for improving decision models: Finally, we asked the interviewees to provide their suggestions for improving the decision models. We received several suggestions in which the interviewees suggested presenting patterns with code, measure quantitative values for QAs, and use decision models in industrial microservices projects.

5 THREATS TO VALIDITY

Internal validity helps to measure the soundness of conducted research, i.e., the extent to which data and evidence support the claims about decision models facilitating the architecting process for microservices systems. We addressed the following threats related to internal validity. *Correctness of decision models*: We tried to mitigate this threat through collaborative work between the authors of this study and the analysis of practitioners' feedback. Regarding the collaborative work, two authors in the research team focused on identifying the decision models. In contrast, others used the information to visually represent and cross-check the models (see Step 1 and Step 2 in Figure 1). On the other hand, we also considered the recommendations provided in the semi-structured interviews to improve the decision models. *Responses of semi-structured interviews*: A potential threat in semi-structured interviews is subjectivity and human bias in answers to specific questions after using the models. Based on their experience, the types and industrial domains of the systems that the interviewed practitioners work with may impact their perspective towards design and architectural artifacts. Some of the interviewees may not reveal their true opinions about the decision models. To mitigate this threat, we conducted two pilot interviews to identify any issues, provided briefings and clarifications to practitioners before the interviews, and followed up with any clarifications or information during and after the interview. Moreover, we presented illustrative examples of each decision model in order not to misinterpret the semi-structured interview questions.

The potential threats to **external validity** are related to the degree in which the results of a study can be generalized. In this respect, we considered the validation of decision models as a threat. Although the evaluation we conducted is based on a limited number of practitioners involved, however, we tried our best to ensure diversity in terms of distributed geo-locations, years of experience, type of professional roles, and industrial domains (see Figure 7) for rigorous evaluation. We believe that despite a limited number of interviews, practitioners' feedback helps to validate the models in terms of their familiarity, understandability, completeness, and usefulness in developing microservices systems. Still, we admit that our findings may not generalize and represent all microservices practitioners' perspectives.

Construct validity is related to taking correct operational measures for collecting the data in this study. One potential threat is

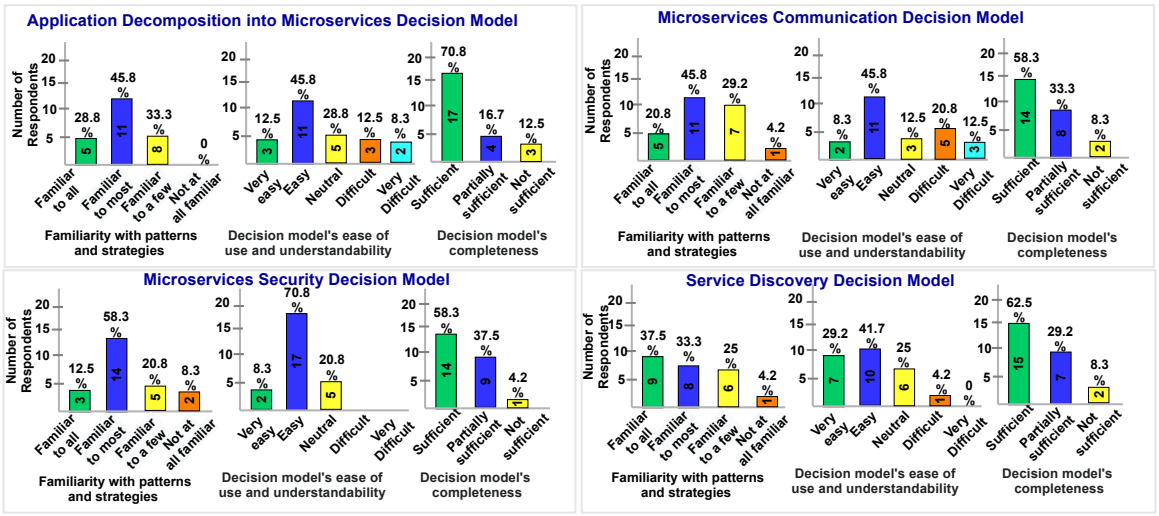

Figure 8: Overview of practitioners' responses for familiarity, understandability, and completeness of the decision models

the inadequate use of the primary constructs of the decision models (i.e., MSA patterns and strategies, QAs, impact of the patterns on QAs). To mitigate this threat, we adopted the following operational measures: (i) we conducted a pilot search to ensure the correctness and appropriateness of the search terms, (ii) we used eight databases (see Table 1) in software engineering research for retrieving the scientific studies, and (iii) we used Google for searching the grey literature. Additionally, we followed the guidelines [3] to review and extract data from the scientific and grey literature.

The threats to **conclusion validity** affect the ability to reach correct conclusions. In order to mitigate this threat, we defined a research methodology based on the practices and guidelines used in recent studies (e.g., [33], [14], [3]) to identify MSA patterns and strategies and to create and evaluate our decision models. Additionally, to ensure the reliability of our study, we have also made the Replication Package available [27].

6 RELATED WORK

6.1 Decision Models and Guidelines for Architecting Microservices Systems

During microservices system development, decision models [5, 7] and practitioners' feedback [8, 17] provide a set of guidelines (e.g., architectural models, patterns, recommended practices) that can empower the practitioners (e.g., architects) to rely on reusable knowledge and best practices to design, develop, validate, and evolve microservices systems [14].

Decision guidance models for microservices systems: Decision guidance models represent concentrated knowledge and rationalization about design decisions, such as modelling notations, patterns, and reference architectures to architect and develop microservices systems [8]. The study in [7] examines existing literature and provides guidance models for microservices discovery and fault tolerance. Regarding migrating microservices systems, Ayas et al. [1] identified three decision-making processes in microservices migrations consisting of 22 decision points and their alternative options by interviewing 19 participants. Data management aspects of microservice systems are reported in [6]. Specifically, this study reports decision guidance models about generating, processing, and managing monitoring data, and disseminating monitoring data to stakeholders for the process automation domain. Harms et al. [5] provide guidelines that support architects while selecting suitable front-end architecture(s) for microservices systems.

Practitioners' perspectives and recommendations for architecting microservices systems: In contrast to decision models, practitioners' perspectives (i.e., developers' feedback) can streamline the industrial practices and experts' recommendations for the design and development of microservices systems. Ntentos et al. [17] present best practices and patterns for microservice systems. Based on identified practices and patterns, the authors have derived a formal architecture decision model containing 325 elements and relations. The derived architectural decision model reduces the (i) efforts needed to understand the architectural decisions for microservice data management and (ii) uncertainty in the design process. An empirical study in [8] interviewed 10 microservices experts to identify 20 design areas and investigate (i) which design areas are relevant for microservices, (ii) how important they are, and (iii) why they are important.

6.2 Decision Models for Selecting Patterns

During the software development life cycle, selecting the most appropriate patterns that can be applied to a particular design context is a critical challenge. Haselböck et al. [8] proposed a decision model that assists developers and architects in selecting appropriate patterns for blockchain-based applications. The proposed decision model was evaluated based on expert opinions regarding its correctness and usefulness in guiding the architecture design and understanding the rationale of various design decisions. The study [14] presents decision models for cyber-foraging systems that maps functional and non-functional requirements to architectural tactics for cyber-foraging.

6.3 Conclusive Summary

Reviewing related research suggests that there is a lack of research on decision models that can leverage patterns and strategies as reusable knowledge to address specific design areas of microservices systems (i.e., application decomposition, microservices security, communication, and service discovery). Existing research on pattern-based architecting of microservices systems [7] exploits decision models but lacks strategies associated with patterns and their impacts on quality attributes (i.e., architecturally significant requirements). In contrast to survey-based studies on finding suitability and application of decision models [17], our work first derives four decision models that can leverage a multitude of patterns and strategies addressing various MSA design areas, and then validates these decision models based on practitioners' feedback.

7 CONCLUSIONS

This research presents decision models that leverage patterns, strategies, and QAs for rationalizing design knowledge to assist architects and developers in engineering microservices systems. The decision models have been identified by systematically reviewing multivocal literature that advocates the role of patterns, architectural strategies, and QAs to support decomposition, security, communication, and service discovery aspects of microservices systems. To validate the decisions models, we engaged a total of 24 microservices practitioners to evaluate the familiarity, understandability, completeness, and usefulness of the decision models. From the practitioners' perspective, the proposed decision models, their underlying patterns, and strategies can empower MSA architects and developers to exploit reusable knowledge and recurring practices for architecture-centric development of microservices systems.

Future research aims to focus on (1) extending the proposed decision models (establishing a decision model repository), exploring the possible combination of patterns and strategies, and validating the models through an industrial scale case study, and (2) developing a recommendation system that supports automation and human-decision in selecting the most appropriate patterns and strategies while analyzing their impacts on quality attributes.

ACKNOWLEDGMENTS

This work was funded by the National Key R&D Program of China with No. 2018YFB1402800 and the NSFC with No. 62172311.

REFERENCES

[1] H. M. Ayas, P. Leitner, and R. Hebig. 2021. Facing the giant: A grounded theory study of decision-making in microservices migrations. In *Proc. of the 15th ACM/IEEE Int. Symp. on Empirical Software Engineering and Measurement (ESEM)*. ACM, 1–11.

[2] N. Dragoni, I. Lanese, S.T. Larsen, M. Mazzara, R. Mustafin, and L. Safina. 2017. Microservices: How to make your application scale. In *Proc. of the 11th Int. Andrei Ershov Memorial Conf. on Perspectives of System Informatics (PSI)*. Springer, 95–104.

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

[4] W. Hari, O.and Tabby and G. Dmitry. 2021. Decomposing Monoliths into Microservices - AWS Prescriptive. https://tinyurl.com/66wcy4j6 accessed on 2021-07-03.

[5] H. Harms, C. Rogowski, and L. Lo Iacono. 2017. Guidelines for adopting frontend architectures and patterns in microservices-based systems. In *Proc. of the 11th Joint Meeting on Foundations of Software Engineering (ESEC/FSE)*. ACM, 902–907.

[6] S. Haselböck and R. Weinreich. 2017. Decision guidance models for microservice monitoring. In *Proc. of the 14th Int. Conf. on Software Architecture Workshops (ICSAW)*. IEEE, 54–61.

[7] S. Haselböck, R. Weinreich, and G. Buchgeher. 2017. Decision guidance models for microservices: Service discovery and fault tolerance. In *Proc. of the 5th European Conf. on the Engineering of Computer-Based Systems (ECBS)*. ACM, 1–10.

[8] S. Haselböck, R. Weinreich, and G. Buchgeher. 2018. An expert interview study on areas of microservice design. In *Proc. of the 11th Conf. on Service-Oriented Computing and Applications (SOCA)*. IEEE, 137–144.

[9] Okta Inc. 2021. 8 Ways to Secure Your Microservices Architecture. https://tinyurl.com/rrm462wz accessed on 2021-07-05.

[10] M. Jim and M. Jakub. 2020. Microservices Security Cheat Sheet. https://tinyurl.com/nmsw7r3n accessed on 2021-07-05.

[11] M. Kamimura, K. Yano, T. Hatano, and A. Matsuo. 2018. Extracting candidates of microservices from monolithic application code. In *Proc. of the 25th Asia-Pacific Software Engineering Conf. (APSEC)*. IEEE, 571–580.

[12] M. Katherine. 2020. Process Orchestration vs Choreography in Microservices. https://tinyurl.com/2zrm8pzm accessed on 2021-07-06.

[13] K. Kobayashi, M. Kamimura, K. Yano, K. Kato, and A. Matsuo. 2013. SArF map: Visualizing software architecture from feature and layer viewpoints. In *Proc. of the 21st Int. Conf. on Program Comprehension (ICPC)*. IEEE, 43–52.

[14] G.A. Lewis, P. Lago, and P. Avgeriou. 2016. A decision model for cyber-foraging systems. In *Proc. of the 13th Working IEEE/IFIP Conf. on Software Architecture (WICSA)*. IEEE, 51–60.

[15] S. Li, H. Zhang, Z. Jia, Z. Li, C. Zhang, J. Li, Q. Gao, J. Ge, and Z. Shan. 2019. A dataflow-driven approach to identifying microservices from monolithic applications. *Journal of Systems and Software* 157 (2019), 110380.

[16] R. Matt. 2020. Security Patterns for Microservice Architectures. https://tinyurl.com/zs85z9as accessed on 2021-07-05.

[17] E. Ntentos, U. Zdun, K. Plakidas, D. Schall, F. Li, and S. Meixner. 2019. Supporting architectural decision making on data management in microservice architectures. In *Proc. of the 13th European Conf. on Software Architecture (ECSA)*. Springer, 20–36.

[18] V. F. Pacheco. 2018. *Microservice Patterns and Best Practices: Explore Patterns Like CQRS and Event Sourcing to Create Scalable, Maintainable, and Testable Microservices*. Packt Publishing Ltd.

[19] P. Raj, H. Subramanian, and A. C. Raman. 2017. *Architectural Patterns: Uncover Essential Patterns in the Most Indispensable Realm of Enterprise Architecture*. Packt Publishing Ltd.

[20] M. Richards. 2015. *Microservices vs. Service-Oriented Architecture*. O'Reilly Media.

[21] C. Richardson. 2018. *Microservices Patterns: With Examples in Java*. Simon and Schuster.

[22] G. Sanchi. 2019. Service Discovery in Microservice Architecture. https://tinyurl.com/9scm8pad accessed on 2021-07-04.

[23] S. Satish. 2019. Microservices Design Patterns: Implementation Patterns, Part 2 (Anti-Corruption Layer). https://tinyurl.com/s63ywrhn accessed on 2021-07-06.

[24] P. Singh. 2021. Microservices and Its Security Patterns. https://dzone.com/articles/microservices-and-its-security-patterns accessed on 2021-07-05.

[25] D. Taibi, A. Florian, L. Valentina, and F. Michael. 2021. From monolithic systems to microservices: An assessment framework. *Information and Software Technology* 137 (2021), 106600.

[26] M. Tusjunt and W. Vatanawood. 2018. Refactoring orchestrated web services into microservices using decomposition pattern. In *Proc. of the 4th Int. Conf. on Computer and Communications (ICCC)*. IEEE, 609–613.

[27] M. Waseem, P. Liang, A. Ahmad, M. Shahin, AA. Khan, and G. Márquez. 2021. Replication Package for the Paper: Decision Models for Selecting Patterns and Strategies in Microservices Systems and their Evaluation by Practitioners. https://doi.org/10.5281/zenodo.5852603

[28] M. Waseem, P. Liang, G. Márquez, and A. Di Salle. 2020. Testing microservices architecture-based applications: A systematic mapping study. In *Proc. of the 27th Asia-Pacific Software Engineering Conf. (APSEC)*. IEEE, 119–128.

[29] M. Waseem, P. Liang, and M. Shahin. 2020. A Systematic mapping study on microservices architecture in DevOps. *Journal of Systems and Software* 170 (2020), 110798.

[30] M. Waseem, P. Liang, M. Shahin, A. Ahmad, and AR. Nassab. 2021. On the nature of issues in five open source microservices systems: An empirical Study. In *Proc. of the 25th Int. Conf. on Evaluation and Assessment in Software Engineering (EASE)*. ACM, 201–210.

[31] M. Waseem, P. Liang, M. Shahin, A. Di Salle, and M. Gastón. 2021. Design, monitoring, and testing of microservices systems: The practitioners' perspective. *Journal of Systems and Software* 182 (2021), 111061.

[32] M. Waseem, P. Liang, M. Shahin, AA. Khan, and A. Ahmed. 2021. A decision model for selecting patterns and strategies to decompose applications into microservices. In *Proc. of the 19th Int. Conf. on Service Oriented Computing (ICSOC)*. Springer, 1–8.

[33] X. Xu, D. Bandara, Q. Lu, I. Weber, L. Bass, and L. Zhu. 2021. A decision model for choosing patterns in blockchain-based applications. In *Proc. of the 18th Int. Conf. on Software Architecture (ICSA)*. IEEE, 47–57.