### COVER FEATURE ARTIFICIAL INTELLIGENCE AND SOFTWARE ENGINEERING: ARE WE READY?



Hironori Washizaki, Waseda University, NII, SYSTEM INFORMATION, and eXmotion
Foutse Khomh, Polytechnique Montréal
Yann-Gaël Guéhéneuc, Concordia University
Hironori Takeuchi, Musashi University
Naotake Natori, Aisin Corporation
Takuo Doi, Lifematics Inc.
Satoshi Okuda, Japan Advanced Institute of Science and Technology

In this study, a multivocal literature review identified 15 software-engineering design patterns for machine learning applications. Findings suggest that there are opportunities to increase the patterns' adoption in practice by raising awareness of such patterns within the community.

Digital Object Identifier 10.1109/MC.2021.3137227 Date of current version: 11 March 2022 generates algorithms, develops capabilities to learn from input data, and produces representative models. The latter is employed for implementation and performance.

Many works have investigated the mathematics and computer science on which the ML techniques are built, but few have examined implementation. This situation raises concerns such as the complexity of ML techniques and the quality of the available implementations, which software defects may negatively impact. These concerns should be alleviated if developers could demonstrate the software quality of their implementations. Consequently, researchers and practitioners study best practices to design ML application systems and software to address issues with software complexity and the quality of ML techniques. Such practices are often formalized as design patterns. These patterns encapsulate reusable solutions to commonly occurring problems within ML application design. There are surveys and case studies on practices and practitioners' insights on ML systems development in general.<sup>1–3</sup> However, none of them focus on the use of concrete ML design patterns.

Herein, we report the results of a multivocal literature review of design patterns for ML. Based on the results, we report on developers' perceptions to validate these patterns in practice. Preliminary literature review results and preliminary study on practitioners' perceptions were presented at conferences.<sup>4,5</sup> In this article, we examine all patterns and conduct a large-scale in-depth study on developers' perceptions. We also describe one major ML design pattern to show how the ML design patterns are documented and used for resolving design problems.

# ML DESIGN PATTERNS IN THE LITERATURE

We define "software-engineering patterns for ML application systems and software design" (hereafter, "ML design patterns") as any patterns that include design structure directly or address design concerns of ML software systems indirectly. We performed a multivocal literature review of both academic and gray literature to collect them.

For the academic literature, we chose Engineering Village, which is a search platform that provides access to 12 engineering document databases, such as Ei Compendex and Inspec. Engineering Village can search all recognized scholarly engineering journals, conferences, and workshop proceedings with a unique search query. On 14 August 2019, we designed and used the following query specifying "pattern" as well as keywords related to patterns to search for documents addressing ML design practice. Based on the broad definition of ML design patterns in this article, we included relevant keywords such as "implementation pattern" and "architecture pattern" since they may handle design concerns indirectly.

((((system) OR (software)) AND (machine learning) AND ((implementation pattern) OR (pattern) OR (architecture pattern) OR (design pattern) OR (antipattern) OR (recipe) OR (workflow) OR (practice) OR (issue) OR (template))) WN ALL) + ((cpx OR ins OR kna) WN DB) AND (({ca} OR {ja} OR {ip} OR {ch}) WN DT).

For the gray literature, we used a Google search performed on 16 August 2019. The query was the same as that for the academic literature: (system OR software) "machine learning" (pattern OR "implementation pattern" OR "architecture pattern" OR "design pattern" OR antipattern OR recipe OR workflow OR practice OR issue OR template) and:

"machine implementation pattern" OR "architecture pattern" OR "design pattern" OR antipattern OR recipe OR workflow OR practice OR issue OR template.

We retrieved 32 scholarly documents and 48 gray literature documents. Two of the authors examined whether each document should be included in our review using the following criteria: 1. Documents written in English addressing concrete software-engineering patterns or practices to design ML application systems and software should be included. 2. Documents focusing on design of ML techniques and algorithms should be excluded. This process identified 19 scholarly documents and 19 gray documents. All the data are available.<sup>6</sup> Among these documents, there was no paper published at Pattern Languages of Programs (LPoP) series that are conferences on patterns and pattern languages, although PLoP series proceedings published by ACM have been included in the search using the Engineering Village.

Figure 1 shows the trend in the number of documents related to the design of ML application systems in the past decade. ML application systems have recently become popular due to the promotion of artificial intelligence (AI). Since 2008, academic and gray documents have discussed good practices of ML application design.

#### OVERVIEW AND CLASSIFICATION OF ML DESIGN PATTERNS

Two of the authors each read half of the documents. Each author extracted patterns independently. Then one of the authors checked each pattern by reading the entire document to determine whether the pattern pertained to software-engineering design practices for ML systems. The extraction process identified 69 patterns. However, the checking process reduced this to 33 patterns related to the architecture and design of ML systems. Finally, three industrial ML developers reviewed the 33 candidates from the viewpoint of practical usefulness. During the review process, any disagreement has been resolved by discussion. They identified only 15 ML design patterns (Table 1). The remaining 18 candidates were not identified as ML design patterns due to their unclear descriptions or shortage of information supporting their usefulness.

Not all of the identified ML design patterns are well-documented in a standard pattern format, which includes a clear problem statement and the corresponding solution descriptions. Thus, we described most of these ML design patterns in a standard pattern format so that practitioners can easily (re)use them in their contexts.<sup>7–9</sup>

Through our literature review and reading of the documents, we noted various characteristics that could help classify ML design patterns. Figure 2 shows an abstract structural overview of ML applications consisting of models, data, and infrastructures. Based on the overview, we classified these ML design patterns into three categories according to their scopes (Table 2):

- > P<sub>1</sub>-P<sub>6</sub> are ML system topology patterns that define the entire system architecture.
- P<sub>7</sub>-P<sub>10</sub> are ML system programming patterns that define the design of a particular component.
- P<sub>11</sub>-P<sub>15</sub> are ML model operation patterns that focus on ML models.

Topology patterns can be regarded as architecture patterns that handle

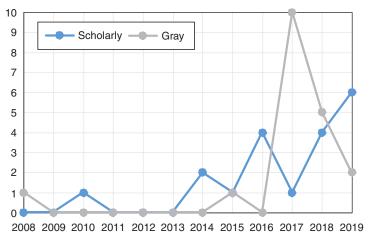


FIGURE 1. The number of documents per year.

unique architectural rules specific to ML systems, while programming patterns can be seen as design patterns that are relatively less specific to ML. Nevertheless, the programming patterns still address some design characteristics of ML software in addition to the general design characteristics. Model operation patterns are all specific to ML models.

Furthermore, any design pattern should address one or more quality attributes that are associated with design problems. For ML design patterns, we assumed that the following product quality attributes defined in ISO/IEC 25010:2011 as well as model and prediction quality attributes can be addressed:

- System and software product quality attributes: Functional suitability, performance efficiency (denoted as "E" in the table), compatibility (C), usability, reliability (R), security (S), maintainability (M), and, portability (P).
- > ML model and prediction quality attributes: Model robustness (Mr), model explainability (Me), prediction accuracy (Pa), and, prediction fairness.

One of the authors analyzed the quality attributes by reading problems and solutions descriptions of the 15 ML design patterns and identifying related specific descriptions or keywords (for example, "If ... has data dependency, it is difficult to localize the erroneous part" implies maintainability). Then, four of the authors reviewed and confirmed the result. Many ML design patterns address maintainability (Table 2). Most operation patterns address model and

ID	Pattern Name	Problem (Excerpt)	Solution (Excerpt)
<i>P</i> <sub>1</sub>	Different Workloads in Different Computing Environments <sup>8,10</sup>	It is necessary to separate and quickly change the ML data workload and stabilize the training workload to maximize efficiency.	Physically isolate different workloads to separate machines. Then optimize the machine configurations and the network usage.
P <sub>2</sub>	Distinguish Business Logic from ML Models <sup>7,11</sup>	The overall business logic should be isolated as much as possible from the ML models so that they can be changed/overridden as necessary without impacting the rest of the business logic.	Separate the business logic and the inference engine, loosely coupling the business logic and ML-specific dataflows.
P <sub>3</sub>	ML Gateway Routing Architecture <sup>11</sup>	When a client uses multiple services, it can be difficult to set up and manage individual endpoints for each service.	Install a gateway before a set of applications, services, or deployments. Use application layer routing requests to the appropriate instance.
<i>P</i> <sub>4</sub>	Microservice Architecture for ML <sup>7,12</sup>	ML applications may be confined to some "known" ML frameworks, missing opportunities for more appropriate frameworks.	Define consistent input and output data. Provide well-defined services to use for ML frameworks.
P <sub>5</sub>	Lambda Architecture for ML <sup>9,13</sup>	Real-time data processing requires scalability, fault tolerance, predictability, and other qualities. It must be extensible.	The batch layer keeps producing views at every set batch interval while the speed layer creates the relevant real-time/ speed views. The serving layer orchestrates the query by querying both the batch and speed layer, and then merges them.
P <sub>6</sub>	Kappa Architecture for ML <sup>9,14</sup>	It is necessary to deal with huge amount of data with less code resource.	Support both real-time data processing and continuous reprocessing with a single stream processing engine.
P <sub>7</sub>	Data Lake for ML <sup>7,13</sup>	We cannot foresee the kind of analyses that will be performed on the data and which frameworks will be used to perform such analyses.	Store data, which range from structured to unstructured, as "raw" as possible into a data storage.
P <sub>8</sub>	Separation of Concerns and Modularization of ML Components <sup>2</sup>	ML applications must accommodate regular and frequent changes to their ML components.	Decouple at different levels of complexity from the simplest to the most complex.
P <sub>9</sub>	Encapsulate ML Models within Rule-base Safeguards <sup>8,15</sup>	ML models are known to be unstable and vulnerable to adversarial attacks, noise in data, and data drift overtime.	Encapsulate functionality provided by ML models and appropriately deal with the inherent uncertainty of their outcomes in the containing system using deterministic and verifiable rules.
P <sub>10</sub>	Discard PoC Code <sup>16</sup>	The code created for PoC often includes code that sacrifices maintainability for efficient implementation of trial and error, and code that is ultimately no longer needed.	Discard the code created for the PoC and rebuild maintainable code based on the findings from the PoC.
P <sub>11</sub>	Parameter-Server Abstraction <sup>16</sup>	For distributed learning, widely accepted abstractions are lacking.	Distribute both data and workloads over worker nodes, while the server nodes maintain globally shared parameters, which are represented as vectors and matrices.
P <sub>12</sub>	Data Flows Up, Model Flows Down <sup>17</sup>	Standard ML approaches require centralizing the training data on one machine or in a datacenter.	Enable mobile devices to collaboratively learn a shared prediction model in the cloud while keeping all of the training data on the device as federated learning.
P <sub>13</sub>	Secure Aggregation <sup>17</sup>	The system needs to communicate and aggregate model updates in a secure, efficient, scalable, and fault-tolerant way.	Encrypt data from each mobile device in collaborative learning and calculate totals and averages without individual examination.
P <sub>14</sub>	Deployable Canary Model <sup>18</sup>	A surrogate ML that approximates the behavior of the best ML model must be built to provide explainability.	Run the explainable inference pipeline in parallel with the primary inference pipeline to monitor prediction differences.
P <sub>15</sub>	ML Versioning <sup>1,7,10,16</sup>	ML models and their different versions may change the behavior of the overall ML applications.	Record the ML model structure, training data set, training system and analytical code to ensure a reproducible training process and an inference process.

PoC: Proof of Concept.

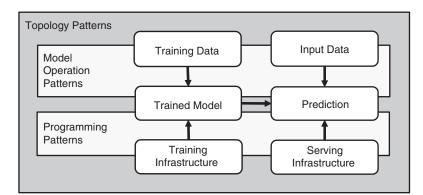


FIGURE 2. The ML system overview and categories of ML design patterns.

TABLE 2. Classification of ML design patterns.									
ID	E	С	R	S	М	Р	Mr	Ме	Pa
Category: Topology									
P <sub>1</sub>	E				М				
P <sub>2</sub>					М				
P <sub>3</sub>		С			М				
<i>P</i> <sub>4</sub>		С			М	Р			
P <sub>5</sub>	Е		R						
P <sub>6</sub>	E		R						
Category: Programming									
P <sub>7</sub>	E	С			М				
P <sub>8</sub>					М				
P <sub>9</sub>			R	S					
P <sub>10</sub>					М				
Category: Model operation									
P <sub>11</sub>	E		R						
P <sub>12</sub>	E						Mr		Pa
P <sub>13</sub>				S			Mr		Pa
P <sub>14</sub>			R					Ме	
P <sub>15</sub>					М		Mr		Pa

prediction quality attributes. Since no ML design pattern addresses usability and prediction fairness, these attributes are excluded from the table.

#### **ENGINEERS' PERCEPTIONS**

ML techniques are concrete solutions to practical problems. Hence, ML developers may have already built a body of knowledge on good design practices of ML development. To clarify how ML developers perceive existing ML design patterns, we surveyed 600+ software and ML developers who participated in an online seminar on ML design patterns in March 2021. During the seminar, we explained the concept of software patterns and introduced the 15 ML design patterns. Afterward, developers answered the following questions about reuse practices and patterns anonymously:

- SQ1. How do you solve and share design challenges of ML application systems?
- SQ2. (For each pattern) Have you ever referred to this ML design pattern?

Of the 600+ participants, 118 answered our questionnaire, which corresponds to a response rate of approximately 20%. Table 3 summarizes the survey result of SQ1. Of the 118 respondents, 37 (that is, 31%) organized design patterns and past design results. Then they reused them to resolve ML design problems. These are the most mature practices in terms of design solution reuse. Thirty-one (26%) reused externally documented patterns but were not organizing patterns or past results by themselves. These are the second most mature practices in terms of reuse. Thirty-seven (31%) resolved problems in an ad hoc way without reusing patterns. These are the worst practices.

Table 3 also shows numbers of ML design patterns used and the usage ratios, which are calculated by #Patterns used / (#Respondents×15). For example, 37 respondents organized patterns, and they answered that in total they had used 64 patterns. They had the opportunity to use 37 × 15 patterns in total, so their pattern usage ratio is 11.5%  $(=64/(37 \times 15))$ . As respondents became more organized in their approach to design problems by reuse, the pattern usage ratio increased, as shown in the table. from 6.3% to 10.8% and even to 11.5%. Based on the result, it is expected that development teams and organizations will reuse more ML design patterns to resolve design problems effectively and efficiently as they become more consistent in their reuse approach.

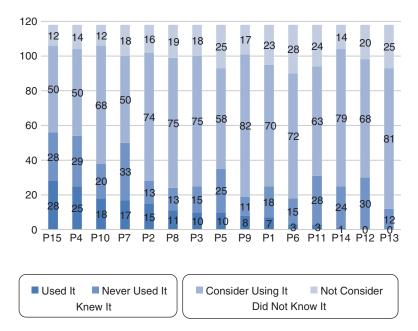
Figure 3 summarizes the result of SQ2. The most used patterns were  $P_{15}$ (used by 24% of the respondents),  $P_4$ (21%), and  $P_{10}$  (15%). In terms of the use rate calculated by #Used/#Knew,  $P_2$  was the most frequently used pattern with a use rate = 15/28 = 0.54. On the other hand, no respondents actually used  $P_{12}$  or  $P_{13}$ , although some respondents knew of these patterns. There is a threat to validity that some participants might answer "yes" for patterns that they generally know and have used the essential part of the patterns' problems and solutions, while some might answer the same but have less understanding (or even worse, misunderstanding) of the patterns. Nevertheless, the survey result should help grasp the general tendency of acceptance of ML design patterns.

In terms of quality attributes, our previous survey targeting 300+ developers showed that maintainability is most considered among nonfunctional attributes during their ML system developments.<sup>5</sup> And the most used patterns  $P_{15}$ ,  $P_4$ , and  $P_{10}$  commonly address maintainability, as shown in Table 2. Their frequent use may suggest that they consider them effective for improving maintainability since maintainability was reported to be their primary concern.

The developers were unfamiliar with most ML design patterns, although there were several major patterns used

#### TABLE 3. Survey result of SQ1 (N = 118).

Design Solution and Reuse Practice	# Respondents	# Patterns Used	Pattern Usage Ratio
Organizing patterns and past design results and reusing them	37	64	11.5%
Reusing externally documented patterns	31	50	10.8%
Resolving problems in an ad hoc way without patterns	37	35	6.3%
Other (incl. those with little experience in ML system development)	13	3	1.5%



**FIGURE 3.** The survey result of SQ2 of seminar participants (N = 118): Knew and Used It, Knew but Never Used It, Did Not Know It but Will Consider Using It, and Did Not Know It and Will Not Consider Using It.

by 20+% of the respondents. For all patterns, most respondents indicated that they would consider using them in future designs. These findings suggest that the identified ML design patterns are expected to help resolve particular problems, and there are opportunities to utilize existing ML design patterns and realize more consistent reuse by increasing awareness of such patterns within the ML community.

#### EXAMPLE OF A MAJOR ML DESIGN PATTERN

Here, we describe one major ML design pattern and its usage. We selected "Distinguish Business Logic from ML Model" ( $P_2$ ) since it was one of the most popular patterns among our survey participants. Moreover, it provides a basis for other patterns (such as  $P_7$ "Data Lake for ML") by clearly decomposing the ML system into multiple layers and components. For brevity, participants, collaborations, implementation, and known uses are omitted here.

#### Pattern name

Distinguish Business Logic from ML Model<sup>7</sup> (original name "Multi-Layer Architectural Pattern"<sup>11</sup>)

#### Intent

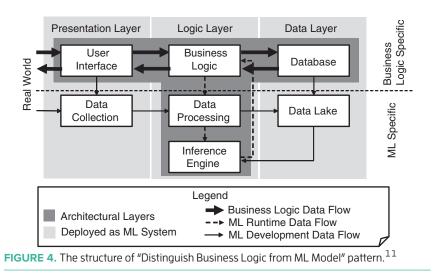
Isolate failures between business logic and ML learning layer to help developers debug ML application systems easily.

#### Problem

ML application systems are complex because their ML components must be (re)trained regularly and have an intrinsic nondeterministic behavior. Similar to other systems, the business requirements for these systems and the ML algorithms change over time.

#### Solution

Define clear APIs between the traditional and ML components. Place the business and ML components with different responsibilities into three layers (Figure 4). Divide data flows into three.



#### Applicability

It is applicable to any ML application system with outputs that depend on ML techniques.

#### Consequences

Decoupling "traditional" business and ML components allows the ML components to be monitored and adjusted to meet users' requirements and changing inputs.

#### Usage example

Figure 5 presents an implementation example of the pattern in a Slack-based Chatbot system. By referring to the pattern, the necessary elements as well as their relationships are easily specified while having clear separation between the Chatbot service (as the business logic) and the underlying ML components.

L application systems are quite popular due to the recent promotion of AI. To bridge the gap between traditional software systems and ML application systems with respect to design, software-engineering design patterns for ML applications were analyzed via a multivocal literature review and a survey of developers. From the 32 scholarly documents and 48 gray documents identified in the literature review, 15 ML design patterns were identified. A survey of developers revealed that there are some major ML design patterns.

Although the literature review was conducted in 2019, we believe this is the first step to explore ML design patterns and build on them to propose refined patterns. We plan to revise the identified patterns by sharing them to obtain reviews from the public. Since we surveyed the practitioners' perceptions on the patterns two to five years after their original publications, our survey should

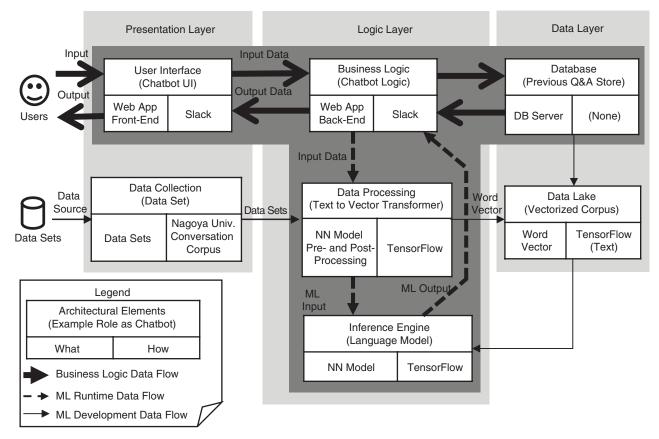


FIGURE 5. An example of Chatbot system architecture by applying "Distinguish Business Logic from ML Model."

reveal the meaningful perceptions. And practitioners may not be aware of recent patterns, <sup>19,20</sup> which have emerged after our literature review. As our future work, we will continue our survey by extending the scope of ML design patterns to include these recent patterns and ones published at some of the PLoP series proceedings, which were not included in the original search.

We also plan to create a map of the relationships among these ML design patterns and other related patterns. Furthermore, we will investigate applications of these ML design patterns in actual ML systems and software design.

#### ACKNOWLEDGMENTS

The authors would like to thank Hiromu Uchida for his help. This work was supported by JST-Mirai JPMJMI20B8 Engineerable AI (eAI), JSPS JPJSBP 120209936, KAKENHI 21KK0179, and enPiT-Pro Smart SE.

#### REFERENCES

- S. Amershi et al., "Software engineering for machine learning: A case study," in Proc. 41st Int. Conf. Softw. Eng., Softw. Eng. Pract. (ICSE-SEIP), 2019, pp. 291–300, doi: 10.1109/ ICSE-SEIP.2019.00042.
- 2. M. S. Rahman, E. Rivera, F. Khomh, Y.-G. Guéhéneuc, and B. Lehnert,

"Machine learning software engineering in practice: An industrial case study," 2019, *arXiv*:1906.07154.

- A. Serban, K. van der Blom, H. Hoos, and J. Visser, "Adoption and effects of software engineering best practices in machine learning," in Proc. Int. Symp. Empirical Softw. Eng. Meas. (ESEM), ACM, 2020, pp. 1–12, doi: 10.1145/3382494.3410681.
- H. Washizaki, H. Uchida, F. Khomh, and Y. Guéhéneuc, "Studying software engineering patterns for designing machine learning systems," in Proc. 10th IEEE Int. Workshop Empirical Softw. Eng.

## ABOUT THE AUTHORS

HIRONORI WASHIZAKI is a professor in the Department of Computer Science and Engineering at Waseda University, Tokyo, 1698555, Japan, and a visiting professor at the National Institute of Informatics, Tokyo, 1018430, Japan. He also works in industry as outside director of SYSTEM INFORMATION and eXmotion. His research interests include software design, reuse, quality assurance, machine learning engineering, project and business management, and ICT education. Washizaki received a Doctoral degree in information and computer science from Waseda University. Washizaki is IEEE Computer Society Vice President for the Professional & Educational Activities Board. Contact him at washizaki@waseda.jp.

FOUTSE KHOMH is a full professor at Polytechnique Montréal, Quebec, H3T1J4, Canada. His research interests include software maintenance and evolution, machine learning systems engineering, cloud engineering, and dependable and trustworthy machine learning/artificial intelligence. Khomh received a Ph.D. in software engineering from the University of Montreal. Contact him at foutse.khomh@polymtl.ca.

YANN-GAËL GUÉHÉNEUC is a full professor in the Department of Computer Science and Software Engineering at Concordia University, Montréal, Quebec, H3H 2L9, Canada. His research interests include evaluating and enhancing the quality of the software systems, focusing on the Internet of Things and researching new theories, methods, and tools to understand, evaluate, and improve the development, release, testing, and security of such systems. Guéhéneuc received a Ph.D. in software engineering from the University of Nantes. Contact him at yann-gael.gueheneuc@concordia.ca.

HIRONORI TAKEUCHI is a professor at Musashi University, Tokyo, 1768534, Japan. His research interests include enterprise modeling, requirements engineering, and text analytics in software engineering. Takeuchi received a Ph.D. in engineering from Keio University. Contact him at h.takeuchi@ cc.musashi.ac.jp.

NAOTAKE NATORI is with Aisin Corporation, Kariya, 1010021, Japan. His research interests include artificial intelligence and machine learning. Natori received a master's degree in engineering from Waseda University. Contact him at naotake. natori@aisin.co.jp.

TAKUO DOI is with Lifematics Inc., Tokyo, 1010051, Japan. His research interests include machine learning and agile development. Doi received a Ph.D. in engineering from the University of Electro-Communications. Contact him at doi@ lifematics.co.jp.

SATOSHI OKUDA is with the Japan Advanced Institute of Science and Technology, Ishikawa, 1086019, Japan. His research interests include machine learning systems and development process. Okuda received a master's degree in engineering from the Japan Advanced Institute of Science and Technology. Contact him at okuda@jaist.ac.jp.

*Pract*. (*IWESEP*), 2019, pp. 49–54, doi: 10.1109/*IWESEP*49350.2019.00017.

- H. Washizaki, H. Takeuchi, F. Khomh, N. Natori, T. Doi, and S. Okuda, "Practitioners' insights on machine-learning software engineering design patterns: A preliminary study," in Proc. IEEE Int. Conf. Softw. Maintenance Evol. (ICSME), 2020, pp. 797–799, doi: 10.1109/ ICSME46990.2020.00095.
- 6. 2021, doi: 10.5281/zenodo.5168886.
- H. Washizaki, F. Khomh, and Y.-G. Guéhéneuc, "Software engineering

patterns for machine learning applications (SEP4MLA)," in Proc. 9th Asian Conf. Pattern Lang. Programs (Asian-PLoP), Hillside, Inc., 2020, pp. 1–10.

- H. Washizaki et al., "Software engineering patterns for machine learning applications (SEP4MLA): Part 2," in Proc. 27th Conf. Pattern Lang. Programs (PLoP), Hillside, Inc., 2020, pp. 1–10.
- J. Runpakprakun and H. Washizaki, "Software engineering patterns for machine learning applications (SEP-4MLA) - Part 3," in Proc. Conf. Pattern Lang. Prog., 2021, pp. 1–9.
- C.-J. Wu et al., "Machine learning at Facebook: Understanding inference at the edge," in Proc. 25th Int. Symp. High Performance Comput. Archit. (HPCA), 2019, pp. 331–344, doi: 10.1109/HPCA.2019.00048.
- H. Yokoyama, "Machine learning system architectural pattern for improving operational stability," in Proc. Int. Conf. Softw. Archit. Companion (ICSA-C), 2019, pp. 267–274, doi: 10.1109/ICSA-C.2019.00055.
- 12. D. Smith, "Exploring development patterns in data science," THEORYLANE,

2017. https://www.theorylane.com/2017/ 10/20/some-development-patterns -in-data-science/

- P. Menon, "Demystifying data lake architecture," TechTarget, 2017. https://rpradeepmenon.medium. com/demystifying-data-lake -architecture-30cf4ac8aa07
- 14. V. Tyagi, "From insights to value Building a modern logical data lake to drive user adoption and business value," 2017. [Online]. Available: https://www.slideshare.net/Hadoop \_Summit/from-insights-to-value
  -building-a-modern-logical-data
  -lake-to-drive-user-adoption-and
  -business-value
- M. Kläs and A. M. Vollmer, "Uncertainty in machine learning applications: A practice-driven classification of uncertainty," in Proc. Comput. Safety, Rel., Security (SAFECOMP) Workshops, 2018, pp. 431–438, doi: 10.1007/978-3-319-99229-7\_36.
- D. Sculley et al., "Hidden technical debt in machine learning systems," in Proc. 28th Int. Conf. Neural Inf. Process. Syst., 2015, pp. 2503–2511.
- B. McMahan and D. Ramage, "Federated learning: Collaborative machine learning without centralized training data," Google AI Blog, 2017.

https://ai.googleblog.com/2017/04/ federated-learning-collaborative. html

- S. Ghanta et al., "Interpretability and reproducability in production machine learning applications," in Proc. 17th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA), 2018, pp. 658–664, doi: 10.1109/ ICMLA.2018.00105.
- V. Lakshmanan et al., Machine Learning Design Patterns. Sebastopol, CA, USA: O'Reilly, 2020.
- Y. Shibui, "Machine learning system design patterns," GitHub, 2020. https://github.com/mercari/ ml-system-design-pattern



Digital Object Identifier 10.1109/MC.2022.3150823