craftworks AI

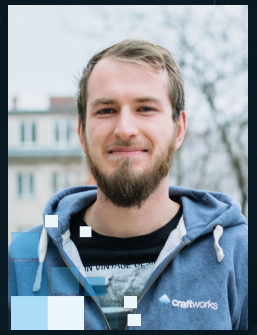
CI/CD for Machine Learning

Continuous Integration and Delivery for
(on-premise) Machine Learning Applications

craftworks AI

craftworks AI

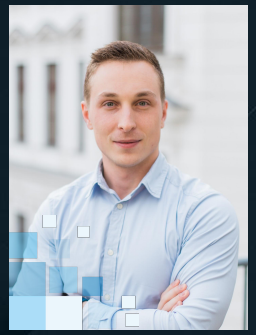
We develop prize-winning
Industrial AI



Bernhard Redl

Head of Infra @ craftworks

bernhard.redl@craftworks.at



Simon Stiebellehner

Head of AI @ craftworks
Lecturer @ WU Wien & FH Wien

simon.stiebellehner@craftworks.at

craftworks AI

We develop prize-winning

Industrial AI

A Selection of our Clients

Predictive Quality

Predictive Analytics

Predictive Analytics

Predictive Quality

Predictive Quality

Software Solution

Computer Vision

Big Data Infrastructure

Predictive Maintenance

Predictive Maintenance

craftworks AI

CI/CD for Machine Learning

Continuous Integration and Delivery for *(on-premise)* Machine Learning Applications

1. CI/CD for Software Engineering
2. A Different Set of Challenges: SE vs. ML
3. CI/CD for Machine Learning
4. Use Case: InvexML

craftworks AI

CI/CD
SE

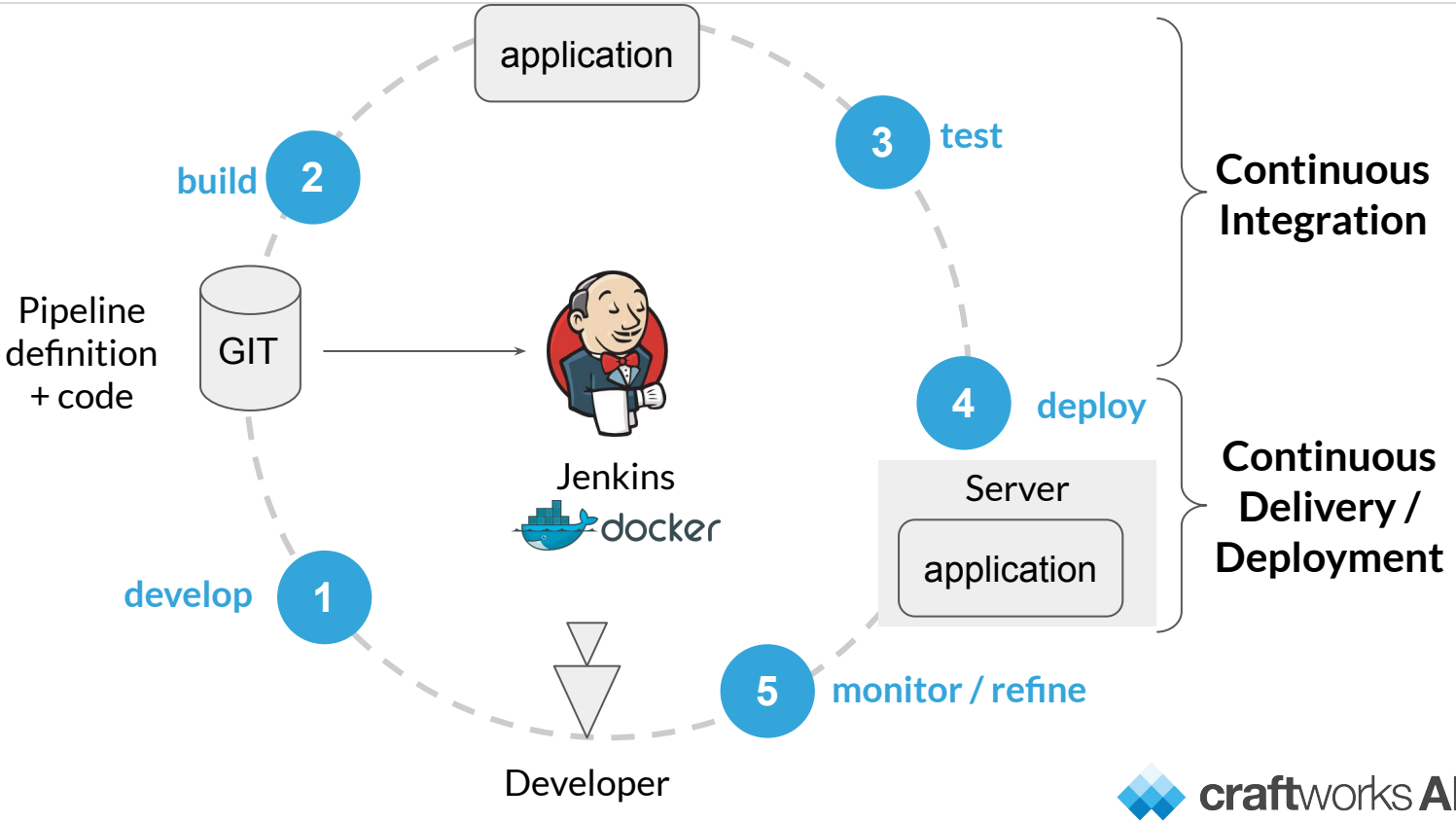
CI/CD

Why?

- **Short iterations** of feedback loop (technical, customer)
- Faster innovation
- Make **release 'easy'**
- Ideally **revertible** if mistakes happen
- Ship every commit (cloud) / **Ship often**
- Scrum / **agile** development process

CI/CD for Software Engineering

How?



craftworks AI

CI/CD
SE

CI/CD for Software Engineering

Toolset

Repo	CI	Quality	Artifacts	Deploy
GitLab	Jenkins	sonarqube	Sonatype Nexus	ANSIBLE
	CI/CD			CHEF
	Travis CI			

craftworks AI

CI/CD for Machine Learning

Continuous Integration and Delivery for
(on-premise) Machine Learning Applications

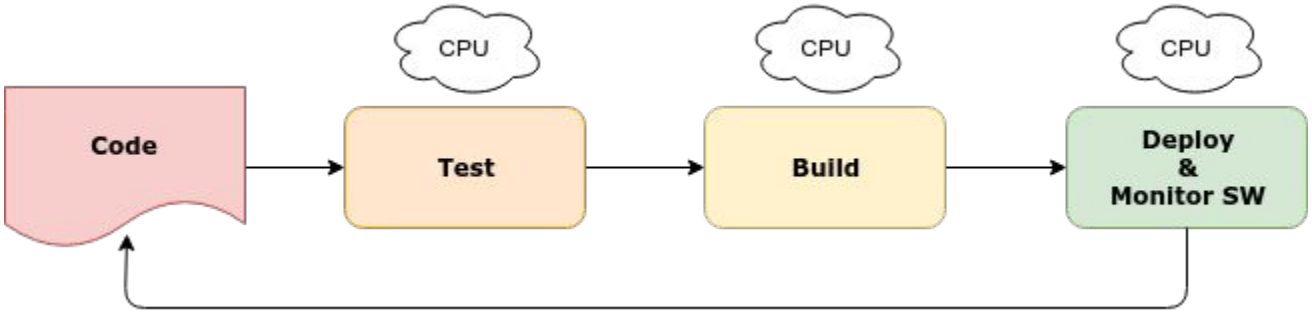
1. CI/CD for Software Engineering
2. A Different Set of Challenges: SE vs. ML
3. CI/CD for Machine Learning
4. Use Case: InvexML

craftworks AI

Challenges
SE vs. ML

A Different Set of Challenges: SE vs. ML

Software Engineering Workflow

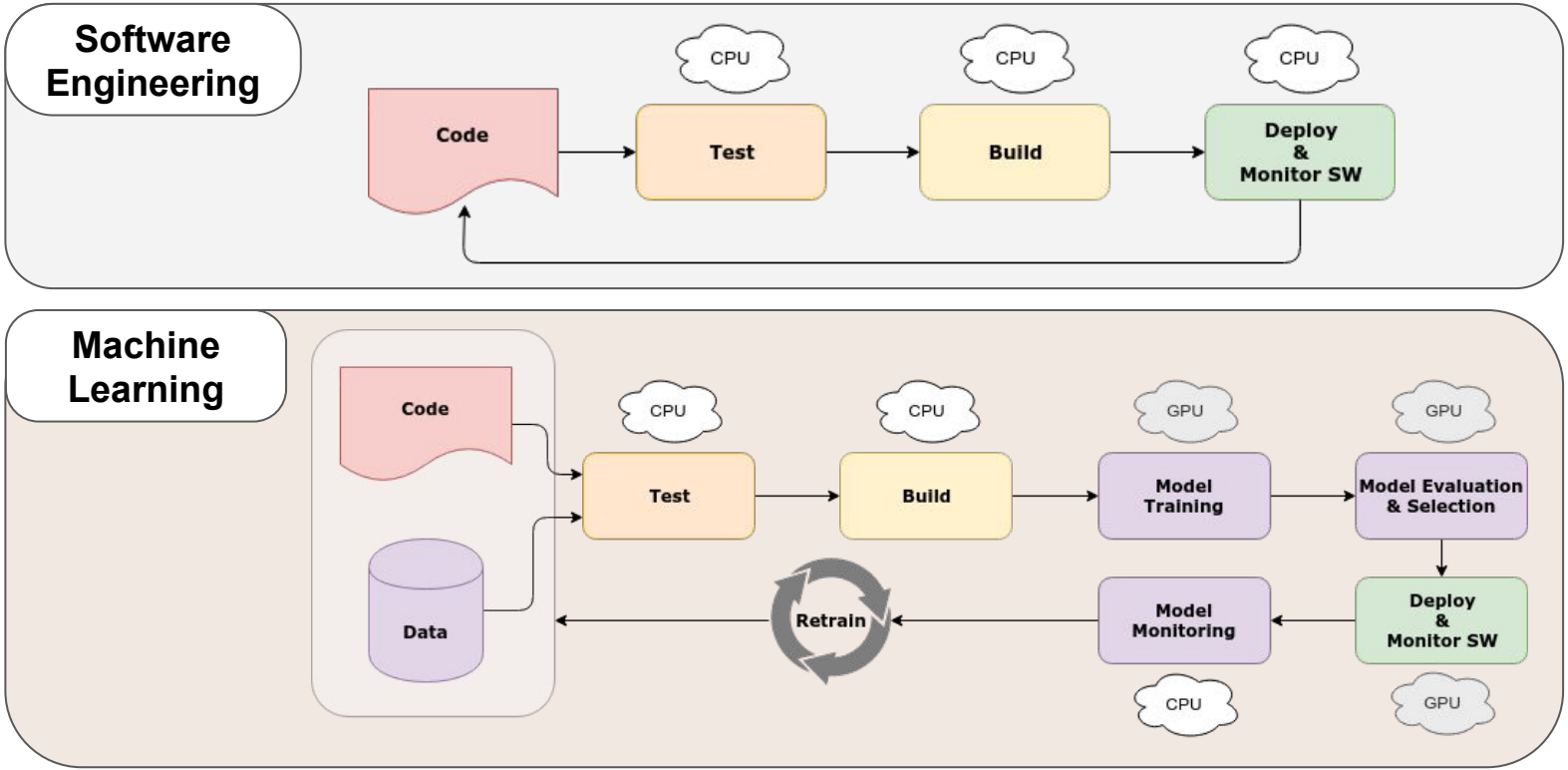


2

Challenges
SE vs. ML

A Different Set of Challenges: SE vs. ML

Workflow: ML vs. SE



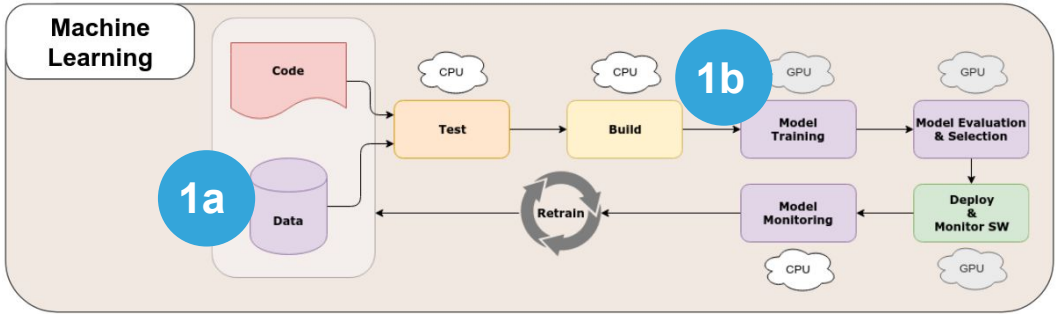
craftworks AI

2

Challenges SE vs. ML

A Different Set of Challenges: SE vs. ML

1 Artifacts



Machine Learning uses and generates **additional artifacts:**

- Data
- Models
  - Estimators
  - Transformers

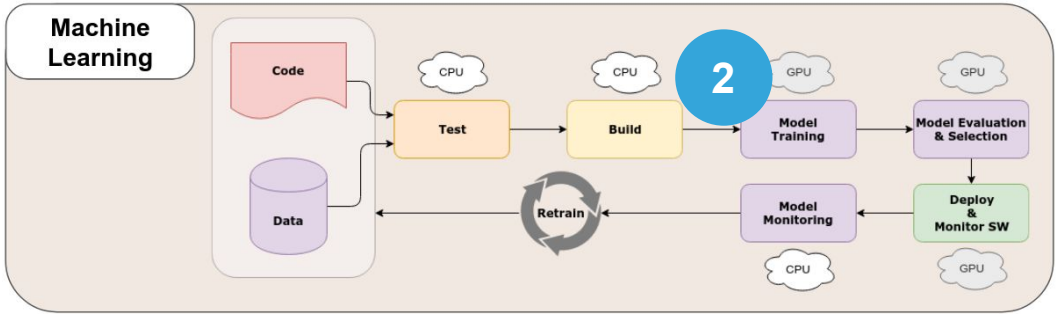
These **artifacts** require...

- Efficient **storing**
  - Model & Data Eviction
- **Versioning**
  - Data
  - Models
- **Documentation**

craftworks AI

A Different Set of Challenges: SE vs. ML

2 Model Training



Model training is **highly critical**:

- Computationally expensive
- Time-consuming
- Determines model quality
- Error-prone
- Expensive errors

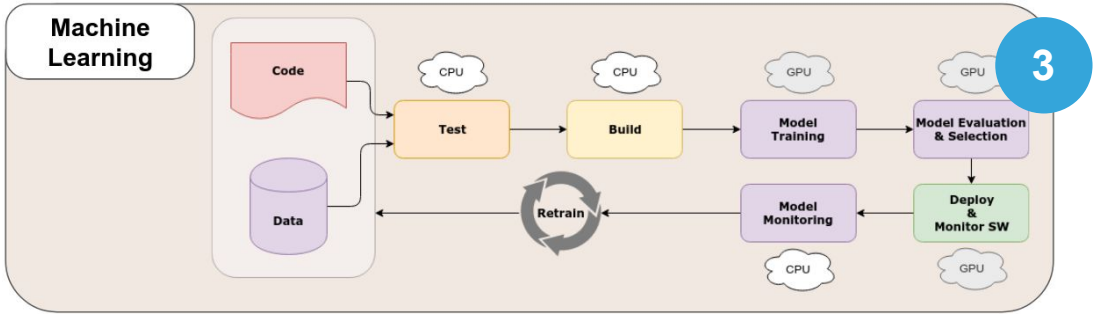
Efficient & **robust training** requires ...

- **Smart testing**
  - Small test-runs,
  - Data validation
- Saving of **intermediate results**

craftworks AI

A Different Set of Challenges: SE vs. ML

3 Model Evaluation & Selection



Pipelines need to be **evaluated before deployment**:

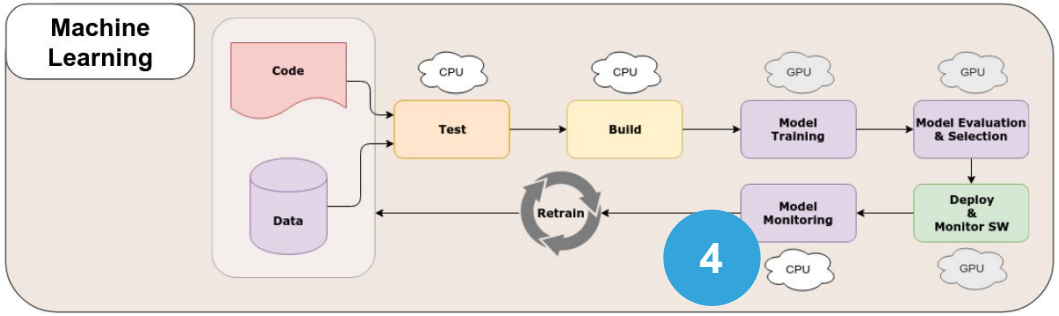
- **Multi-dimensional** evaluation
  - Candidate vs. candidate
  - Incumbent vs. candidate
- **Robust** evaluation
  - Historical data
  - New data
- **Feasible** evaluation
  - "10-fold CV" often not possible

Good evaluation requires ...

- **Documentation** of data & models
- **Feasible** evaluation strategies
- **Flexible deployment**

A Different Set of Challenges: SE vs. ML

4 Monitoring & Degradation Measuring



Pipeline performance may deteriorate over time:

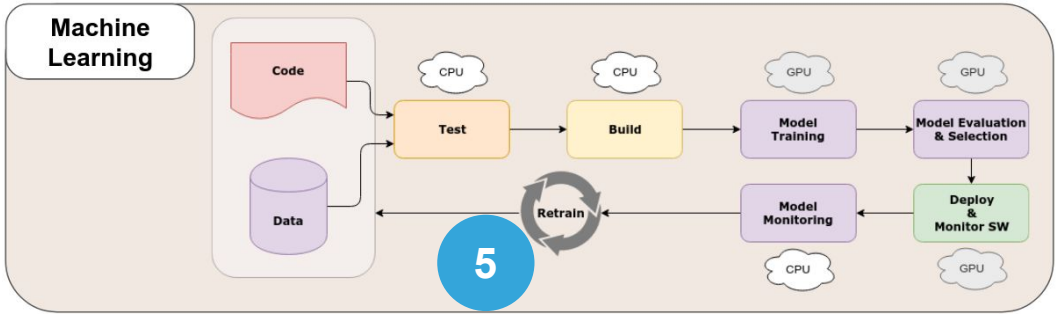
- **Distribution** of data changes (non-stationarity):
  - Increasing data size,
  - Seasonality,
  - Change of customer behavior,
  - New classes emerge, old vanish

Potentially changing data requires ...

- Continuous **monitoring** of **input feature space**,
- Continuous **evaluation** of **prediction quality**,
- **Real-time** adaptation
  - A/B testing

A Different Set of Challenges: SE vs. ML

5 Retraining



Changing data requires **retraining:**

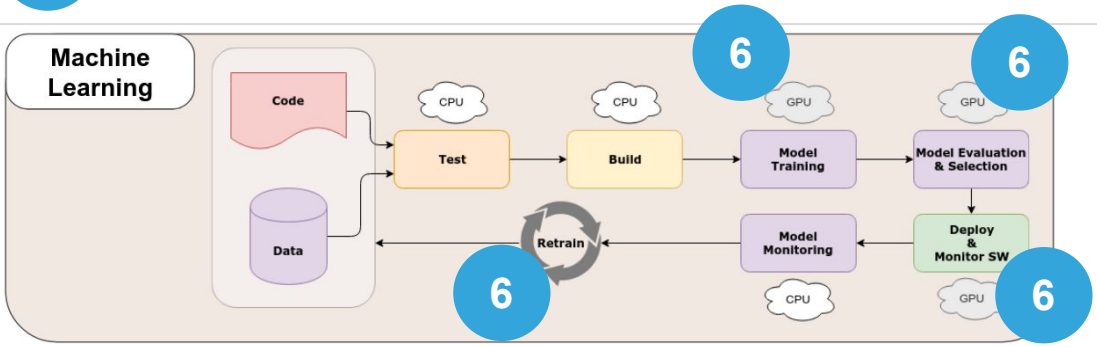
- **Performance**-dependent
- Input-**feature-space**-dependent
- **Time**-dependent (periodical)
- **On-demand** (“button-press”)

Retraining requires ...

- **Reproducibility,**
- **Selection of data** used for training
  - Only fraction of data needed?
  - Newer data more relevant?
  - Class distribution changed?

A Different Set of Challenges: SE vs. ML

6 Hardware



Depending on the workflow stage, different **hardware** may be required:

- (clusters of...)
- CPUs,
- GPUs,
- TPUs
- ...

Increasing **hardware complexity** requires ...

- **Availability** at required time,
- Smart scheduling and testing to **minimize costs**,
- **Maximize utilization** of existing (on-premise) hardware

CI/CD for Machine Learning

Continuous Integration and Delivery for *(on-premise)* Machine Learning Applications

1. CI/CD for Software Engineering

2. A Different Set of Challenges: SE vs. ML
3. CI/CD for Machine Learning
4. Use Case: InvexML

craftworks AI

CI/CD
ML

CI/CD for Machine Learning

CI/CD for ML is of Great Importance

In **production settings** we need **ML pipelines** that are

- **Up-to-date**
  - Models that are adapted to **changes in data**
  - Timely and safe productionalization of **changes in code** (e.g. data processing steps)
- **Documented**
  - Code, data & model **versioning**,
  - **Prediction quality**

CI/CD
ML

CI/CD for Machine Learning

There is a Variety of Tools that Help us

Sonatype Nexus

Jenkins

DVC

Data Science Version Control System

mlflow

pytest

ANSIBLE

Kubeflow

craftworks AI

CI/CD for Machine Learning

CI Tools - On premise

Jenkins

Used for

- Continuous Integration
- Configuration as Code
- Graphical representation of pipeline

Features

- Active development, open source
- Powerful pipeline language
- Many plugins
- Sometimes lack of documentation

CI/CD
ML

mlflow

CI/CD for Machine Learning

CI Tools - MLflow

MLflow - Tracking

- Python/R interface for test runs
- Track parameter, record metrics + artifacts
- Storage local or tracking server
- UI

MLflow - Projects

- Single entrance point like train / validate
- Environments docker / conda

MLflow - Models

- Serve model as REST endpoint

CI/CD
ML

CI/CD for Machine Learning

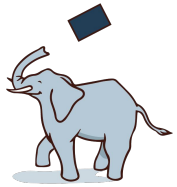
CI Tools - K8 Related

K8s + Spinnaker

- Delivery platform - Jenkins integration
- multi cloud
- Node GPU support, red/black, green/blue, canary

Kubeflow

- Jupyter based, multi environments
- Pipelines defined in Python code and transformed



Pachyderm

- Pipeline (scrap, clean, ..) definitions as json,
- CLI access to artifacts / files per commit
- Special directories for artifacts in docker container

CI/CD for Machine Learning

CI Tools - Data/Model Versioning

Git

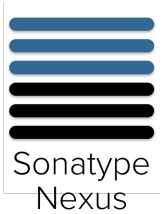
- In case no data is deleted

GitLFS (**L**arge **F**ile **S**ystem)

- Git extension

DVC (**D**ata Science **V**ersion **C**ontrol System)

- Tracks ML models and data sets
- In addition to git, local or remote storage



Nexus

- Version tracking with filename, custom tool for clean up

CI/CD
ML

CI/CD for Machine Learning

Outlook

- Specialized cloud offering SaaS (proprietary)
- Trend for (semi) UI tools (dashboards)
- “Deploy jupyter” - no transformation to production code
- Glue code by provider (Jupyter-as-a-REST-service)

  \+ Fast exploration to production but
  \- Results often in poor code quality (no tests etc.)

CI/CD for Machine Learning

Continuous Integration and Delivery for *(on-premise)* Machine Learning Applications

1. CI/CD for Software Engineering

2. A Different Set of Challenges: SE vs. ML

3. CI/CD for Machine Learning

4. Use Case: InvexML

Use Case: InvexML

Use Case: InvexML

What?

“System to extract structured data from documents”
(mostly PDF invoices)

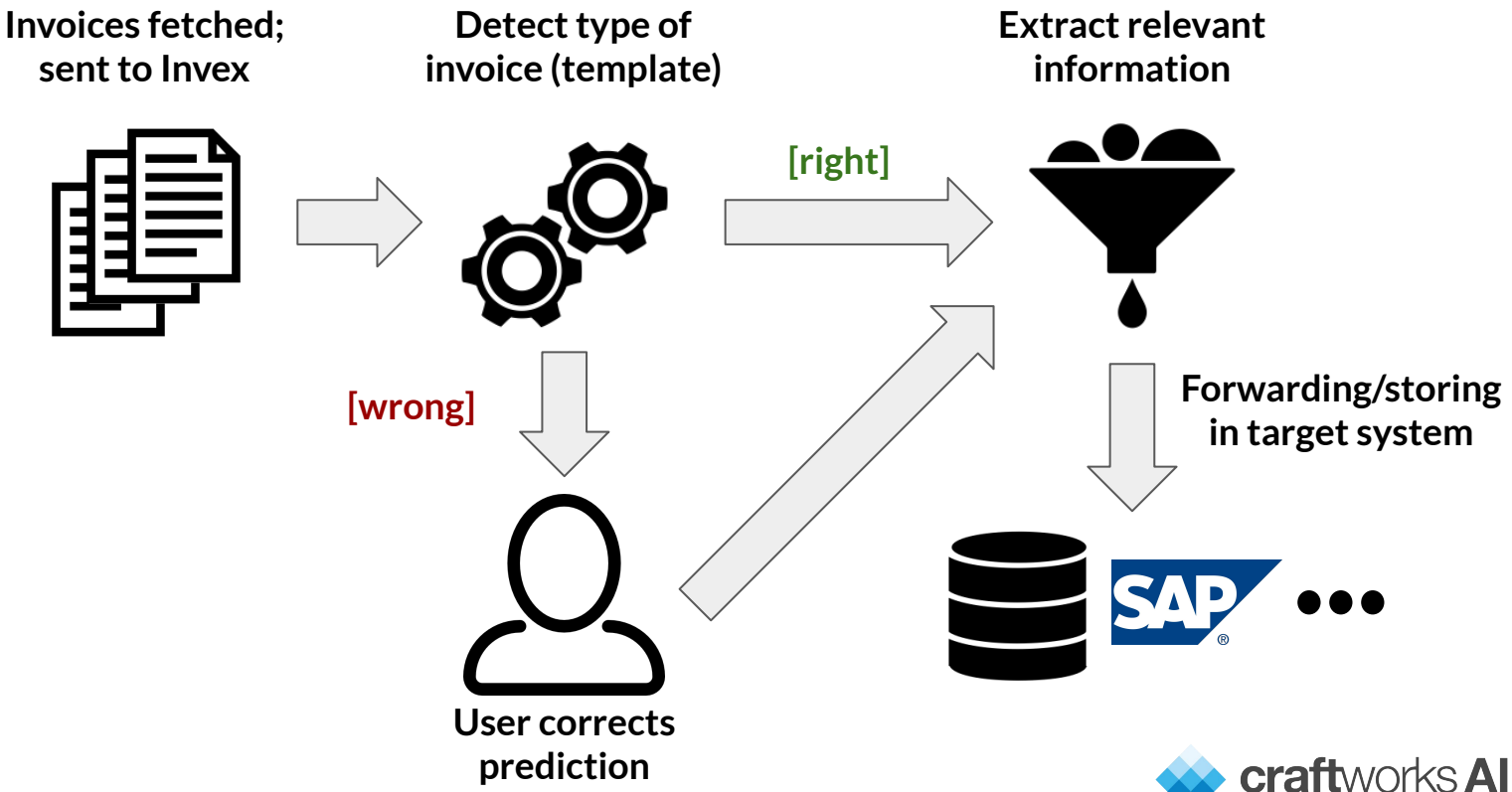
- **User creates templates** to define data to extract
- **Batch upload** of documents
  1. Data extraction
  2. Results accessible over REST Endpoint
- **QA View** where user can check and correct results

4

Use Case: InvexML

Use Case: InvexML

High-level Process of Example Use Case of Invex



craftworks AI

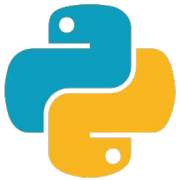
Use Case: InvexML

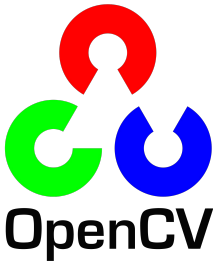
Use Case: InvexML

Software Stack

Backend

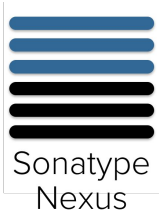
Computer Vision & Deep Learning





Frontend

Misc:

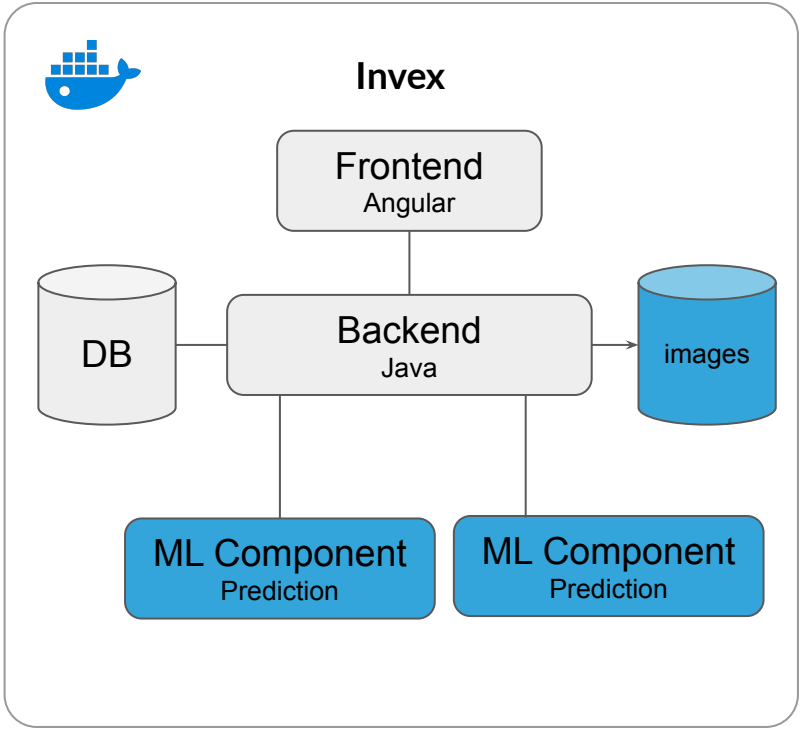


4

Use Case: InvexML

Use Case: InvexML

High-level Architecture



Use Case: InvexML

Use Case: InvexML

Constraints

- **On-premise** training
- **Shared resources:**
  retraining without interference with Data Scientists
- **Remote** hosting

4

Use Case:
InvexML

Machine Learning Perspective

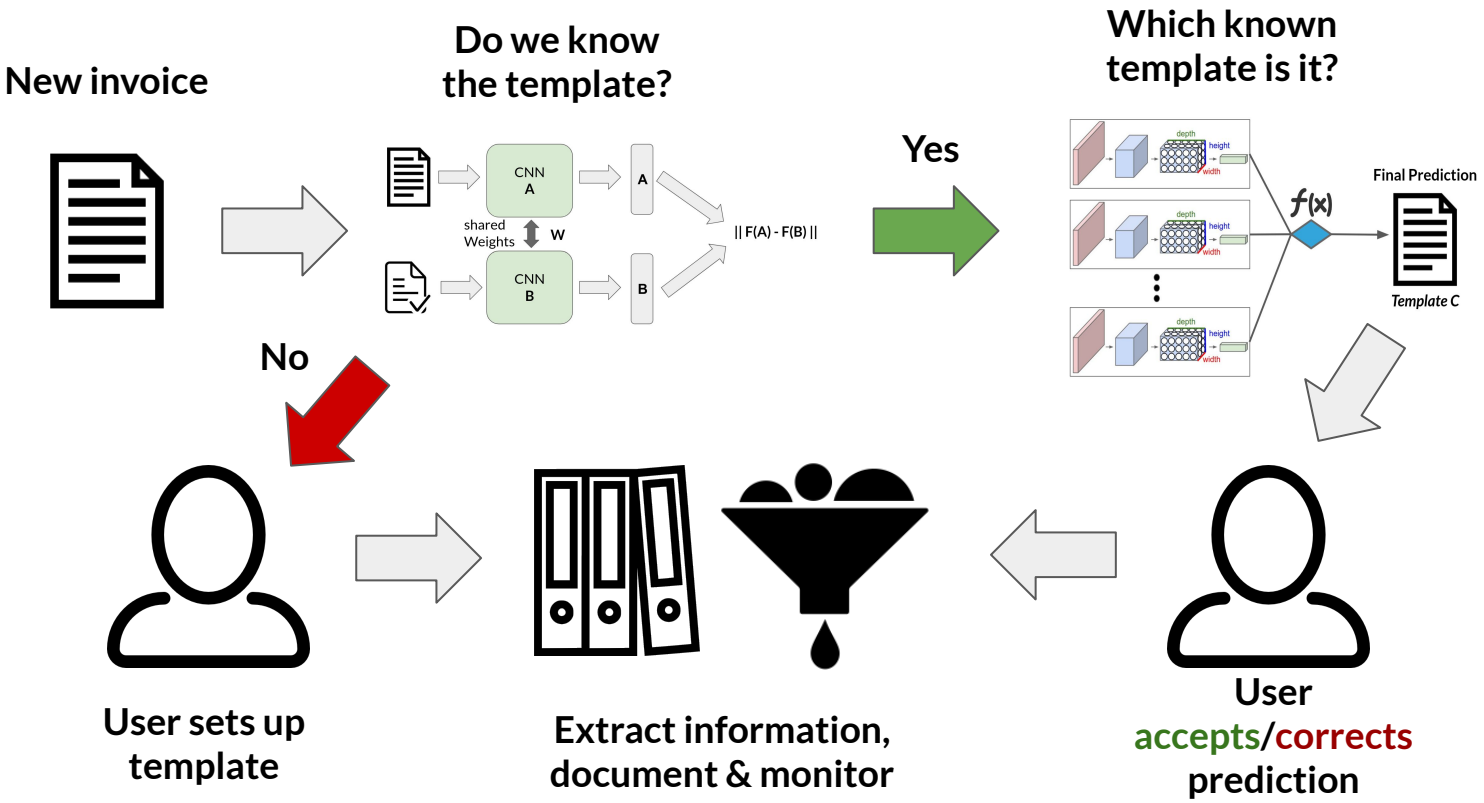
craftworks AI

4

Use Case: InvexML

Use Case: InvexML

ML Perspective on Process

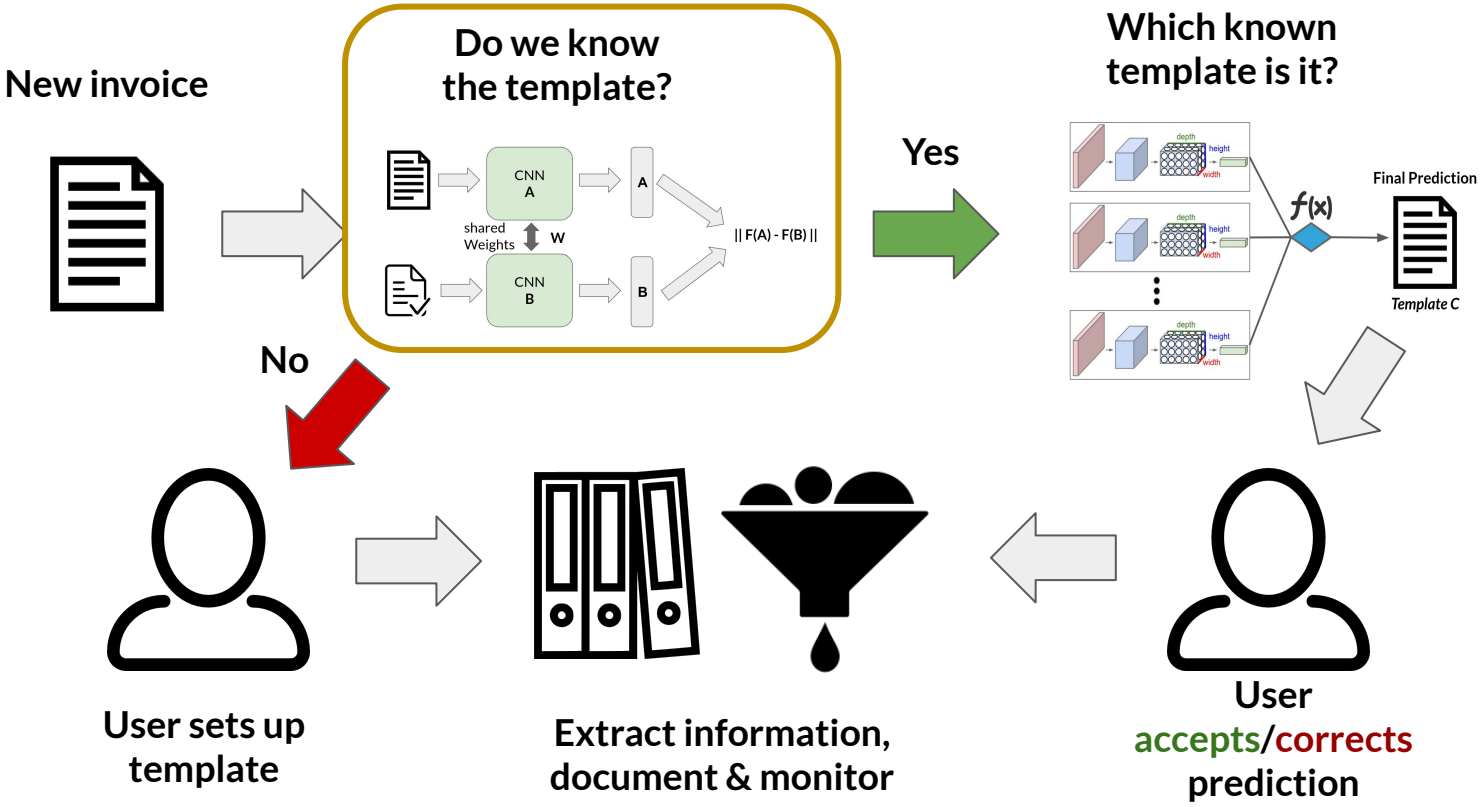


4

Use Case: InvexML

Use Case: InvexML

ML Perspective on Process

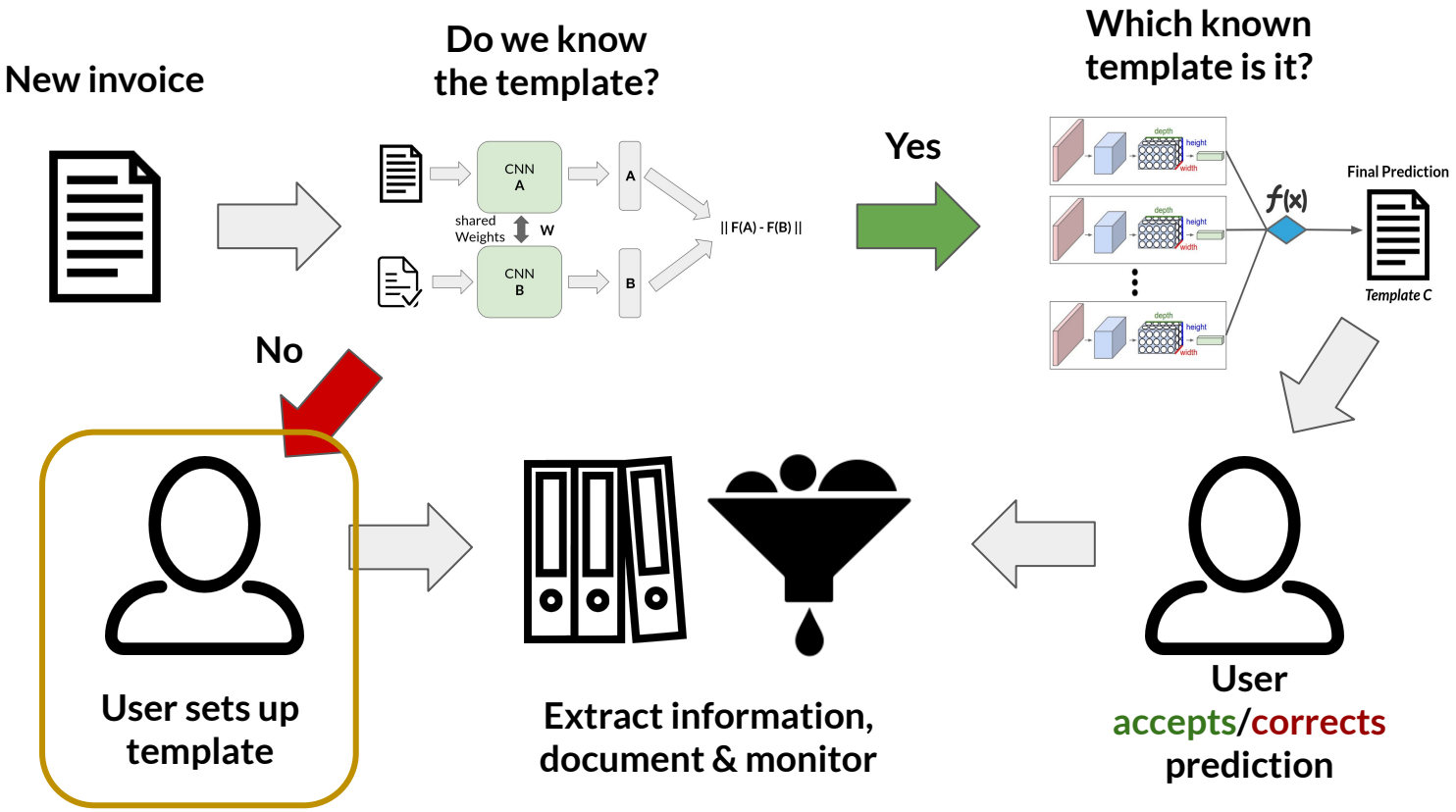


4

Use Case: InvexML

Use Case: InvexML

ML Perspective on Process

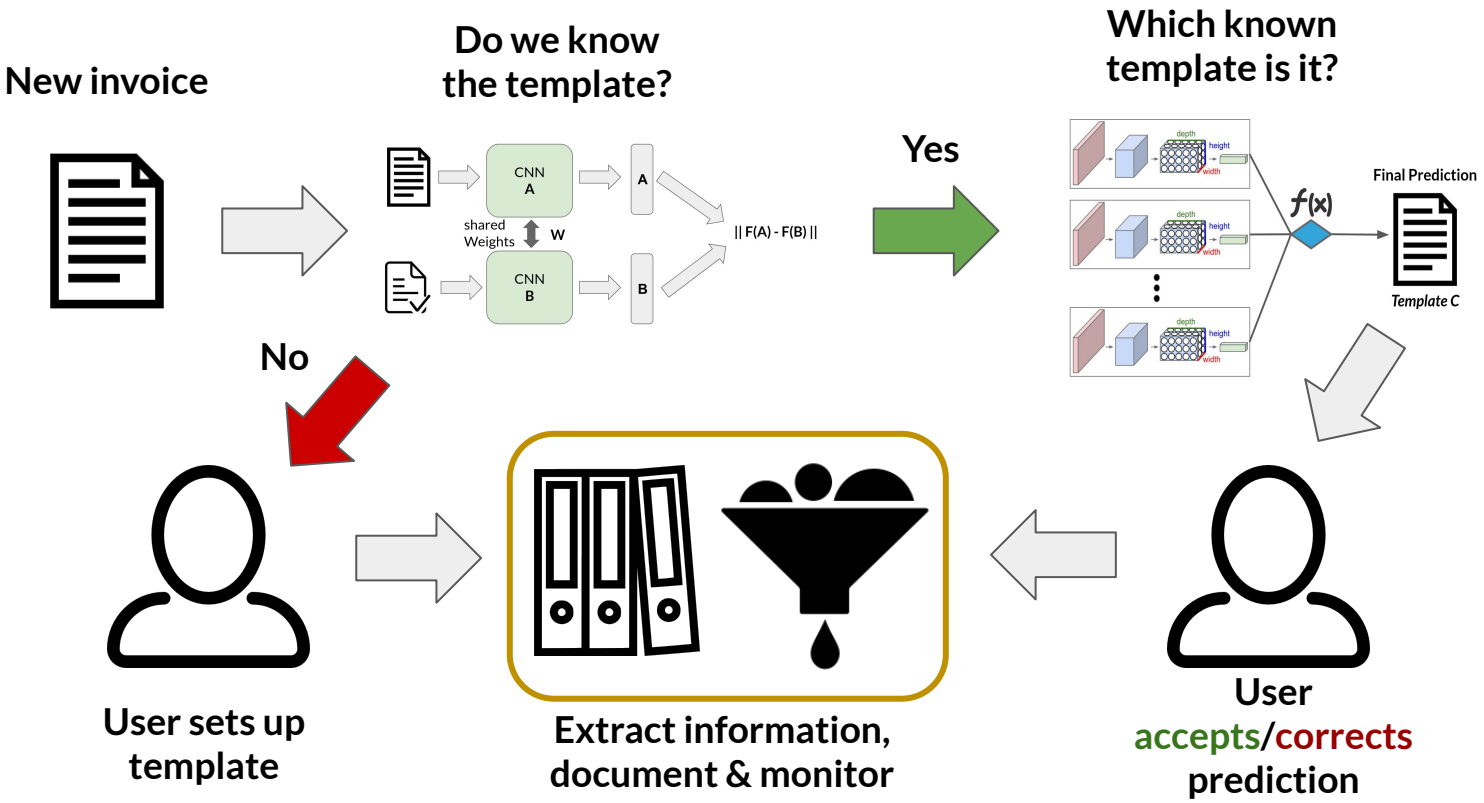


4

Use Case: InvexML

Use Case: InvexML

ML Perspective on Process

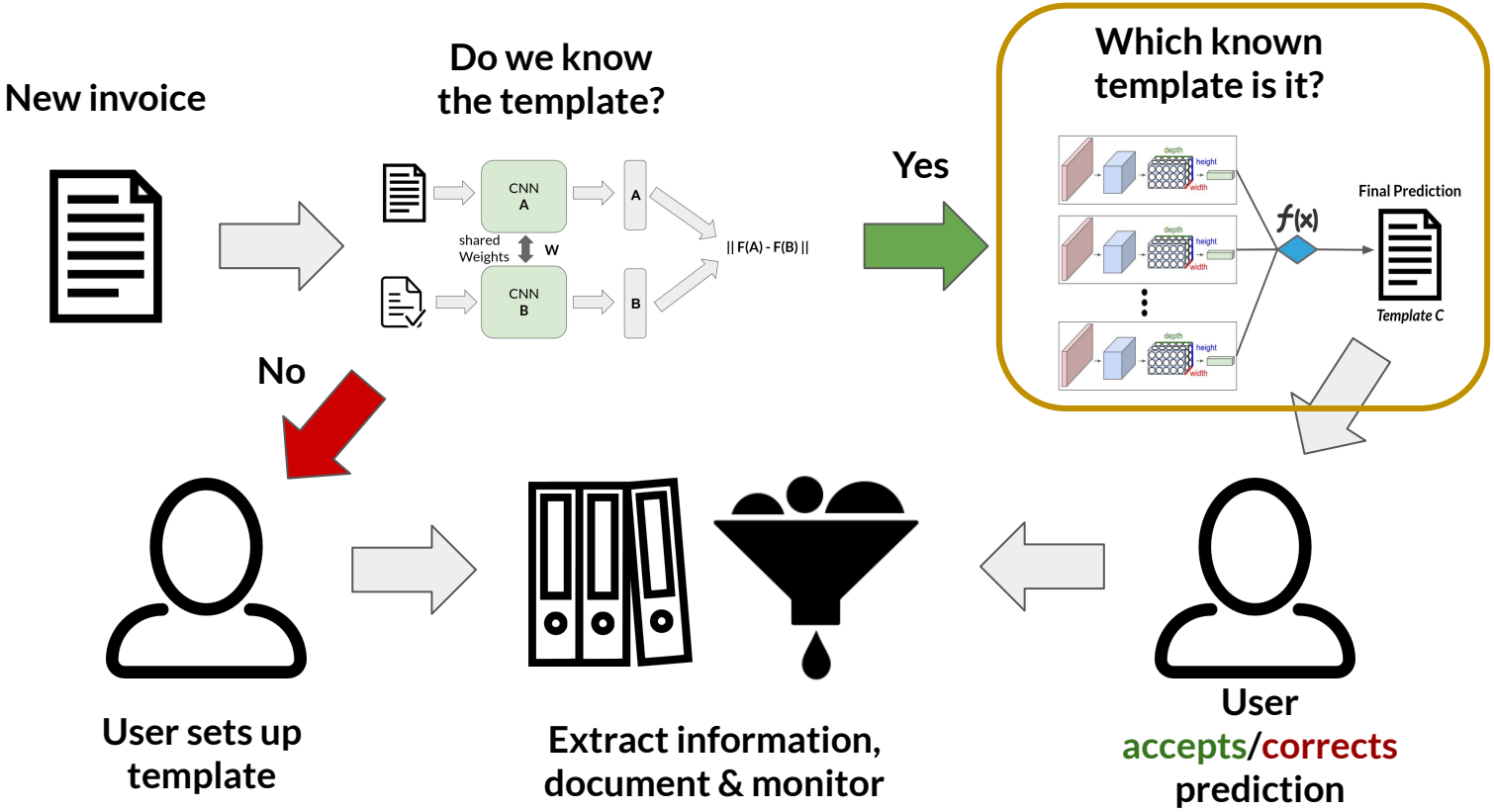


4

Use Case: InvexML

Use Case: InvexML

ML Perspective on Process

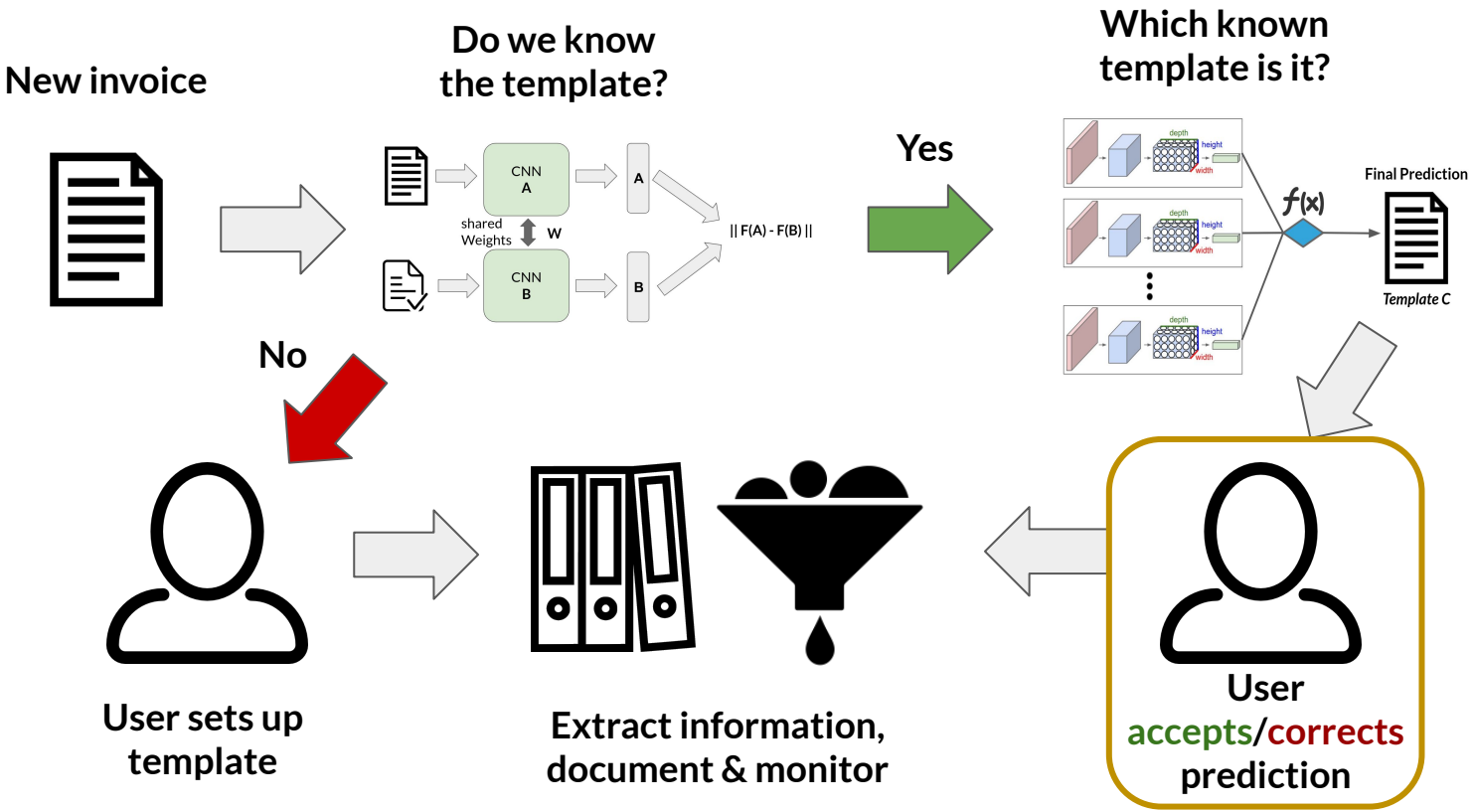


4

Use Case: InvexML

Use Case: InvexML

ML Perspective on Process

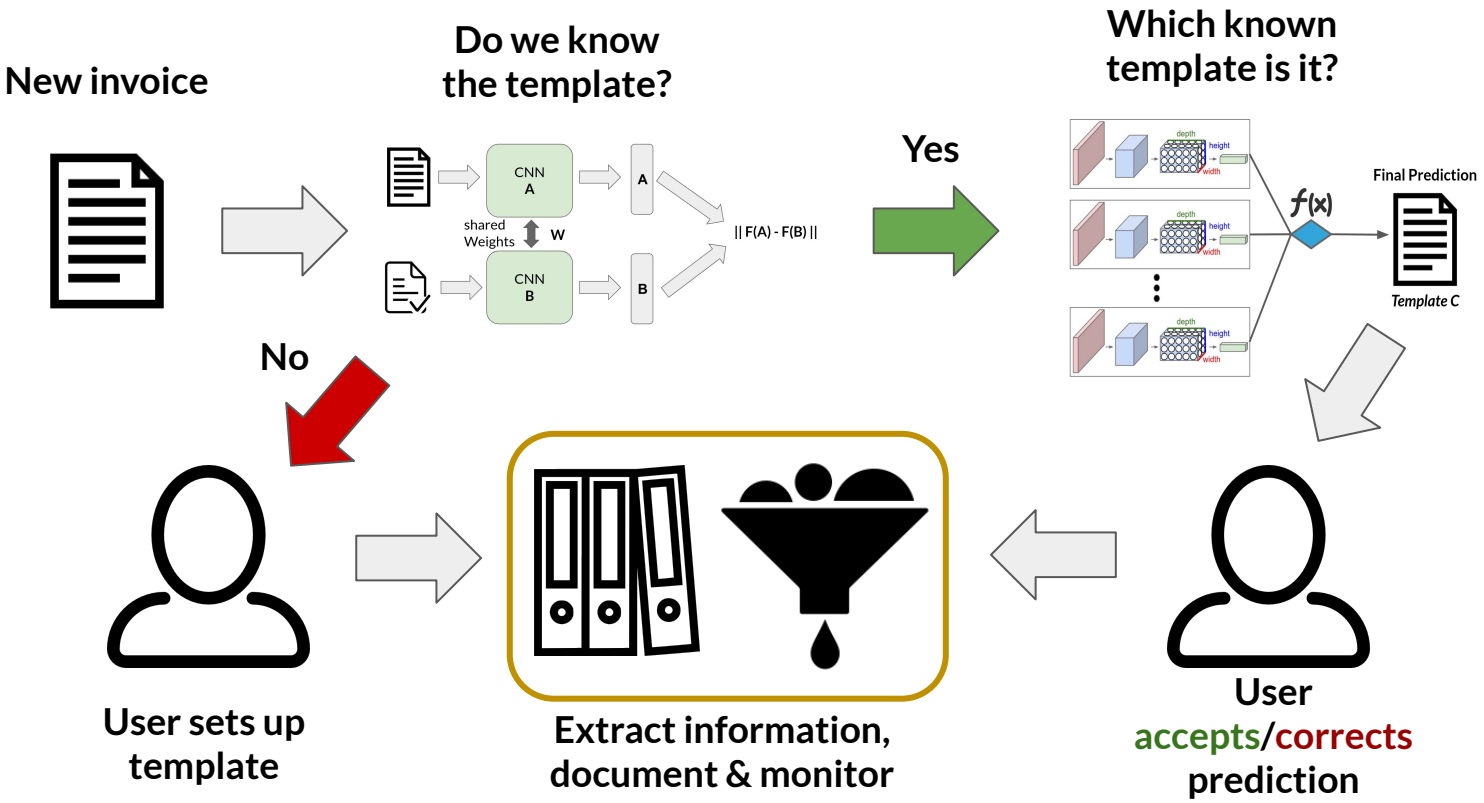


4

Use Case: InvexML

Use Case: InvexML

ML Perspective on Process

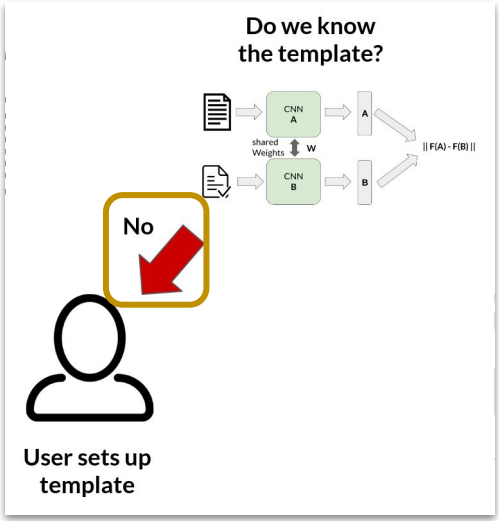


Use Case: InvexML

Retraining

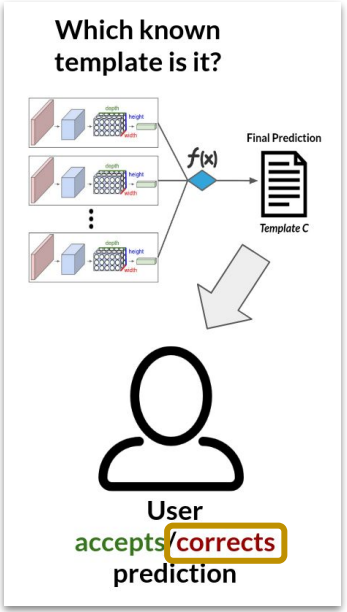
Retrain IF ...

 # unknown templates > threshold



OR

classification accuracy < threshold



4

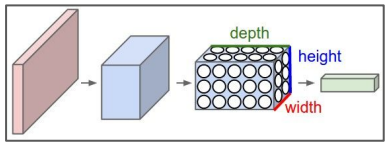
Use Case: InvexML

Use Case: InvexML

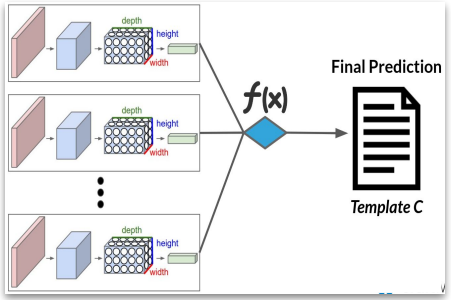
Model Evaluation & Selection

- **Evaluation** result and **user preference** may lead to usage of
  - (a) Single model,
  - (b) Ensemble,
  - (c) Parallel deployment of multiple models & dynamic, real-time evaluation

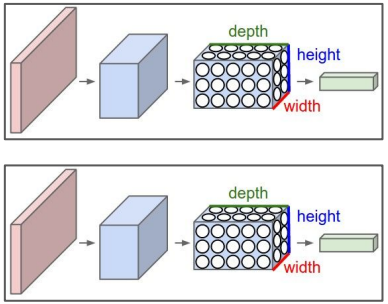
a) Single model



b) Ensemble



c) Parallel



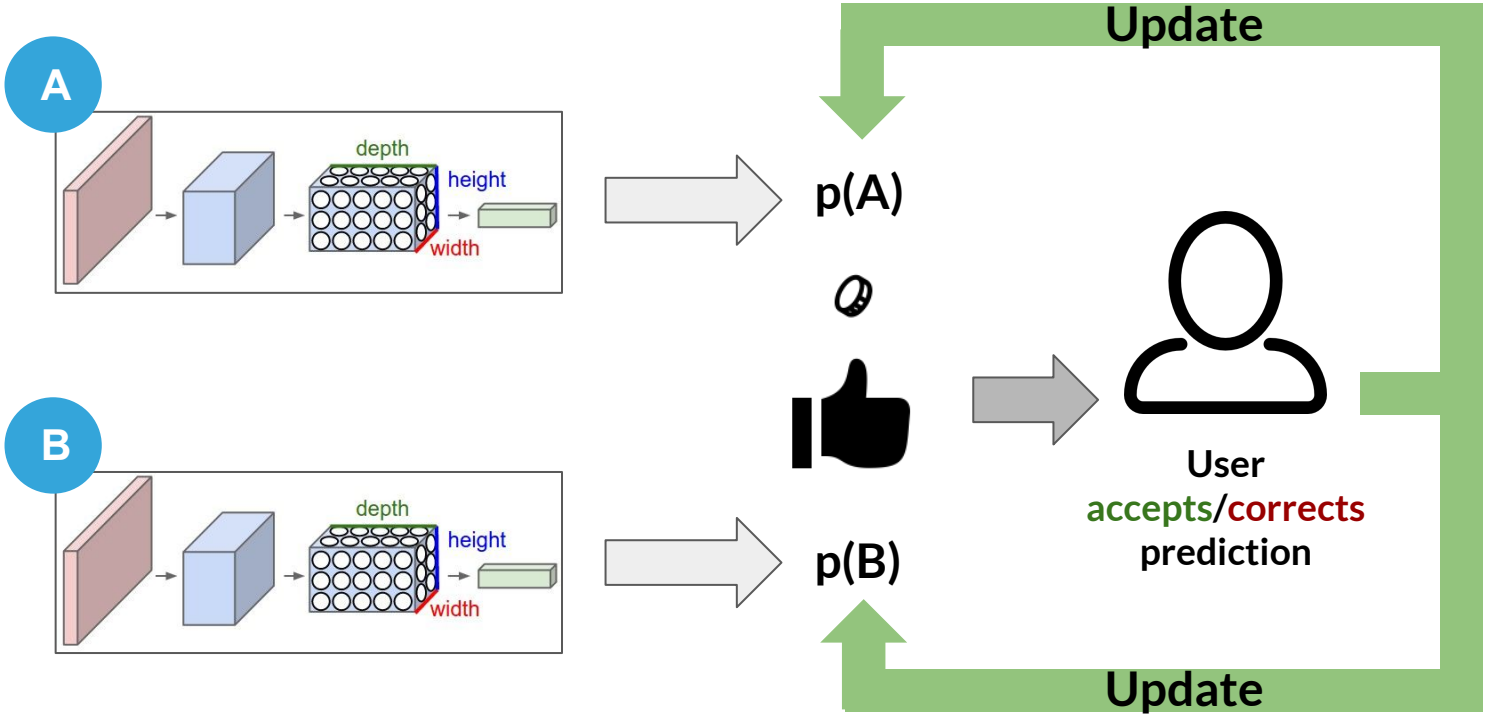
craftworks AI

4

Use Case: InvexML

Use Case: InvexML

Parallel Deployment & Dynamic Real-Time Evaluation



craftworks AI

Use Case:
InvexML

CI/CD Perspective

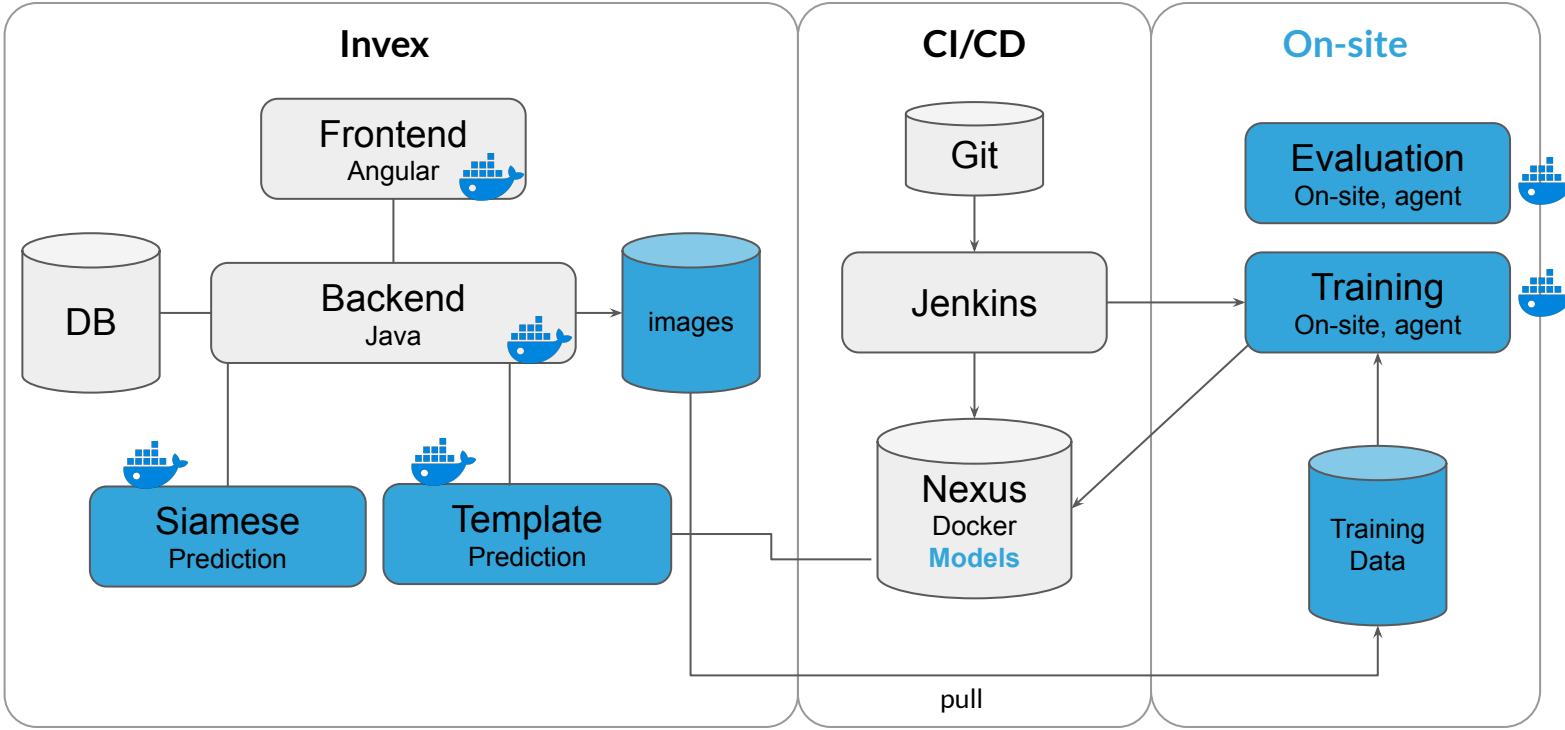
craftworks AI

4

Use Case: InvexML

Use Case: InvexML

High-level Architecture - Extended



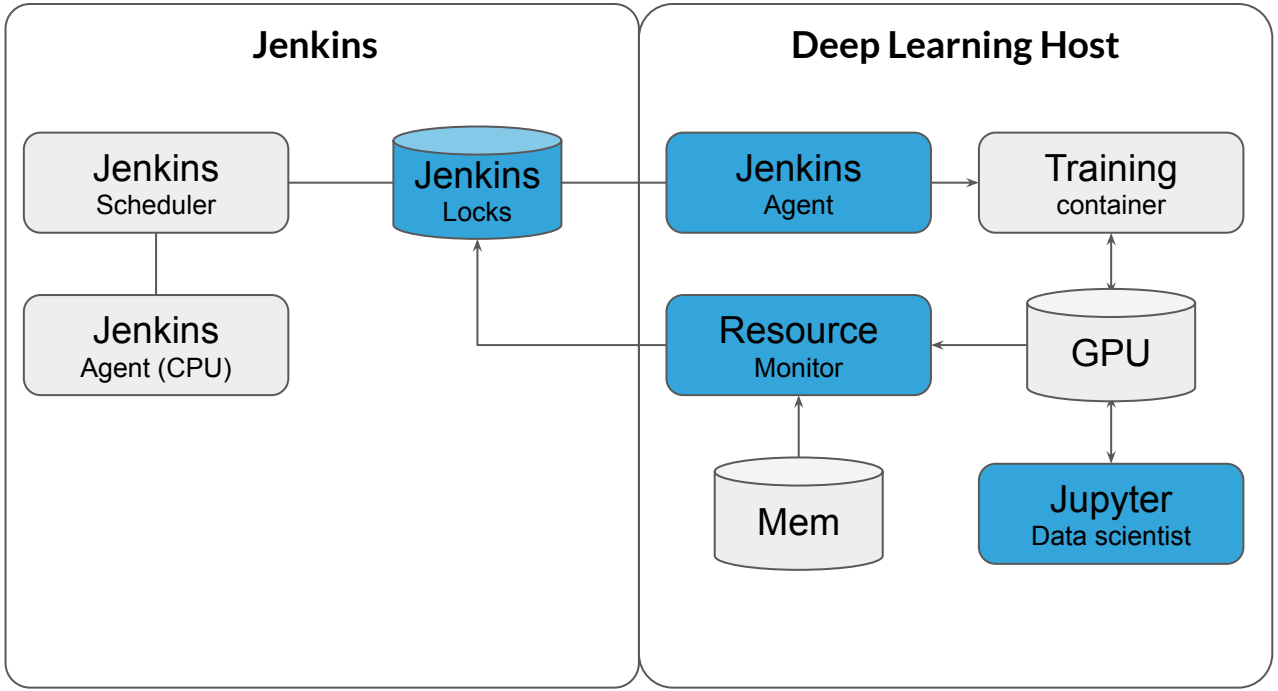
craftworks AI

4

Use Case: InvexML

Use Case: InvexML

Resource Management



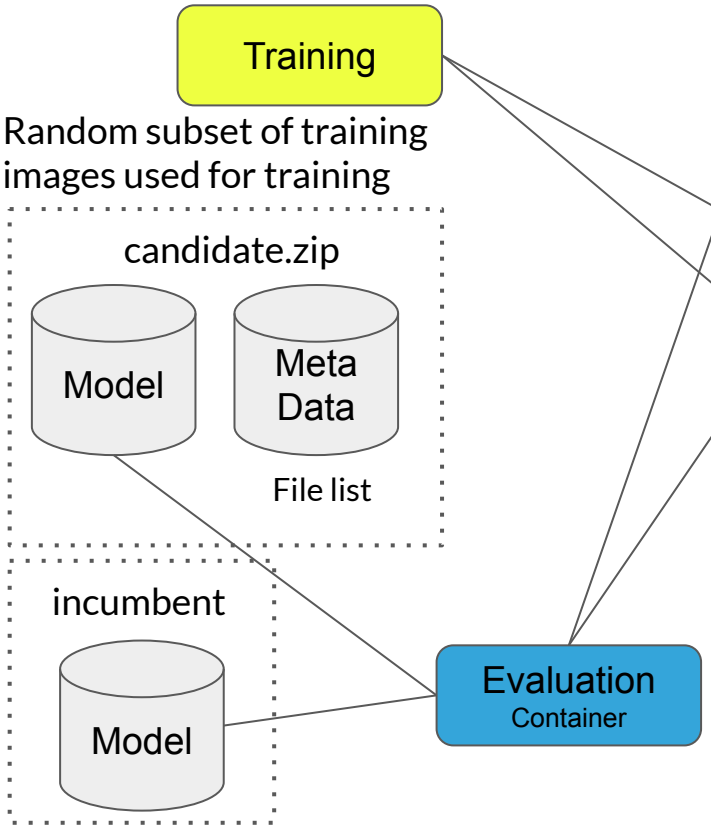
craftworks AI

4

Use Case: InvexML

Use Case: InvexML

Data Versioning & Evaluation



Global image table with all images

img1.jpg	templ1	holdout
img2.jpg	templ1	
..	..	..
img3.jpg	templ2	holdout
img4.jpg	templ2	
img5.jpg	?	

craftworks AI

Use Case: InvexML

Use Case: InvexML

Model Versioning

- **Model versioning**
  - **Major.Minor.Patch** (specified by Data Scientist)
  - Build ID automatically increased - global unique

Build ID example:

`Project-0.18.0-build.112`

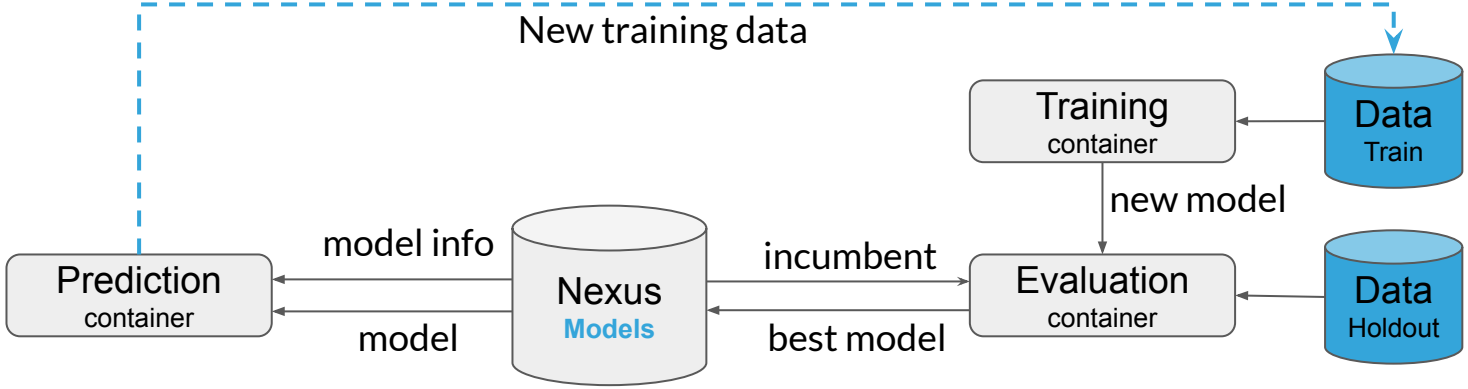
craftworks AI

4

Use Case: InvexML

Use Case: InvexML

Model Deployment




```
{
     "fixedVersions": ["0.2.0", "0.2.1"] # blocked from eviction
     "bestModels": { # these are the models used by invex
          "repository": "ml-invex",
          "mode": "A/B",
          "modelA": "invex/models/cw_prod/model-0.2.1-build.123.zip",
          "modelB": "invex/models/cw_prod/model-1.0.2-build.130.zip"
     }
}
```

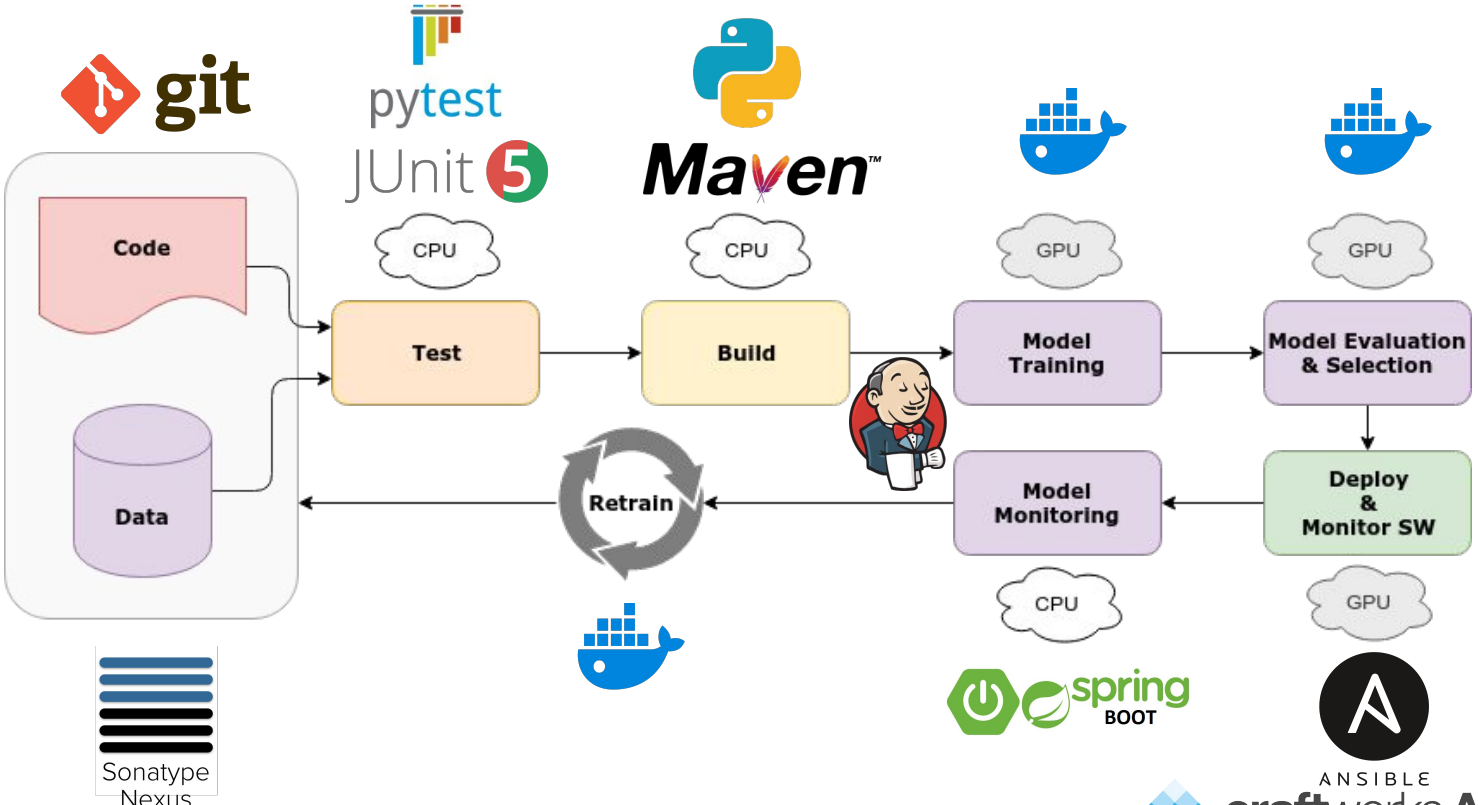
craftworks AI

4

Use Case: InvexML

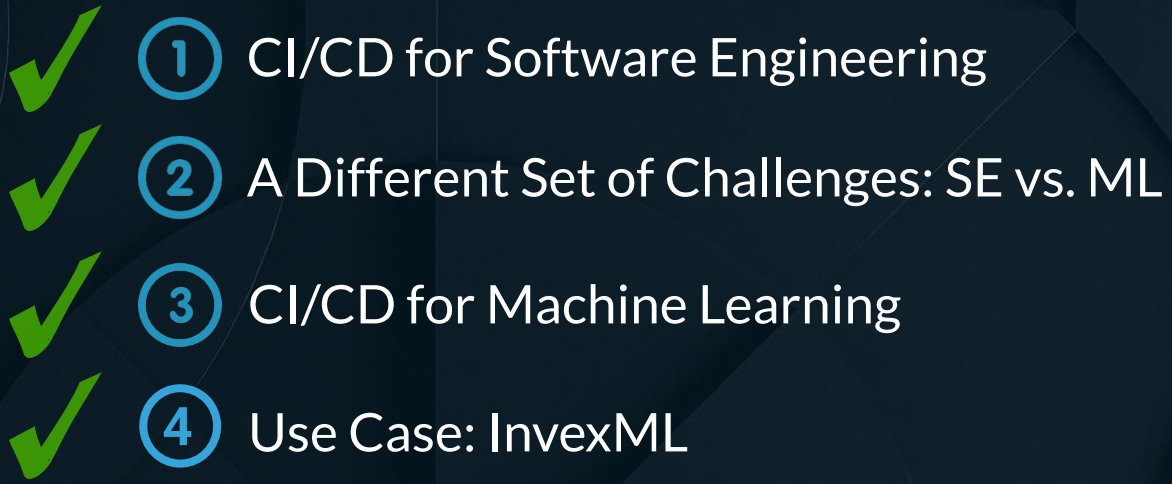
Use Case: InvexML

Putting Things Together



CI/CD for Machine Learning

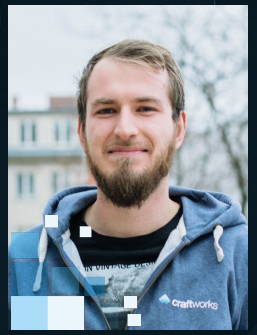
Continuous Integration and Delivery for *(on-premise)* Machine Learning Applications



craftworks AI

craftworks AI

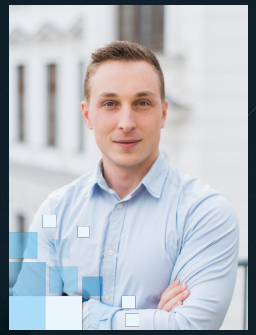
We develop prize-winning
Industrial AI



Bernhard Redl

Head of Infra @ craftworks

bernhard.redl@craftworks.at



Simon Stiebellehner

Head of AI @ craftworks
Lecturer @ WU Wien & FH Wien

simon.stiebellehner@craftworks.at

Join us!

Computer Vision Engineer / Data Scientist

(Senior) Web Developer

Marketeer/Growth Hacker

Agile Project Manager

No fit for you? Send us your application anyway - we are always looking for **talent**.

jobs@craftworks.at

Research with us!

Are you a student?

We offer exciting research **internships** and **thesis** topics!

Currently, topics are available in the **areas** ...

Reinforcement Learning

Unsupervised Deep Learning

talent@craftworks.at

craftworks.at/working-at-craftworks/

craftworks AI