Industrial Cloud Security and Machine Learning

Prof. Dr. Christoph Reich
rch@hs-furtwangen.de
Institute for Data Science, Cloud Computing and IT Security
Idacus.hs-furtwangen.de
Hochschule Furtwangen University
Profile
Prof. Dr. Christoph Reich

- professor at the faculty of computer science at Furtwangen University
- teaches: network technologies, IT security, machine learning, and distributed systems
- CISO of the HFU
- since 2009 head of the institute Data Science, Cloud Computing and IT Security
Institute for Data Science, Cloud Computing und IT-Sicherheit (IDACUS)

Facts:
- head: Prof. Dr. Christoph Reich (rch@hs-furtwangen.de)
- 4 Professors and 13 researchers
- 8 PhDs, 12 masters, 18 bachelors
- actual 12 research projects
- idacus.hs-furtwangen.de

Research area:
- Distributed system
- Cloud Computing
- IT security
- IoT/Industry 4.0
- Maschine Learning
• Smart-Factory, Use Cases
• Machine Learning
  • Halfback, SensoGrind, HMT
  • (data quality, model quality, devOps)
  • Machine Learning Operations (12min)
• Security IoT and ML
• Architecture
• Blockchain-Accountability (12min)
• Security Monitoring of HPC containers (12min)
Smart Factory

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)

https://www.it-zoom.de/it-mittelstand/e/auf-dem-weg-zur-smart-factory-28622/
Smart Factory

Customer order: 50 gears till Monday!

Magazine empty, please fill!

Capacity through Friday booked out!

Saturday I can not come.

I take the filling of the magazines.

Switching to me!

I can work this Saturday.

Must be in 2h at the outgoing goods!

Legend:

Machine talking!

Human talking!
Applications in Industry 4.0 (CPS)

Process optimization, condition monitoring, remote monitoring, remote maintenance, predictive maintenance, quality control, quality prediction, etc.

Smart Products: How to connect products, self-diagnosis, tracking, etc.

Industrial manufacturing: monitoring, self-diagnosis, one lot production, flexible production, etc.
Machine Learning
Research Project A: Predictive Maintenance
Predictive Maintenance

Data Collection → Data Preprocessing → Data Analysis

Time

Machine Condition

Condition is starting to change
Predictive Maintenance

Data Collection → Data Preprocessing → Data Analysis

- Machine Condition is starting to change
- Vibration

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
Predictive Maintenance

Data Collection → Data Preprocessing → Data Analysis

Condition is starting to change

Machine Condition

Vibration

current

month

weeks

bearing failure

Time

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
Predictive Maintenance

Data Collection → Data Preprocessing → Data Analysis

Machine Condition is starting to change

Vibration

Condition

current

maintenance

planed maintenance

bearing failure

Time

Machine Condition

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
HALFBACK
Highly Avialable Smart Factories in the Cloud

04/2017 - 03/2020
Goal: High Availability Production

- Resources
- Processes
- Machines
- Tools
- Quality of work piece

Condition Monitoring
Predictive Maintenance
Quality Prediction, etc.
## AI Methods

**Data Collection** → **Analysis** → **Quality Prediction Predictive Maintenance**

### Preprocessing

<table>
<thead>
<tr>
<th>Problem</th>
<th>Approach</th>
<th>Prediction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time for machine failure</td>
<td>Chronical mining</td>
<td>Machine failure events</td>
</tr>
<tr>
<td>Time for machine failure</td>
<td>Neural networks</td>
<td>Machine componentent failure</td>
</tr>
<tr>
<td>Visual surface defects</td>
<td>Convolutional neural networks</td>
<td>Detection of Surface failure</td>
</tr>
</tbody>
</table>
Production

SME
Broker/Machine as a Service
Research Project
B: Quality Control with a SME

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
Metal Surface Defect Detection

coil
ML Workflow: From Data to Model

Image Collection
First Images, for Proof of Concept

- 109 images 1200x1920px
ML Workflow: From Data to Model

1. Image Collection
2. Image Cutting
Cutting

- Original image 1920x1200px
- Cutting image to 416x416px
ML Workflow: From Data to Model

Image Collection → Image Cutting → Image Labeling (mark defects)
Labeling

- Marking of defects in the images
- Throw away bad images (e.g. blurred images)
ML Workflow: From Data to Model

Image Collection → Image Cutting → Image Labeling (mark defects)

Pre-Processing (CLAHE) with OpenCV
Verbesserung durch Datenvorverarbeitung: Contrast Limit Adaptive Histogram Equalization (CLAHE)

Original

after CLAHE Filter
Augmentierung

- Für jedes Foto wurden drei weitere Fotos erstellt durch Augmentierung
- Welche Augmentierung dabei verwendet wird, wird per Zufall entschieden
- Durch das Augmentieren mit dem Programm Albuments werden alle Bounding Boxen automatisch mit gedreht / gespiegelt

Original  |  Drehung 270°  |  Gespiegelt vertikal  |  Drehung 180°
ML Workflow: From Data to Model

Image Collection -> Image Cutting -> Image Labeling (mark defects)

training

Augmentation (flip, rotate)

OpenCV
Pre-Processing (CLAHE)
YOLO (You Only Look Once)
ML Workflow: From Data to Model

Image Collection → Image Cutting → Image Labeling (mark defects)

- Image Cutting
- Augmentation (flip, rotate)
- Pre-Processing (CLAHE)
- OpenCV

Model good enough → training → YOLO

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
ML Workflow: From Data to Model

Image Collection → Image Cutting → Image Labeling (mark defects)

- Pre-Processing (CLAHE)
- Augmentation (flip, rotate)
- OpenCV

YOLO

training

Model good (if better then use new one)

Usage for defect detection

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
Results

Prof. Dr. Ch. Reich (rch@hs-furtwangen.de)
Research Project C: Prozess Optimization
SensorGrind

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
Grind Burn Prediction & Data Augmentation

Grinding Burn Prediction with Artificial Neural Networks
based on Grinding Parameters

Christian Reser and Christoph Reich
Institute for Cloud Computing and IT Security
Furtwangen University of Applied Science
Furtwangen, Germany
{christian.reser, christoph.reich}@hs-furtwangen.de

DCGAN-Based Data Augmentation for Enhanced Performance of Convolutional Neural Networks

Christian Reser and Christoph Reich
Institute for Data Science, Cloud Computing and IT Security
Furtwangen University of Applied Science
Furtwangen, Germany
Email: (christian.reser, christoph.reich)@hs-furtwangen.de
Need for IT Security
# Need for IT Security

Average annualized cost of cyber attacks on companies in selected countries in 2018
(in million U.S. dollars)

<table>
<thead>
<tr>
<th>Country</th>
<th>Average Cost (in million U.S. dollars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>27.37</td>
</tr>
<tr>
<td>Japan</td>
<td>13.27</td>
</tr>
<tr>
<td>Germany</td>
<td>13.12</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>11.46</td>
</tr>
<tr>
<td>France</td>
<td>9.72</td>
</tr>
<tr>
<td>Singapore</td>
<td>9.32</td>
</tr>
<tr>
<td>Canada</td>
<td>9.20</td>
</tr>
<tr>
<td>Spain</td>
<td>8.16</td>
</tr>
<tr>
<td>Italy</td>
<td>5.61</td>
</tr>
<tr>
<td>Brazil</td>
<td>7.24</td>
</tr>
<tr>
<td>Australia</td>
<td>6.79</td>
</tr>
</tbody>
</table>
Need for IT Security

CVE entry of the last years (CVE: security vulnerabilities and Exposures)

https://www.cve.org/About/Metrics#PublishedCVERecords

CVE entry of the last 4 years

https://www.cve.org/About/Metrics#PublishedCVERecords
Cyber-attack

Pegasus spyware used to snoop on Catalan politicians
19 April 2022

'Exceptionally dangerous'
Critical infrastructure entities on red alert over new ICS malware
14 April 2022

Credit card industry standard revised to repel card-skimmer attacks
14 April 2022

African banking sector targeted by malware campaign
13 April 2022

OpenSSH 9.0 future proofs against quantum computing attacks
12 April 2022

Attackers abusing Spring4Shell flaw to spread Mirai
11 April 2022

PacketStreamer
New tool can aid research by revealing potential hacking behaviors
11 April 2022

Third member of FIN7 cybercrime gang jailed over card skimming scheme
09 April 2022

Wake-up call
Is the infosec skills gap causing a mental health crisis?
07 April 2022

Point of assail?
UK retailer The Works blames store closures on POS problems after attack
06 April 2022

https://portswigger.net/daily-swig/cyber-attacks
Known Attacks - Mirai Botnet (Malware)

- Created botnets with everyday objects: Router, Digital Video Recorder, TVs, etc.
- Standard Passwords have been used
- Goal: DDoS
- 2016: 500,000 IoTs corrupted
- It is expected more than 3,000,000 IoTs.

Countermeasures:
No standard password
Known Attacks - WannaCry (Ransomware)

- May 2017 - 3 days 300,000 Windows computer in 150 nations
- Crypt data and tried to get ransom money

**Countermeasures:**
- 8 weeks before the outbreak, there have been provided a Windows
- Periodical data backup
- Do not open unknown appendix
- Limit or block access to data and systems

estimated damage billions of dollars

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
Industry 4.0
Infrastructure
Cyber Attacks

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
Industry 4.0 and Cloud and ML

Cloud Gateway (Edge Gateway, IoT Gateway)

CPS: Cyber Physical System

Cloud

virtual sensor/actors

transform

ERP
Level
Management Level
(MES: Manufacturing Execution System)
Supervision Level
(SCADA: Supervisory Control and Data Acquisition)
Control Level
(PLC: Programmable Logic Controllers)
Sensors/Actors

Machine A

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
Architecture of Industry Cloud

- Attack on a machine
- Attack on communication
- Attack on Cloud infrastructure

Virtual Resources
(Machines, sensors, actors, PLC, SCADA, MES, ERP, ….)

Smart Factory as a Service (communication, deploy on demand, scalability, …)

Application Services
- Condition Monitoring
- Process-Control and Monitoring
- Maintenance Prediction
- Product-quality

System Services
- Info-Extractor
- Machine Learning
- domain knowledge
- Simulation

Cloud Gateway

external services/information
Architecture of Industry Cloud

- Attack on a machine
- Attack on communication
- Attack on Cloud infrastructure

Virtual Resources (Machines, sensors, actors, PLC, SCADA, MES, ERP, ….)

Smart Factory as a Service (communication, deploy on demand, scalability, …)

Application Services
- Condition Monitoring
- Process-Control and Monitoring
- Maintenance Prediction
- Product-quality

System Services
- Info-Extractor
- Machine Learning
- domain knowledge
- Simulation

Cloud Gateway

Security Goals:
CIA (Confidentiality, Integrity, Availability)
Authenticity, Liability, Privacy

External services/information

Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
Security Threats of a Blockchain-Based Platform for Industry Ecosystems in the Cloud

Philipp Ruß*; Jan Studt†; Christoph Reich*

*Institute for Data Science, Cloud Computing and IT-Security (IDMCUS) – Furtwangen University of Applied Sciences, Furtwangen, Germany
†Email: philipp.russ; jan.studt, christoph.reich@hs-furtwangen.de

Abstract—In modern industrial production lines, the integration and interconnection of various manufacturing components, like robots, laser cutting machines, welding machines, and execution implemented as smart contracts. While the BC itself must be generally secure, the security requirements for the broad KOSMs ecosystem which feeds the BC and

Security Threats of Industry Ecosystems in the Cloud

<table>
<thead>
<tr>
<th>Exposure</th>
<th>Threat</th>
<th>Impact</th>
<th>Risk</th>
<th>Vulnerability</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td>Cloud Infrastructure Information Discovery</td>
<td>Low</td>
<td>Middle</td>
<td>Low</td>
<td>User account management, least privilege, periodic audits</td>
</tr>
<tr>
<td></td>
<td>Public Facing Applications</td>
<td>Critical</td>
<td>Low</td>
<td>Low</td>
<td>Firewall, access policies configured carefully</td>
</tr>
<tr>
<td></td>
<td>Patch Deficit</td>
<td>Critical</td>
<td>Middle</td>
<td>Probable</td>
<td>Continuous patch management</td>
</tr>
<tr>
<td></td>
<td>Denial of Service</td>
<td>Critical</td>
<td>Middle</td>
<td>Middle</td>
<td>Firewall, DDOS protection services</td>
</tr>
<tr>
<td></td>
<td>Malware</td>
<td>Critical</td>
<td>Middle</td>
<td>Probable</td>
<td>Malware detection, awareness training</td>
</tr>
<tr>
<td></td>
<td>SCA/DN System Attack</td>
<td>Critical</td>
<td>Middle</td>
<td>Probable</td>
<td>Least privilege, periodic audits, network segmentation</td>
</tr>
<tr>
<td>Human</td>
<td>Social Engineering</td>
<td>Critical</td>
<td>Critical</td>
<td>Probable</td>
<td>Awareness training, behavior anomaly detection, least privilege</td>
</tr>
<tr>
<td></td>
<td>Identity Spoofing</td>
<td>Critical</td>
<td>Critical</td>
<td>Low</td>
<td>2 factor authentication, identity fraud detection, physical key cards</td>
</tr>
<tr>
<td></td>
<td>Misconfiguration</td>
<td>Critical</td>
<td>Critical</td>
<td>Low</td>
<td>4 eyes configuration, periodic audits, config file validation</td>
</tr>
<tr>
<td>Business</td>
<td>Failed Defined KOSMs Contract Tempalte</td>
<td>Critical</td>
<td>Low</td>
<td>Low</td>
<td>Carefully defined templates by experts</td>
</tr>
<tr>
<td></td>
<td>Service Provider Manipulates Data</td>
<td>Critical</td>
<td>Low</td>
<td>Low</td>
<td>Audit data collector securely connected to blockchain</td>
</tr>
<tr>
<td></td>
<td>Error in Data Collection</td>
<td>Probable</td>
<td>Low</td>
<td>-</td>
<td>Monitoring, anomaly detection</td>
</tr>
<tr>
<td></td>
<td>Contract Manipulation</td>
<td>Critical</td>
<td>Low</td>
<td>-</td>
<td>Blockchain nodes must have consensus for contract changes</td>
</tr>
<tr>
<td>Use Case</td>
<td>Dental of Service</td>
<td>Critical</td>
<td>Low</td>
<td>Probable</td>
<td>Data caching on premise</td>
</tr>
<tr>
<td>Use Case (Infrastructure Specific)</td>
<td>Malware</td>
<td>Middle</td>
<td>Probable</td>
<td>Male detection, awareness training</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Duplgiating</td>
<td>Critical</td>
<td>Low</td>
<td>Low</td>
<td>Audit container image before publish</td>
</tr>
<tr>
<td></td>
<td>Man in the Middle</td>
<td>Critical</td>
<td>Low</td>
<td>Probable</td>
<td>Message encryption and authentication (certification)</td>
</tr>
<tr>
<td></td>
<td>Non Compliance</td>
<td>Critical</td>
<td>Low</td>
<td>Low</td>
<td>Anonymization</td>
</tr>
<tr>
<td></td>
<td>Edge Misconfiguration</td>
<td>Critical</td>
<td>Middle</td>
<td>-</td>
<td>4 eyes configuration, periodic audits, config file validation</td>
</tr>
<tr>
<td>Use Case (Human Specific)</td>
<td>Social Engineering</td>
<td>Critical</td>
<td>Low</td>
<td>Probable</td>
<td>Awareness training, behavior anomaly detection, least privilege</td>
</tr>
<tr>
<td></td>
<td>Identity Spoofing</td>
<td>Critical</td>
<td>Low</td>
<td>Low</td>
<td>2 factor authentication, identity fraud detection, physical key cards</td>
</tr>
<tr>
<td></td>
<td>Insider Attacker</td>
<td>Critical</td>
<td>Middle</td>
<td>-</td>
<td>Intrusion detection system, network segmentation, least privilege</td>
</tr>
<tr>
<td>Use Case (Business Specific)</td>
<td>Sensor Data Manipulation</td>
<td>Critical</td>
<td>Low</td>
<td>Low</td>
<td>Blockchain nodes must have consensus for contract changes</td>
</tr>
<tr>
<td></td>
<td>Smart Contract Manipulation</td>
<td>Critical</td>
<td>Low</td>
<td>Low</td>
<td>Monitoring, anomaly detection</td>
</tr>
<tr>
<td></td>
<td>Machine Usage Data Manipulation</td>
<td>Critical</td>
<td>Low</td>
<td>Low</td>
<td>Periodic audit, data caching, anomaly detection</td>
</tr>
<tr>
<td></td>
<td>Non-Determinism</td>
<td>Critical</td>
<td>Middle</td>
<td>Low</td>
<td>Blockchain node that acts as intermediary / curator</td>
</tr>
<tr>
<td>Smart Contract</td>
<td>External Status Services</td>
<td>Critical</td>
<td>Middle</td>
<td>Low</td>
<td>Blockchain oracle that acts as intermediary / curator</td>
</tr>
<tr>
<td></td>
<td>Input Validation / Error Handling</td>
<td>Critical</td>
<td>Middle</td>
<td>Probable</td>
<td>Input validation, strict error handling / safe error behaviour</td>
</tr>
</tbody>
</table>
False Data by Accident/Purpose?

Uber's Self-Driving Car

Problem:
- Sensor has been replaced
  ➔ protect identity
- Sensor is highjacked and delivers wrong data
  ➔ check data plausibility
- Data integrity violation during transport
  ➔ secure data transport

What is detected?

Scene A:

Scene B:
Adversarial Attacks Against Machine Learning

- Label Manipulation (e.g. Flipping Label)
- Backdoor Poisoning (e.g. hidden trigger)


Prof. Dr. Ch. Reich (Institute for Data Science, Cloud Computing and IT Security)
Counter Measurement: Distributed Data Validation Networks

Context-Aware Anomaly Detection for the Distributed Data Validation Network in Industry 4.0 Environments

Kevin Wallis, Fabian Schilling, Elias Backmund, Christoph Reich and Christian Schindelhauer

University of Applied Sciences Furtwangen
Email: {kevin.wallis, elias.backmund, christoph.reich}@hs-furtwangen.de

University of Freiburg
Email: {schilf, schiude}@uni-freiburg.de

Abstract—In the Industry 4.0 context, especially when considering large factories producing costly goods, monitoring sensor values is important to ensure high quality. This reduces large costs for meeting faulty products or recall of these. Different approaches are used to ensure efficient monitoring and validation of sensor values. The Distributed Data Validation Network (DDVN) can remove single points of failure. Still, not every anomaly in the validation procedure means that errors or attacks have occurred. Other reasons like maintenance procedures, updates of firmware, or changed materials can lead to False Positive (FP) or False Negative (FN) detection of errors. To reduce these, we incorporate context information in the validation procedure. Further, we show how the appropriate context information is selected and used on a real machine data set.

Keywords—Anomaly Detection, Context-Awareness, Distributed Data Validation Network, Industry 4.0

The system is applied to consider and evaluate the listed dimensions. Individual solutions are used because most production systems are custom-made. Besides using an external data validation system, there are also production systems that perform the validation on the machine or on the server itself. If the machine does not have a network connection, this will make updating the validation logic, exchanging telemetry data and merging sensor values (sensor fusion) for more accurate and complete data even harder.

Using a single data validation system has the disadvantage of a single point of failure. If the validation system is successfully attacked, correct data can be marked as incorrect and, conversely, incorrect data can be evaluated as valid. Furthermore, if a validation system is used for data evaluation as well as data reconstruction [3], incorrect data can be injected...
Counter Measurement: Blockchain Audit Trails

- KOSMOS research project: [https://www.kosmos-bmbf.de/](https://www.kosmos-bmbf.de/)
- Enables cross-company data-driven business models
- Consens of all participants
- Smart contracts implement rules of communication
- Blockchain provides data integrity and audit trails
Machine Learning for Cyber Security

Deep Learning-based Cybersecurity

- Malware Detection and Analysis
  - PC-based Malware
  - Android-based Malware
- Intrusion Detection
  - Anomaly Detection
- Other
  - Phishing Detection
  - Spam Detection
  - Website Defacement Detection

2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)

Container Anomaly Detection Using Neural Networks Analyzing System Calls

Holger Gantikow, Tom Zöhrer, Christoph Reich
Institute for Data Science, Cloud Computing and IT Security
Furtwangen University of Applied Science
Furtwangen, Germany
Email: {holger.gantikow, tom.zoehrer, christoph.reich}@hs-furtwangen.de

Abstract—Container environments permeate all areas of computing, such as HPC, since they are lightweight, efficient, and ease the deployment of software. However, due to the shared host kernel, their isolation is considered to be weak, so additional protection mechanisms are needed. This paper shows that neural networks can be used to necessarily play an important role. A typical problem however is the risk of misuse of resources, for example by using HPC systems to mine crypto currencies [4]. We therefore selected two applications from this domain as representatives. We utilize OpenSITM (a Computational Fluid Dynamics (CFD)

Fig. 1: Sysdig Architecture
ML Generates new Attack Vectors

- ML generates more realistic phishing mails
- Robots espionage for hackers
- GANs generate flow to overcome IDS
Summary

- **Traditional**
  - Risk analysis (STRIDE)
  - Device analysis (e.g. Common Criteria)
  - Crypto capability of devices
  - RFID tags will not do crypto for some years
  - Security objectives must be risk based
  - Privacy protection must be risk based
  - Identity protection must be risk based
  - Traffic analysis protection
- **Machine Learning-specific**
  - ML has new risks
  - ML can assist in information security
  - ML generates new risks

<table>
<thead>
<tr>
<th>Threat</th>
<th>Desired property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>Authenticity</td>
</tr>
<tr>
<td>Tampering</td>
<td>Integrity</td>
</tr>
<tr>
<td>Repudiation</td>
<td>Non-repudiability</td>
</tr>
<tr>
<td>Information disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Availability</td>
</tr>
<tr>
<td>Elevation of Privilege</td>
<td>Authorization</td>
</tr>
</tbody>
</table>
Thank you very much for your attention!

Christoph Reich
christoph.reich@hs-furtwangen.de
University of Applied Science Furtwangen
Institute for Data Science, Cloud Computing and IT Security

idacus.hs-furtwangen.de