Security Challenges

for Cloud or Fog computing-Based AI Applications

27th June 2023

A. Pakmehr, A. Aßmuth, C. P. Neumann, and G. Pirkl | Cloud Computing 2023, FAST-CAMS – Nice, France

How This Contribution Was Created...

Amir Pakmehr

fog

cloud

Christoph P. Neumann

Andreas Aßmuth

security

AI

Gerald Pirkl

How This Contribution Was Created...

Amir Pakmehr

Andreas Aßmuth

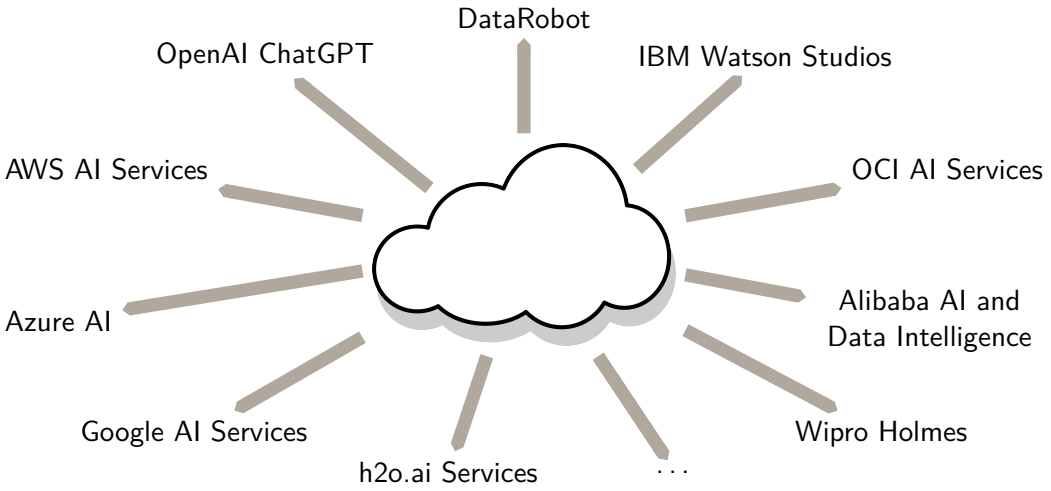
conference paper

Christoph P. Neumann

Gerald Pirkl

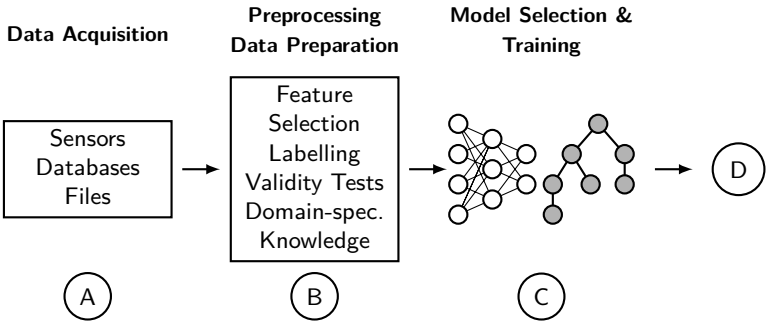
Outline

AI Services On The Internet



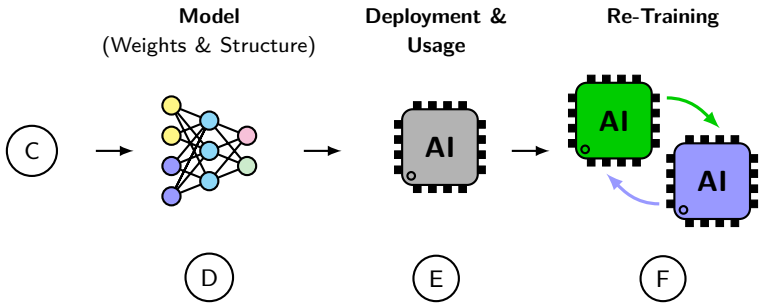
Typical AI Workflow

Steps A to C



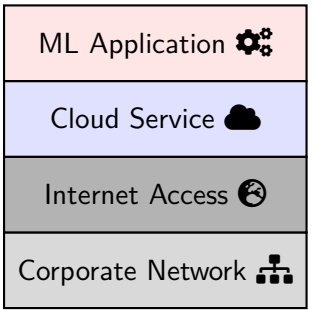
Typical AI Workflow

Steps D to F



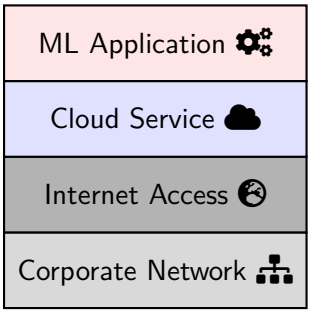
AI Services in Use – Cloud, Fog And Edge

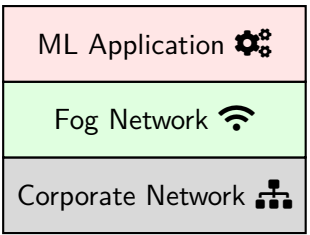
Naive Architectures



AI Services in Use – Cloud, Fog And Edge

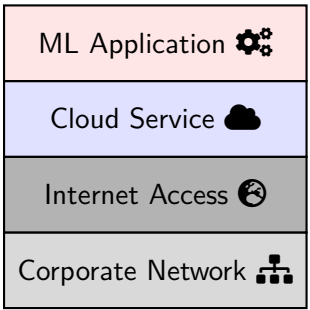
Naive Architectures

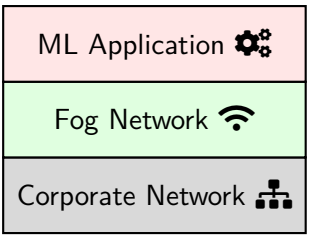


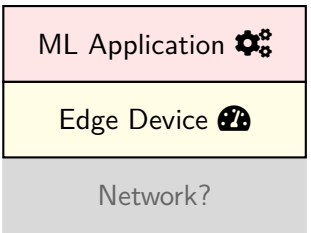


AI Services in Use – Cloud, Fog And Edge

Naive Architectures



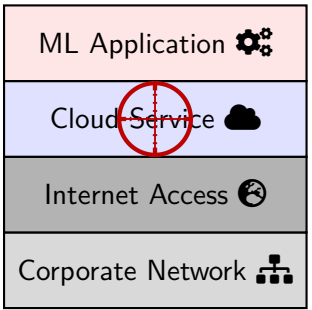


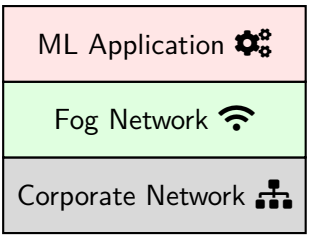


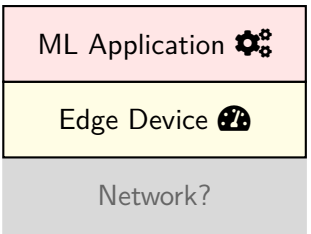
AI Services in Use – Cloud, Fog And Edge

Naive Architectures

attractive targets



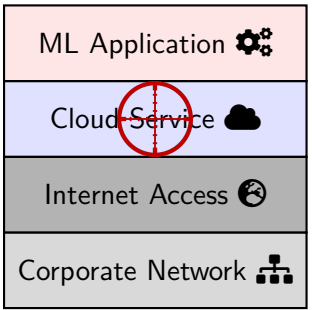


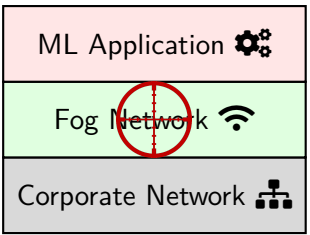


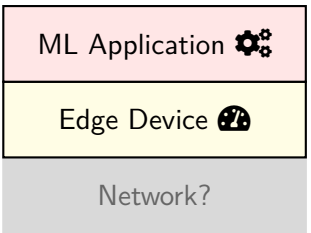
AI Services in Use – Cloud, Fog And Edge

Naive Architectures

attractive targets



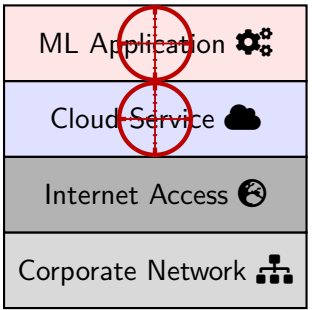


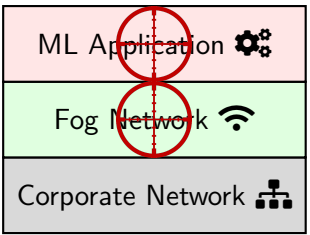


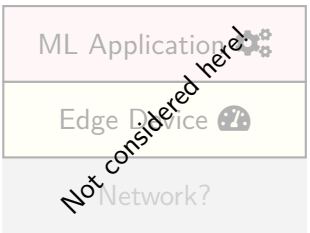
AI Services in Use – Cloud, Fog And Edge

Naive Architectures

attractive targets







Cloud Computing Security Challenges

Cloud Computing Security Challenges

Ostbayerische Technische Hochschule Amberg-Weiden

A. Data Breaches

Cloud Computing Security Challenges

Osthayerische
Technische Hochschule
Amberg-Weiden

A. Data Breaches

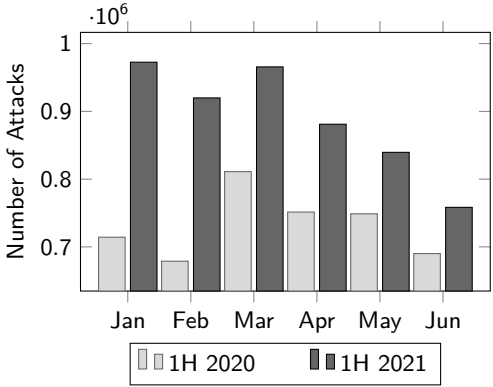
B. Ransomware Attacks

Cloud Computing Security Challenges

A. Data Breaches

B. Ransomware Attacks

C. Distributed Denial of Service Attacks



Monthly DDoS attack frequency during the Covid-19 pandemic in 2020 and 2021 (Germany) according to Netscout "Threat Intelligence Report, Issue 7: Findings from 1H 2021", p. 7, 2021.

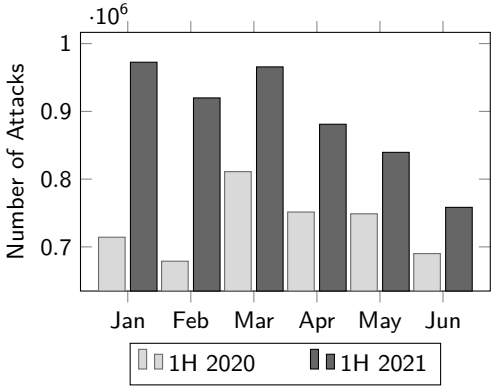
Cloud Computing Security Challenges

A. Data Breaches

B. Ransomware Attacks

C. Distributed Denial of Service Attacks

D. Dependence on 3rd Party Software



Monthly DDoS attack frequency during the Covid-19 pandemic in 2020 and 2021 (Germany) according to Netscout "Threat Intelligence Report, Issue 7: Findings from 1H 2021", p. 7, 2021.

Cloud Computing Security Challenges

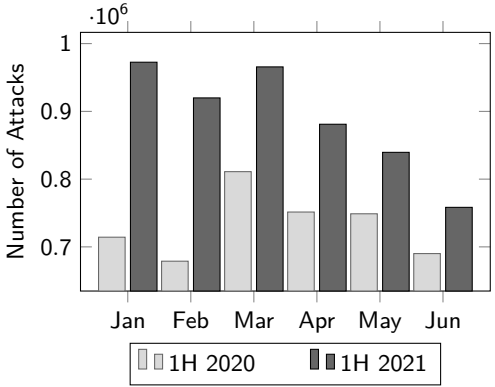
A. Data Breaches

B. Ransomware Attacks

C. Distributed Denial of Service Attacks

D. Dependence on 3rd Party Software

E. Unsecure APIs



Monthly DDoS attack frequency during the Covid-19 pandemic in 2020 and 2021 (Germany) according to Netscout "Threat Intelligence Report, Issue 7: Findings from 1H 2021", p. 7, 2021.

Fog Computing Security Challenges

Fog Computing Security Challenges

Osthayerische Technische Hochschule Amberg-Weiden

A. Physical Attacks

Fog Computing Security Challenges

Osthayerische Technische Hochschule Amberg-Weiden

A. Physical Attacks

B. Fog & User Impersonation Attack

Fog Computing Security Challenges

A. Physical Attacks

B. Fog & User Impersonation Attack

C. Malicious Fog Nodes

Fog Computing Security Challenges

A. Physical Attacks

B. Fog & User Impersonation Attack

C. Malicious Fog Nodes

D. Rogue Fog Nodes

Fog Computing Security Challenges

A. Physical Attacks

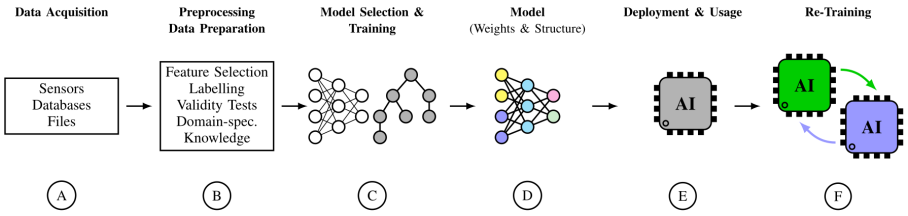
B. Fog & User Impersonation Attack

C. Malicious Fog Nodes

D. Rogue Fog Nodes

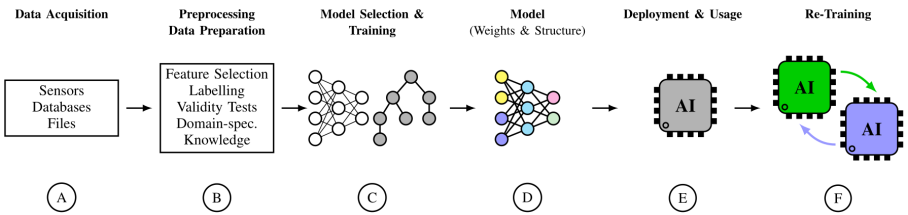
E. Ephemeral Secret Leakage Attack

Special Security Challenges For AI Applications



Osthayerische Technische Hochschule Amberg-Weiden

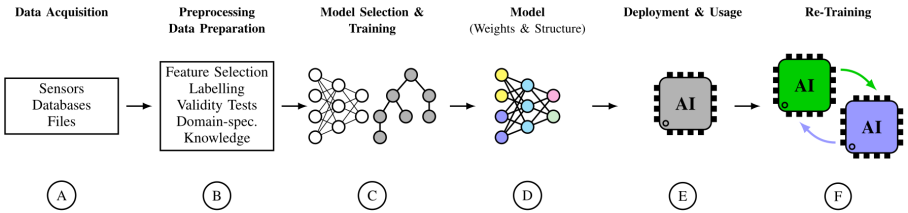
A. Data Representing ML Model



Special Security Challenges For AI Applications

A. Data Representing ML Model

B. Special AI-related Security Issues

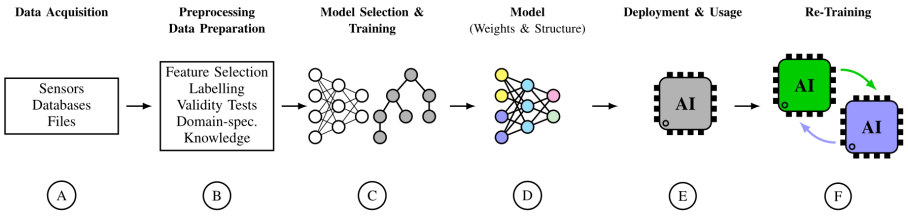


Special Security Challenges For AI Applications

A. Data Representing ML Model

B. Special AI-related Security Issues

C. Special Attacks on Language Models



Conclusion & Future Work

Osthayerische
Technische Hochschule
Amberg-Weiden

- Dependency of AI applications on underlying cloud or fog-based services

Conclusion & Future Work

Ostbayerische Technische Hochschule Amberg-Weiden

- Dependency of AI applications on underlying cloud or fog-based services
- Attacks against cloud services or fog computing networks ☞ difficulties, data breaches, failures, or malfunctioning of AI applications based on these

Conclusion & Future Work

Ostbayerische Technische Hochschule Amberg-Weiden

- Dependency of AI applications on underlying cloud or fog-based services
- Attacks against cloud services or fog computing networks ☞ difficulties, data breaches, failures, or malfunctioning of AI applications based on these
- AI currently a hot topic ☞ attractive target for cybercriminals

Conclusion & Future Work

Ostbayerische Technische Hochschule Amberg-Weiden

- Dependency of AI applications on underlying cloud or fog-based services
- Attacks against cloud services or fog computing networks ☞ difficulties, data breaches, failures, or malfunctioning of AI applications based on these
- AI currently a hot topic ☞ attractive target for cybercriminals
- interplay between AI and information security promises huge potential for future applications and research

Wordcloud created by Ashashyou, CC BY-SA 4.0

Prof. Dr. Andreas Aßmuth
Professor of Computer Networks and Mathematics

Ostbayerische Technische Hochschule Amberg-Weiden
Department of Electrical Engineering, Media and Computer Science

Kaiser-Wilhelm-Ring 23, 92224 Amberg, Germany
Phone: +49 9621 482 3604
Email: a.assmuth@oth-aw.de
PGP: 0xE1895723
Web: https://www.oth-aw.de