Improving the Resilience of Critical IT Infrastructures Using AIOps

Prof. Wahab Hamou-Lhadj
Concordia University
Montréal, QC, Canada
wahab.hamou-lhadj@Concordia.ca

GRIC Cybersecurity Forum
Université de Sherbrooke
Sherbrooke, Quebec, Canada
April 27, 2023

What is AIOps?

- ✓ Application of **AI to enhance and automate IT** operations
- ✓ An important enabler **of digital transformation**

Application Areas

Quality of Service	**Governance & Regulatory Compliance**
✓ Detection of anomalies ✓ Fault diagnosis and repair ✓ Cybersecurity ✓ Performance analysis ✓ Incident reduction ✓ Incident report management ✓ Self-healing and self-adaptation	✓ Strategic governance ✓ Meeting regulatory requirements ✓ Risk management ✓ Resource optimization ✓ IT standards ✓ Workforce management

Why AIOps?

The Digital Shift

- More and more organizations in all industry sectors are turning to IT for business process automation
- From 2019-2020, "business channels being replaced by digital grew from 16% to 34%"[1]

Emerging Practices and Technologies

- DevOps and CI
- Highly dynamic and distributed architectures
- Hardware/software co-design
- System of systems
- Autonomous systems

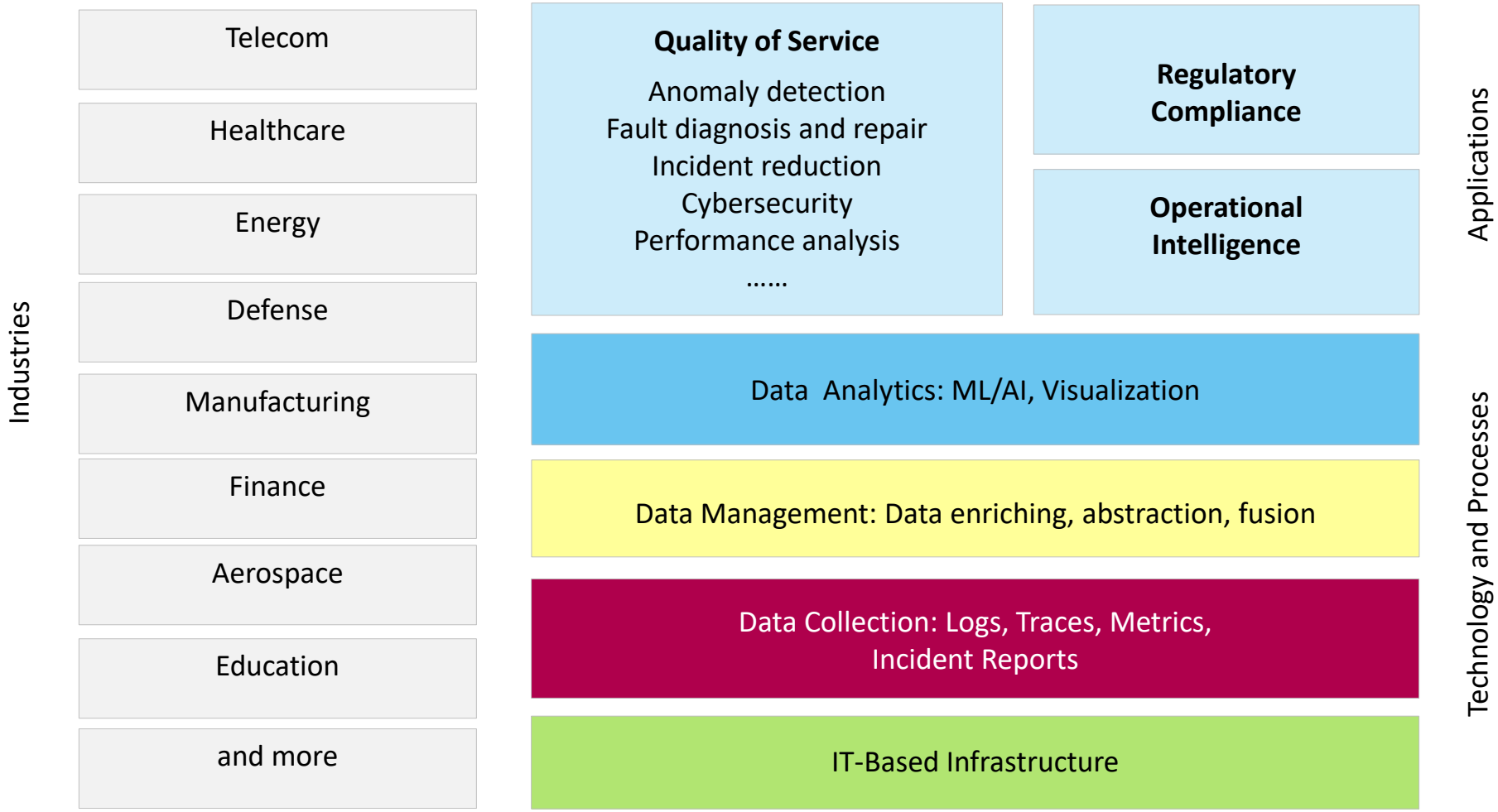
Operational Complexity

- Companies use a large number of IT tools to manage critical infrastructures
- A large amount of heterogenous (and unstructured) data generated at high velocity
- Difficult to gain full observability over the entire system stack
- 91% of IT practitioners believe that gaining full observability into their systems would be revolutionary for their business[2]
- Labour shortage calls for more automation

[1]Based on a McKinsey & Company Report. Text taken from: https://community.ibm.com/community/user/automation/blogs/rob-geier/2022/08/09/a-golden-opportunity-for-business-partners

[2]https://www.appdynamics.com/blog/full-stack-observability/momentum-is-building-on-thejourney-to-observability/

AIOps Stack


Industries
Telecom
Healthcare
Energy
Defense
Manufacturing
Finance
Aerospace
Education
and more
Quality of Service
Anomaly detection
Fault diagnosis and repair
Incident reduction
Cybersecurity
Performance analysis
……
Regulatory Compliance
Operational Intelligence
Applications
Data Analytics: ML/AI, Visualization
Data Management: Data enriching, abstraction, fusion
Data Collection: Logs, Traces, Metrics, Incident Reports
IT-Based Infrastructure
Technology and Processes

Current Projects

Log Management

- ✓ Understanding and improving the practice of logging and tracing
- ✓ Developing log parsing, fusion, and abstraction APIs
- ✓ Developing adaptive logging techniques

Incident Report Handling

- ✓ Reducing lead time to resolution
- ✓ Reducing number of incidents
- ✓ Automatic recommendation of fixes

Anomaly Detection

- ✓ Developing anomaly detection techniques using Boolean combination of classifiers and topology graphs
- ✓ Integrating human feedback

AIOps and System Modeling

- ✓ Bringing observability to early stages of SDLC
- ✓ Observability analysis assisted by system models

Current Projects

Log Management

- ✓ Understanding and improving the practice of logging and tracing
- ✓ Developing log parsing, fusion, and abstraction APIs
- ✓ Developing adaptive logging techniques

Incident Report Handling

- ✓ Reducing lead time to resolution
- ✓ Reducing number of incidents
- ✓ Automatic recommendation of fixes

Anomaly Detection

- ✓ Developing anomaly detection techniques using Boolean combination of classifiers and topology graphs
- ✓ Integrating human feedback

AIOps and System Modeling

- ✓ Bringing observability to early stages of SDLC
- ✓ Observability analysis assisted by system models

Current Projects

Log Management

- ✓ Understanding and improving the practice of logging and tracing
- ✓ Developing log parsing, fusion, and abstraction APIs
- ✓ Developing adaptive logging techniques

Incident Report Handling

- ✓ Reducing lead time to resolution
- ✓ Reducing number of incidents
- ✓ Automatic recommendation of fixes

Anomaly Detection

- ✓ Developing anomaly detection techniques using Boolean combination of classifiers and topology graphs
- ✓ Integrating human feedback

AIOps and System Modeling

- ✓ Bringing observability to early stages of SDLC
- ✓ Observability analysis assisted by system models

Current Projects

Log Management

- ✓ Understanding and improving the practice of logging and tracing
- ✓ Developing log parsing, fusion, and abstraction APIs
- ✓ Developing adaptive logging techniques

Incident Report Handling

- ✓ Reducing lead time to resolution
- ✓ Reducing number of incidents
- ✓ Automatic recommendation of fixes

Anomaly Detection

- ✓ Developing anomaly detection techniques using Boolean combination of classifiers and topology graphs
- ✓ Integrating human feedback

AIOps and System Modeling

- ✓ Bringing observability to early stages of SDLC
- ✓ Observability analysis assisted by system models

Contact Information:

Prof. Wahab Hamou-Lhadj
Department of Electrical and Computer Engineering
Gina Cody School of Engineering and Computer Science
Concordia University
wahab.hamou-lhadj@concordia.ca

SRT Research Lab:

http://www.ece.concordia.ca/~abdelw