AI-ENABLED SECURITY

Prof. Amin Beheshti

- Director, AI-enabled Processes (AIP) Research Centre

- Head, Data Analytics Research Lab

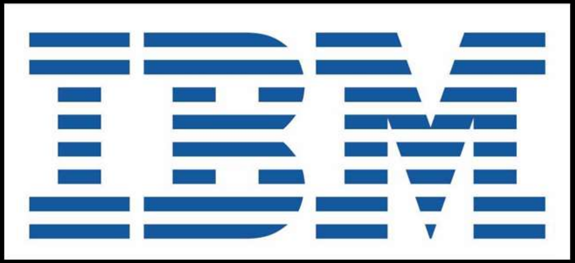
- Founder, Big Data Society

School of Computing

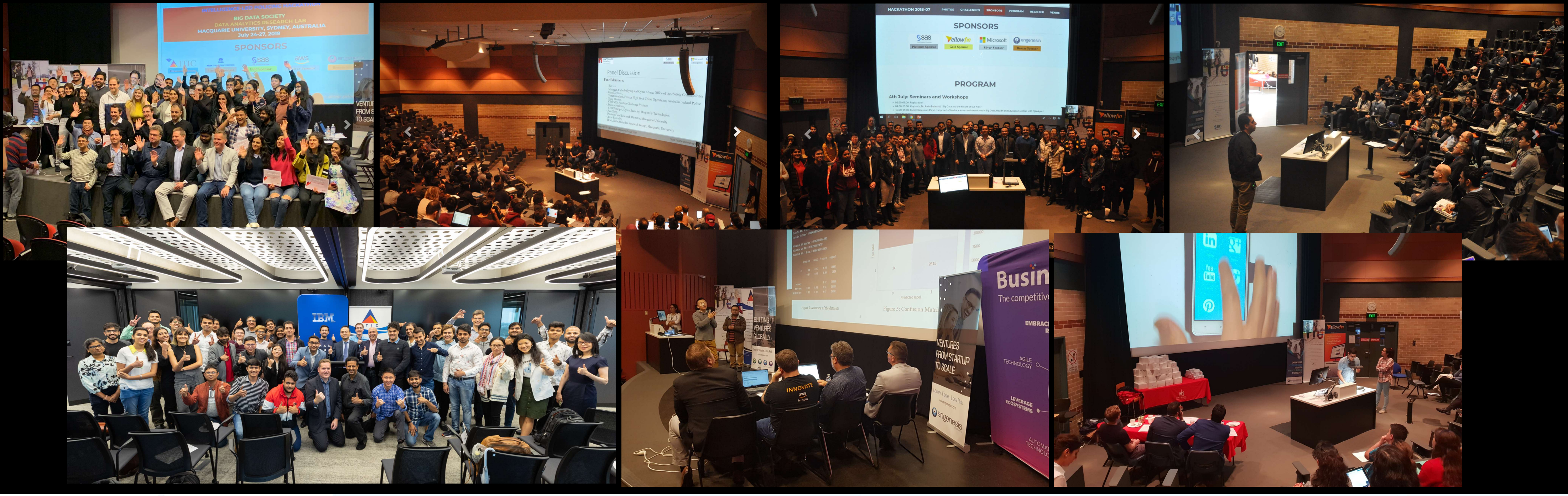
MACQUARIE University
SYDNEY · AUSTRALIA

8 September 2022

HACKATHON SPONSORS



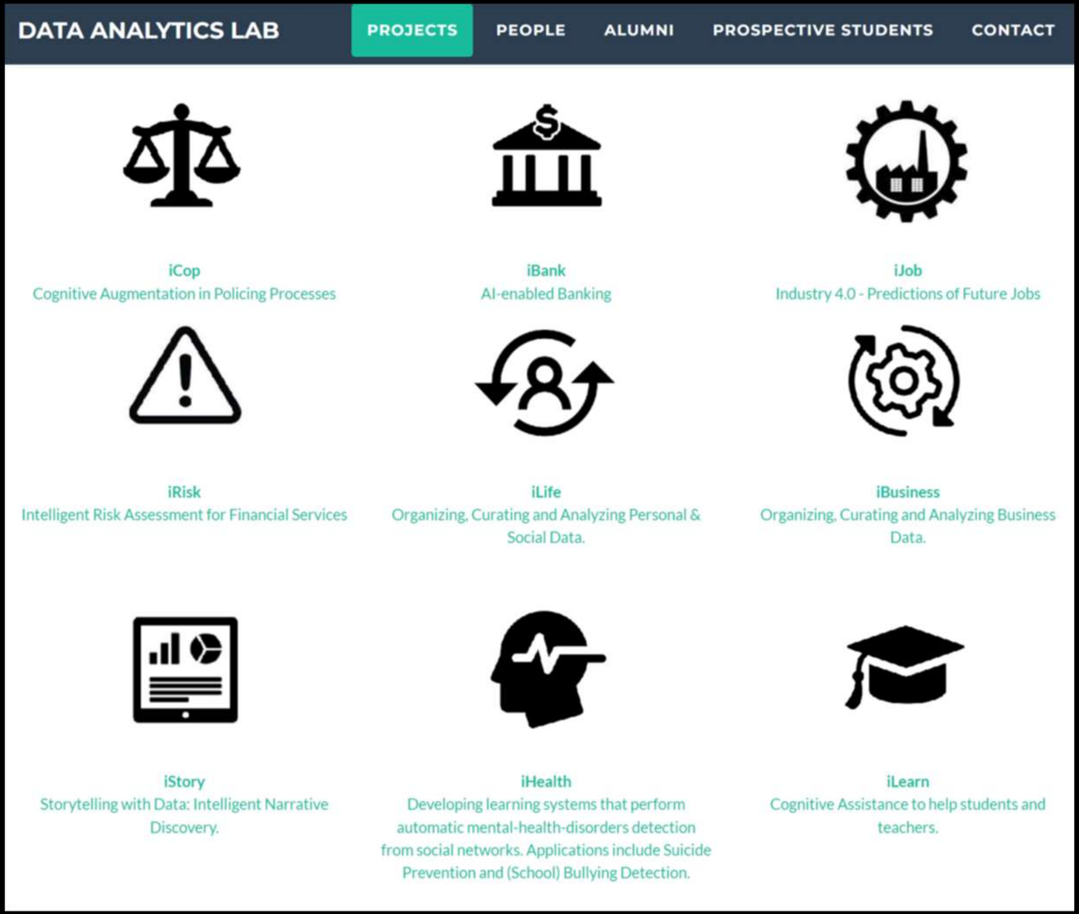
THE BIG DATA SOCIETY


BIG DATA SOCIETY
DATA ANALYTICS RESEARCH LAB
MACQUARIE UNIVERSITY, SYDNEY, AUSTRALIA
July 24-27, 2019
SPONSORS
Panel Discussion
HACKATHON 2018-07
SPONSORS
PROGRAM
4th July: Seminars and Workshops
IBM
INNOVATE
BUILDING VENTURES GLOBALLY
VENTURES FROM STARTUP TO SCALE
engenesis
Busin
The competitive

ITIC	Diamond Sponsor
TATA CONSULTANCY SERVICES	Platinum Sponsor
IBM	Diamond Sponsor
Microsoft	Silver Sponsor
aws	Gold Sponsor
sas THE POWER TO KNOW.	Platinum Sponsor
Yellowfin	Gold Sponsor
engenesis	Bronze Sponsor
AGATE™	Platinum Sponsor

DATA ANALYTICS RESEARCH LAB

- 20+ Projects
- 50+ industry-based MRes/PhD Scholarships
- 30+ alumni/graduates
- 70+ publications



DATA ANALYTICS LAB

iCop
Cognitive Augmentation in Policing Processes

iBank
AI-enabled Banking

iJob
Industry 4.0 - Predictions of Future Jobs

iRisk
Intelligent Risk Assessment for Financial Services

iLife
Organizing, Curating and Analyzing Personal & Social Data.

iBusiness
Organizing, Curating and Analyzing Business Data.

iStory
Storytelling with Data: Intelligent Narrative Discovery.

iHealth
Developing learning systems that perform automatic mental-health-disorders detection from social networks. Applications include Suicide Prevention and (School) Bullying Detection.

iLearn
Cognitive Assistance to help students and teachers.

AI-enabled Processes Research Centre

EXTERNAL RESEARCH PARTNERSHIP
OVER $17 MILLION

TATA
TATA CONSULTANCY SERVICES

ITIC LIVE
Genius at WORK

FÆTHM

truuth

Cinglevue

locii
YOUR DATA IS YOUR DNA

dAIta

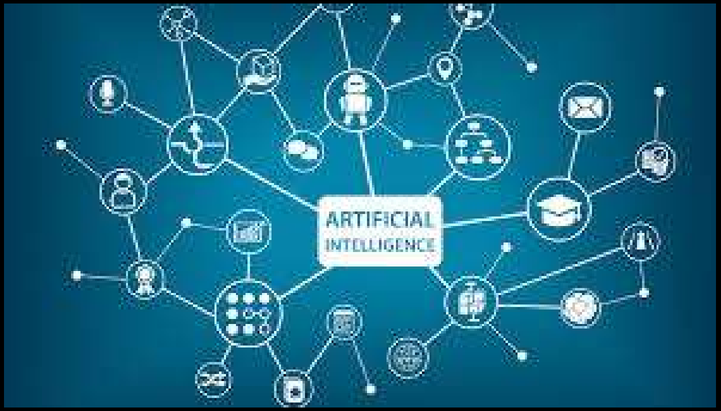
prospa

Yirigaa

Domain

Artificial Intelligence (AI)

"A system's ability to correctly interpret **external** data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation".



Kaplan, Andreas, and Michael Haenlein. "Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence." *Business Horizons* 62.1 (2019).

Artificial Intelligence (AI)

AI Components:

- **External** Data
  (From Data to **Big Data**)
- Learning
  (From **Machine Learning** and **Natural Language Processing** to Software-as-a-Service, Knowledge Graphs and Crowdsourcing)
- Goals and Tasks
  #Business-Process-Management #Decision-Making
  (Data-Driven and Knowledge-Intensive **Processes**)

GAP !!

DATA

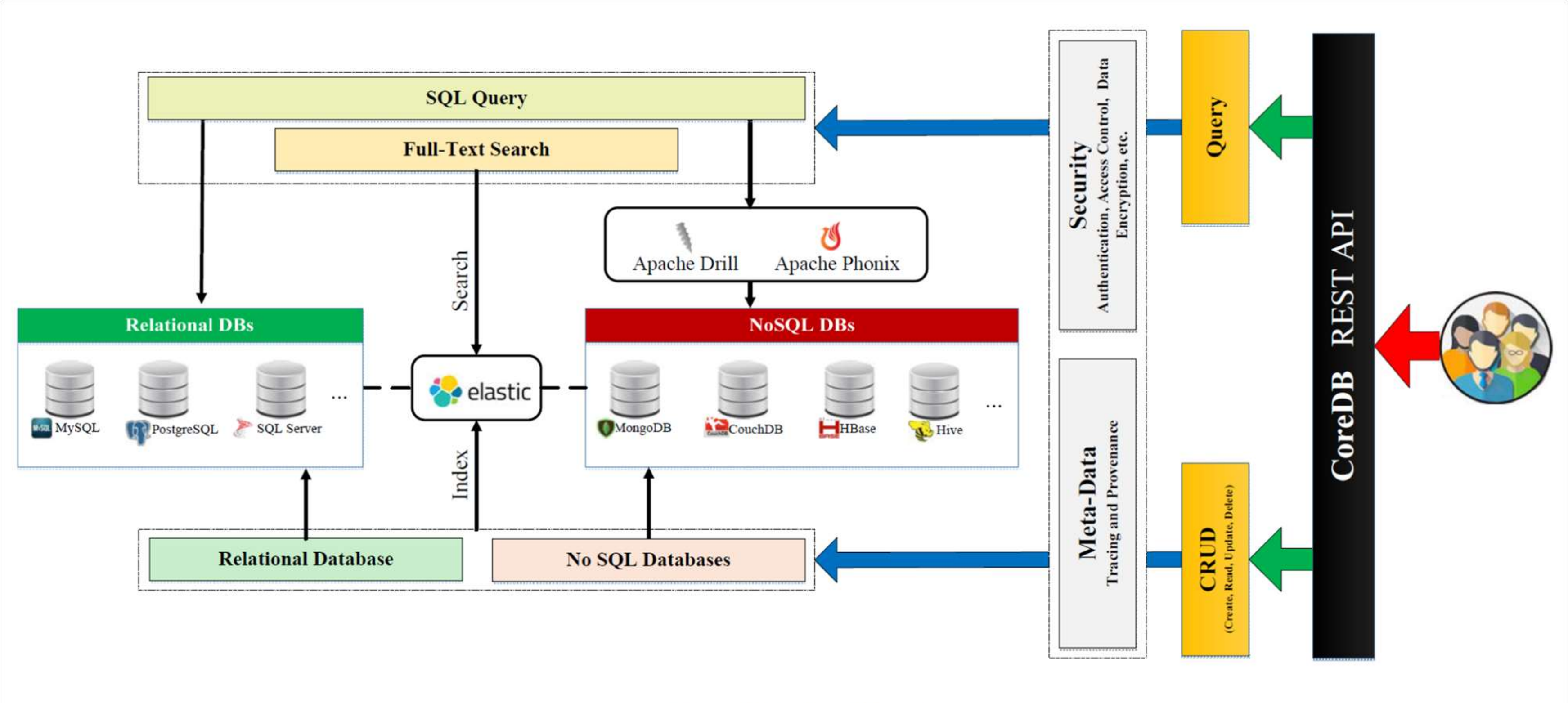
PROCESS

Today, the advancement in Artificial Intelligence (AI) and Data Science has the potential to transform business processes in fundamental ways; by assisting knowledge workers in communicating analysis findings, supporting evidences and to make decisions.

Example Innovations

Data Lake
Knowledge Lake
Knowledge Base 4.0

Data Lake As A Service

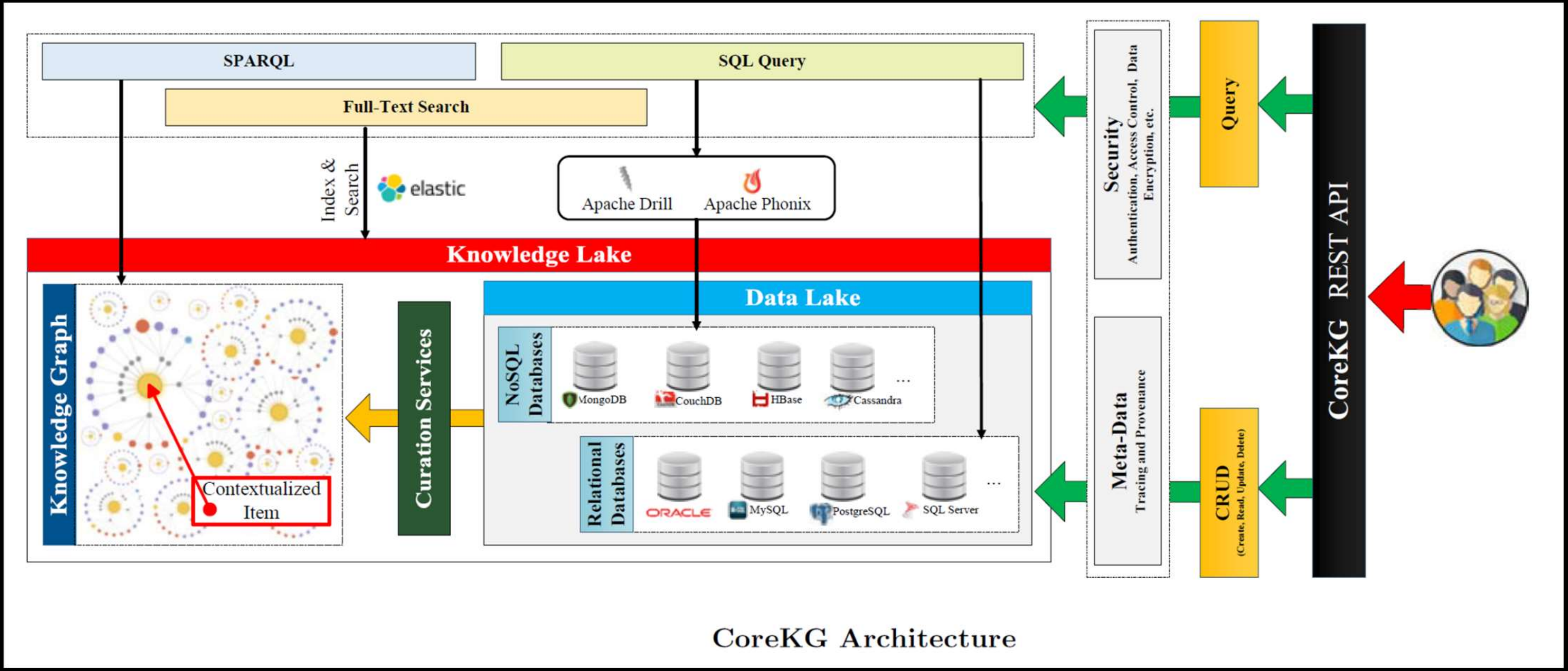


CoreDB Architecture

Beheshti et al., "CoreDB: a **Data Lake** Service", 26th ACM International Conference on Information and Knowledge Management (CIKM), Singapore, 2017.

AI-enabled Processes Research Centre

Knowledge Lake As A Service

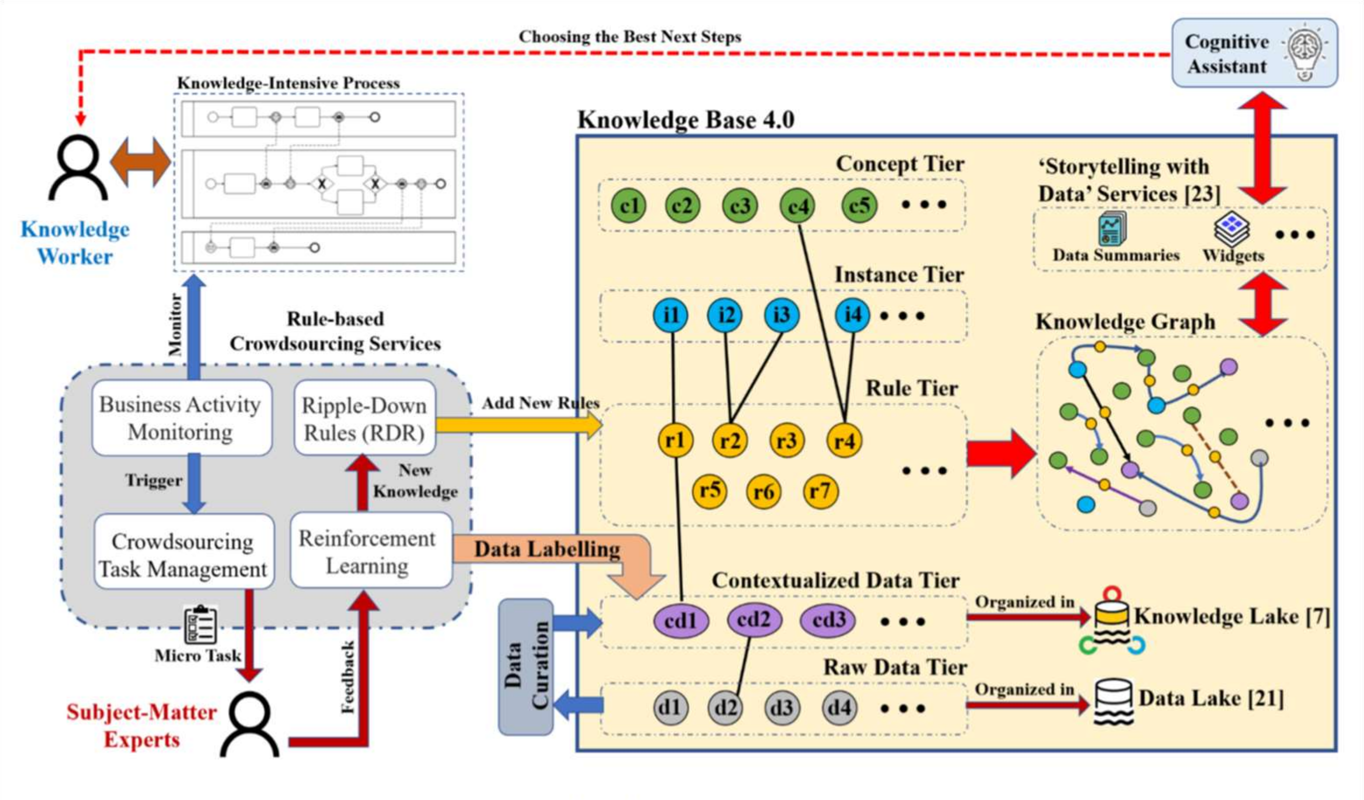


CoreKG Architecture

Beheshti et al., "CoreKG: a **Knowledge Lake** Service", PVLDB 11(12), 2018

AI-enabled Processes Research Centre

Knowledge Base 4.0



Knowledge Base 4.0.

Beheshti, "**Knowledge Base 4.0**: Using Crowdsourcing Services for Mimicking the Knowledge of Domain Experts", ICWS, 2022.

Security

Challenges:

- AI Expansion
- IoT Threats
- Blockchain Revolution
- Serverless Apps Vulnerability
- attacks (Cloud, Phishing, Ransomware, Denial-of-service, ...)
- …

Threats:

- Loss of Data
- Data Breaches
- System Disruption
- Intellectual theft
- …

Applications:

economic security, food security, health security environmental security, personal security, community security, political security, …

Approaches:

- Preventive
- Protective
- Punitive
- Detective

Types:

- Critical infrastructure security.
- Application security.
- Network security.
- Cloud security.
- Internet of Things (IoT) security.

HACKATHON CHALLENGES

AI-enabled Security

The challenges in this hackathon will focus on novel applications of AI in security, from machine learning and data analytics to cognitive assistants. The goal is to leverage AI to stay ahead of threats and learn how to respond w/ greater confidence and speed.

HACKATHON CHALLENGES

Challenge 1: Data Lake and Cloud

The continuous improvement in connectivity, storage and data processing capabilities allow access to a data deluge from open, private, social and IoT data. Data Lakes introduced as a storage repository to organize this raw data in its native format until it is needed. As a user of cloud infrastructure and Data Services, data lakes will remove the system setup challenges and enable you to deploy your workloads faster than ever. But, with that speed comes many security related drawbacks.

Your solution will present an AI-enabled approach to address the Data Loss/Leak Prevention (DLP) challenge in a Data Lake, i.e., the process of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data.

HACKATHON CHALLENGES

Challenge 2: Internet of Things (IoT)

Recently, we have become exposed to a plethora of new IoT security-related threats that never existed before, some of which have the potential to impact our way of life profoundly. This is important as our society is increasingly reliant on smart devices and services, from home automation and manufacturing to finance and transport. These billions of inter-connected devices with sensors and actuators, reachable almost instantaneously through the ubiquitous internet from any location and any other device in the world. All too often, “reachable” means reachable by unauthorized entities as well as intended users.

Your solution will present and AI-enabled approach to address the Reachability challenge to prevent IoT devices from being reachable by unauthorized entities/users.

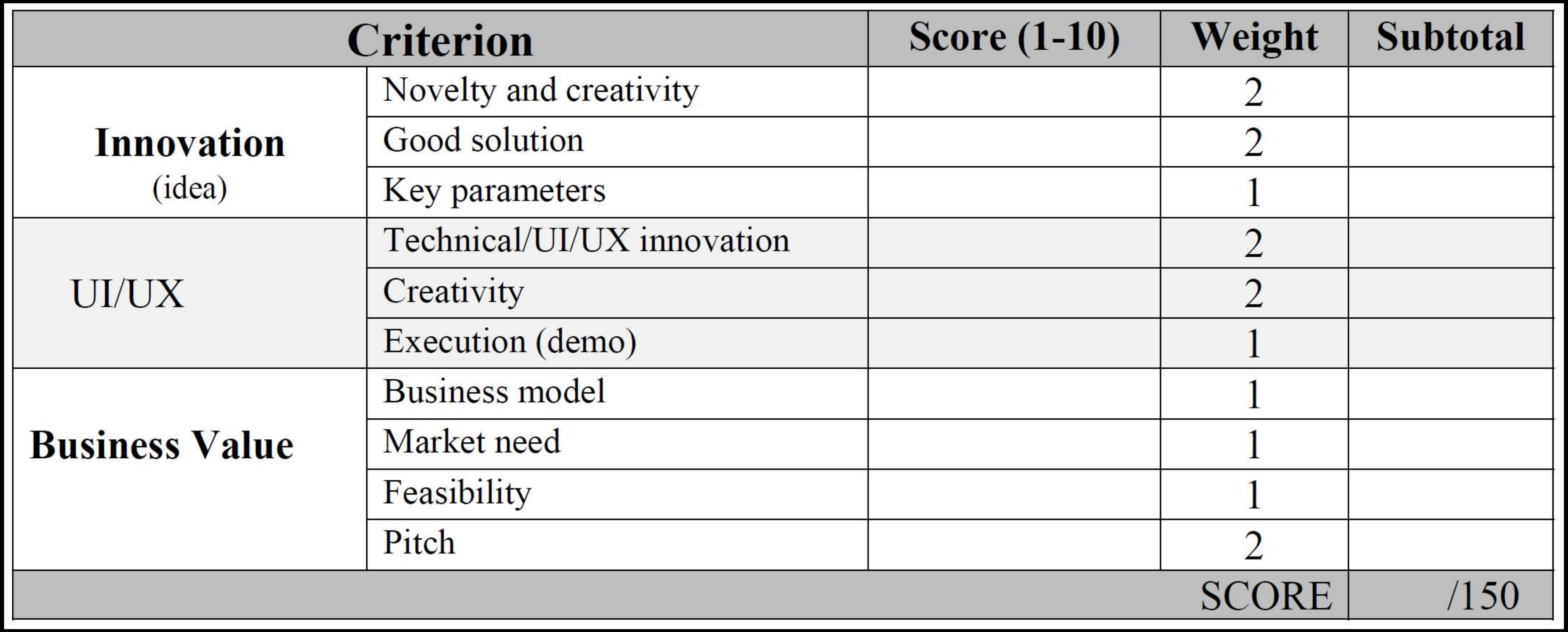
HACKATHON CHALLENGES

Challenge 3: e-Safety, Cyber-safety, and Cybersecurity

In the age of social media, dangerous and damaging online challenges are increasing. Cyber-safety (e.g., protect people from online threats) and Cybersecurity (protect information from malicious threats and cybercrime) play a vital role in helping us have a safer and more positive experiences online.

Your solution will present an AI-enabled approach to protect Australians from online threats; addressing challenges around cyber-safety, protecting personal information, Illegal and restricted online content, Cyberbullying, sharing identities, and more. Your solution can focus on educators, parents, young people, kids, women, and/or seniors.

JUDGING CRITERIA



Criterion		Score (1-10)	Weight	Subtotal
Innovation (idea)	Novelty and creativity		2	
	Good solution		2	
	Key parameters		1	
UI/UX	Technical/UI/UX innovation		2	
	Creativity		2	
	Execution (demo)		1	
Business Value	Business model		1	
	Market need		1	
	Feasibility		1	
	Pitch		2	
			SCORE	/150

THANK YOU