Applications of Formal Methods

L.Georgieva
lilia@macs.hw.ac.uk
Dependable Systems Group
Heriot Watt University
Edinburgh, UK

Structure

Case Studies: formal methods for:

- security
- knowledge management
- disambiguation
- program efficiency
- network modelling: selected projects from two research areas

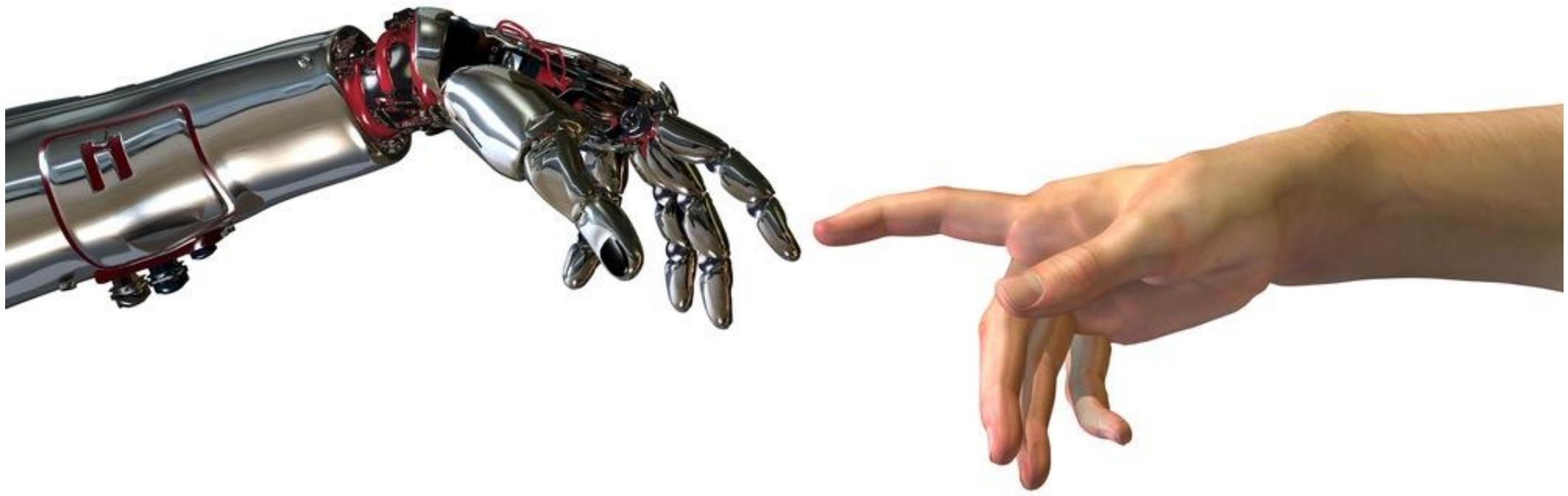
The role of women in computer science: Marie-Curie, ACM and how to get involved.

Your research question

Research is about thinking, reading and writing critically in order to

- present your own views with supporting evidence
- critically evaluate pros and cons
- analyse current trends and identify recurring themes
- discuss, present and debate

Why should we care about research in AI (formal methods)?



Why should we care about research in AI?

- Research in AI is moving at a very rapid pace
- As it gets more complex, the number of people who understand it gets smaller
- People get worried about potential harmful effects and fear of technology
- Or they assume it will solve all problems and trust it too much
- As AI researchers it is our job to be realistic about the potential threats and benefits of technology so we can advice non-experts.

Can anyone think of any current issues relating to science or technology which the public are worried about?

Can the pursuit of AI research teach us anything about human intelligence?

Example 1: Natural Language Processing (NLP)

1954:
"five, perhaps three years hence, interlingual meaning conversion by electronic process in important functional areas of several languages may well be an accomplished fact"

Dr Dostert in IBM press release about the Georgetown project

2014:
It is understood that NLP is an *AI-complete* problem - that is, it requires Strong AI.

Example 2: Chess

1970s:
much debate about whether a machine could ever defeat a competent human

1997:
IBM's Deep Blue beats Kasparov

2014:
much debate about whether computation will ever 'solve chess'

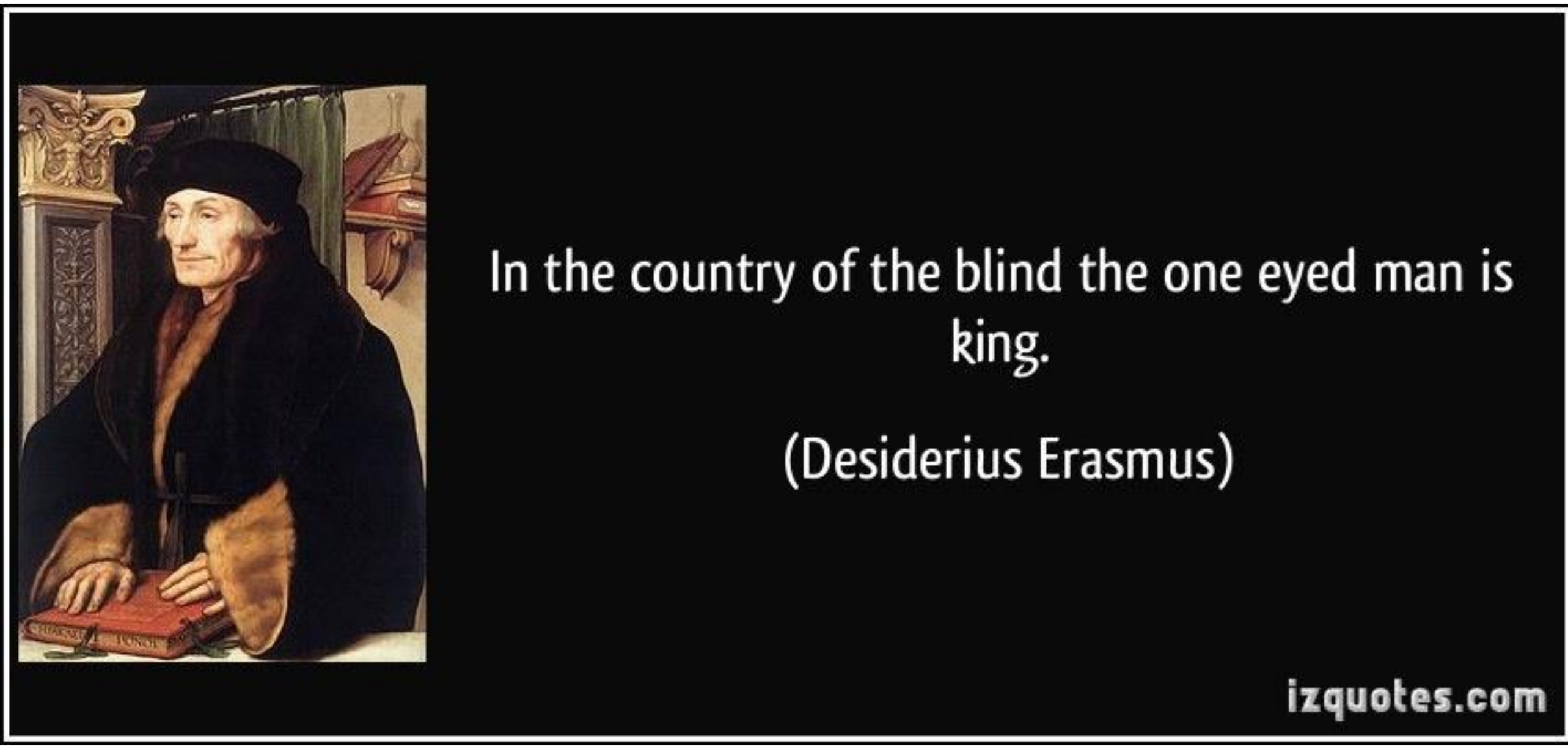
Example 2: Security

Who owns my data?

Who uses my data? For how long?

How do I protect myself?

Country of the Blind



What questions does this story raise about AI?

Research Area 1: Aims

- In one aspect of my research I have aimed to study the usability of formal methods for ensuring correctness. In particular we focus on model checking for modelling and verifying behaviour of **processes** and **properties**.
- I have focused **security** and **navigation** properties along with modelling time constrains.

Why?

- To promote an understanding of the issues involved in building high integrity data-intensive applications.
- To provide both practical and theoretical insights into industrial strength tools and techniques that promote the development of **high integrity** data-intensive applications.

Objectives

- To design a formal model of data-sensitive and time-sensitive web applications using a model checker.
- To include time properties in our models to represent realistic web applications.
- To explore the capabilities of different Model Checking Tools.

Web Applications

Exponential increase in their popularity and usage in the past ten years in many areas:

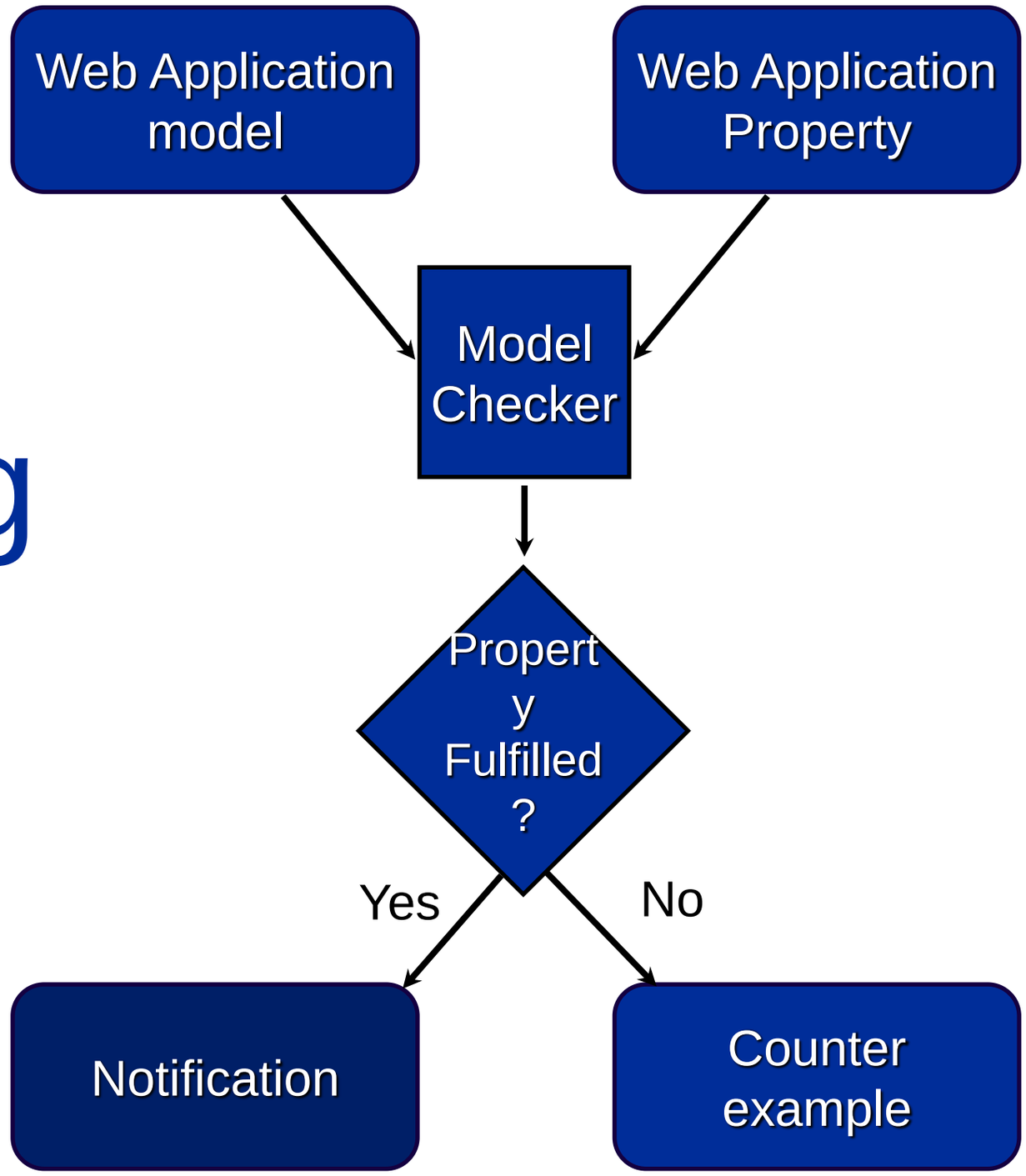
Commerce: online banking, online shopping,
Entertainment: online music, videos, games, learning software, simulation
Interaction: social networks: facebook, twitter, google+

Web Applications Design Issues

- **Navigation errors** mishandle unexpected user requests.
- **Global accessibility** makes them a target for many malicious users.
- **Programmer errors**.
- **External events**.

Model Checking

an automated technique which given a finite-state model of a system and a logical property,systematically checks whether this property holds for a given initial state in that model.



Edmund M. Clarke. The birth of model checking. In 25 Years of Model Checking, volume 5000 of Lecture Notes in Computer Science, pages 1-26, 2008.

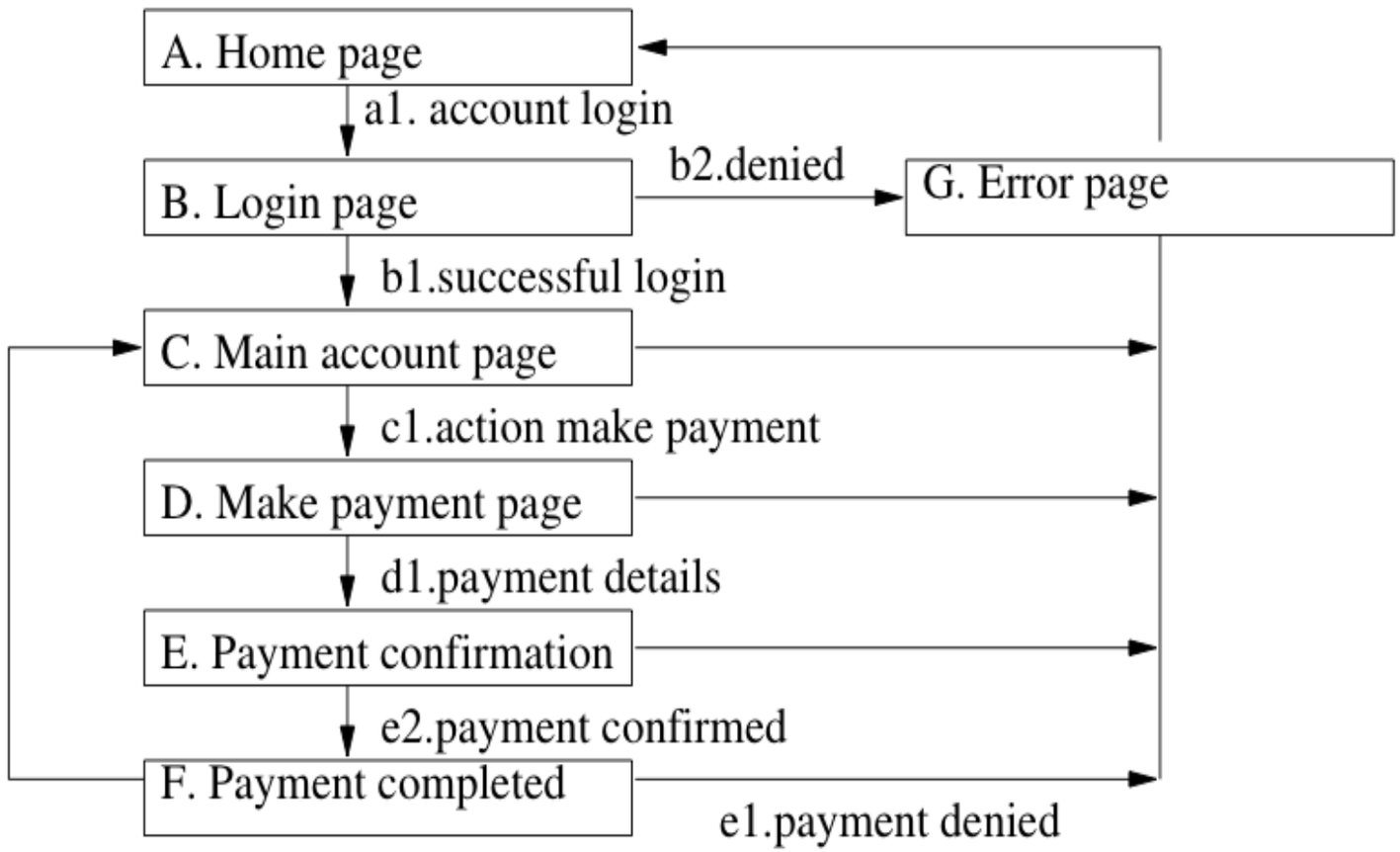
Modelling Time

Modelling time is critical to design realistic models of web applications.

We model the following **scenarios:**

- Timeouts
- Timestamp messages between communicating parties to trace activities
- Attack detection
- Data integrity
- Multi-channel transmission

Modelling the web application as a transition system



Modelling of the web applications as a transition system

Modelling formalism: finite-state automata:

Page Automaton

Internal State Automaton

Captured properties:

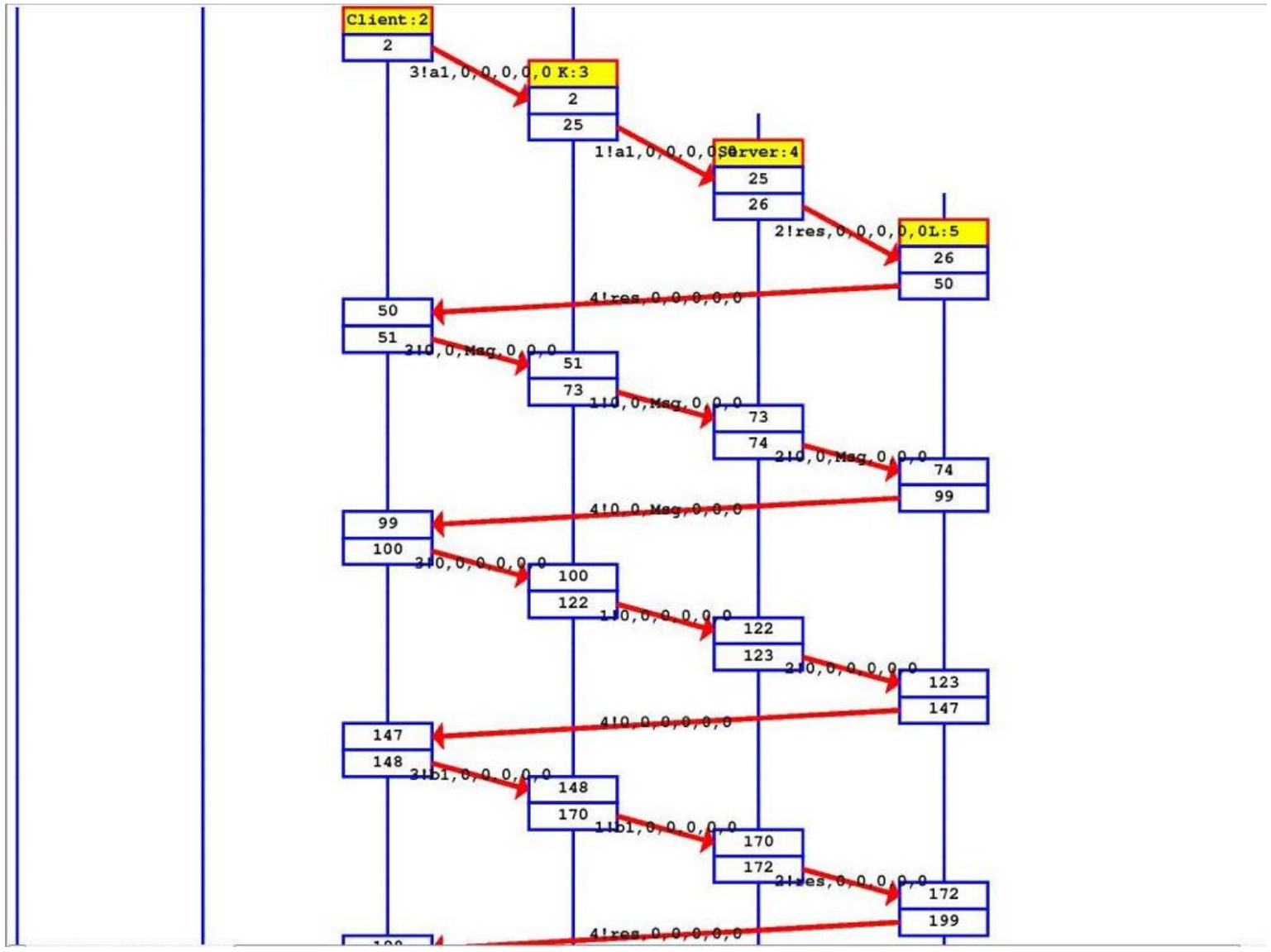
1. Authentication
2. Session management
3. Navigation properties.

Model Simulation

Simulation in **SPIN**:

Clearly identifiable:

Processes: early modelling faults can be detected
Steps
Process ownership
Process termination



Security assurance

- We were able to model both secure and compromised models.
- **Timed actions** versus **time stamps**: the advantage of graphical models.
- We were able to capture multi-channel transmission and formulate criteria for **correctness** and **termination** in both tools.

Additional properties

- Absence of attacks
- Non-repudiation
- Data integrity
- Timed actions
- Traceability

Research area 2

- Knowledge management systems
- Multi-agent systems
- Languages for knowledge modelling
  - -Modal Logic
  - -Epistemic Logic
- Modelling of knowledge processes
- Correctness check

Information Hierarchy

Data

- The raw material of information

Information

- Data organized or presented in some context

Knowledge

- Information read, heard or seen and understood

Wisdom

- Distilled and integrated knowledge and understanding

What is Knowledge Management

Knowledge management is a discipline that promotes an integrated approach to identifying, capturing, evaluating, retrieving and sharing all of enterprises information assets.

Knowledge management is a fluid mix of

- contextual information,
- valuable experiences
- predefined rules.

Static versus dynamic models.

What do we want from a knowledge management system ?

Systemic approach

Goal (for a known information need):

Return as many relevant documents as possible and as few non-relevant documents as possible.

Cognitive approach

Goal (in an interactive information-seeking environment, with a given knowledge management system):

Support the user’s exploration of the problem domain and the task completion.

Stages in Knowledge management

- Knowledge synthesis
- Knowledge modelling:

identification of suitable languages with respect to expressive power and decidability

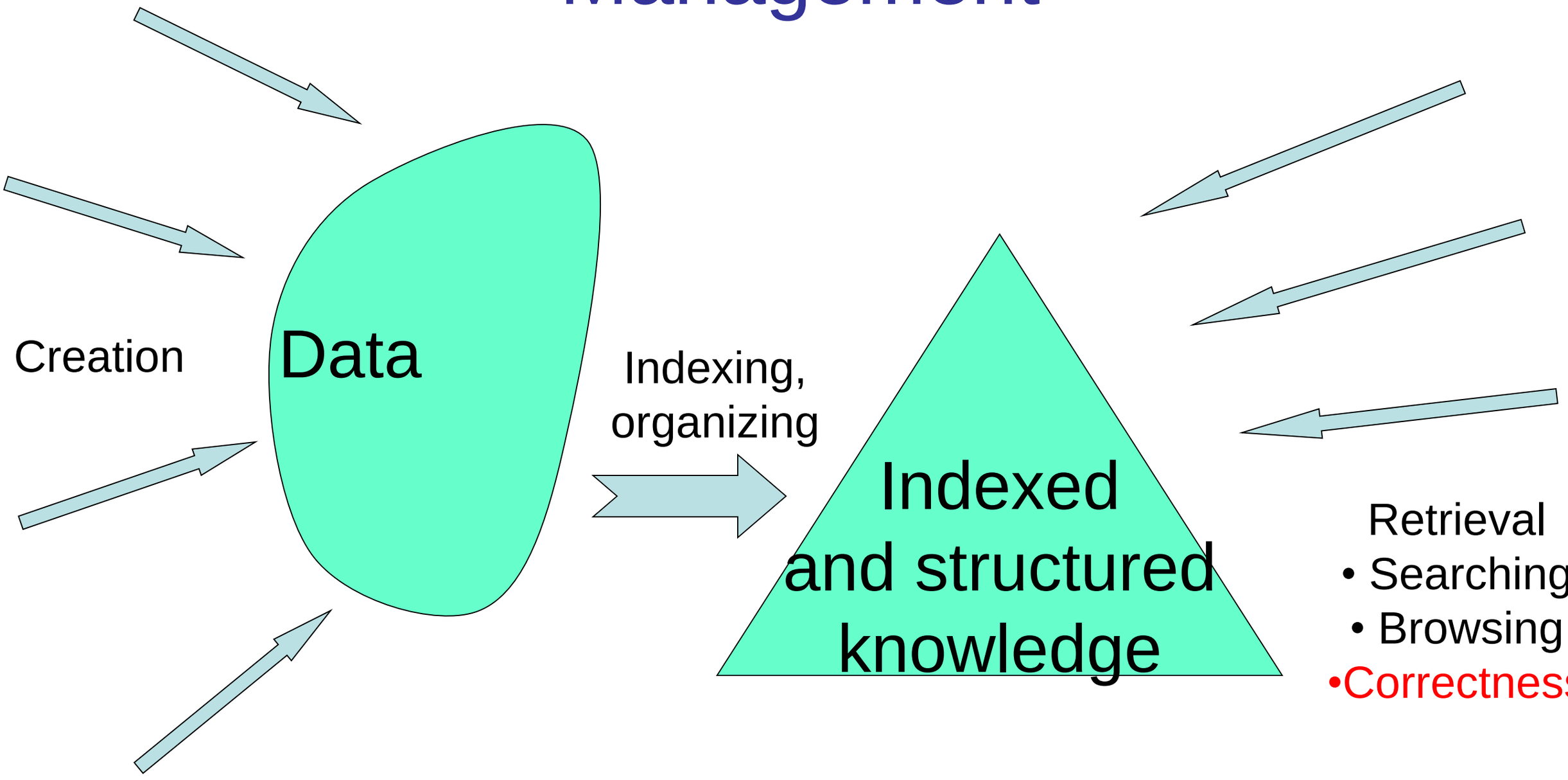
- Knowledge exchange

valid pre- and post-conditions

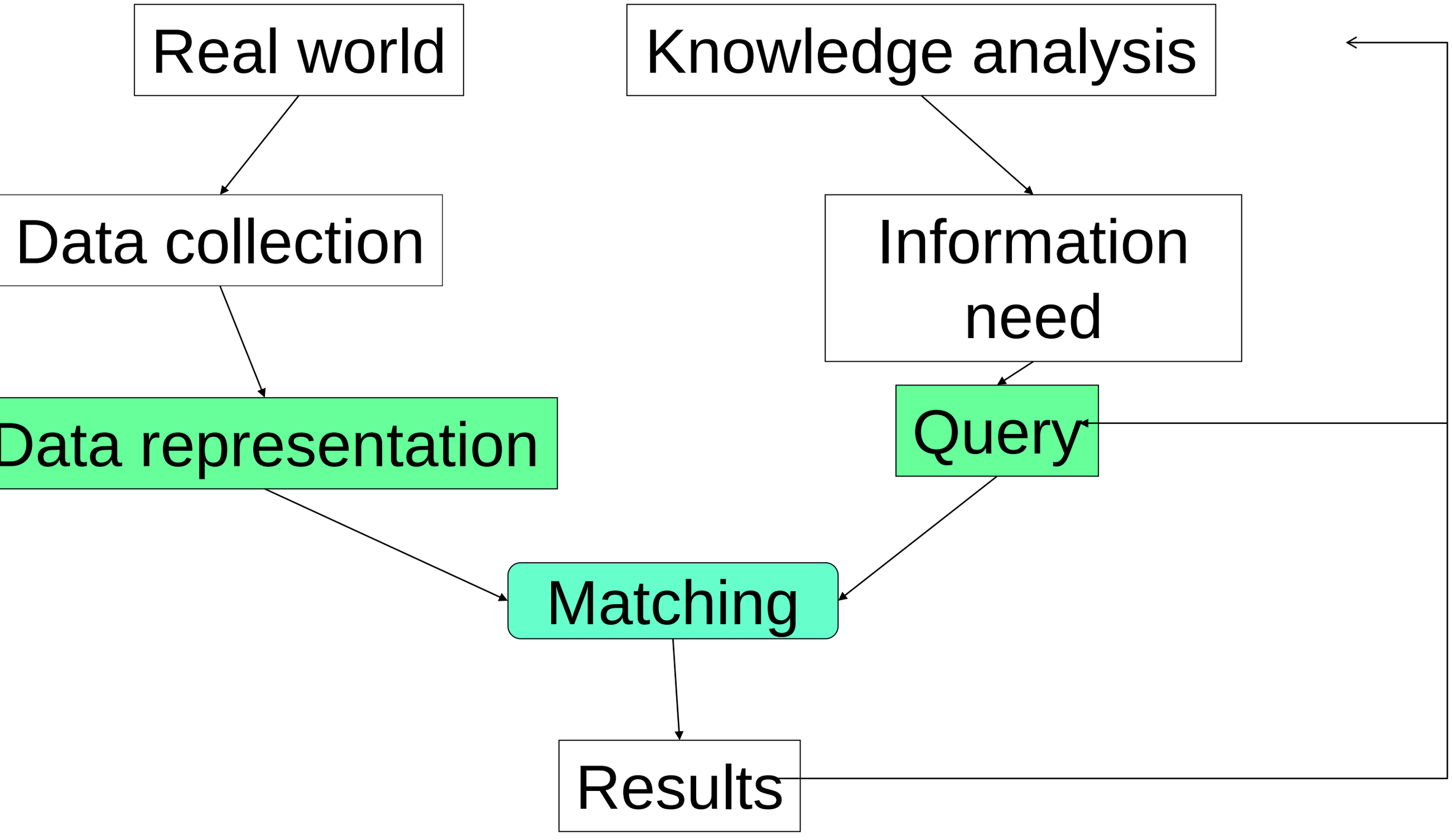
consistency

- The role of multi-agent systems

The stages of Knowledge Management



The formalized knowledge management process



Intelligent agents for knowledge management

- Intelligent agents are usefully applied in domains where flexible, autonomous, and goal directed action is required.
- Application areas:
  - distributed/concurrent systems
  - networks
  - human-computer interfaces

Distributed/concurrent systems

- The agent is seen as a natural metaphor, concurrent object programming.
- Example domains:
  - air traffic control
  - business process management
  - power systems management
  - distributed sensing
  - factory process control

Network applications

- Mobile agents, that can move themselves around a network (e.g., the Internet) and can operate on a user's behalf.
- Applications include:

  hand-held PDAs with limited bandwidth

  information gathering

Human computer interfaces and machine learning

- Use of agent in interfaces
- The idea is to move away from the direct manipulation paradigm.
- Agents sit ‘over’ applications, watching, learning, and eventually doing things without being told — taking the initiative
- Current applications
  - news readers, web browsers, mail readers

Multi-agent framework: static versus dynamic modelling

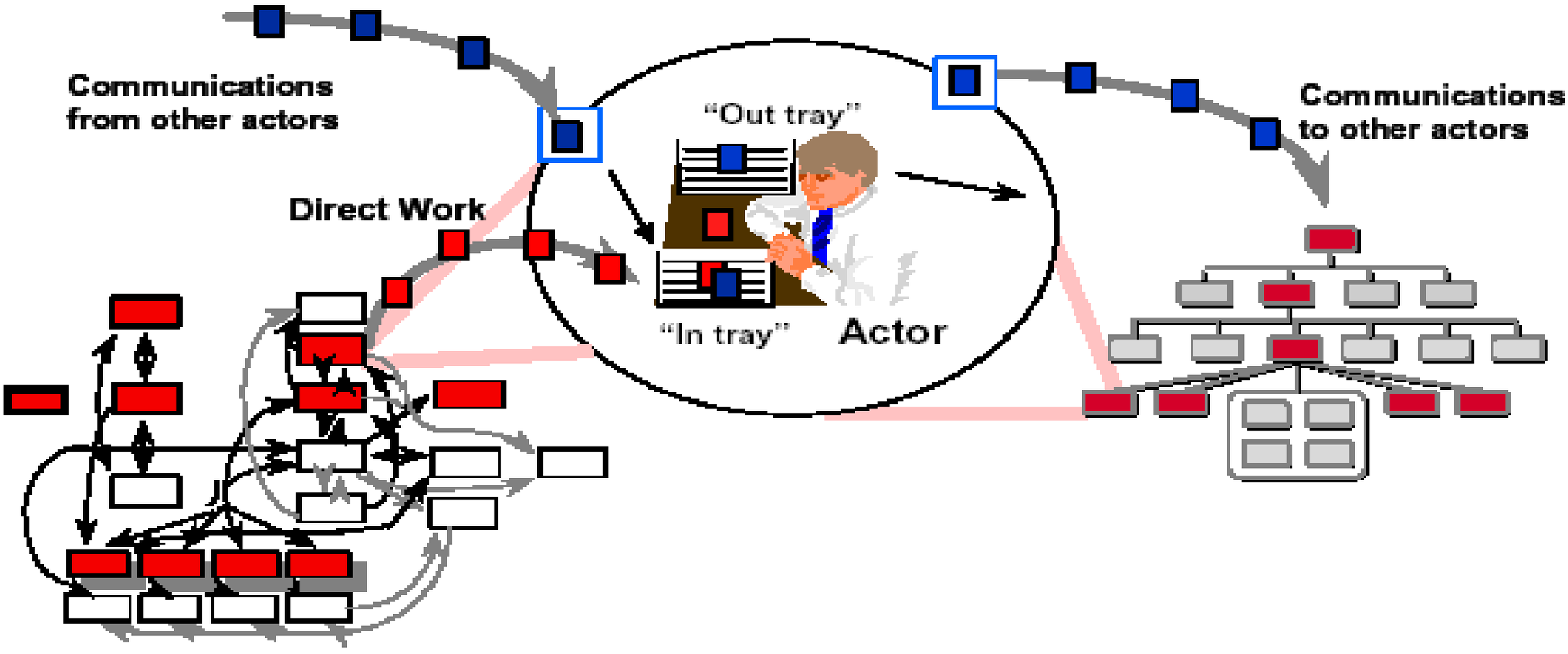


Figure 3 VDT Information Processing View of Knowledge Work

Information processing view of knowledge management is limited to static combination of natural language.

Women in Computing

What is the issue?

- Who? Why? How?
- Marie-Curie Fellowships
- ACM
- Local organizations?

Thank you!

Questions?