Financial Security &Machine Learning

김민경
daengky@naver.com

BICube™

2015.02.10

Outline

- Intorduction
- Immune System
- Machine Learning
- Solutions

• Introduction

Motive

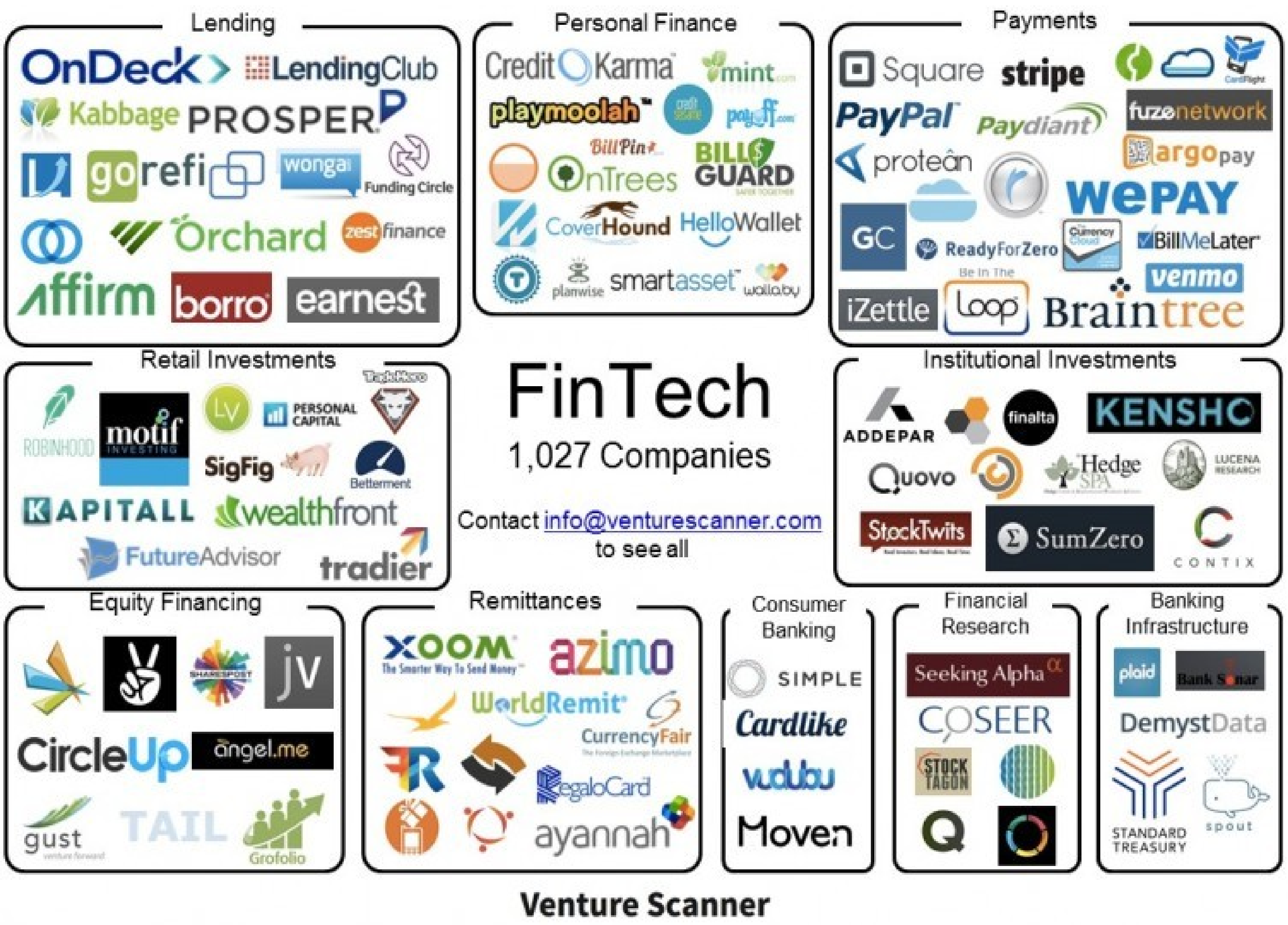
신제윤 금융위원장은 금융보안을 위해 모든 금융권이 이상거래탐지시스템**(FDS)** 구축을 완료해야 한다고 촉구했다.

“핀테크 활성화 방안을 추진하기 위해서 **반드시 전제**돼야 할 사항은 **보안의 중요성**“이라며 **“정보보안이 확보되지 않은 서비스는 결국 사상누각이 될 것**“이라고 우려했다.

그는 핀테크**(Fintech)** 추진 방안과 관련해서는 **“오프라인 위주의 금융제도 개편**을 통해 핀테크 기술이 금융에 자연스럽게 접목될 수 있도록 지원할 것“이라며 **“전자금융업종 규율을 재설계**토록 하겠다“고 밝혔다.

• Introduction

FinTech



Introduction

Fraud Detection Basics

- Outlier Detection
  - detecting data points that don't follow the trends and patters in the data
  - rule base detection
  - anomaly detection
- Two approaches for treating input
  - focus on **instance** of data **point**
  - focus on **sequence** of data **points**
- Three kinds of algorithms
  - building a model out of data
  - using data directly.
  - immunse system base on temporal data
- Real time fraud detection
  - feasible with model based approach
  - A model is built with **batch processing** of training data
  - A real time stream processor ***uses the model*** and makes **predictions in real time**

Economy Imperative

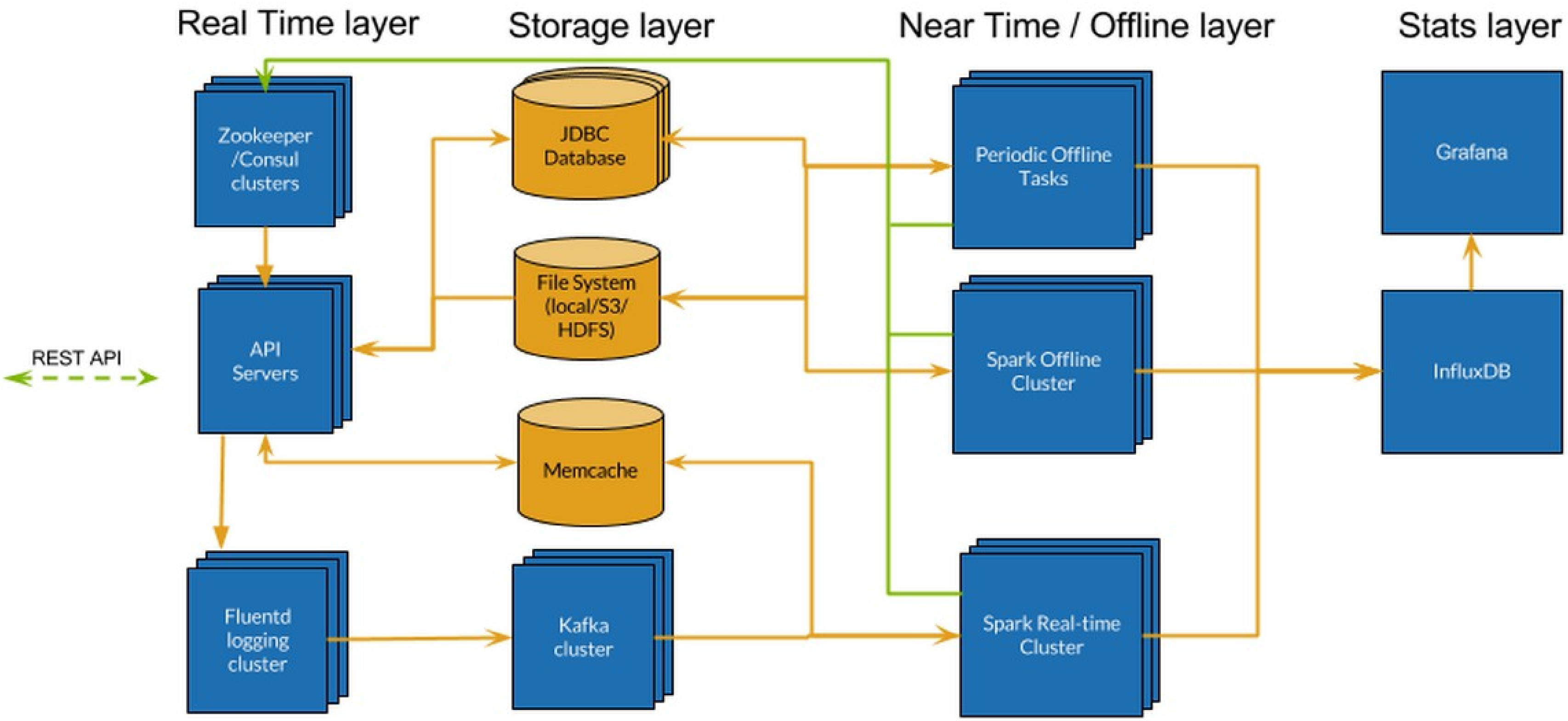
- Not worth spending $200m to stop $20m fraud
- The Pareto principle
  - fthe first 50% of fraud is easy to stop
  - next 25% takes the same effort
  - next 12.5% takes the same effort
- Resources available for fraud detection are always limited
  - around 3% of police resources go on fraud ?
  - this will not significantly increase
- If we cannot outspend the fraudsters we must out-think them

Open Source Bigdata Ecosystem

- Query (NOSQL) : Cassandra, HBase, MongoDB and more
- Query (SQL) : Hive, Stinger, Impala, Presto, Shark
- Advanced Analytic : Hadoop, Spark,H2O
- Real time : Storm, Samza, S4, Spark Streaming

• Introduction

Bigdata Ecosystem



Seldon infrastructure

- Real-Time Layer : responsible for handling the live predictive API requests.
- Storage Layer : various types of storage used by other components.
- Near time / Offline Layer : components that run compute intensive or otherwise non-realtime jobs.
- Stats layer : components to monitor and analyze the running system.

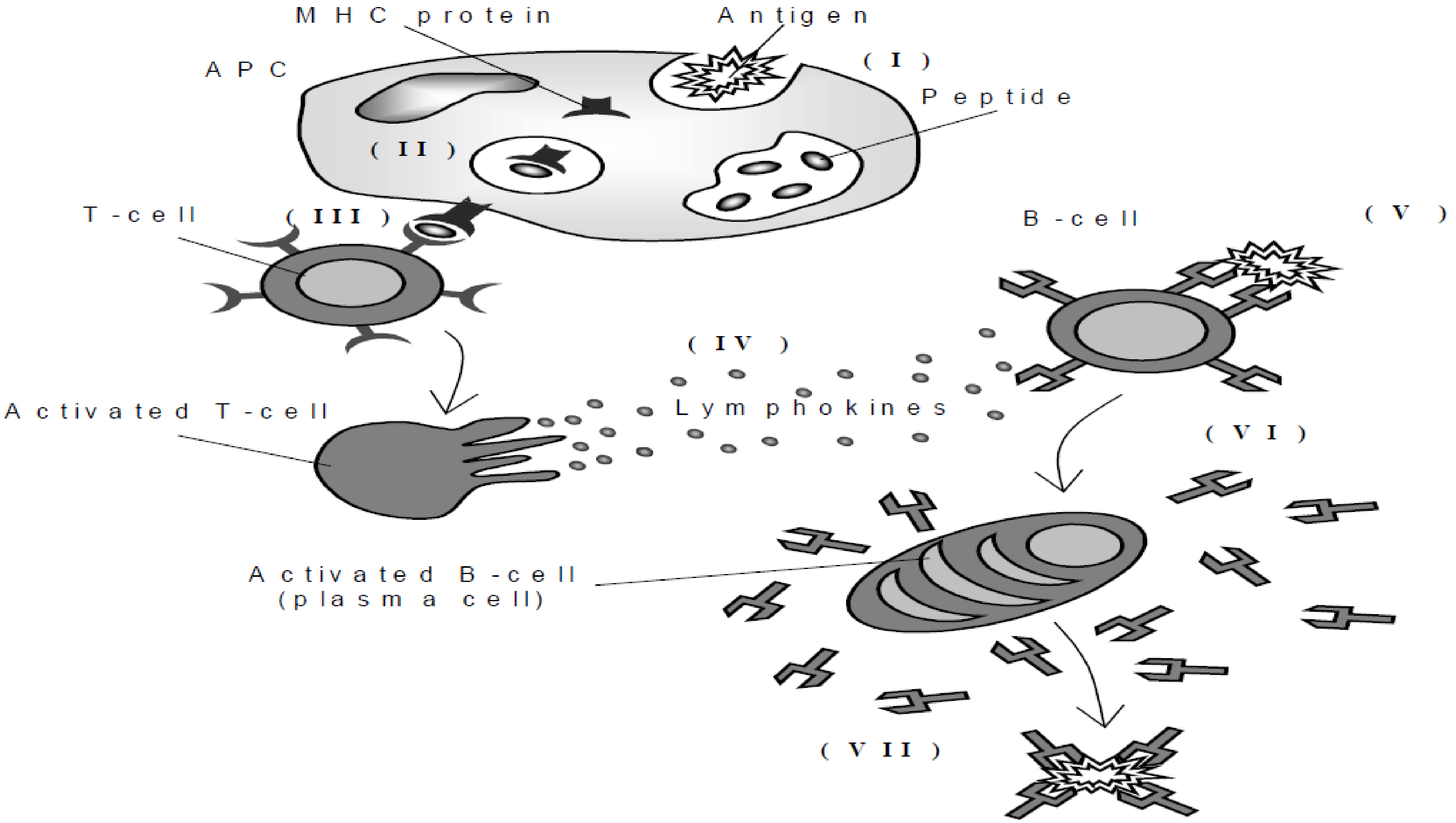
• Immune Systems Aritifical Immune Systems

AIS are adaptive systems inspired by theoretical immunology and observed immune functions, principles and models, which are applied to complex problem domains

- Immune system needs to be able to differentiate between ***self and non-self*** cells
- may result in ***cell death*** therefore
  - Some kind of **positive selection(Clonal Selection)**
  - Some kind of **negative selection**

• Immune Systems

Simple View

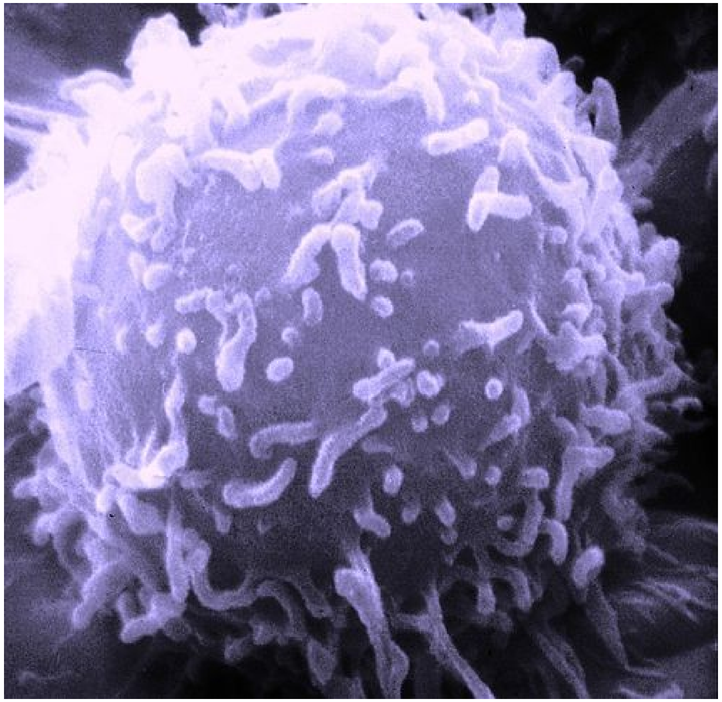


Immune Systems

Lymphocyte(림프구)

무과립성 백혈구(無顆粒性 白血球, **agranulocyte**)의 일종으로 면역 기능 관여하며 전체 백혈구 중에서도 **30%**를 차지한다.

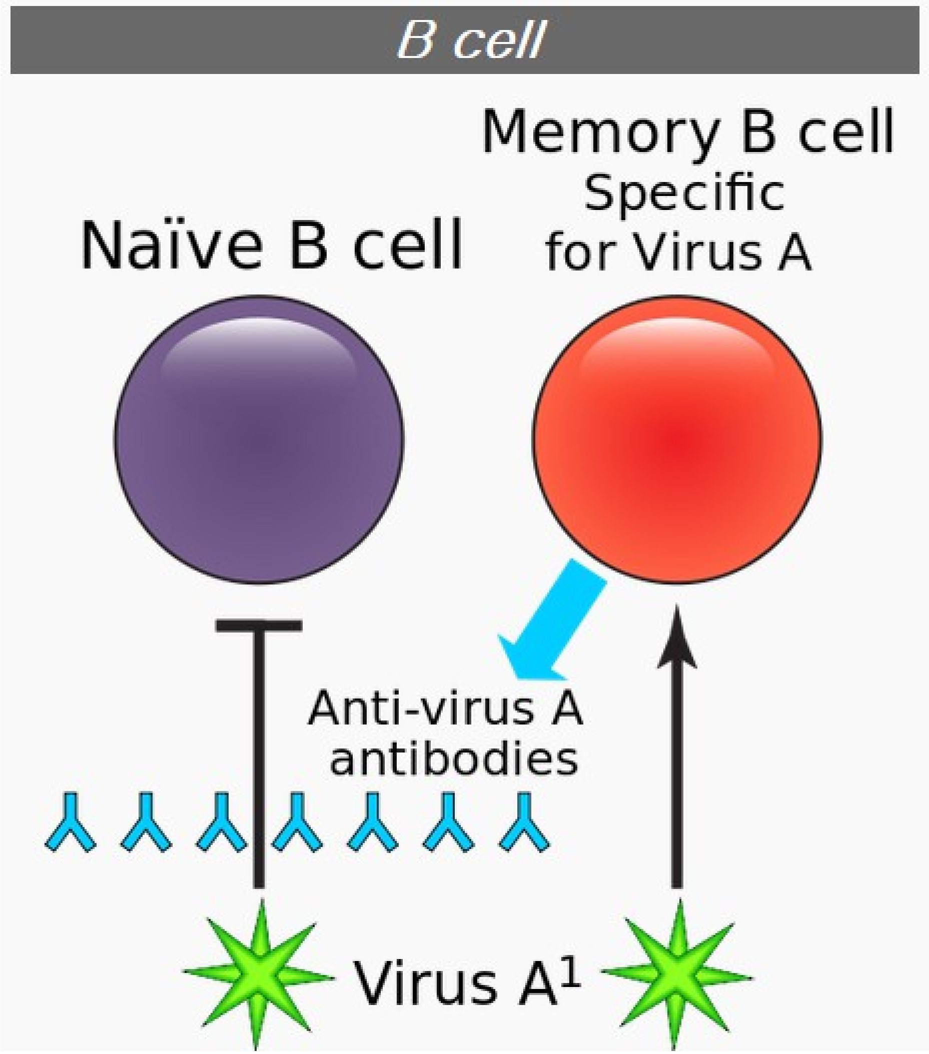
- **T**세포**(T cell)**
  - 보조 **T**세포**(Helper T cell)**
  - 세포독성 **T**세포**(killer T cell)**
  - 억제 **T**세포**(suppressor T cell)**
- **B**세포**(B cell)**
- **NK**세포**(Natural killer cell, NK cell)**

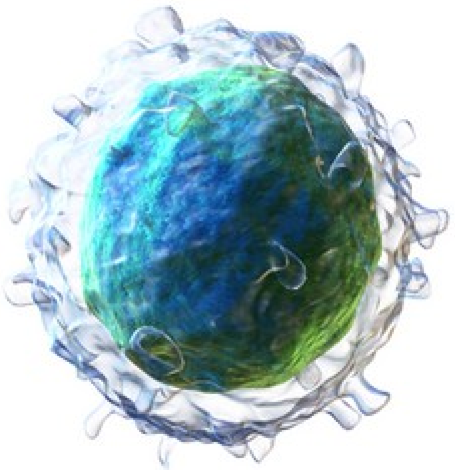


• Immune Systems

B cell

B 세포(**B**細胞, **B cell**)는 림프구 중 항체를 생산하는 세포





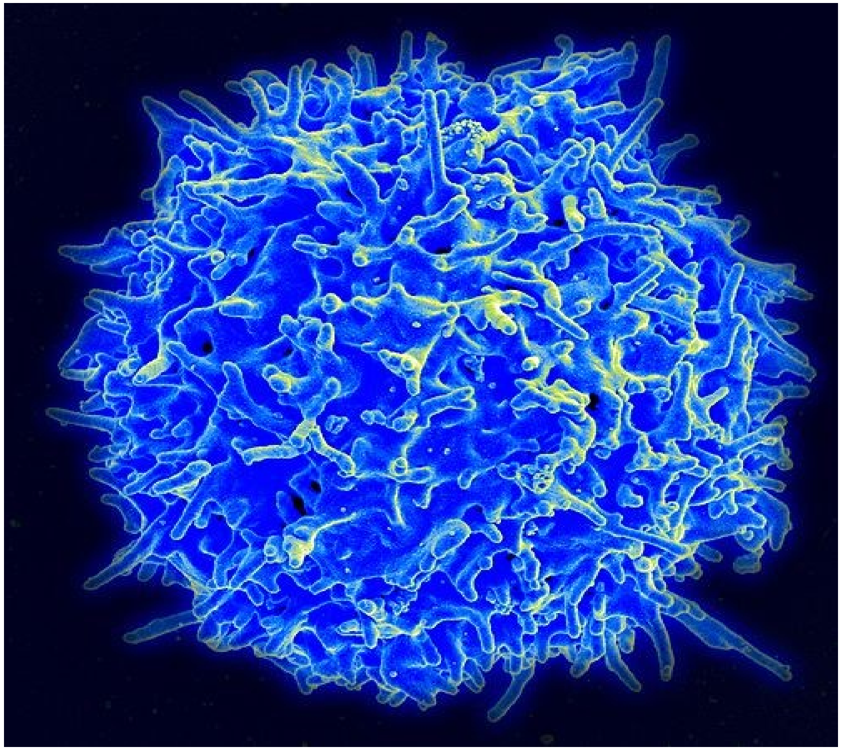
Lymphocyte

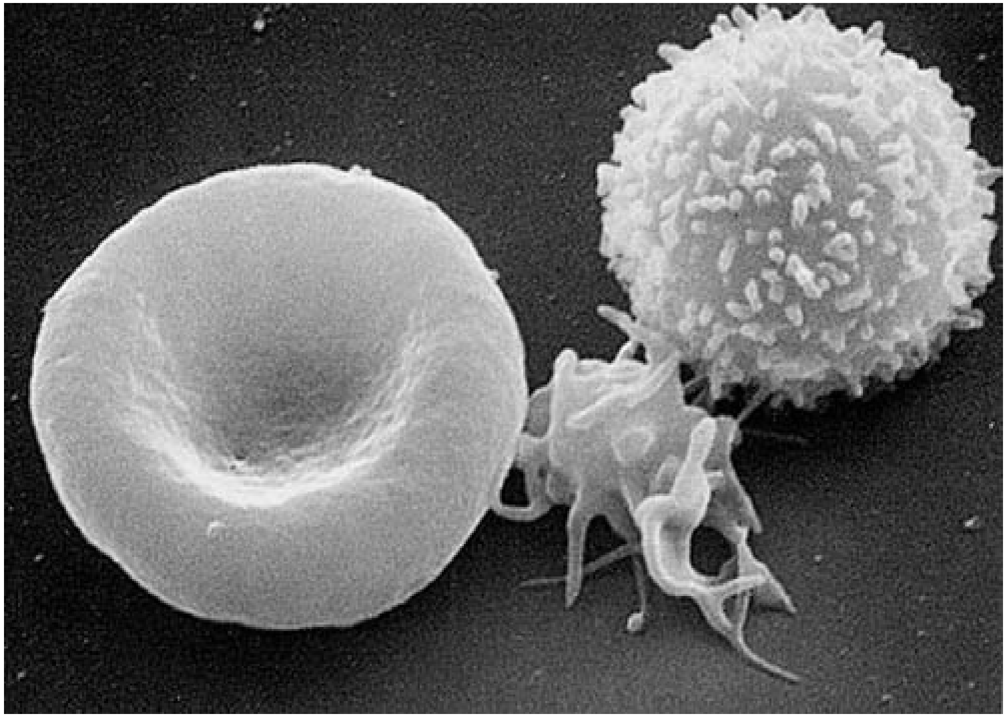
B cell

• Immune Systems

T cell

T세포(T細胞, T cell) 또는 T림프구(T lymphocyte)는 항원 특이적인 적응 면역을 주관하는 림프구의 하나이다. 가슴샘(Thymus)에서 성숙되기 때문에 첫글자를 따서 T세포라는 이름이 붙었다. 전체 림프구 중 약 4분의 3이 T세포



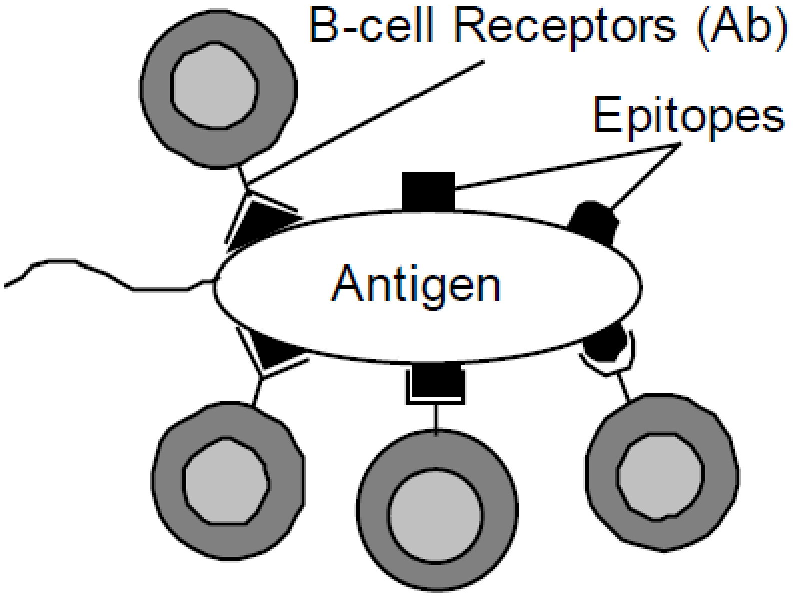


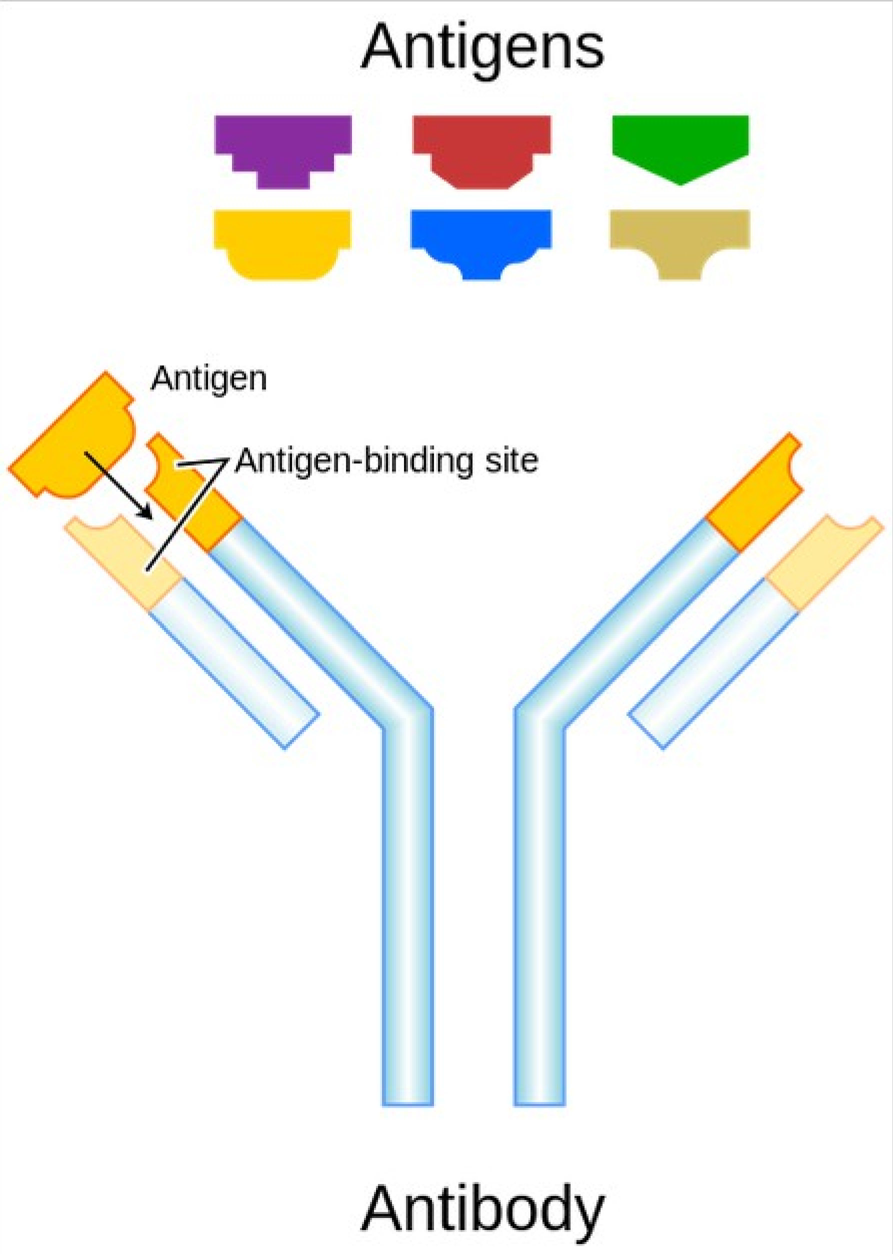
T세포는 아직 항원을 만나지 못한 미접촉 T세포와, 항원을 만나 성숙한 효과 T세포(보조 T세포, 세포독성 T세포, 자연살상 T세포), 그리고 기억 T세포로 분류

• Immune Systems

Antibody, Antigen

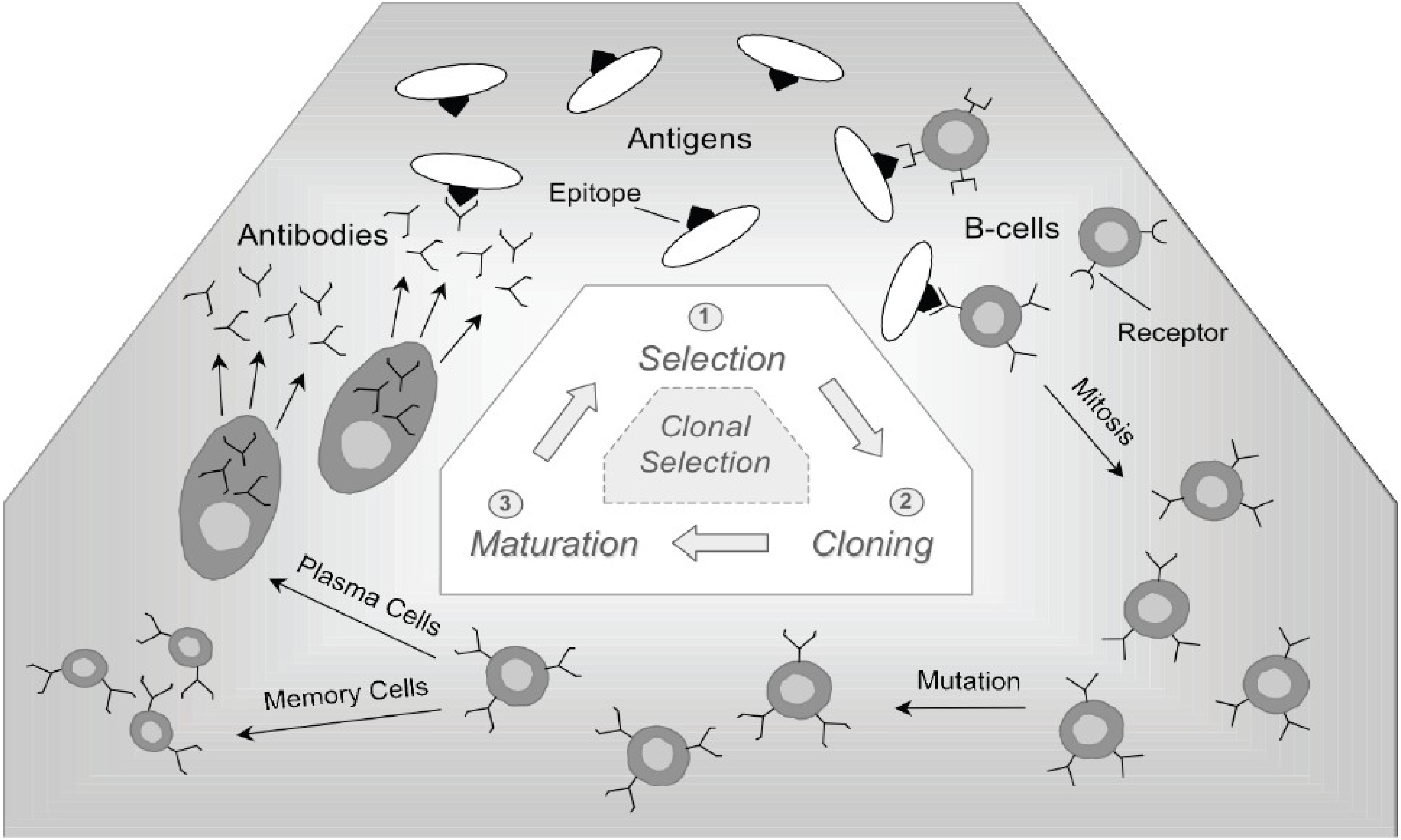
each antibody can recognize a single antigen





• Immune Systems

Biological Immune System



Immune Systems

Danger Theory

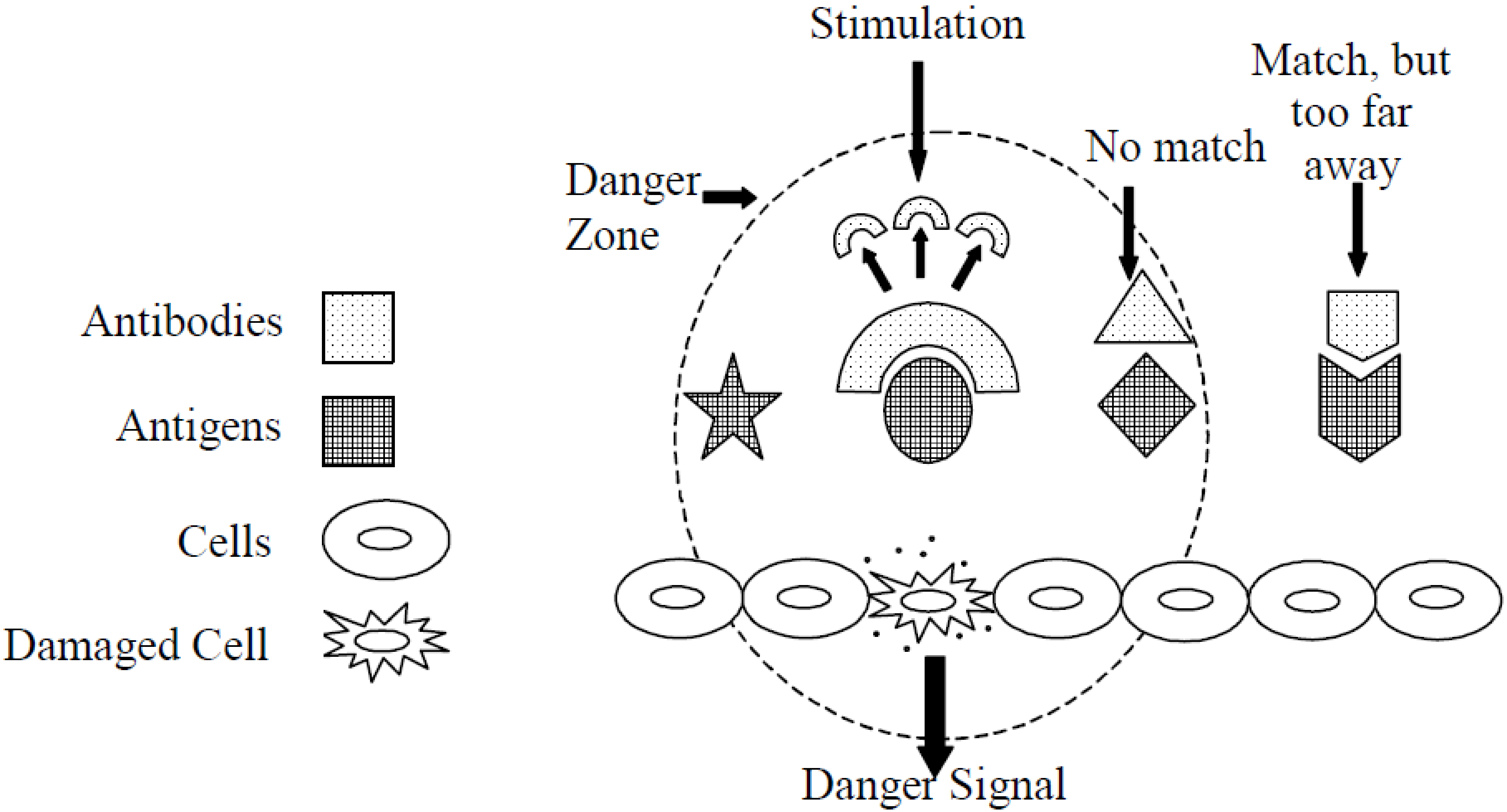
- Proposed by Polly Matzinger, around 1995
- Traditional self/non-self theory doesn't always match observations
  - Immune system always responds to non-self
  - Immune system always tolerates self
- Antigen-presenting cell(APC):T-cell activation by APCs
- Danger theory relates innate and adaptive immune systems
  - Tissues induce tolerance towards themselves
  - Tissues protect themselves and select class of response

Danger Theory

- Tissues induce tolerance by
  - Lymphocytes receive 2 signals
    - antigen/lymphocyte binding
    - antigen is properly presented by APC
  - Signal 1 WITHOUT signal 2 : lymphocyte death
- Tissues protect themselves
  - Alarm Signals activate APCs
    - Alarm signals come from
      - Cells that die unnaturally
      - Cells under stress
  - APCs activate lymphocytes
- Tissues dictate response type
  - Alarm signals may convey information

• Immune Systems

Danger Theory



Artificial Immune System

Artificial Immune Systems

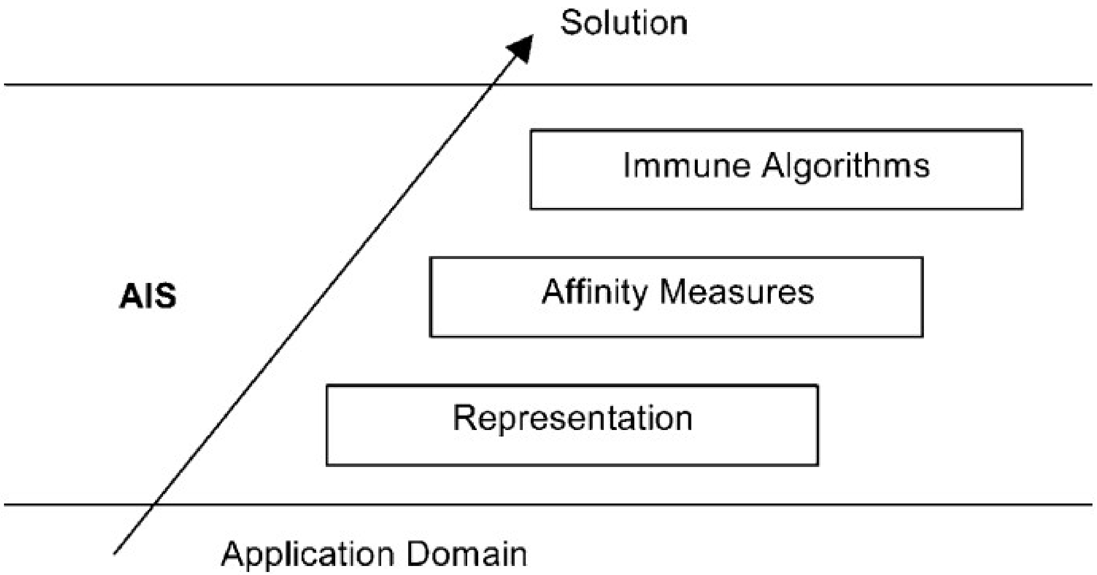
- Vectors

  Ab = {Ab_1, Ab_2, ..., Ab_L}

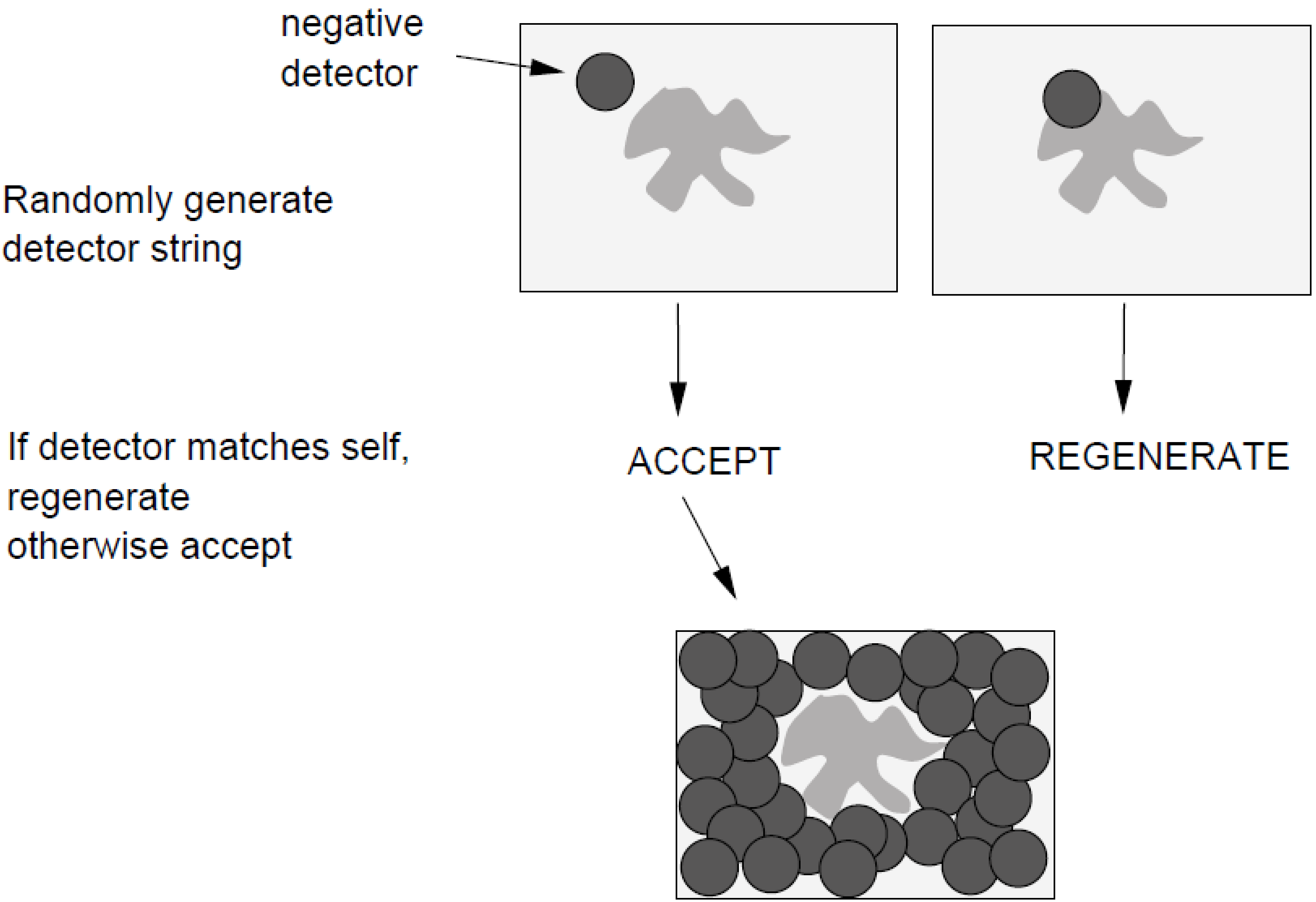
  Ag = {Ag_1, Ag_2, ..., Ag_L}

- Real-valued shape-space
- Integer shape-space
- Binary shape-space
- Symbolic shape-space

$$D=\sqrt{\sum_{i=1}^{L}(Ab_i-Ag_i)^2}$$



Artificial Immune System



negative detector

Randomly generate detector string

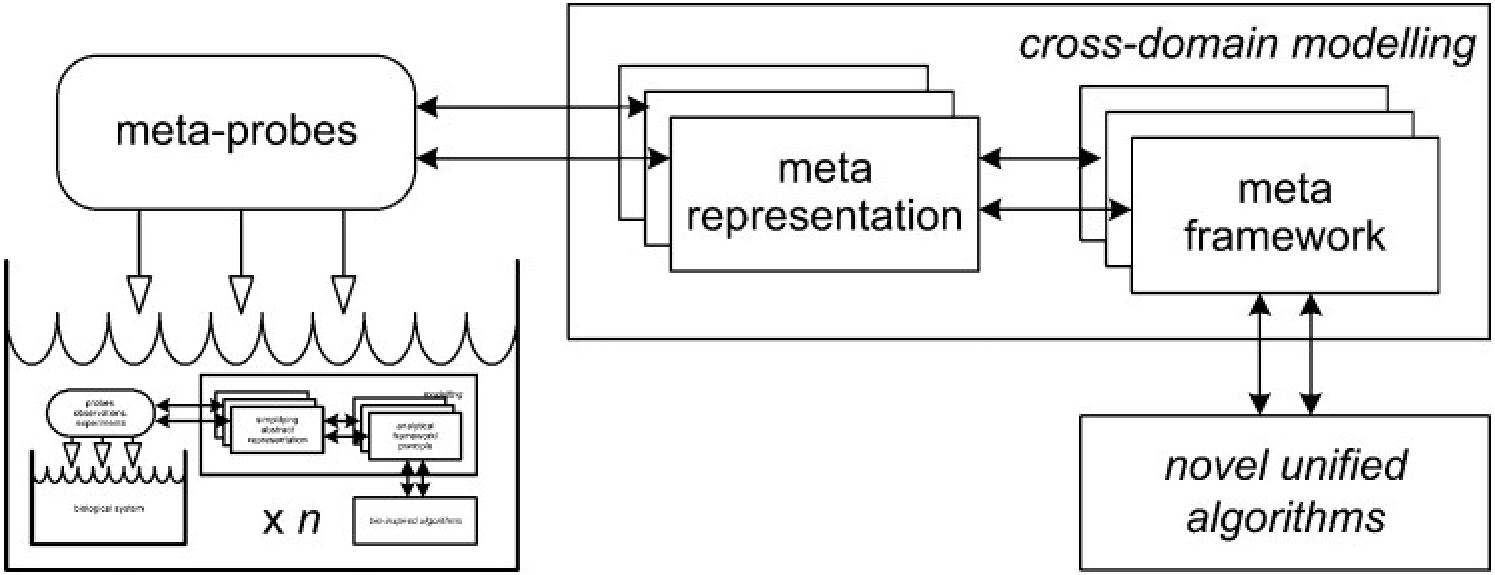
If detector matches self,
regenerate
otherwise accept

ACCEPT

REGENERATE

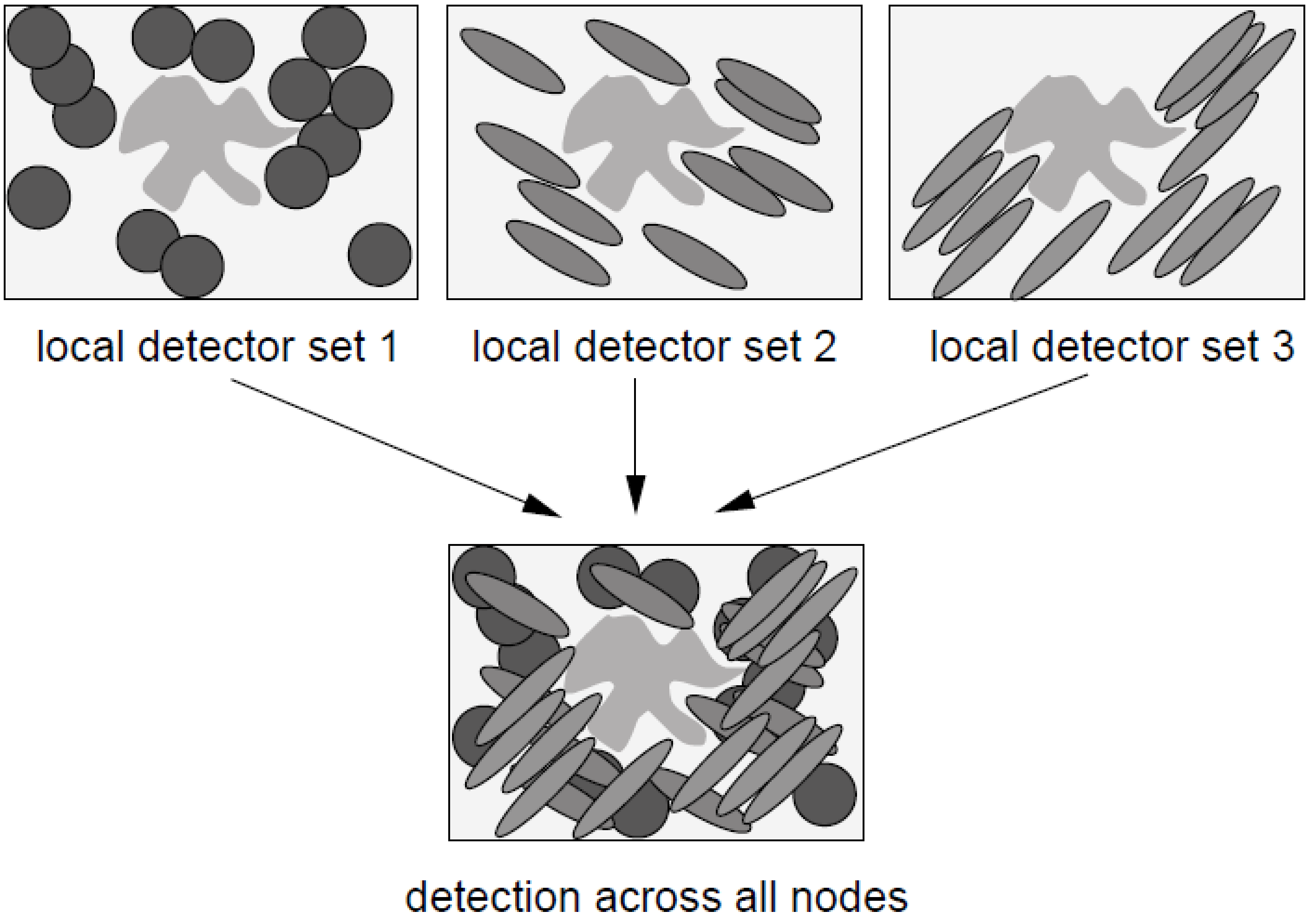
Artificial Immune System

Meta-Frameworks



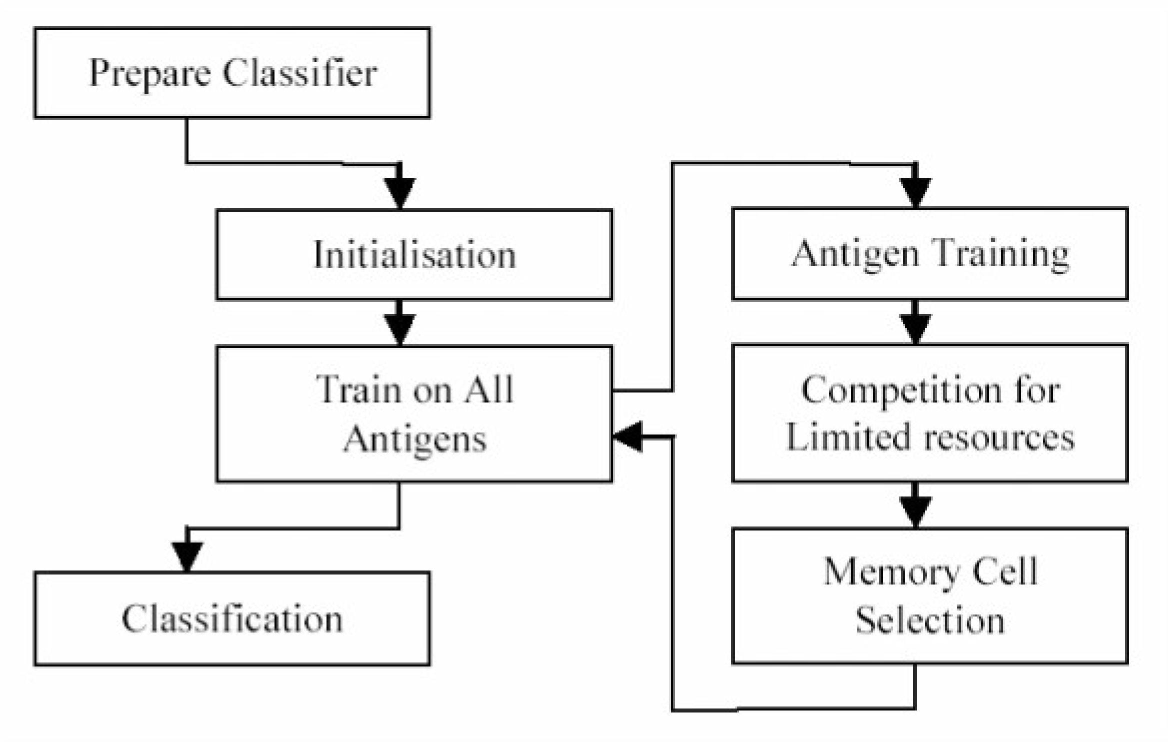
- **Immune Systems**

Artificial Immune System



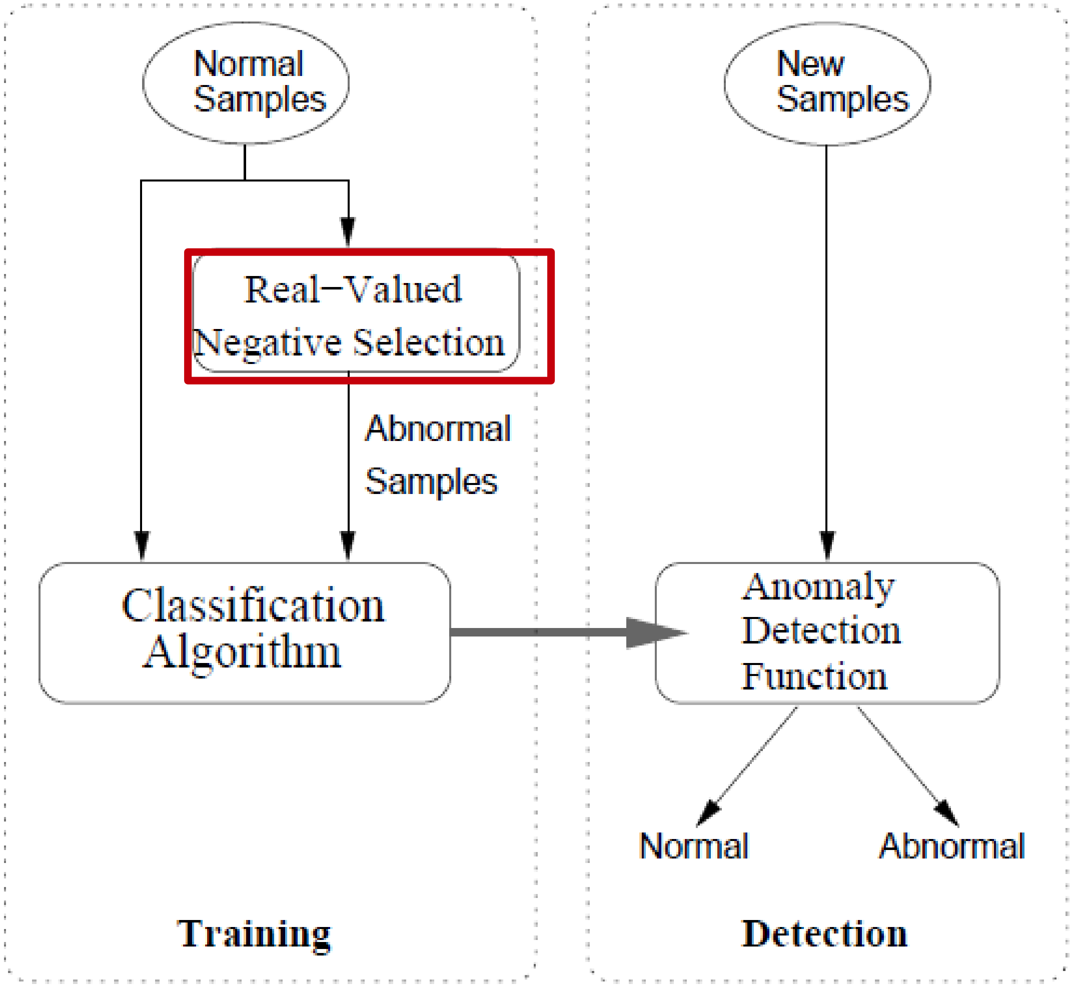
- Immune Systems

Artificial Immune Recognition System



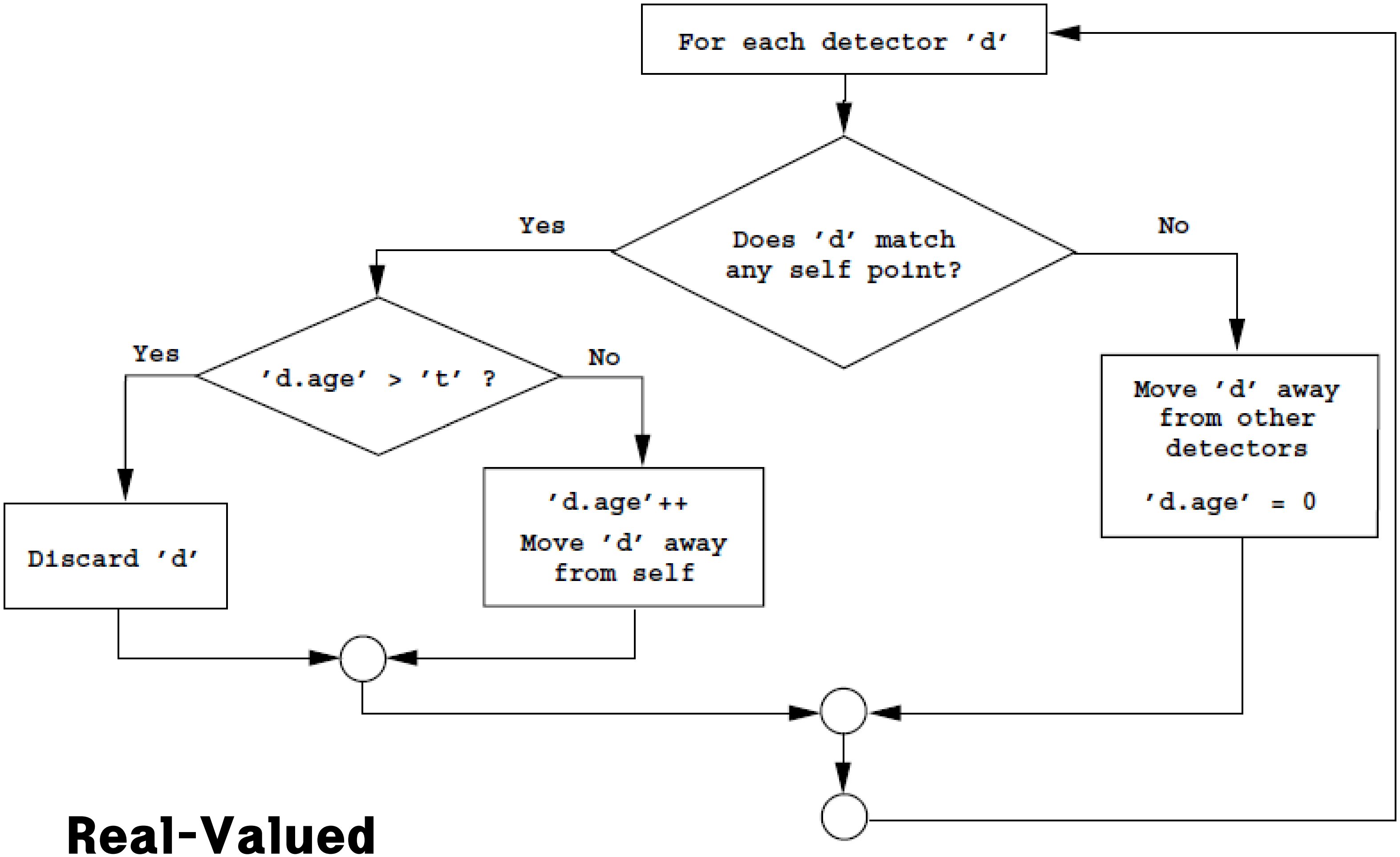
• Immune Systems

Hybrid Immune Learning



- **Immune Systems**

Hybrid Immune Learning

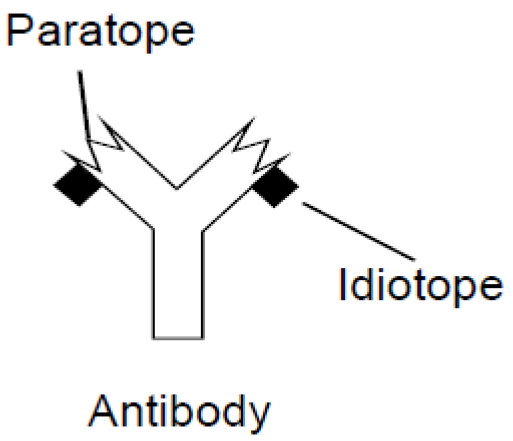


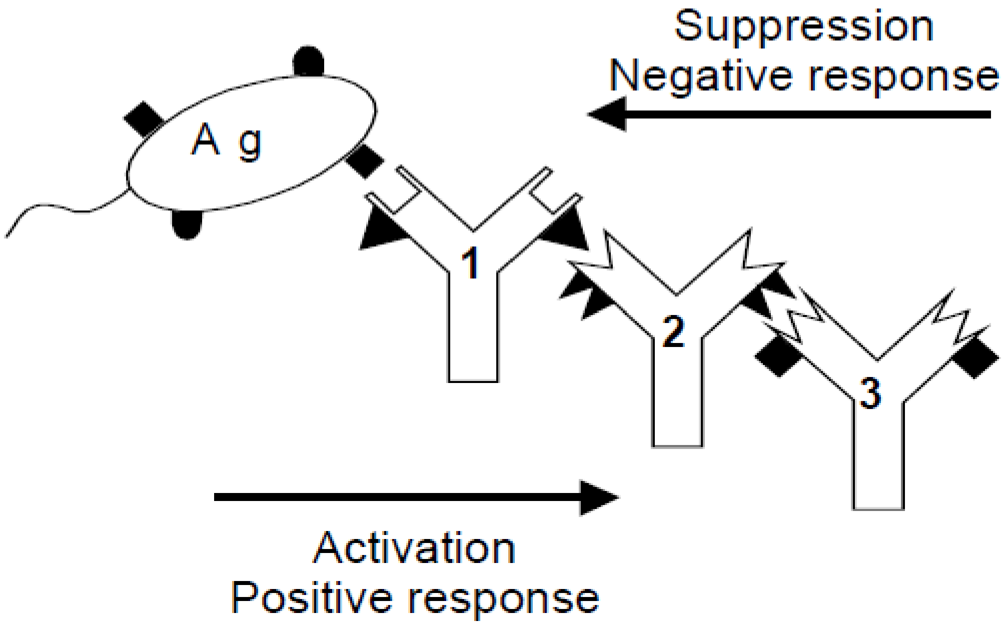
Real-Valued Negative Selection

• Immune Systems

Immune Network Theory

- Idiotypic network (Jerne, 1974)
- B cells <u>co-stimulate</u> each other
  - Treat each other a bit like antigens
- Creates an immunological **<u>memory</u>**



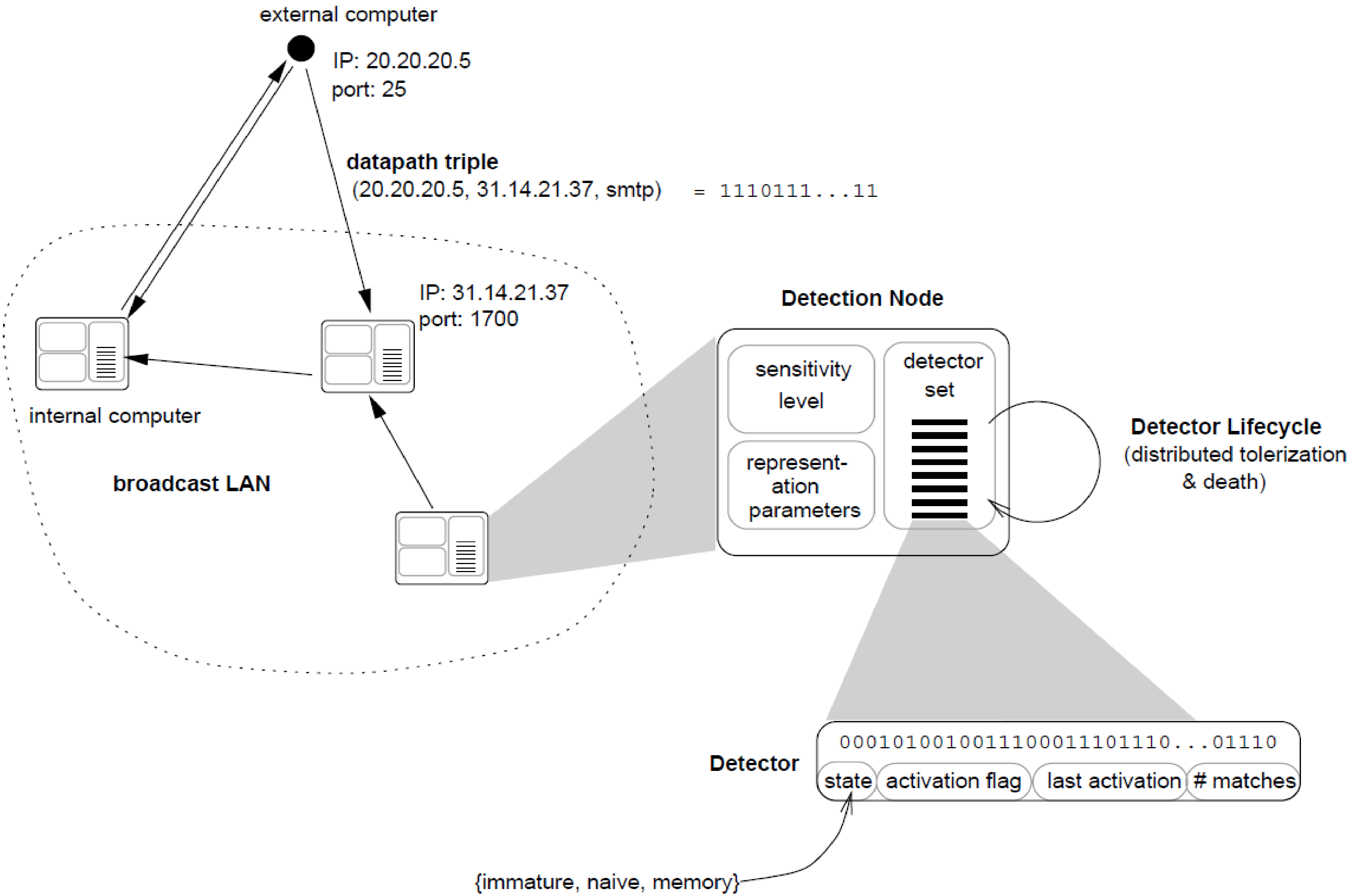


Non-self Detection Principle

For natural immune system, all cells of body are categorized as two types of **self and non-self**. The immune process is to **detect non-self** from cells.

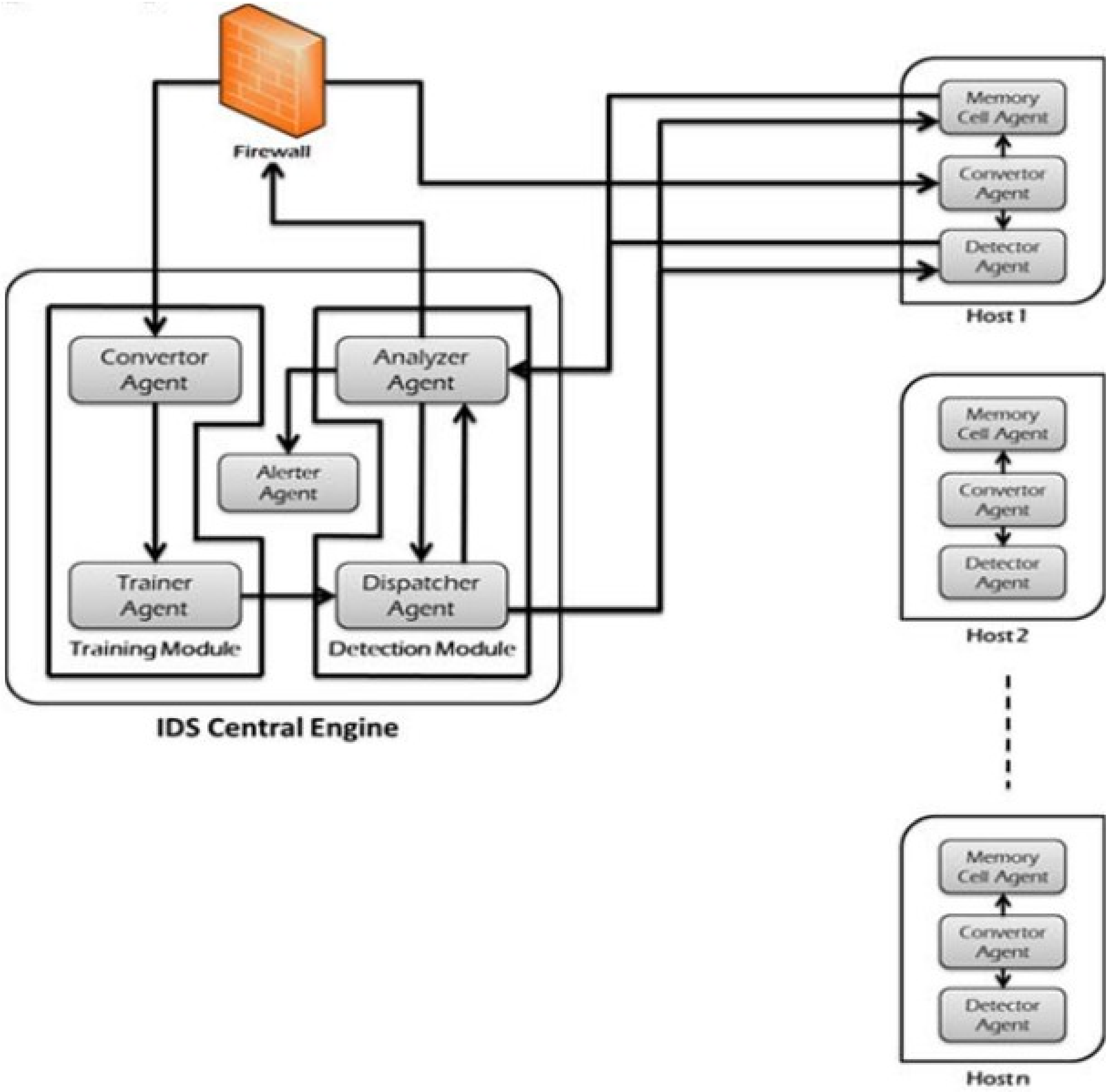
use the Positive Selection Algorithm (PSA) to perform the **non-self detection** for recognizing the malicious executable.

• Immune Systems Network Security

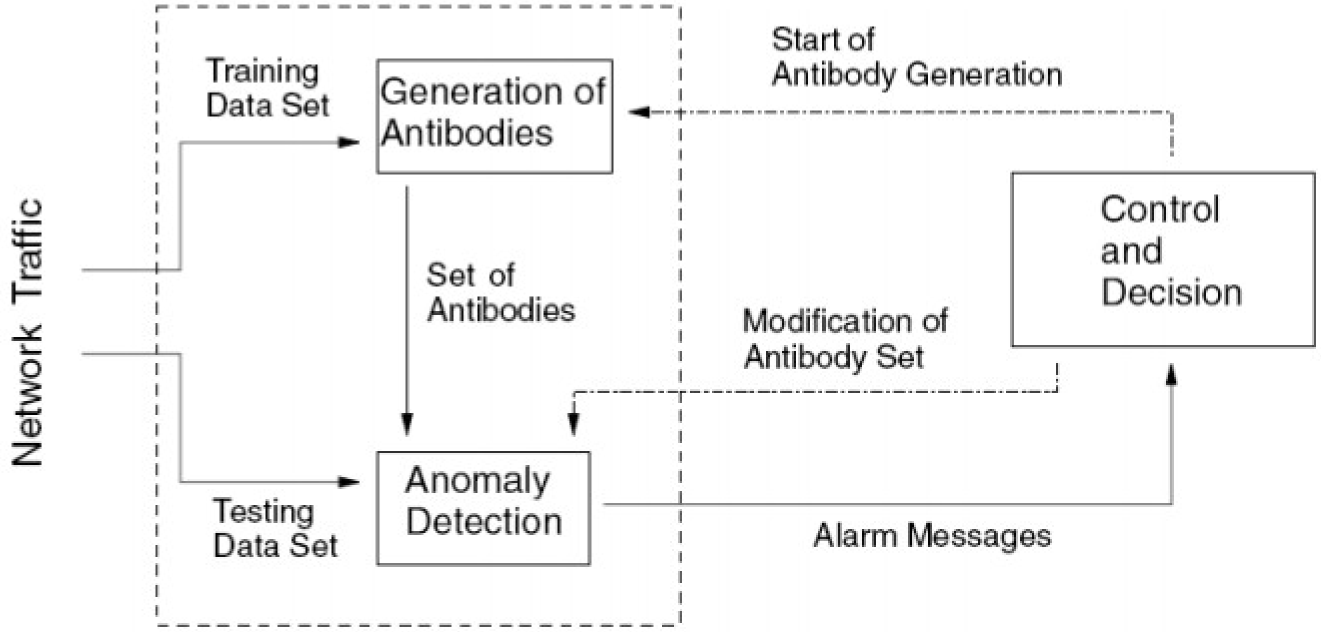


- **Immune Systems**

Intrusion Detection Systems



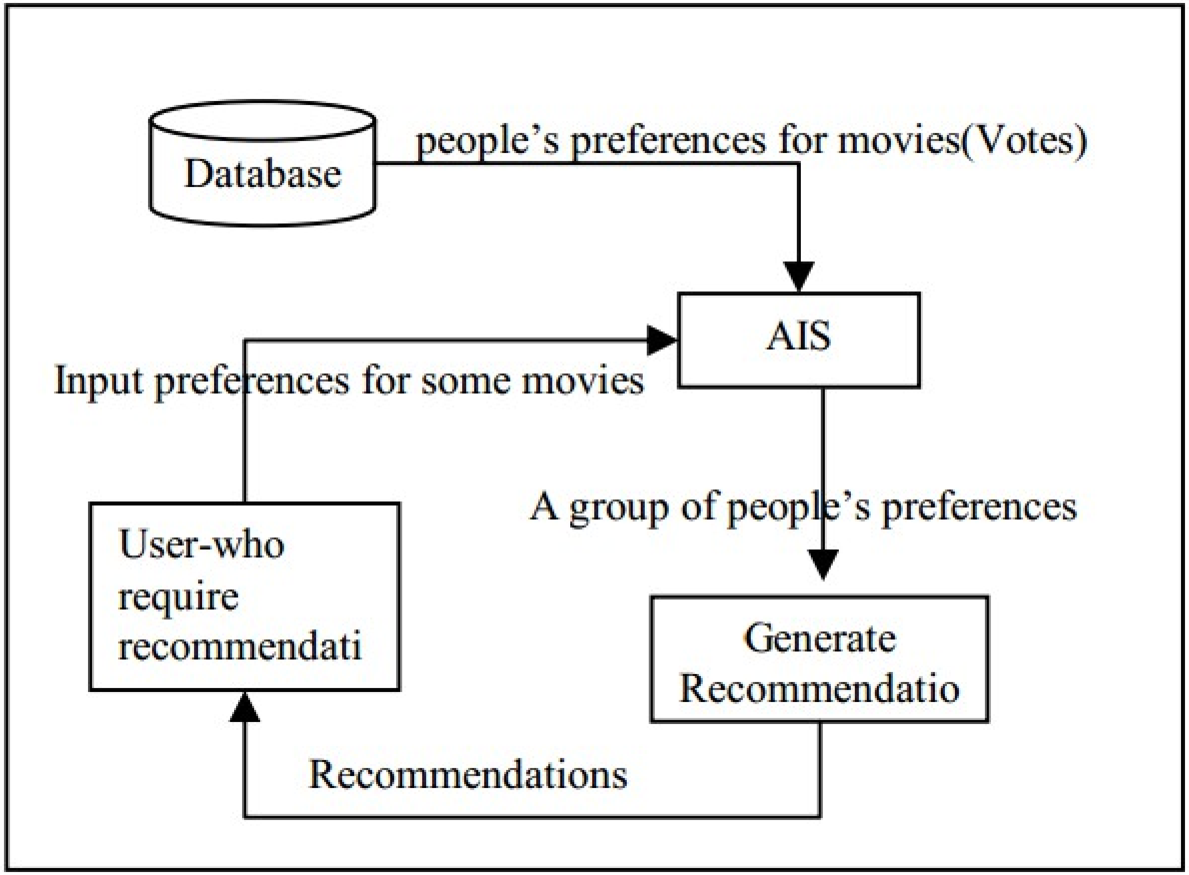
• Immune Systems Network Security



Architecture of anomaly detection system.

- **Immune Systems**

Movie Recomendation Systems

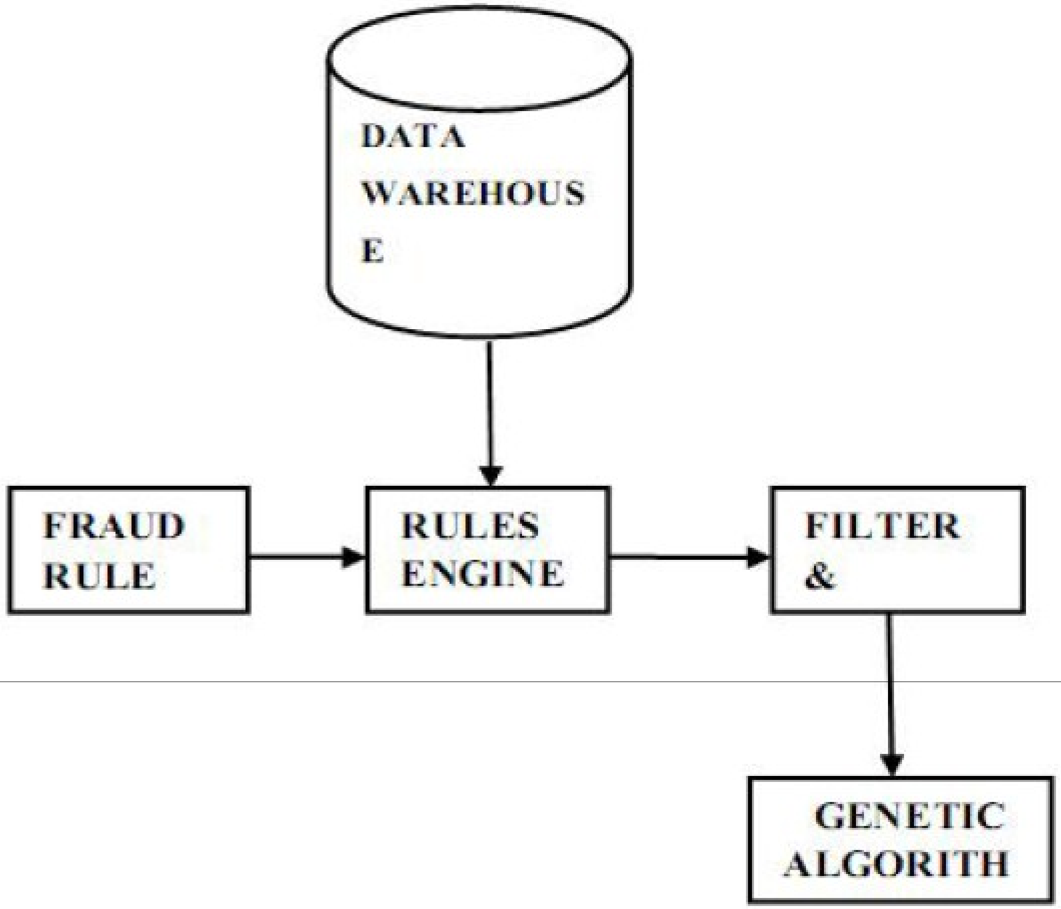

Database
people's preferences for movies(Votes)
AIS
Input preferences for some movies
A group of people's preferences
User-who require recommendati
Generate Recommendatio
Recommendations

Machine Learnig Types

- Supervised learning : 지도학습
  - Data의 종류를 알고 있을 때(Category, Labeled)
  - ex: spam mail
- Unsupervised : 비지도학습
  - Data의 종류는 모르지만 패턴을 알고 싶을 때
  - SNS, Twitter
- Semi-supervised learning : 지도학습 + 비지도학습
- Reinforcement learning : 강화학습
  - 잘못된 것을 다시 피드백
- Evolutionary learning : 진화학습(GA, AIS)
- Meta Learning : Landmark of data for classifier

Machine Learnig

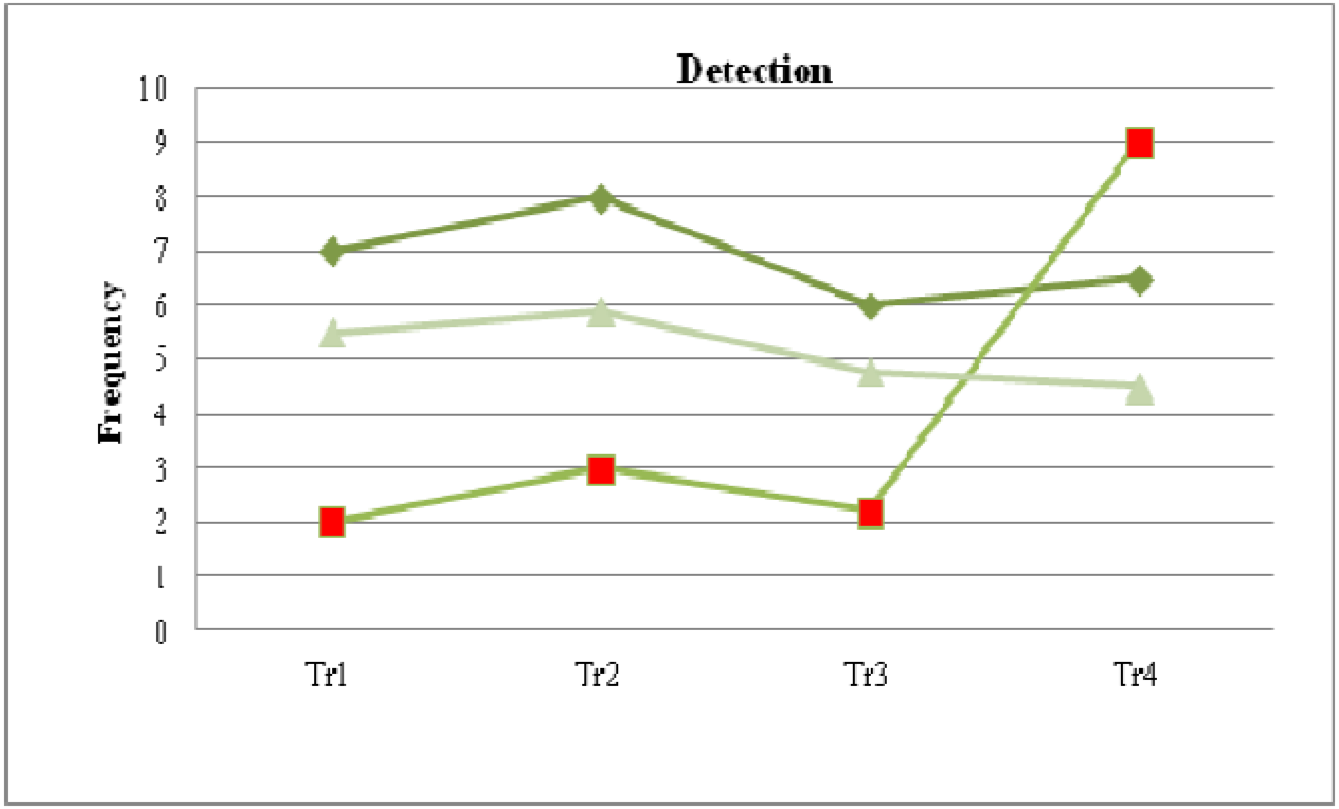
Genetic algorithm



• Machine Learnig

Genetic algorithm

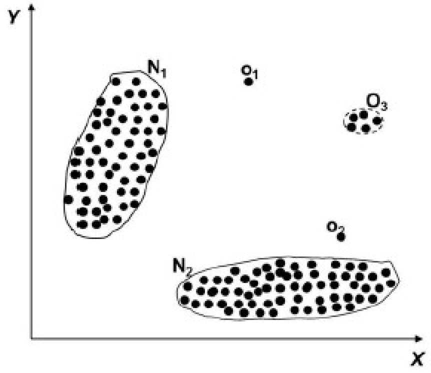
Abnormal Behavior



Types of Anomaly

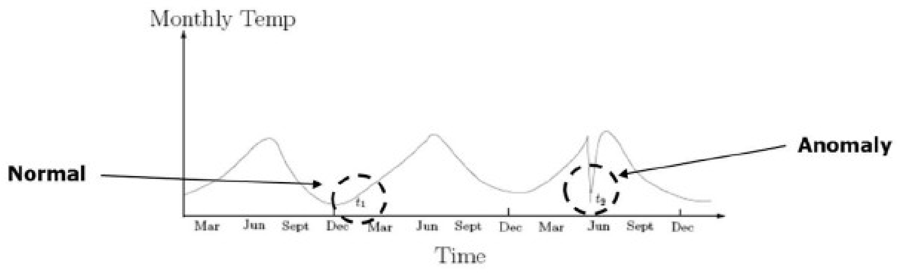
Point Anomalies

- An individual data instance is anomalous w.r.t. the data



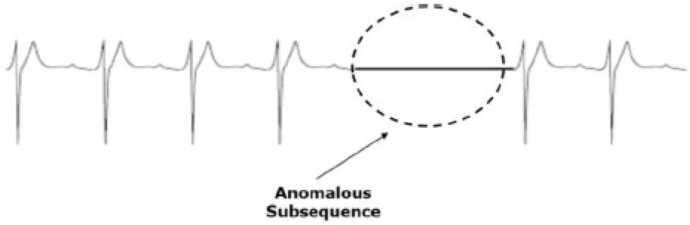
Contextual Anomalies

- An individual data instance is anomalous within a context
- Requires a notion of context
- Also referred to as conditional anomalies*



Collective Anomalies

- A collection of related data instances is anomalous
- Requires a relationship among data instances
  - Sequential Data
  - Spatial Data
  - Graph Data

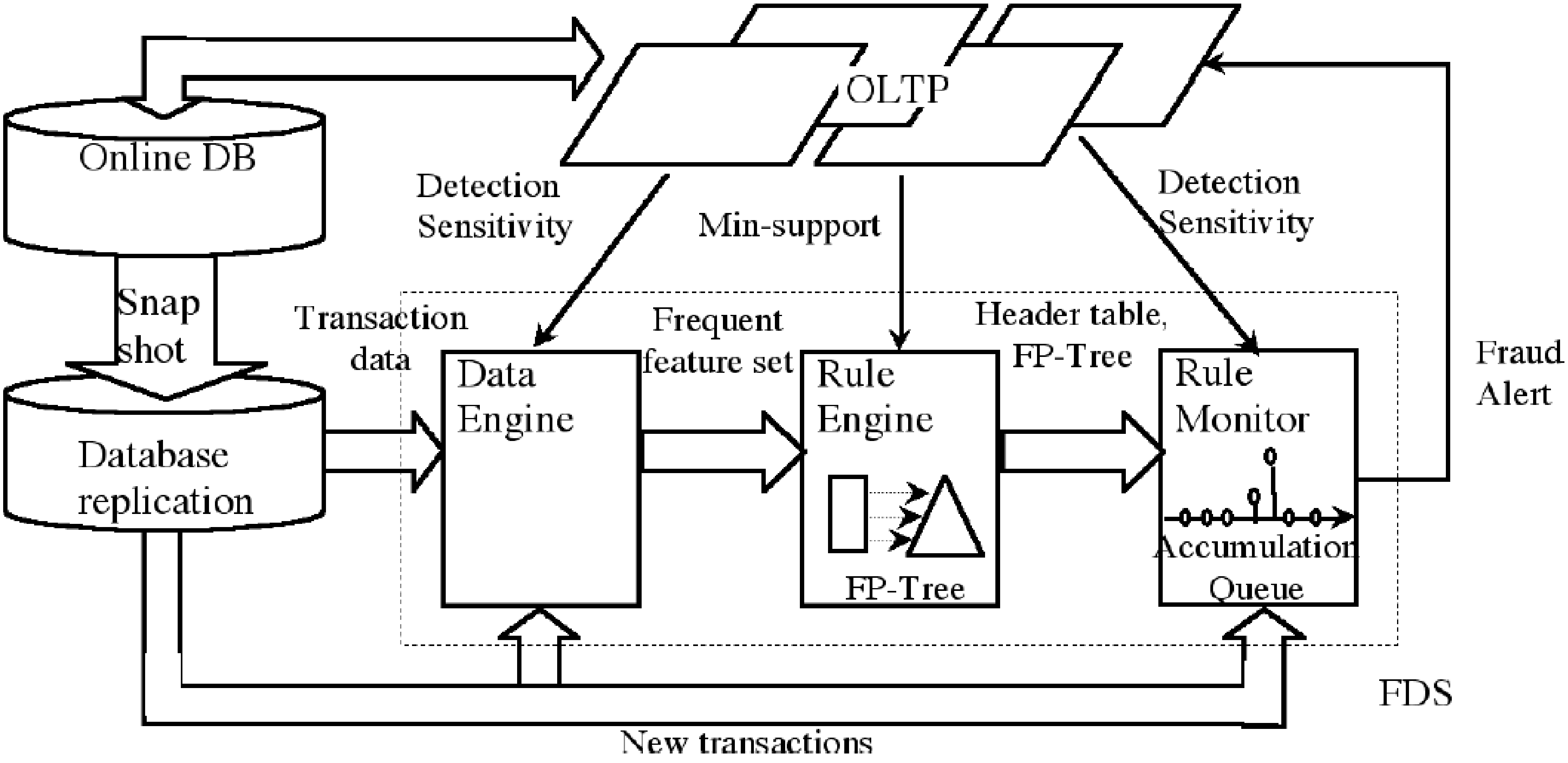


- The individual instances within a collective anomaly are not anomalous by themselves

사이버보안연구본부 2014

- **Machine Learnig**

Association Rule Mining

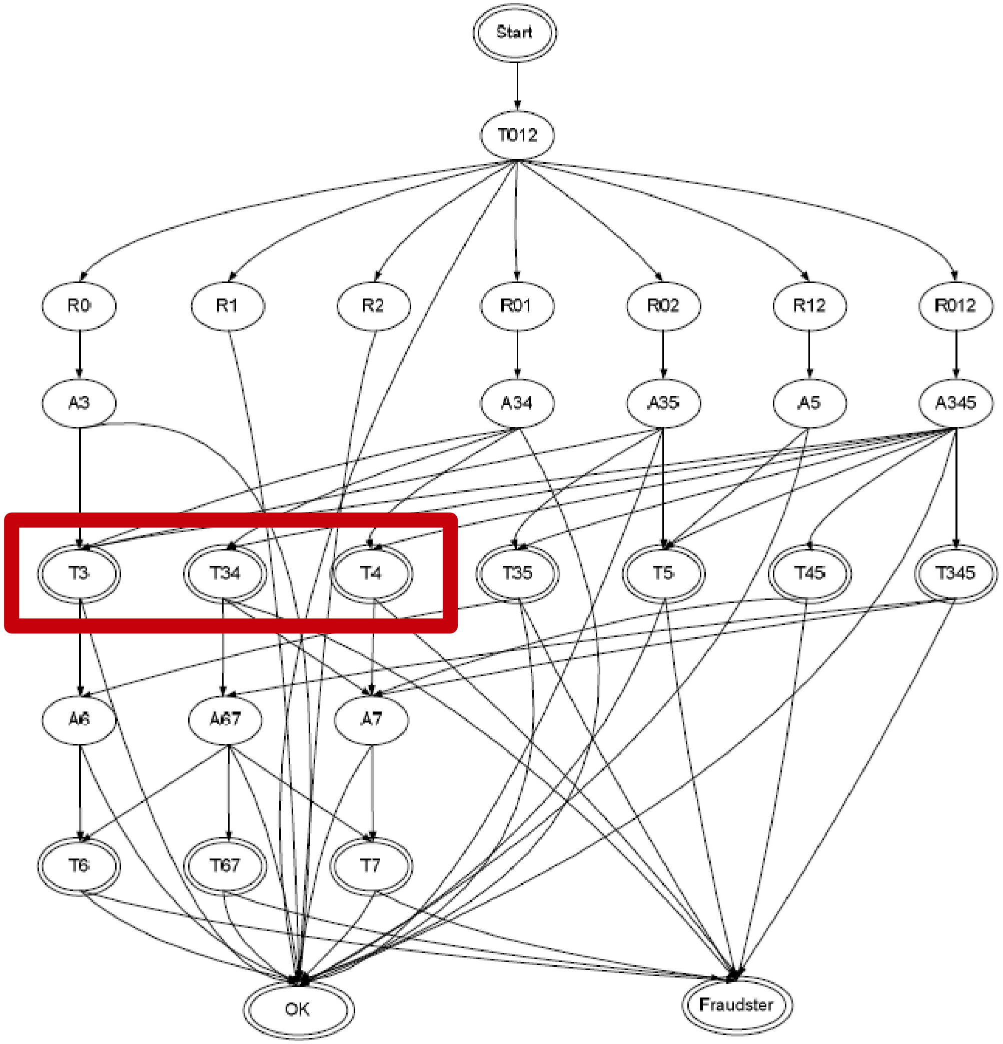


BICube™

- **Machine Learnig**

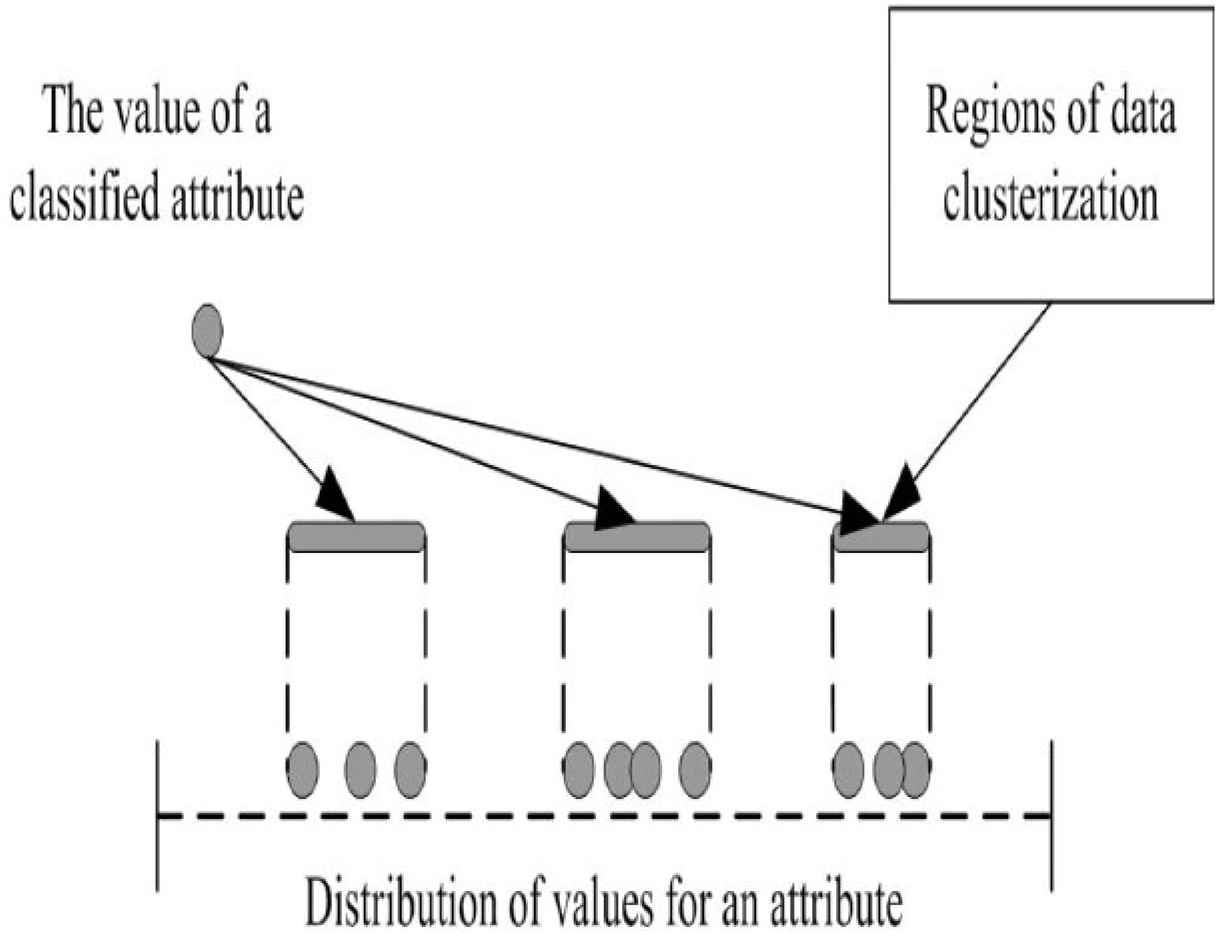
Finite State Automata (FSA)

Since the tests in can be **grouped**, the states can represent the several tests being performed at **the same time. For example, T34 means that T3 and T4 can be done simultaneously**



- **Machine Learnig**

Clustering

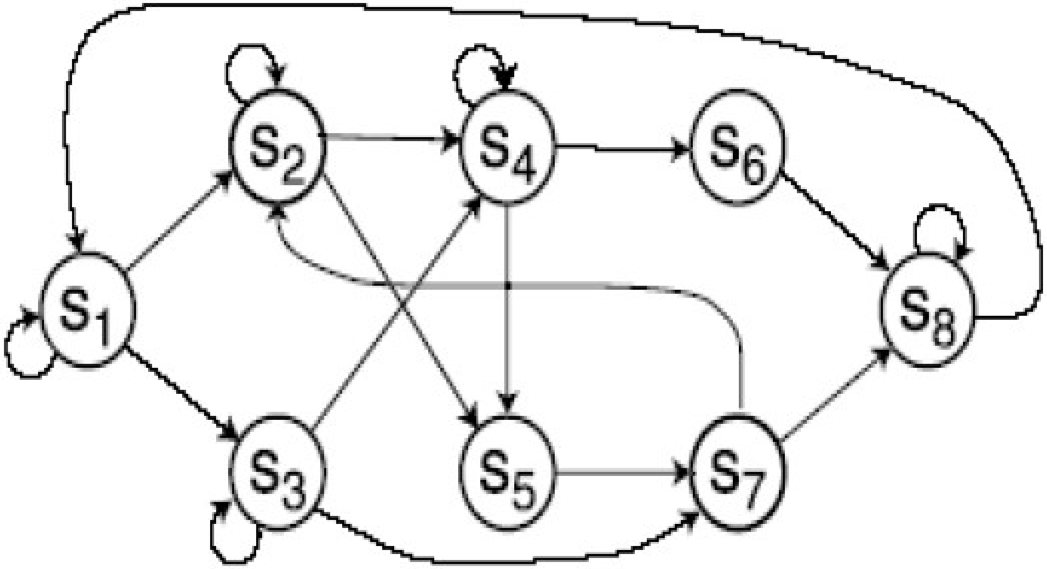

The value of a classified attribute
Regions of data clusterization
Distribution of values for an attribute

• Machine Learnig

Hidden Markov

Sequence Based Algorithm

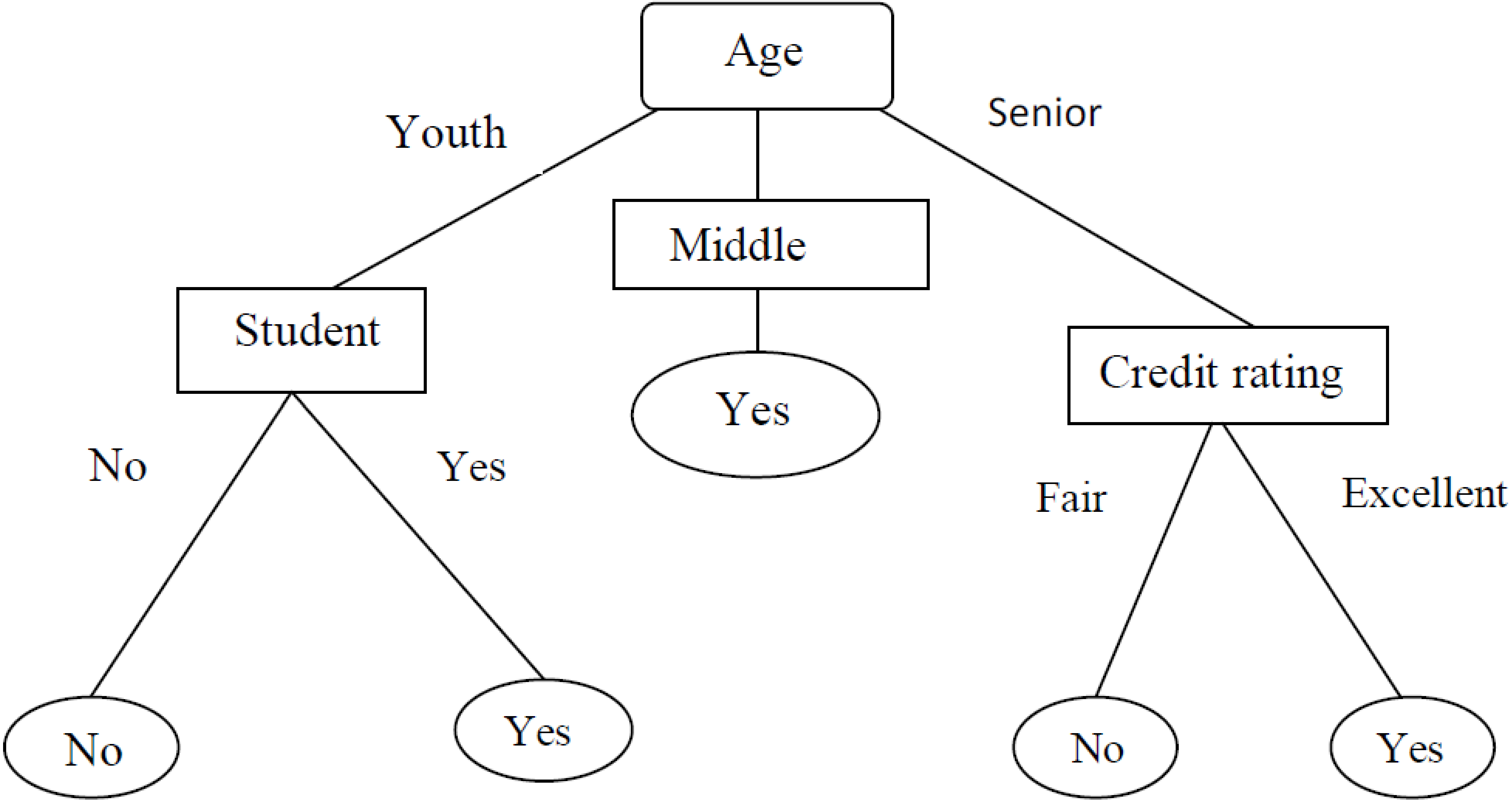
- Certain fraudulent activities may **not be detectable with instance** based algorithms
- **small amount** of money, **instance based** algorithms will **fail** to detect the fraud



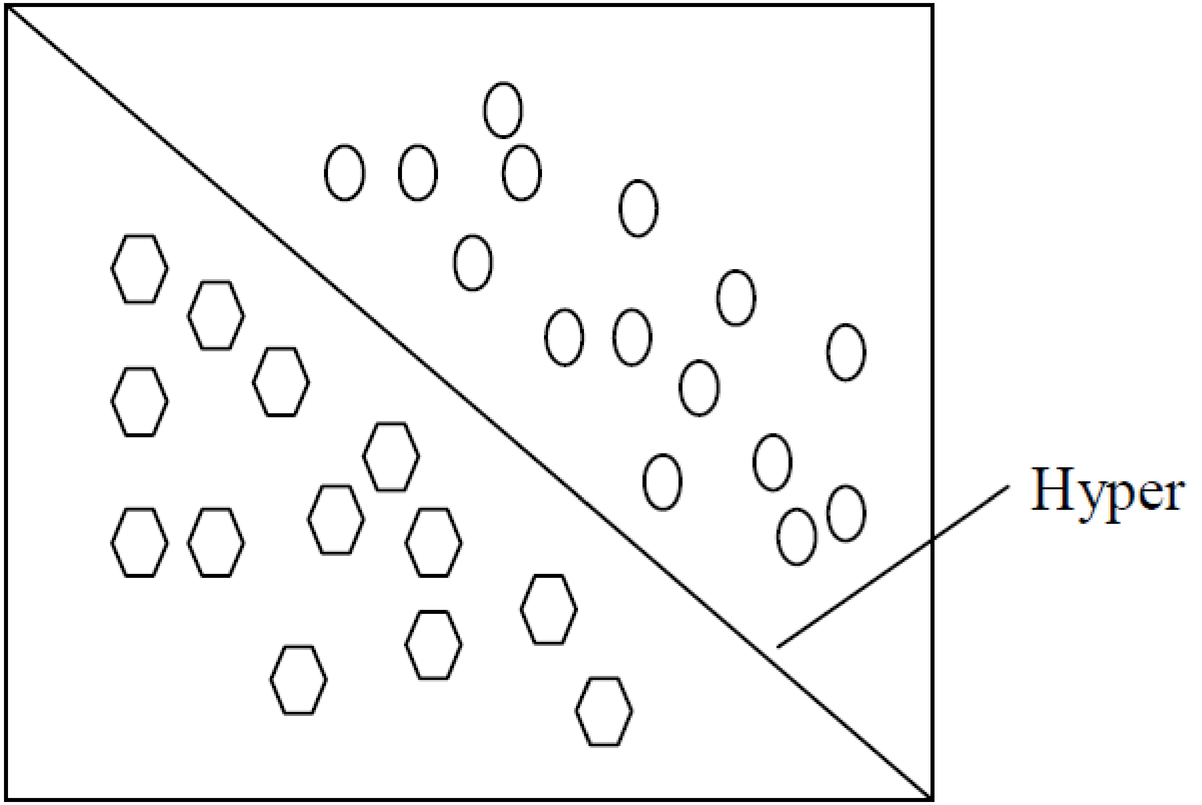
• Machine Learnig

Decision Tree

Profiling?



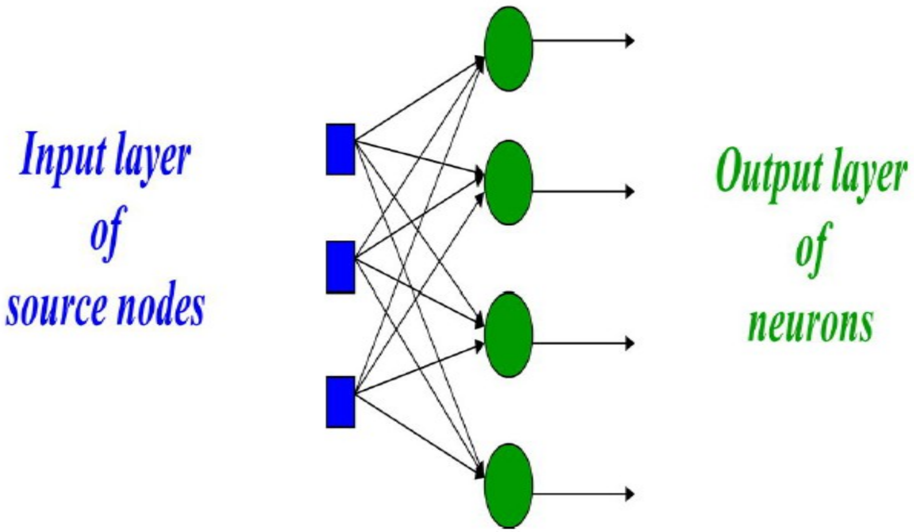
• Machine Learnig Support Vector Machine

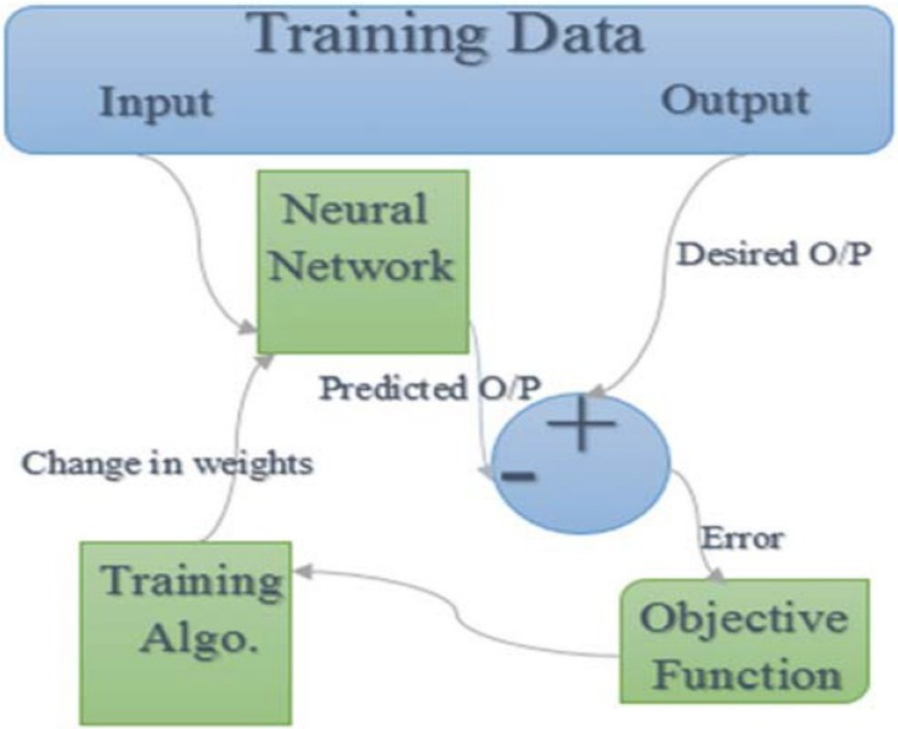


This shows the hyperplane which classify the data from one class to another class

- **Machine Learnig**

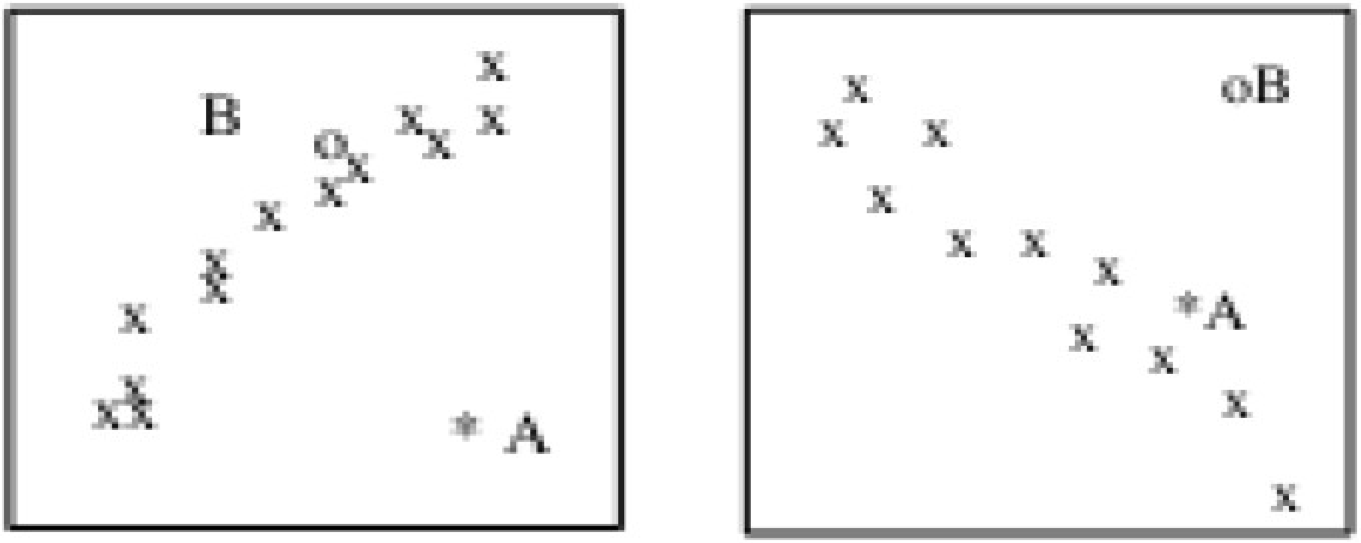
Neural Network





Single Layer Feed Forward Model

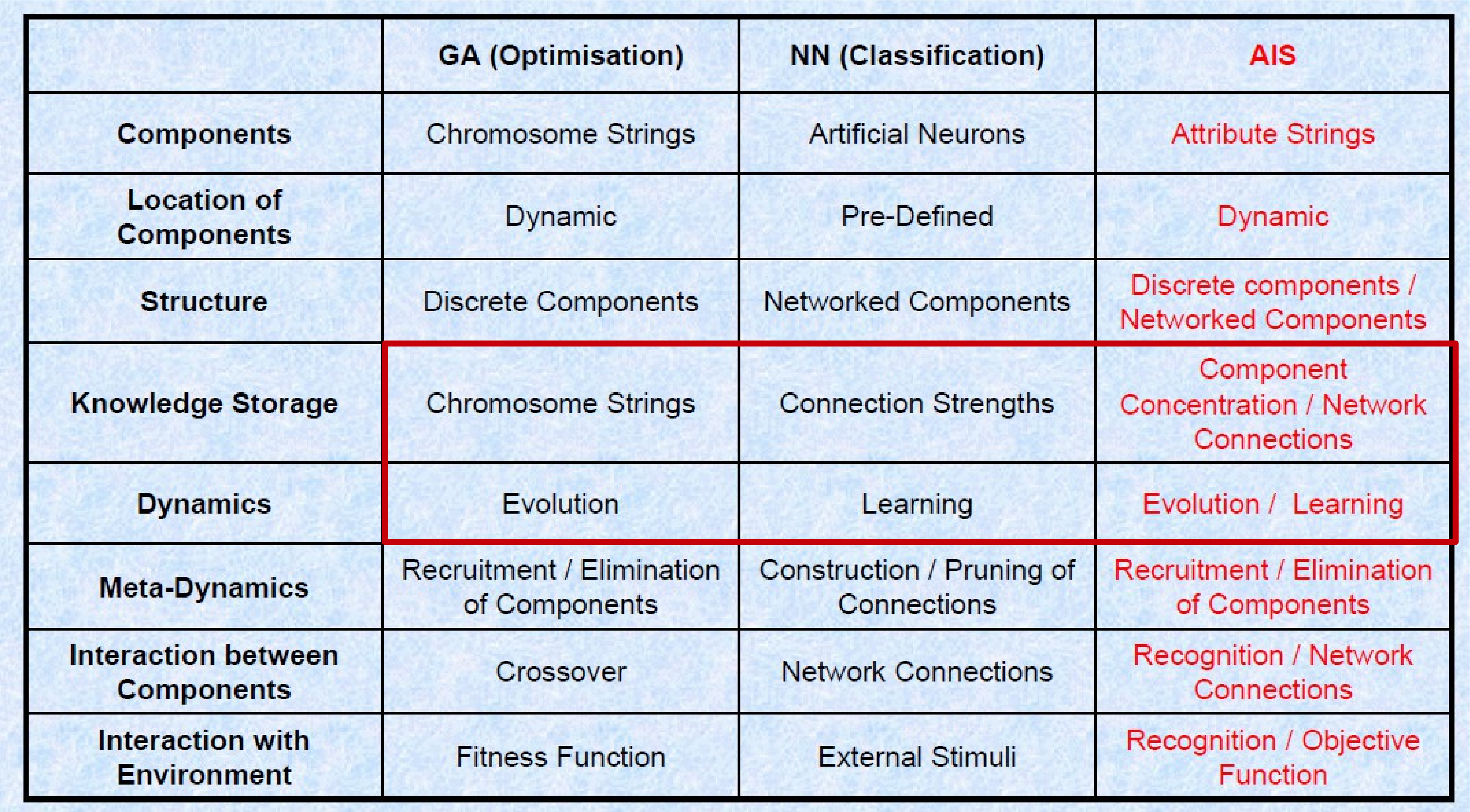
• Machine Learnig anti-k nearest neighbor



Outlier Detection

• Machine Learnig

Comparison of Three Algorithms



	GA (Optimisation)	NN (Classification)	AIS
Components	Chromosome Strings	Artificial Neurons	Attribute Strings
Location of Components	Dynamic	Pre-Defined	Dynamic
Structure	Discrete Components	Networked Components	Discrete components / Networked Components
Knowledge Storage	Chromosome Strings	Connection Strengths	Component Concentration / Network Connections
Dynamics	Evolution	Learning	Evolution / Learning
Meta-Dynamics	Recruitment / Elimination of Components	Construction / Pruning of Connections	Recruitment / Elimination of Components
Interaction between Components	Crossover	Network Connections	Recognition / Network Connections
Interaction with Environment	Fitness Function	External Stimuli	Recognition / Objective Function

• Solutions

Classical rule-based approach

- Always “too late”:
  - New fraud pattern is “invented” by criminals
  - Cardholders lose money and complain
  - Banks investigate complains and try to understand the new pattern
  - A new rule is implemented a few weeks later
- Expensive to build (knowledge intensive)
- Difficult to maintain:
  - Many rules
  - The situation is dynamically changing, so frequently
  - rules have to be added, modified, or removed …

• Solutions

Neural Stream

- Storage
  - hadoop
    - HDFS: Distributed File System(DFS)
    - MapReduce : parallel processing

- Algorithms
  - on-line learning (Immune System and Genetic Algorithms)
  - batch model
  - direct data

- Stream
  - Neural stream
    - Decentralize decision process
    - Cell base detection
    - Network for Artificial Immune Systems
  - Storm, Samja can't use on-line learning

• Solutions

A system based on profiles

- Every bank user gets a vector of parameters that describe his/her behavior: an “average–behavior” profile
- The system constantly compares this “long–term” profile with the recent behavior of cardholder
- Transactions that do not fit into bank user’s profile are flagged as suspicious (or are blocked)
- Profiles are updated with every single transaction, so the system constantly adopts to (slow and small) changes in bank user’ behavior

Q&A

Thanks

BICube™