Sharing Talk :

Strategi Studi Literatur

Dr. Kurniabudi, M.Kom
Faculty of Computer Science
Universitas Dinamika Bangsa
2023

Defenisi

- Studi Literatur = Tinjauan Pustaka/ Literatur Review
- adalah proses menemukan (*locating*), memperoleh (*obtaining*), membaca (*reading*), dan mengevaluasi (*evaluating*) literatur penelitian di bidang minat Anda (Bordens and Abbott, 2018).


Finding Gap
Research Problems
Current Research
Methods/ Teories
Research Challenges
Research Contribution
LR Objective

LR Benefit

- Can Increase the knowledge of researchers
- Get updates on research developments on research topics of interest
- Familiar with important authors
- Etc…

Motivasi melakukan Literatur Review

- Menyusun Latar Belakang Penelitian
  - *State-of-the-art*
  - *Research Gap*
  - *Formulate Research Question*
  - *Propose solution/ method*
  - *Research Contribution*
- Menulis Artikel *Literature Review* (*Survey Paper*)
  - *Systematic Literatur Review (SLR)*
  - *Traditional Review*
  - *Systematic Mapping Study*

Sumber Literatur

- Makalah dari Jurnal Ilmiah Internasional bereputasi:
  - Index ISI, Scopus, dll
- Makalah dari bookchapter
- Makalah dari seminar (*Conference Proceedings)*
- Thesis dan Disertasi
- Makalah dari Jurnal ilmiah Nasional yg Diakreditasi Dikti (arjuna.ristekdikti.go.id)
- Laporan dari lembaga/organisasi terpercaya

Sumber: Romi SW

Jurnal Nasional Terakreditasi

- Jurnal nasional terakreditasi adalah terbitan berkala ilmiah yang memenuhi kriteria sebagai jurnal nasional
- Mendapat status terakreditasi dari Direktur Jenderal Pendidikan Tinggi, Riset, dan Teknologi
- Peringkat SINTA 1 - 6

Jurnal Internasional

- Karya ilmiah yang diterbitkan ditulis dengan memenuhi kaidah ilmiah dan etika keilmuan;
- Memiliki ISSN;
- Ditulis dengan menggunakan bahasa resmi PBB (Inggris, Perancis, Arab, Rusia, dan Tiongkok);
- Dewan editor (editorial board) adalah pakar di bidangnya dan sedikitnya berasal dari 4 negara;
- Artikel ilmiah yang diterbitkan dalam satu terbitan (issue) ditulis oleh penulis dari berbagai negara; dan
- Memuat karya ilmiah dari penulis yang berasal dari berbagai negara dalam setiap terbitannya.

Jurnal Internasional Bereputasi

- Jurnal internasional bereputasi adalah terbitan berkala ilmiah yang memenuhi kriteria jurnal internasional
  - Terindeks oleh pangkalan data internasional bereputasi (Scopus, Web of Science),
  - dan memiliki faktor dampak (impact factor) dari ISI Web of Science (Thomson Reuters),
  - atau Scimago Journal Rank (SJR), atau memunyai faktor dampak (SJR) dari SCImago Journal and Country Rank serendah-rendahnya Q3 (kuartil tiga)

Where to Find Research Paper?

ScienceDirect

MENDELEY

Jenis Paper/ makalah ilmiah

- Technical Paper
  - Paper yang isinya adalah hasil penelitian dan eksperimen yang dilakukan seorang peneliti
  - Penilaian kualitas technical paper dari kontribusi ke pengetahuan
- Survey Paper
  - Paper yang isinya adalah review dan survey tentang topik/tema suatu penelitian, biasanya jumlah penelitian yang direview mencapai ratusan atau ribuan
  - Rujukan dan panduan penting bagi peneliti yang baru memulai penelitian untuk memahami suatu topic/tema penelitian secara komprehensif

Sumber: Romi SW

Computer Networks 174 (2020) 107247

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Building an efficient intrusion detection system based on feature selection and ensemble classifier

Yuyang Zhou [a,b,c], Guang Cheng [a,b,c,*], Shanqing Jiang [a,d], Mian Dai [a,b,c]

[a] School of Cyber Science and Engineering, Southeast University, Nanjing, China
[b] Key Laboratory of Computer Network and Information Integration, Ministry of Education, Nanjing, China
[c] Jiangsu Provincial Key Laboratory of Computer Network Technology, Southeast University, Nanjing, China
[d] National Key Laboratory of Science and Technology on Information System Security, Beijing, China

ARTICLE INFO

Keywords:
Cyber security
Intrusion detection system
Data mining
Feature selection

ABSTRACT

Intrusion detection system (IDS) is one of extensively used techniques in a network topology to safeguard the integrity and availability of sensitive assets in the protected systems. Although many supervised and unsupervised learning approaches from the field of machine learning have been used to increase the efficacy of IDSs, it is still a problem for existing intrusion detection algorithms to achieve good performance. First, lots of redundant and irrelevant data in high-dimensional datasets interfere with the classification process of an IDS. Second, an indi-

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 25, 2020, accepted November 27, 2020, date of publication December 2, 2020,
date of current version December 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3041951

A Survey on Machine Learning Techniques for Cyber Security in the Last Decade

KAMRAN SHAUKAT[1,4], SUHUAI LUO[1], VIJAY VARADHARAJAN[1], (Senior Member, IEEE), IBRAHIM A. HAMEED[2], (Senior Member, IEEE), AND MIN XU[3], (Member, IEEE)

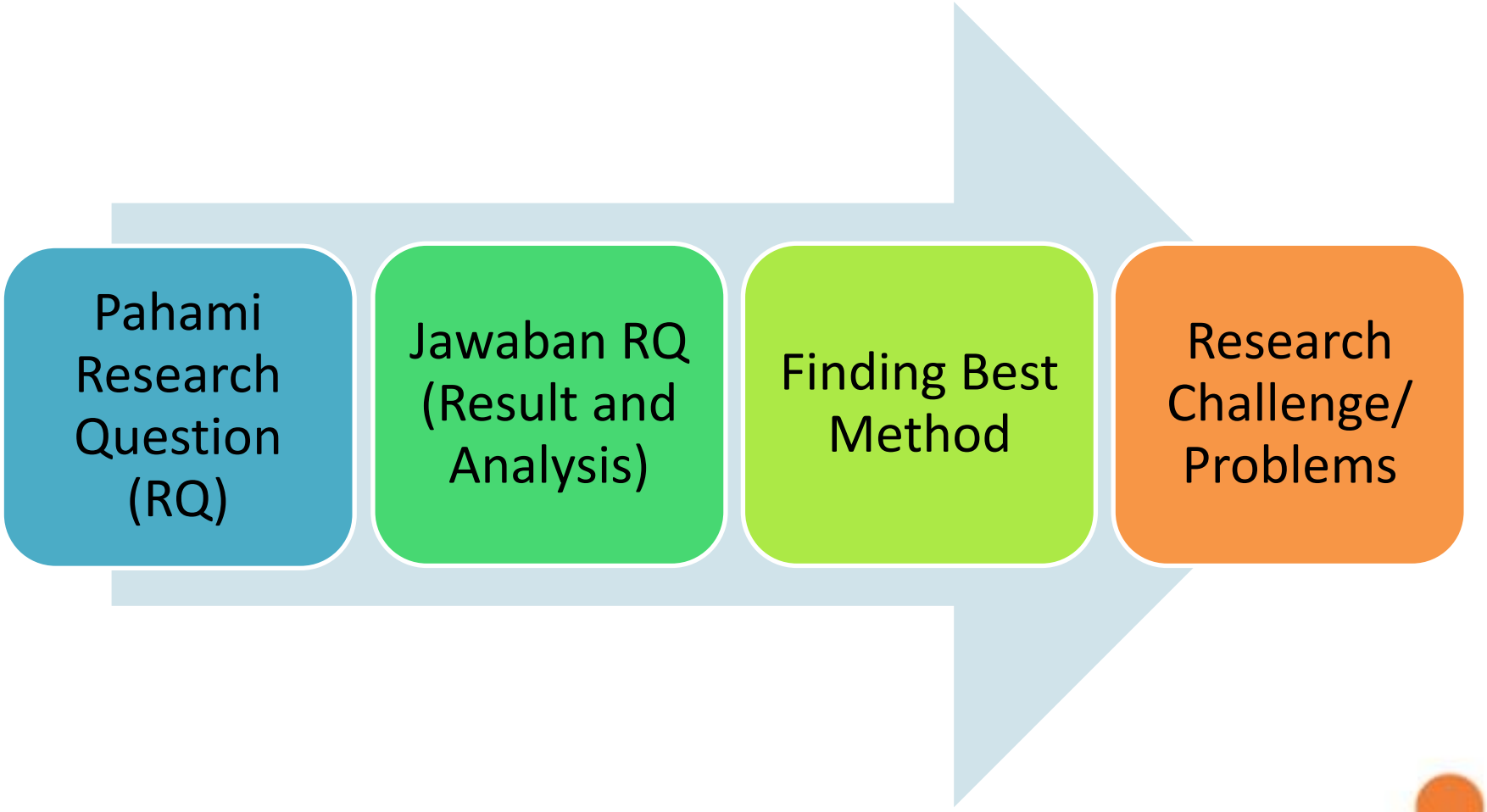
[1]School of Electrical Engineering and Computing, The University of Newcastle, Callaghan, NSW 2308, Australia
[2]Department of ICT and Natural Sciences, Norwegian University of Science and Technology, 7491 Trondheim, Norway
[3]School of Electrical and Data Engineering, University of Technology Sydney, Ultimo, NSW 2007, Australia
[4]Punjab University College of Information Technology, University of the Punjab, Lahore 54590, Pakistan

Corresponding authors: Kamran Shaukat (kamran.shaukat@uon.edu.au) and Ibrahim A. Hameed (ibib@ntnu.no)

This work was supported by the Norwegian University of Science and Technology, Norway.

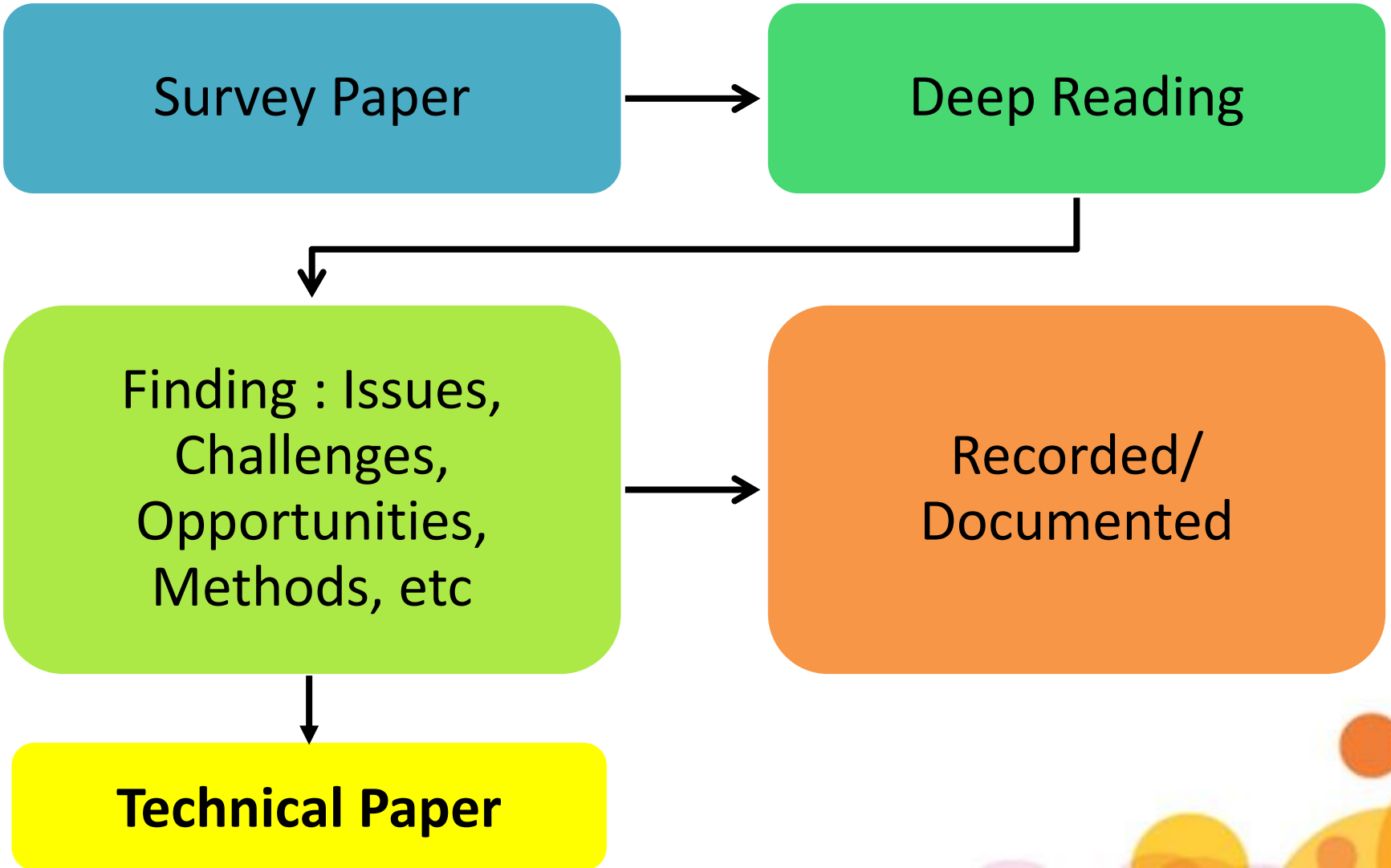
ABSTRACT Pervasive growth and usage of the Internet and mobile applications have expanded cyberspace. The cyberspace has become more vulnerable to automated and prolonged cyberattacks. Cyber security techniques provide enhancements in security measures to detect and react against cyberattacks. The previously used security systems are no longer sufficient because cybercriminals are smart enough to evade

Kiat Review Survey Paper



Sumber : Romi SW

Data Extraction in Survey Paper



Kiat mereview Technical Paper

Masalah Penelitian?

- **Dibuat-buat?**
- **Ada landasan dan validasi?**

Kontribusi?

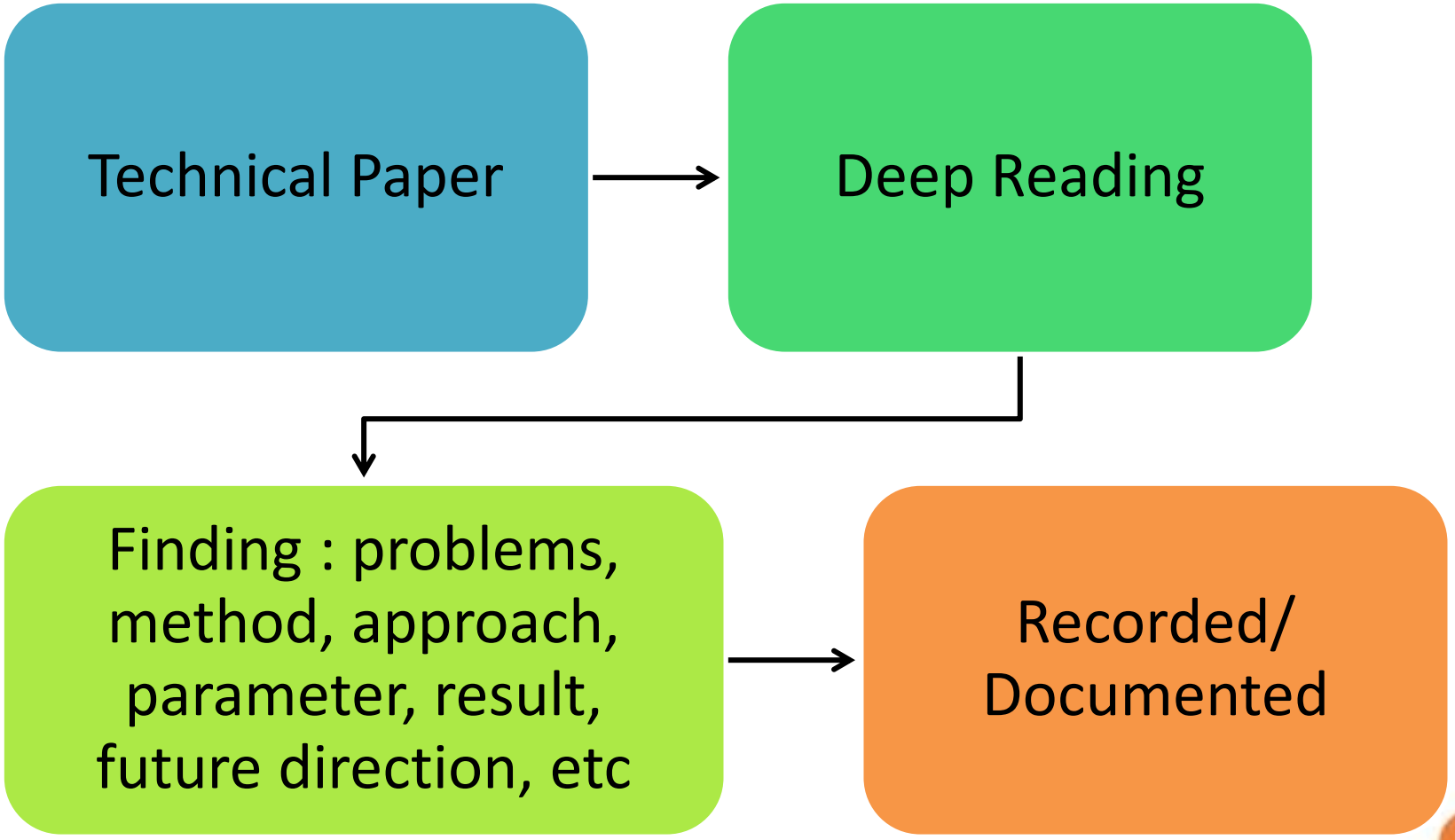
- **Mengulang yg sudah ada?**
- **Mempertimbang literatur yang relevan?**
- **Apa yang baru?**

Validasi Kontribusi?

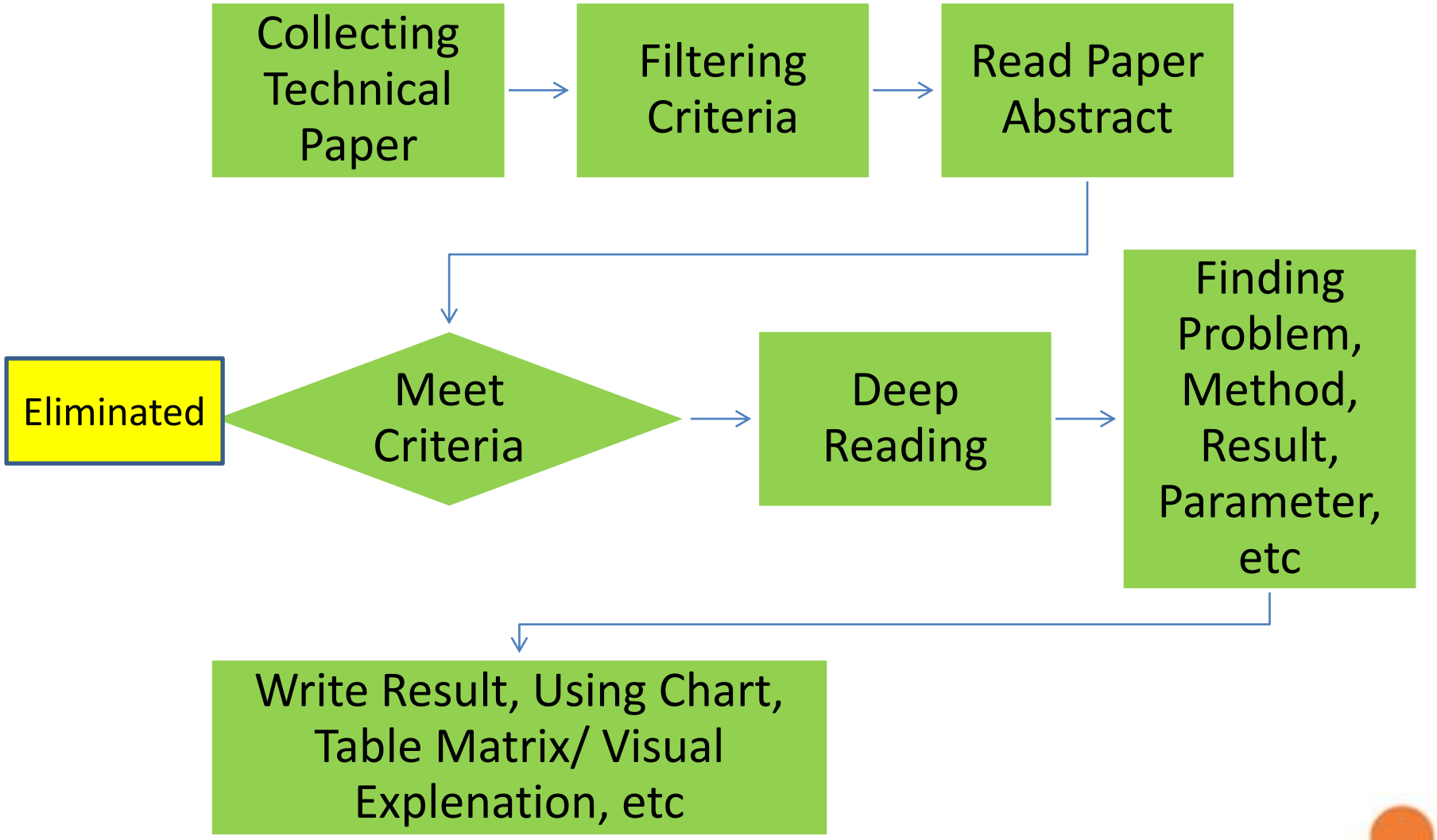
- **Teori/model terbukti benar?**
- **Faktor2 aneh dalam eksperimen?**
- **Benchmark realistis?**
- **Generalisasi valid?**

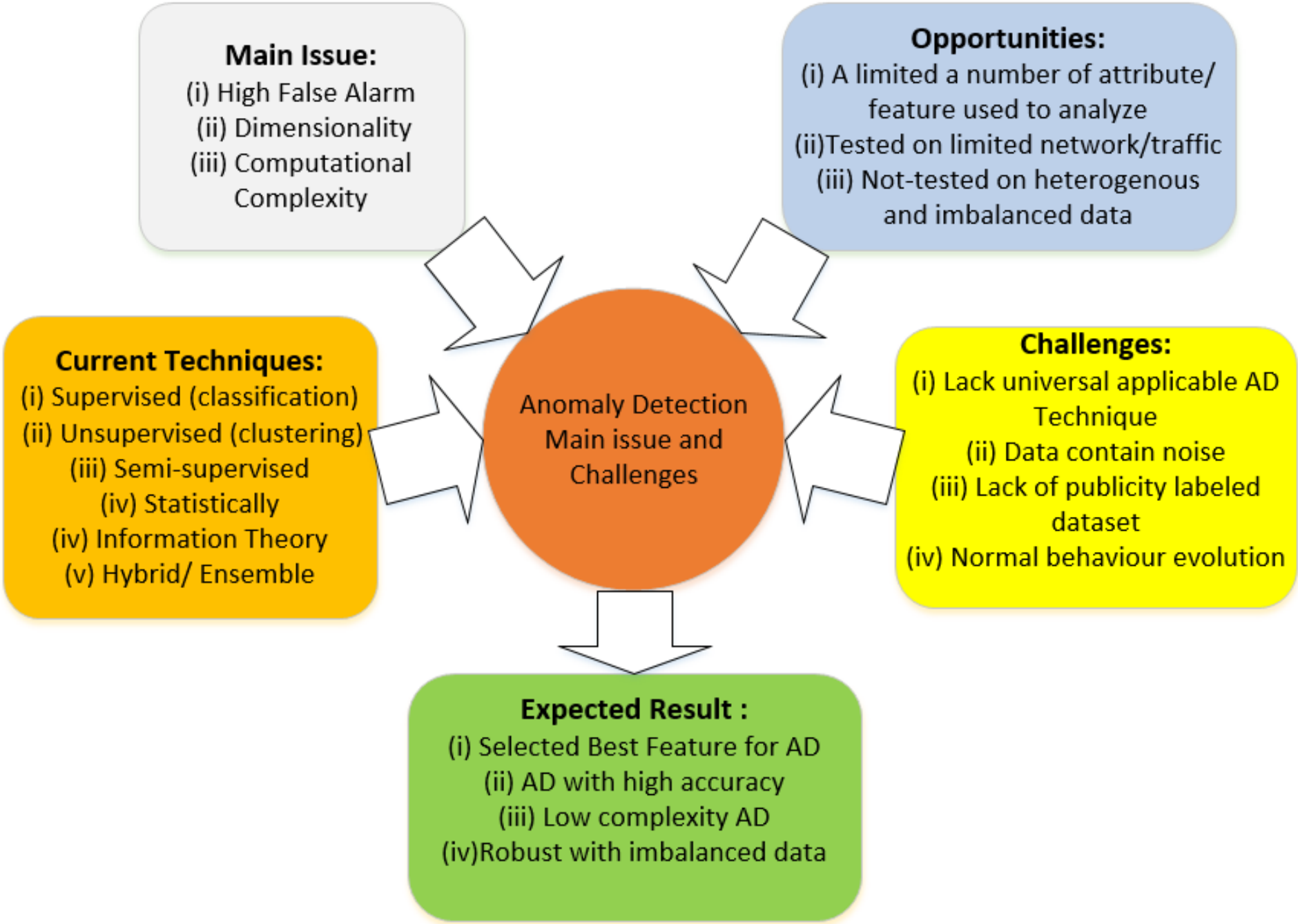
Sumber : Romi SW

Data Extraction in Technical Paper

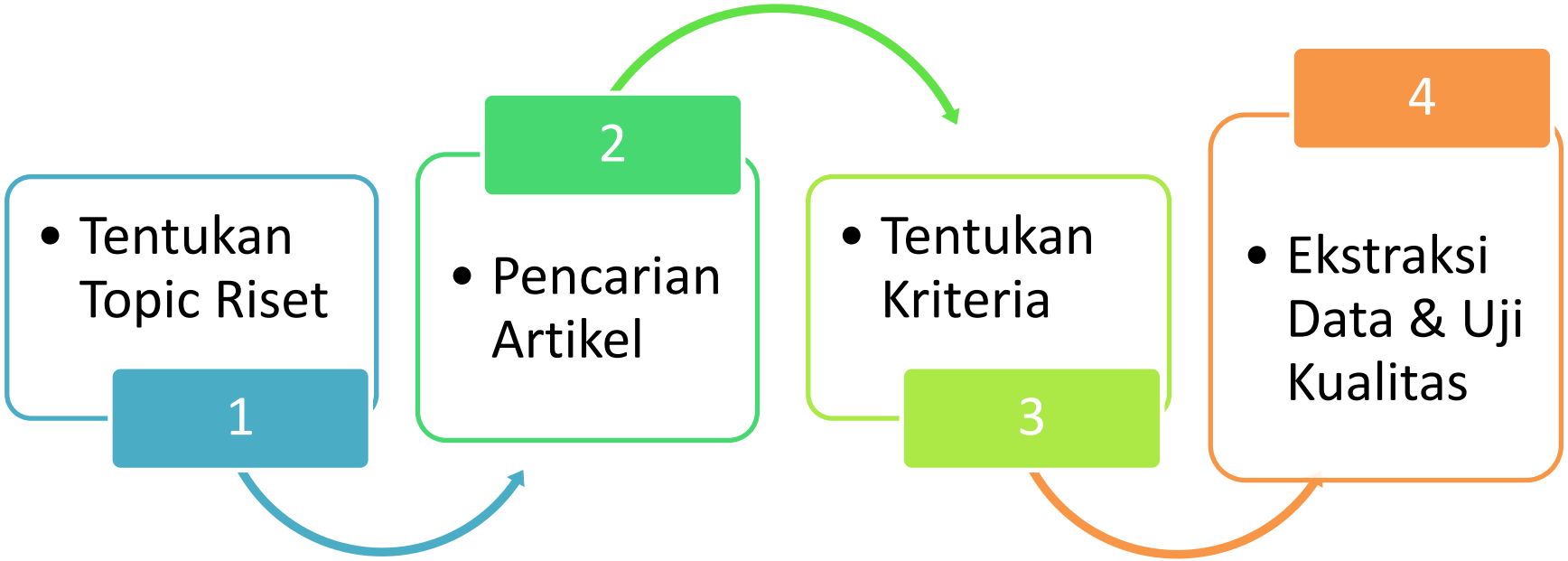


LR to Finding Research Gap



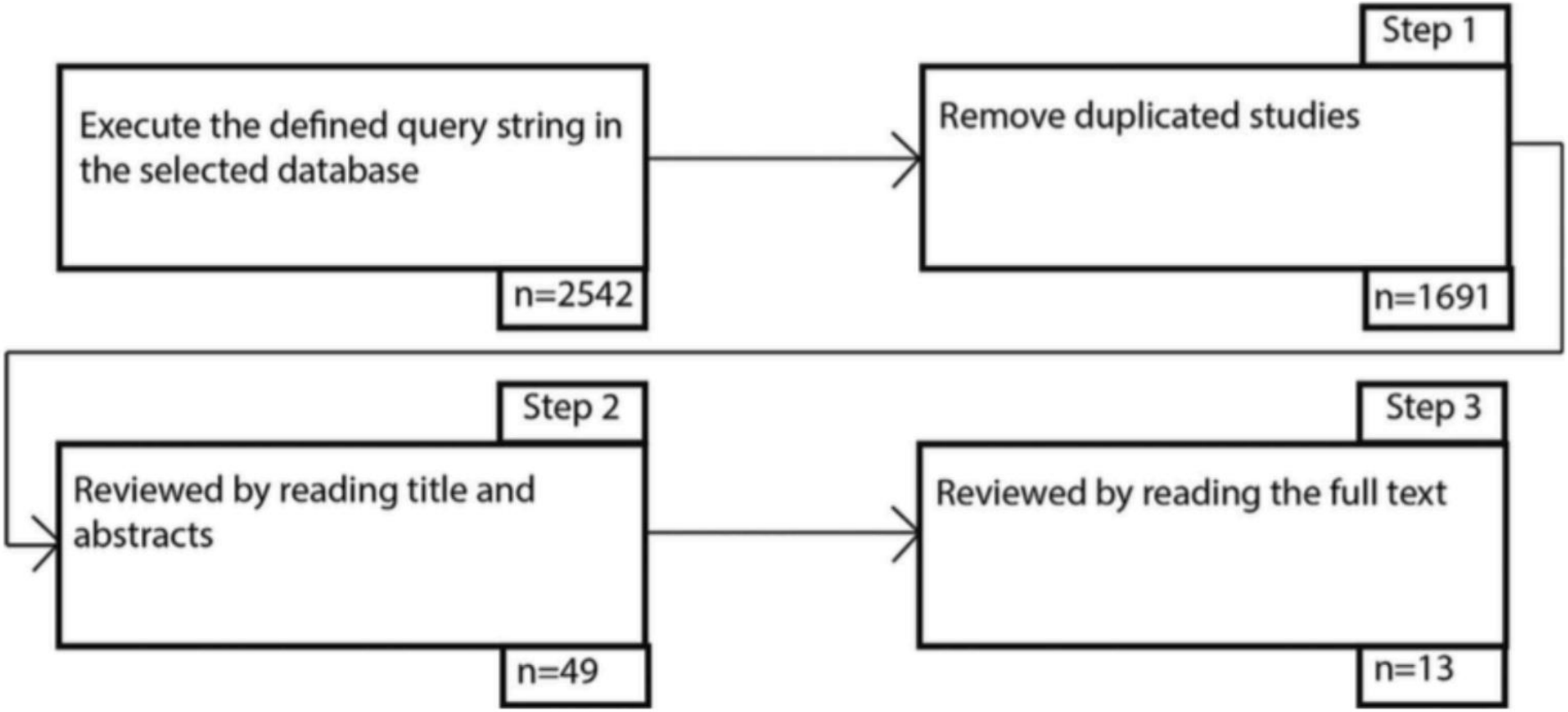

Main Issue:
(i) High False Alarm
(ii) Dimensionality
(iii) Computational Complexity
Opportunities:
(i) A limited a number of attribute/ feature used to analyze
(ii)Tested on limited network/traffic
(iii) Not-tested on heterogenous and imbalanced data
Current Techniques:
(i) Supervised (classification)
(ii) Unsupervised (clustering)
(iii) Semi-supervised
(iv) Statistically
(iv) Information Theory
(v) Hybrid/ Ensemble
Anomaly Detection Main issue and Challenges
Challenges:
(i) Lack universal applicable AD Technique
(ii) Data contain noise
(iii) Lack of publicity labeled dataset
(iv) Normal behaviour evolution
Expected Result :
(i) Selected Best Feature for AD
(ii) AD with high accuracy
(iii) Low complexity AD
(iv)Robust with imbalanced data

Systematic Literatur Review (SLR)

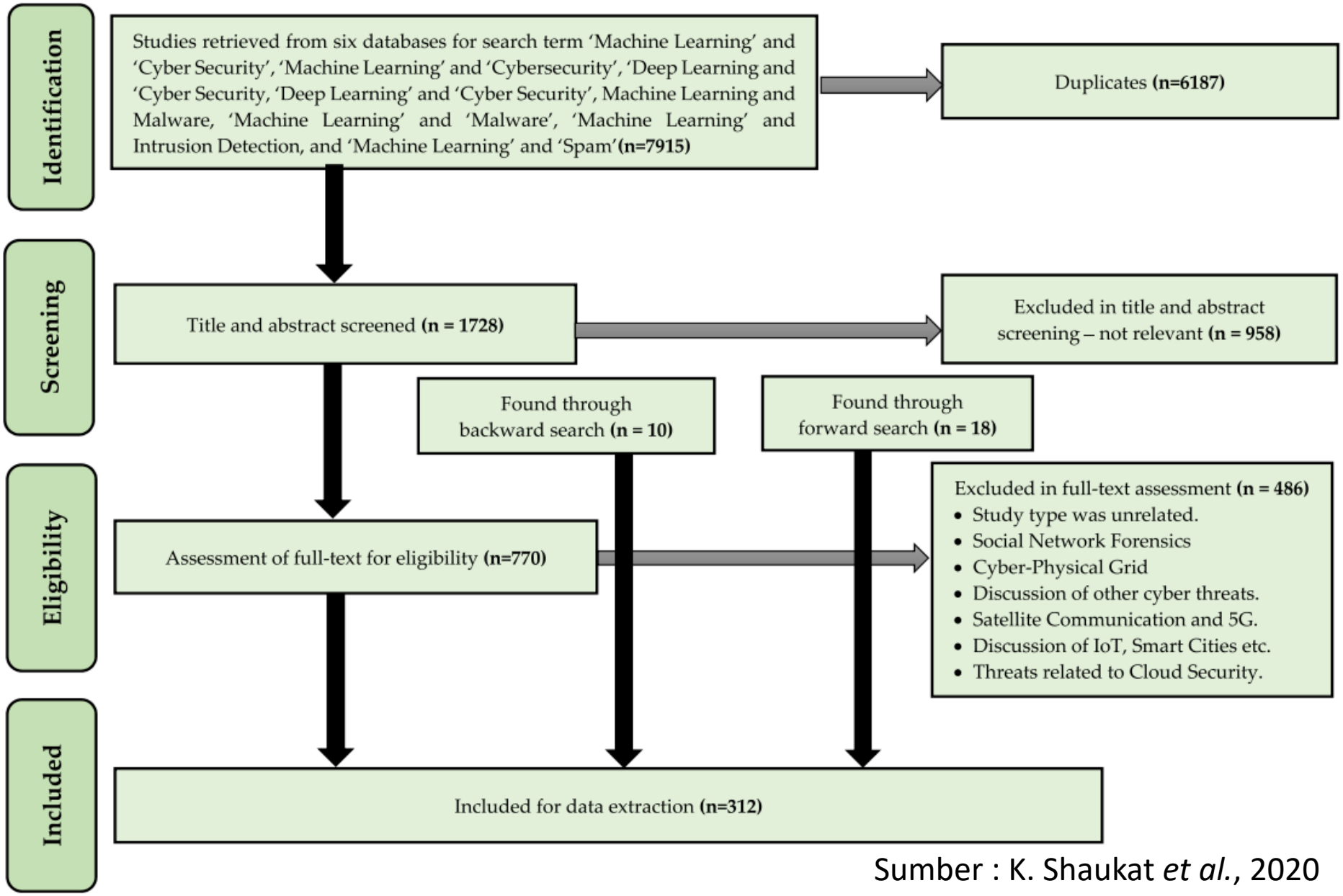


(Sumber : A.H. Azni et al , 2015)

Conducting SLR



Example : Process Paper Selection



Sumber : K. Shaukat *et al.*, 2020

Example : LR Result (trends)

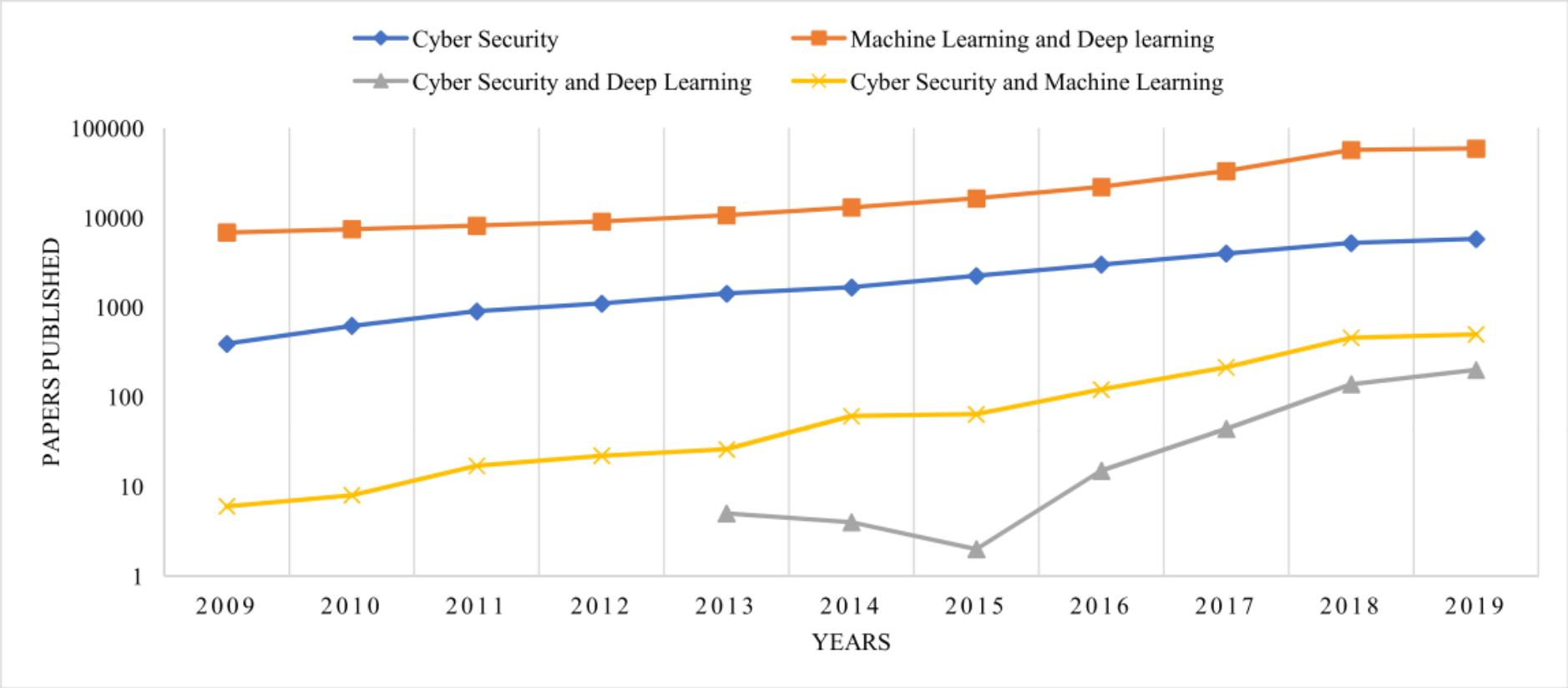
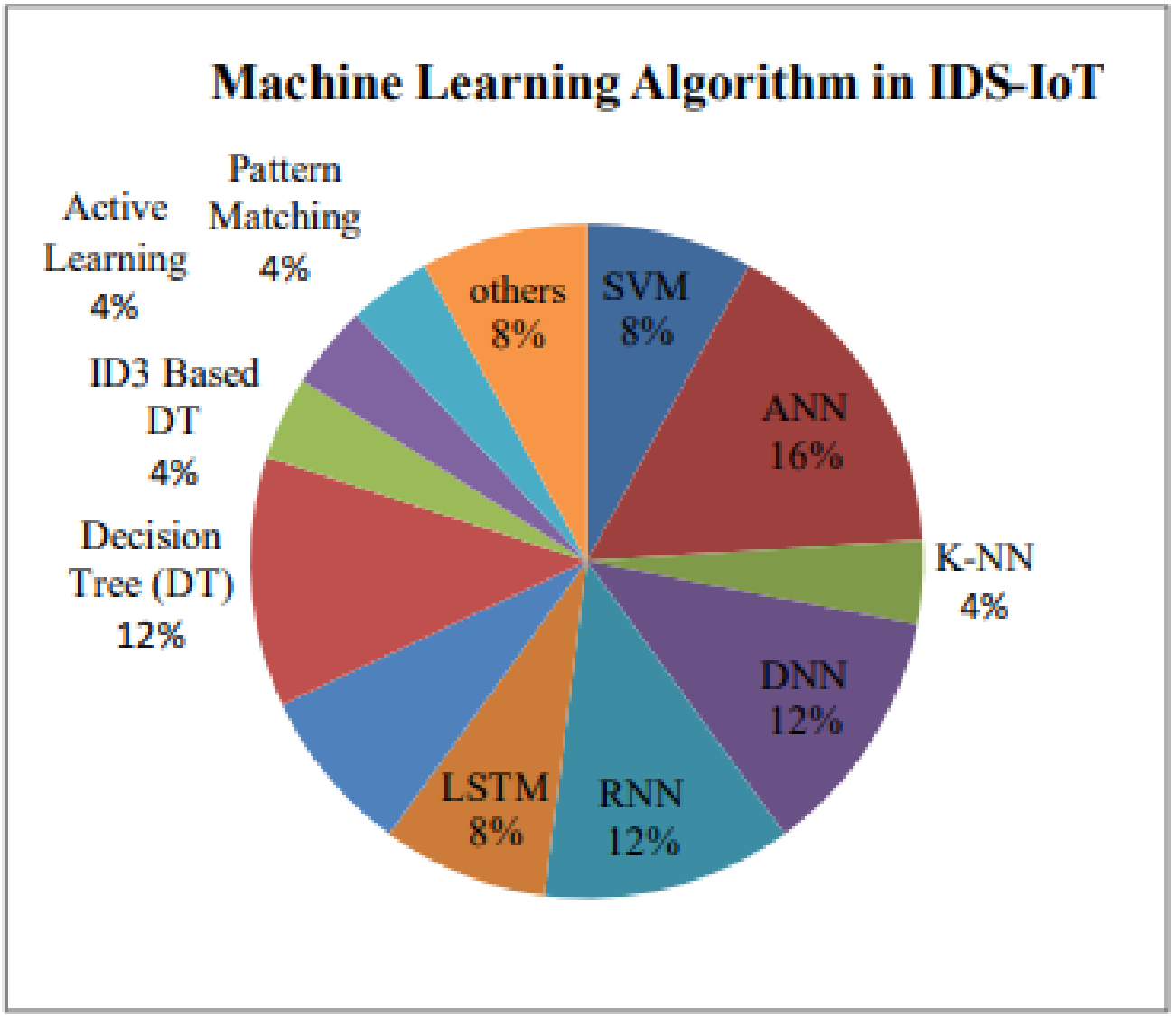


FIGURE 1. Publications Trends of Machine Learning and Cyber Security (source: Scopus).

Sumber : K. Shaukat *et al.*, 2020

Example : LR Result (chart)



Sumber : Eddy Prasetyo Nugroho et.al 2021

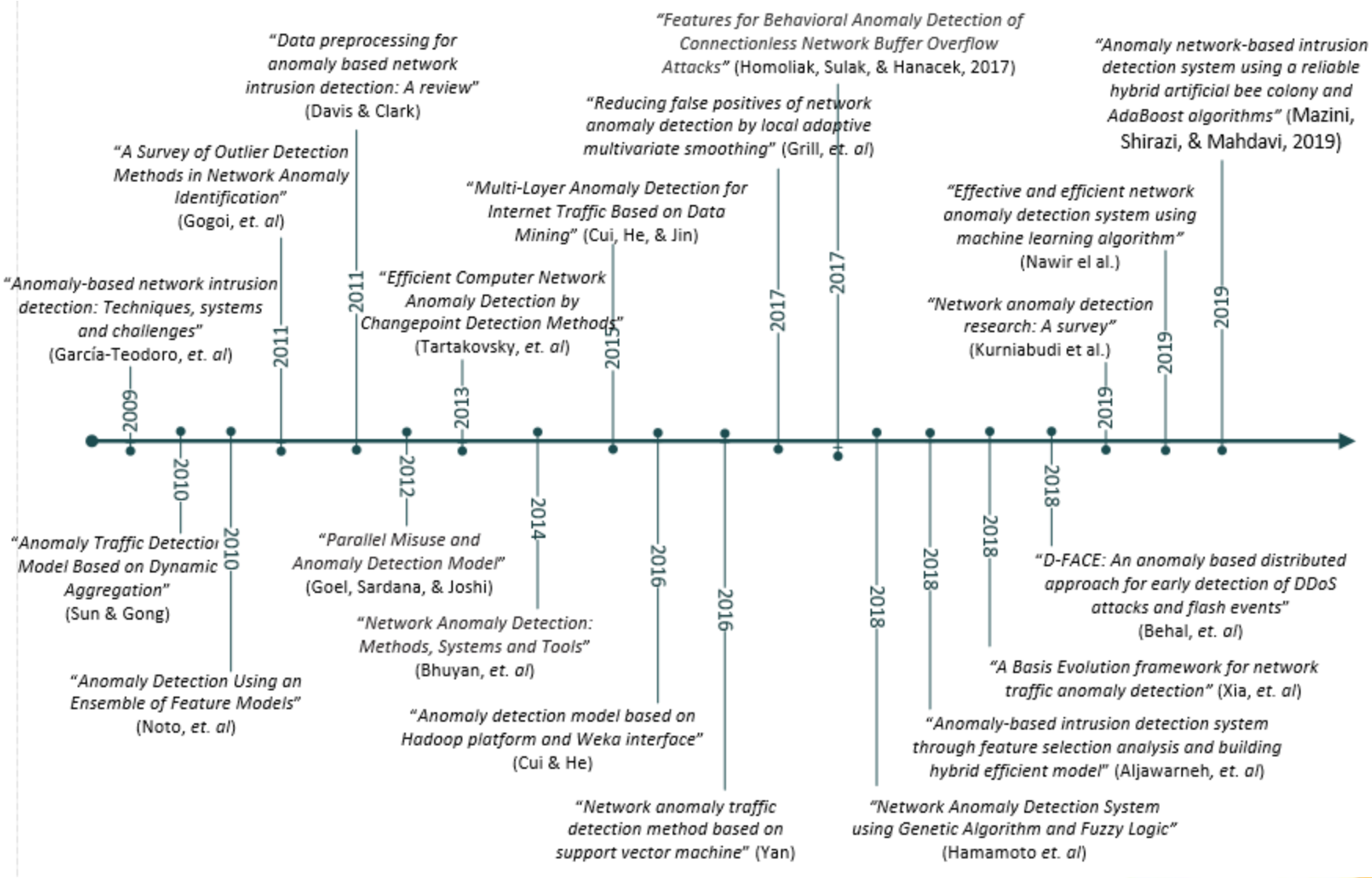
Example Result (table)

Table 3. Comparison the method types of anomaly and attacks

Author Name	Methods	Algorithm	Pros and contras
Gharbaoui et al.,2013 [30]	Statistical	Sequential Hypothesis Testing (SHT)	Detection capabilities achieve a good performance, Reduce false alarm, Tested on realtime situation is needed
Nguyen & Roughan, 2013 [37]	Statistical	Hidden Markov Model (HMM)	Low computation and communication overheads, Suitable for adoption by ISPs, Only on small size data
Fernandes et al., 2016 [60]	Statistical	PCA + Ant Colony	Able to detect anomalous behavior, Computation very complex
Parwez et al.,2017 [46]	Clustering	k-means and hierarchical clustering + neural-network	Low complexity in k-means clustering, Better performance with hierarchical clustering, Hierarchical clustering facing space complexity for large data set
Zhu, C. et al., 2015 [9]	Classification	Bayesian Network	Very effective to detect anomaly, Requires user interference (expert) to adapt changed probabilities
Z. Zhang et al., 2016 [45]	Information theory	Information entropy + Neural Network back propagation	Can improve the stability of the system, Dynamica-lly adjust to traffic change, lower false alarm rate, Entropy value is detected to be too sensitive
Shabtai et al., 2010 [69]	Knowledge based	knowledge-based temporal abstraction (KBTA)	Support misuse detection and anomaly detection, KBTA was adapted for mobile devices that are limited in resources (i.e., CPU, memory, battery).
Usman et al., 2015 [70]	Soft computing	Fuzzy Logic	High accuracy in detect cross-layer anomalies, Low energy consumption, Initial domain knowledge is needed, Unreliable to transmit mobile agent (in poor communication)
Alipour, H. et al.,2015 [14]	Supervised	n-grams	System can detect difference attack, High detection rate, Low false alarm, Work with pre-labeled data
Dromard et al., 2017 [5]	Unsupervised	grid clustering algorithm	High performance in detection rate, Low false alarm, The speed must be improve
Lu & Ghorbani, 2009 [71]	Digital signal processing	Wavelet analysis	High-detection rates, Not accurate for real large-scale Wifi traffic

Sumber : Kurniabudi et.al, 2019

LR to knowing previous studies



LR- to Classifying

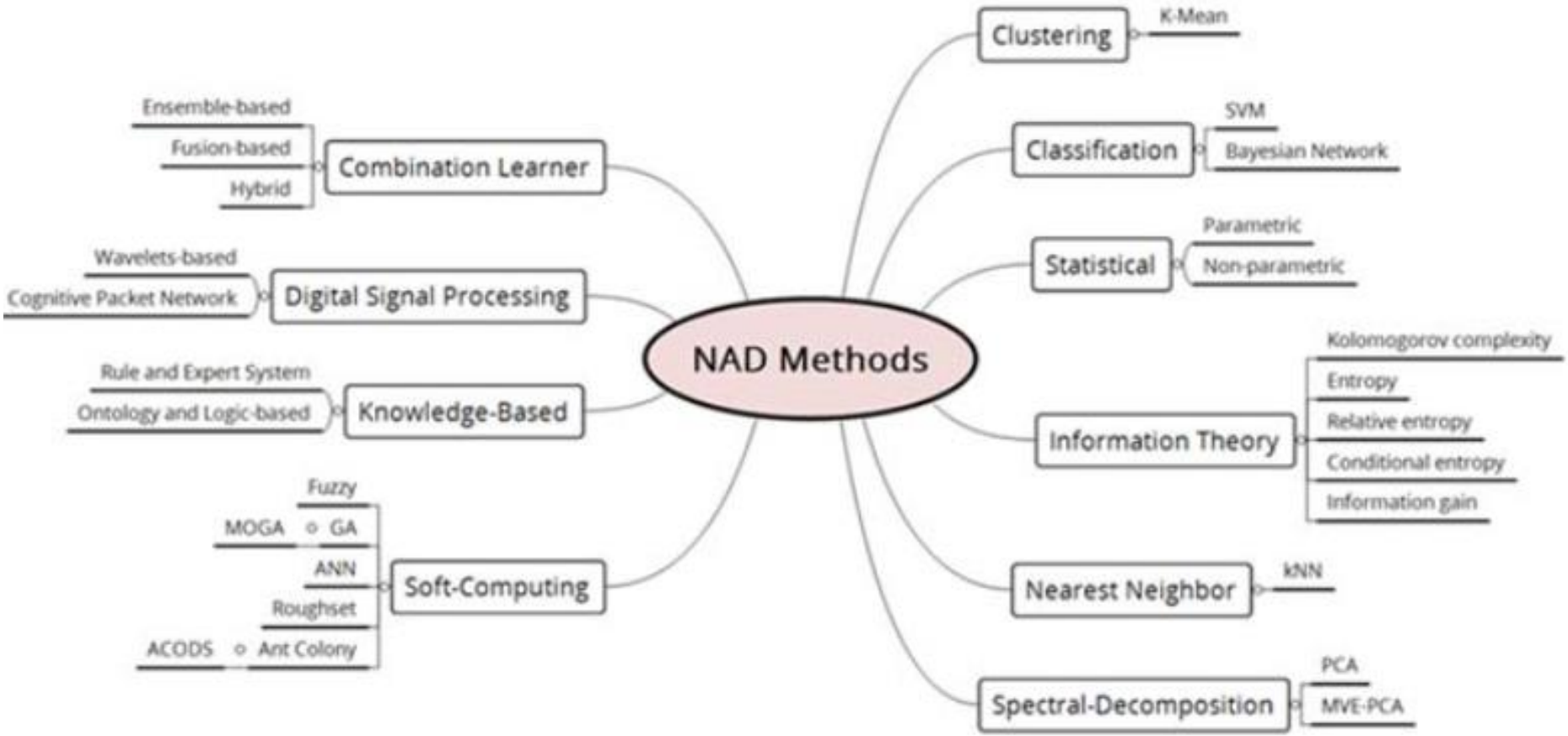


Figure 1. Network anomaly detection methods.

Sumber : Kurniabudi et.al, 2019

LR to Compare Previous SLR Article

Table 1. Comparing our survey with existing survey

Discussion Topics	Researchers							This paper
	Chandola et al., 2009 [7]	Zhang et al., 2010 [1]	Gogoi et al.,2011 [22]	Marnerides & Mauthe, 2014, [23]	Bhuyan et al., 2014 [6]	Weller-Fahy et al., 2015 [24]	M.Ahmed et al.,2016 [27]	Kurniabudi et al., 2019
Detection Technique/ Method	√	√	√	√	√	√	√	√
Type of Anomaly/ Outlier	√	√	√	√	√	√	√	√
Type of Attack	-	-	-	-	-	√	√	√
Output anomaly/ outlier	√	√	-	-	-	-	√	√
Data Repositaries	√	-	√	√	√	√	√	√
Data Types	√	√	√	-	√	√	-	√
Anomaly/ Outlier identity	-	√	-	-	-	-	-	√
Research Challenge	√	√	√	-	√	-	√	√
Categorize Network	-	-	-	-	-	-	-	√
Evaluation method	-	-	-	-	-	-	-	√

Sumber : Kurniabudi et.al, 2019

LR to Produce SLR Article

Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 7, No. 1, March 2019, pp. 37~50
ISSN: 2089-3272, DOI: 10.11591/ijeei.v7i1.773

Network anomaly detection research: a survey

Kurniabudi[1], Benni Purnama[2], Sharipuddin[3], Darmawijoyo[4], Deris Stiawan[5], Samsuryadi[6], Ahmad Heryanto[7], Rahmat Budiarto[8]
[1,2,3]STIKOM Dinamika Bangsa, Indonesia
[4,5,6,7]Faculty of Computer Science, Universitas Sriwijaya, Indonesia
[8]Albaha University, Saudi Arabia

Article Info

Article historys:

Received Oct 19, 2018
Revised Jan 09, 2019
Accepted Jan 21, 2019

Keywords:

ABSTRACT

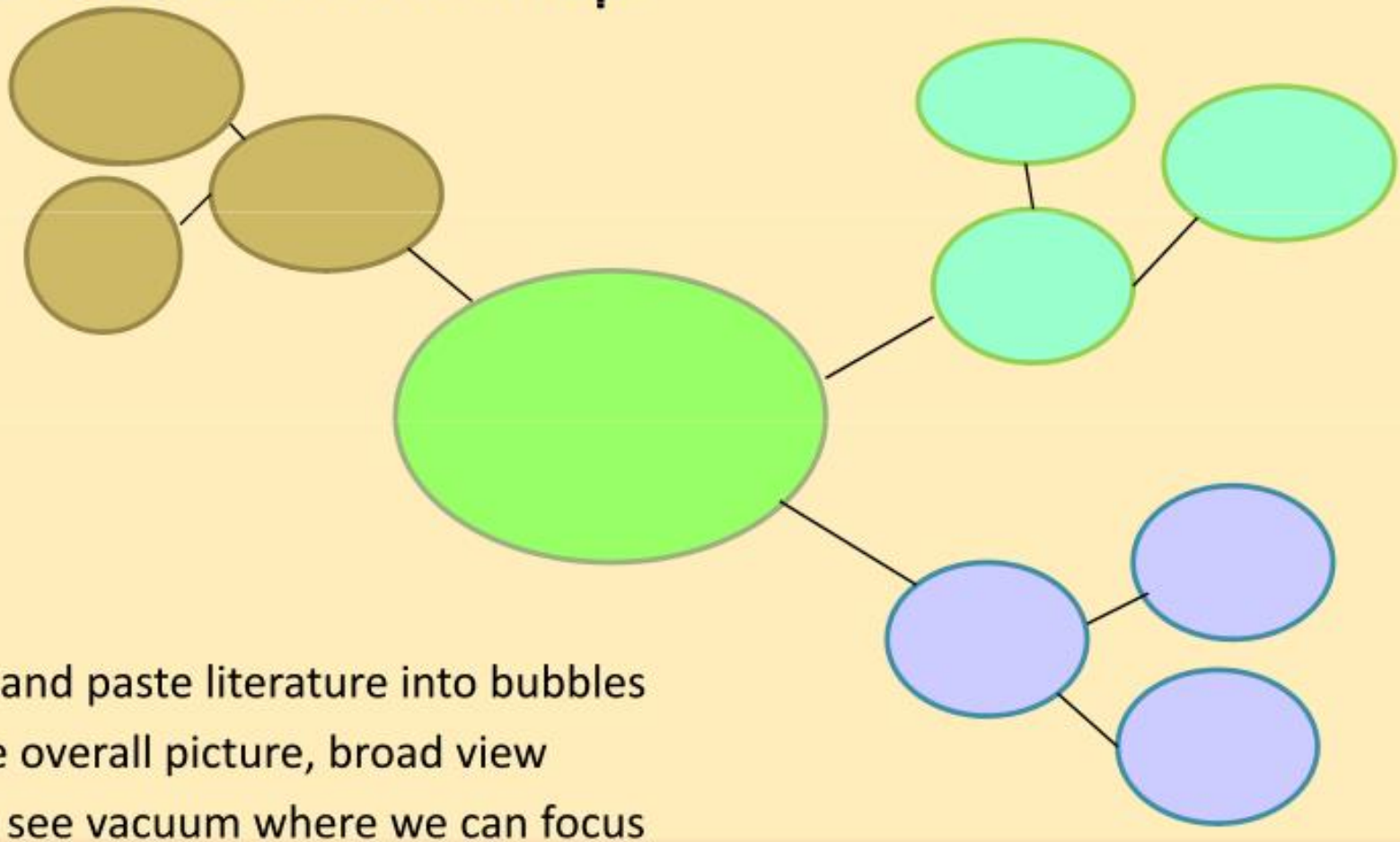
Data analysis to identifying attacks/anomalies is a crucial task in anomaly detection and network anomaly detection itself is an important issue in network security. Researchers have developed methods and algorithms for the improvement of the anomaly detection system. At the same time, survey papers on anomaly detection researches are available. Nevertheless, this paper attempts to analyze futher and to provide alternative taxonomy on anomaly detection researches focusing on methods, types of anomalies, data repositories, outlier identity and the most used data type. In addition, this

Where to Publish

- Conferences
- Journals
- Books

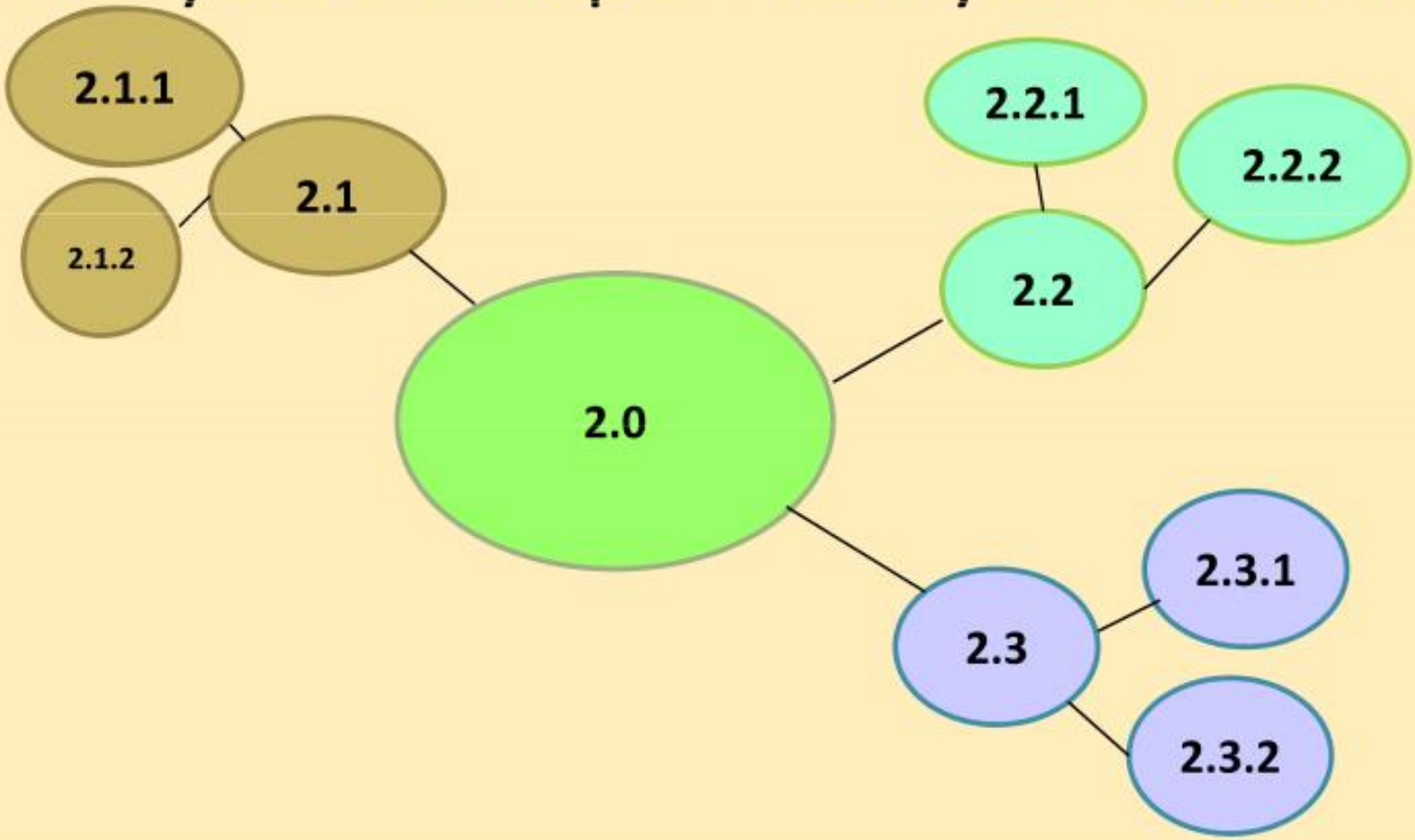
LR to Taxonomy Diagrams

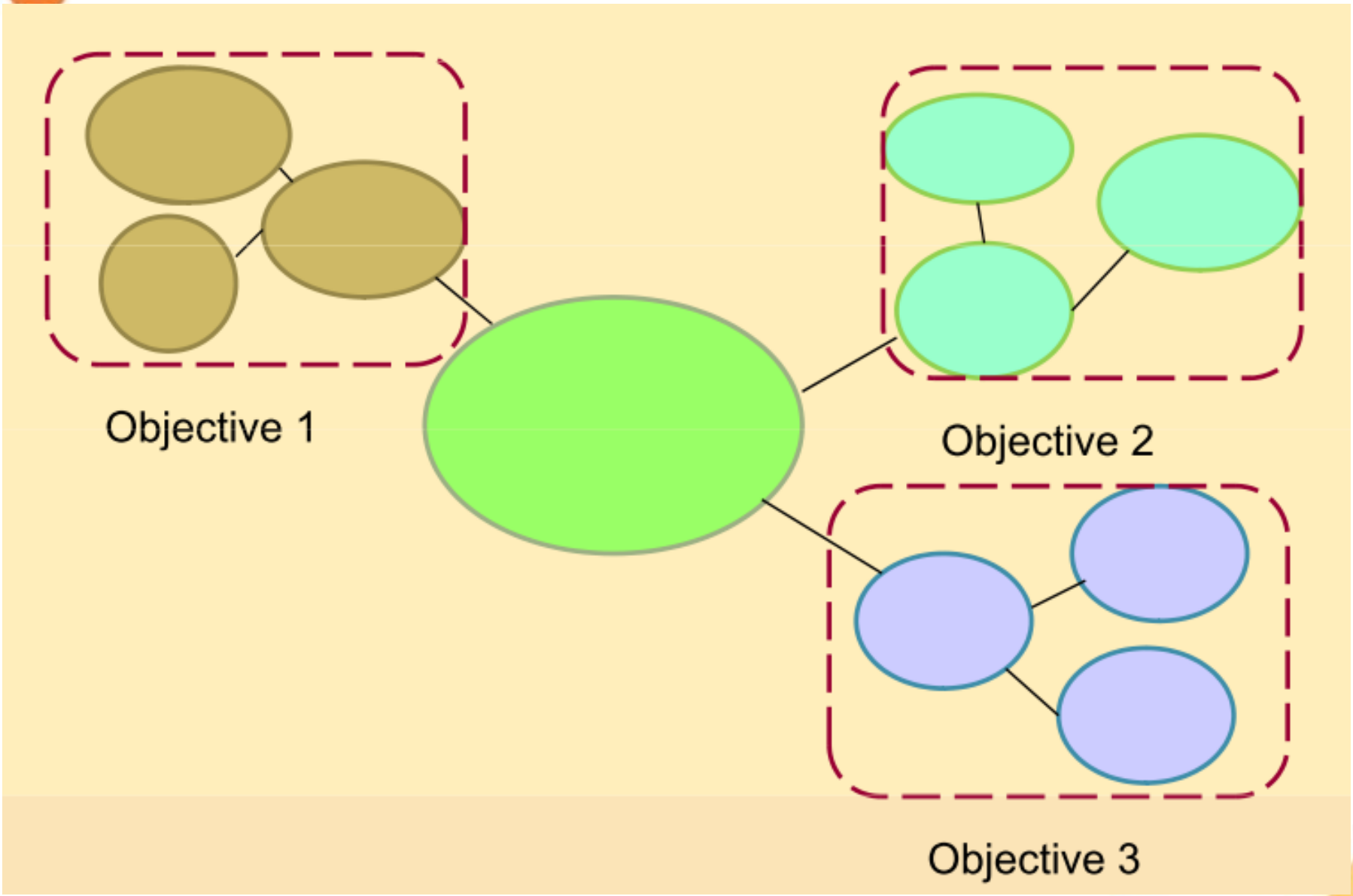
Start with a mind-map

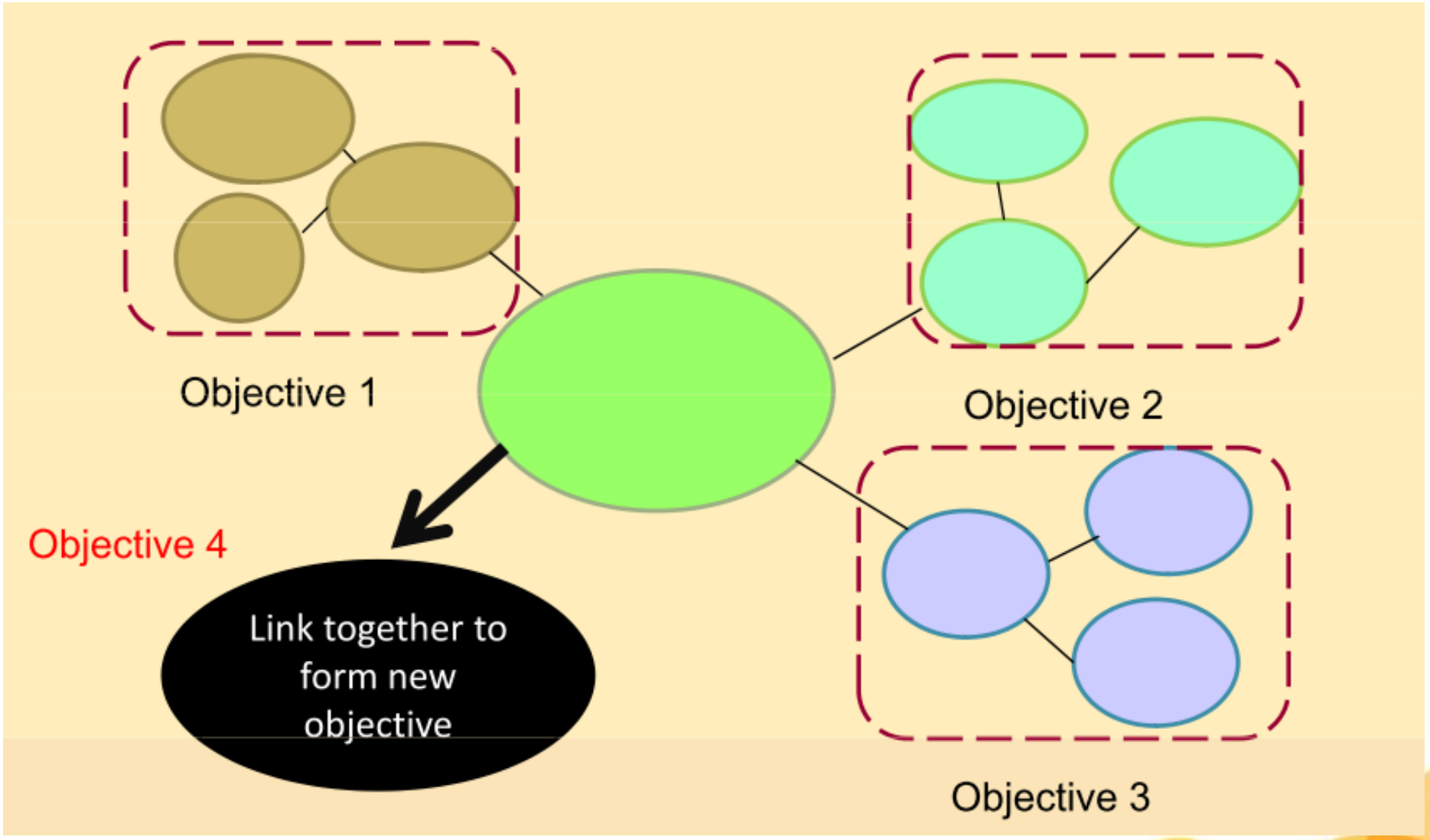


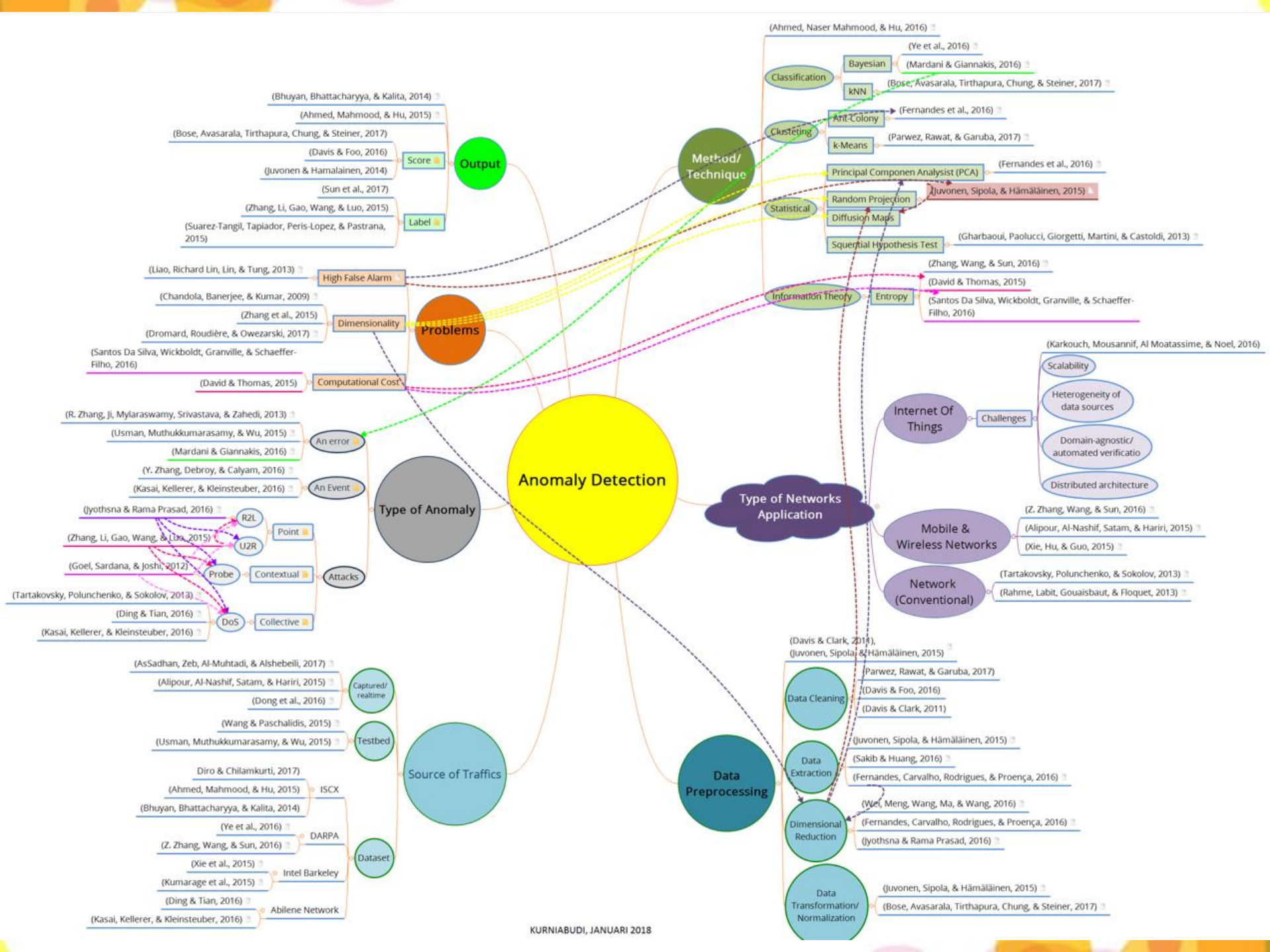
- Cut and paste literature into bubbles
- Give overall picture, broad view
- Can see vacuum where we can focus
- Know where to put boundaries, scope, limitations

Organize your LR chapter from your mind-map




Objective 1
Objective 2
Objective 3


Objective 1
Objective 2
Objective 4
Link together to form new objective
Objective 3



KURNIABUDI, JANUARI 2018

SEKIAN, TERIMAKASIH