



TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN - ĐHQG-HCM

KHOA HỆ THỐNG THÔNG TIN



Seminar

A Human-Centered Artificial Intelligence Approach for Conducting a Systematic Literature Review

Diễn giả chia sẻ



GS. LÊ ĐÌNH THẮNG

Full professor in Information systems
UQTR Business school,
Université du Québec à Trois-Rivières



TS. LÊ TRẦN ĐỨC

Postdoctoral researcher
Université du Québec à Trois-Rivières

Thời gian - Địa điểm

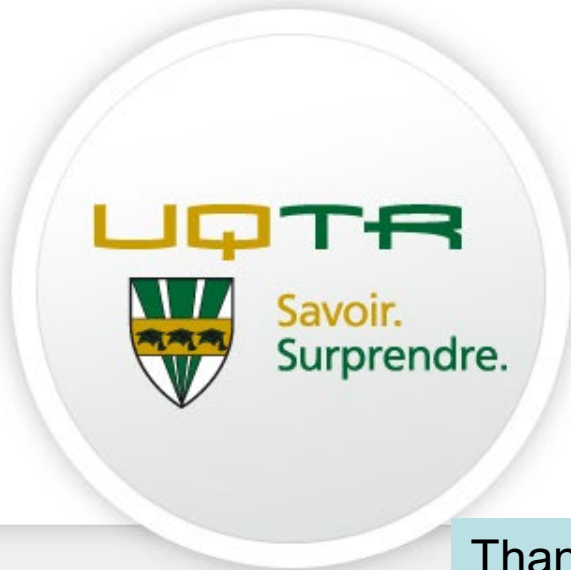


09h00 sáng Thứ Ba, ngày 26 tháng 03 năm 2024



Hội trường E, Trường ĐH Công nghệ Thông tin

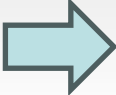




A Human-Centered Artificial Intelligence Framework for Conducting a Systematic Literature Review

Thang Le Dinh, professor in information systems
Tran Duc Le, postdoctoral researcher, INRPME

Outline

- 
- » **Introduction**
 - » **HCAI-SLR Framework**
 - » **Operationalization of the HCAI-SLR framework**
 - » **Demonstration of HCAI-SLR system**
 - » **Discussions & Conclusions**

Introduction

» Context

- Artificial intelligence (AI)-powered tools, such as chatGPT, have a significant impact on the conduct of a research project.

» Challenges

- *"...these tools can be used for educational purposes. These can help to understand an article by summarizing or translating it, or serve as a starting point and reflection.*
- *"Beyond the issue of plagiarism, AI tools raise all kinds of issues (bias, no guarantee), which the academic community must be made aware of."*

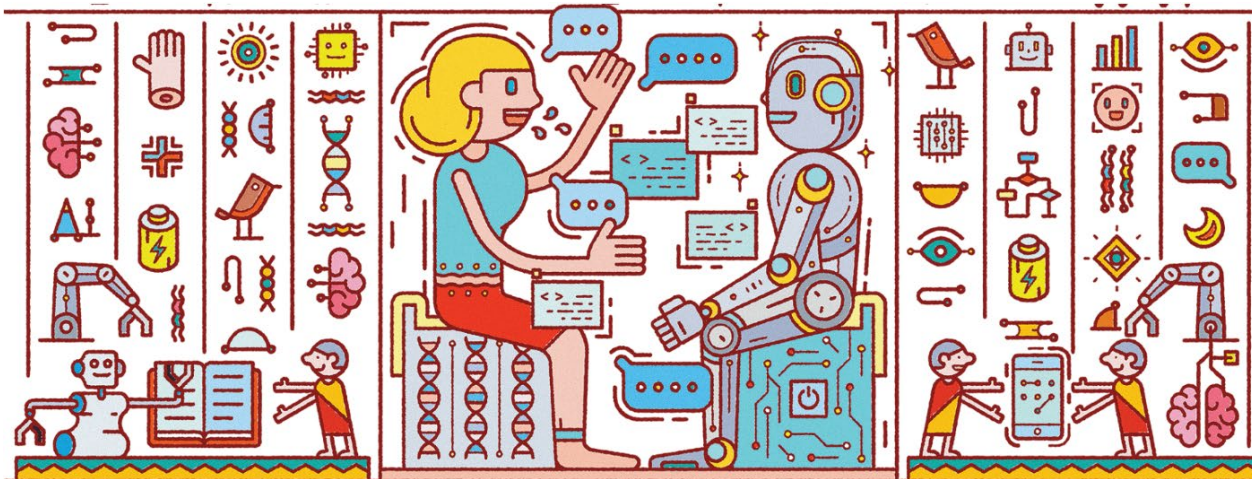
• Suggestion

- *"The arrival of generative AI (text generators) raises the need for reflection and guidelines for their ethical use in academia."*
- *"To date, very few universities have issued **guidelines**, and these are often vague and difficult to apply."*

Motivation

» Intelligence Collaborative

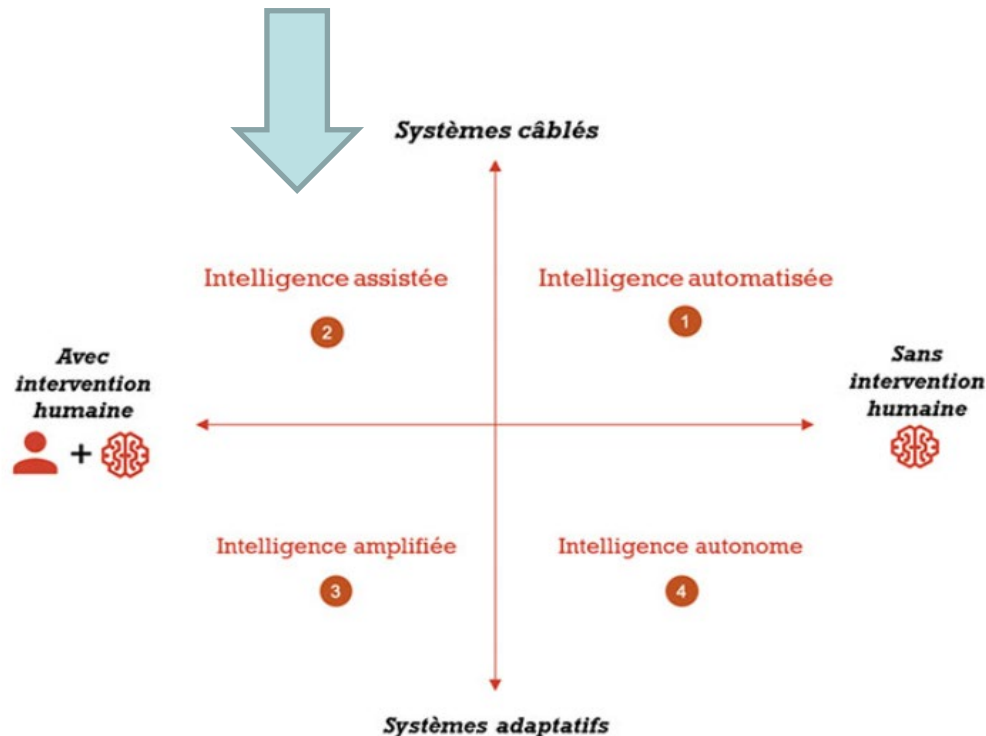
- **Humans Assisting Machines:** Humans need to perform three crucial roles. They must train machines to perform certain tasks; explain the outcomes of those tasks, especially when the results are counterintuitive or controversial; and sustain the responsible use of machines.
- **Machines Assisting Humans:** Smart machines are helping humans expand their abilities in three ways. They can amplify our cognitive strengths; interact with customers and employees to free us for higher-level tasks; and embody human skills to extend our physical capabilities.



Motivation

» Human-centered AI

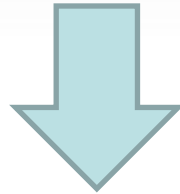
- **Assisted intelligence:** A number of actions or decisions require human judgment.
- **Amplified intelligence:** Data analytics and advanced AI can learn from human judgments and incorporate them into their recommendations.



Motivation

» Application domain

- Literature review (systematic)



“Generative AI can also conduct literature searches to find out who has written on a given topic and contribute to literature reviews.

..... If I use Boolean operators in a search engine, I will get 1,000 articles that mention my topic

Generative AI, on the other hand, draws directly from the right databases and offers a more selective list.”

Research purpose

» Motivation

- AI-powered tools (AI-powered tools) should be used as a way to augment (increase) the literature review process rather than replace it entirely.

» Objective

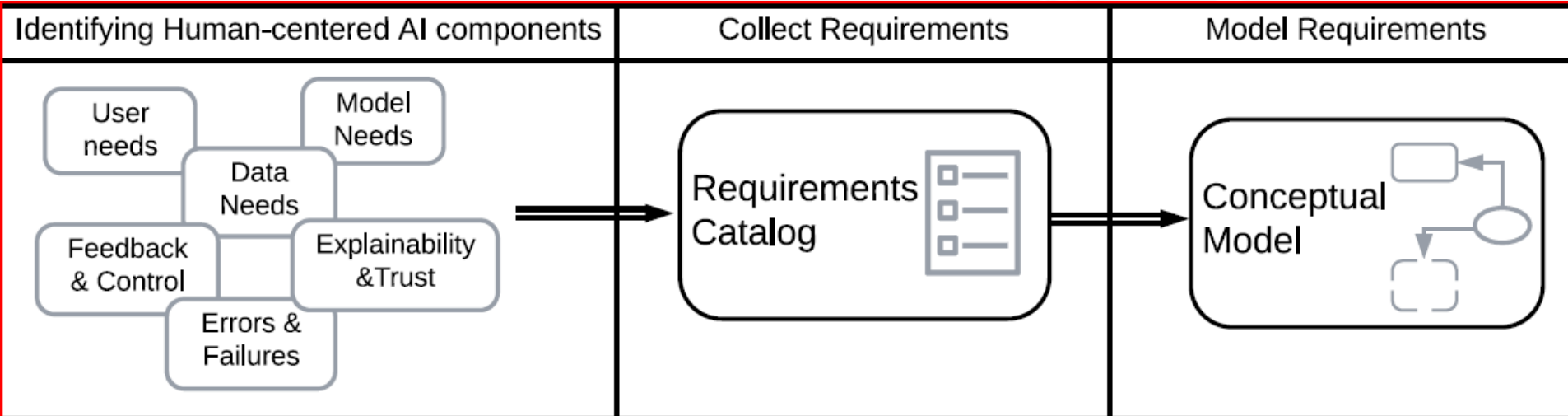
- A framework based on human-centered AI (HCAI) for conducting a systematic literature review (SLR) --> **HCAI-SLR framework.**
- To **amplify and increase** rather than replace human capabilities and to ensure that AI-powered tools operate transparently and ethically.

Outline

- » Introduction
- ➔ » **HCAI-SLR Framework**
- » Operationalization of the HCAI-SLR framework
- » Demonstration of HCAI-SLR system
- » Discussions & Conclusions

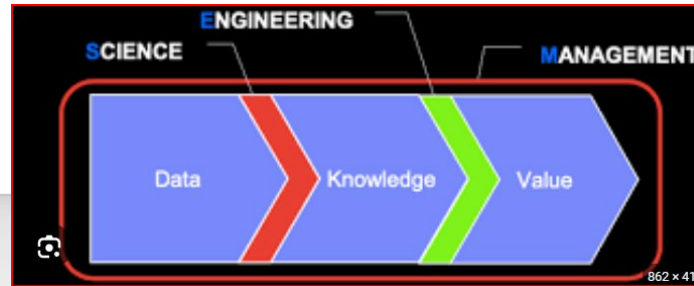
Research design

» HCAI approach

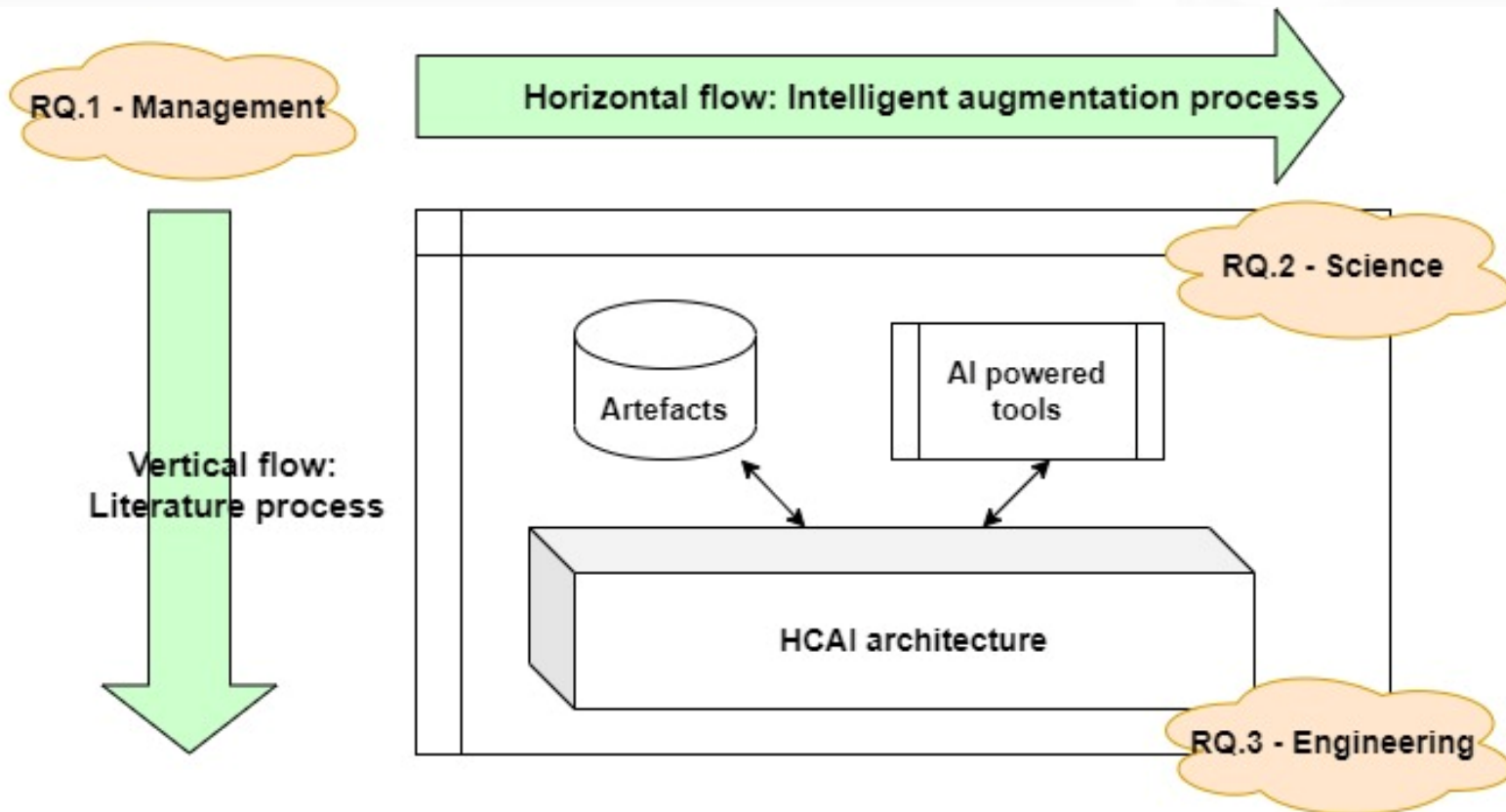


K. Ahmad, M. Abdelrazek, C. Arora et al. (2023), Applied Soft Computing 143

Research design



- **HCAI approach**
 - **Based on service science**



Methodology: Design Science

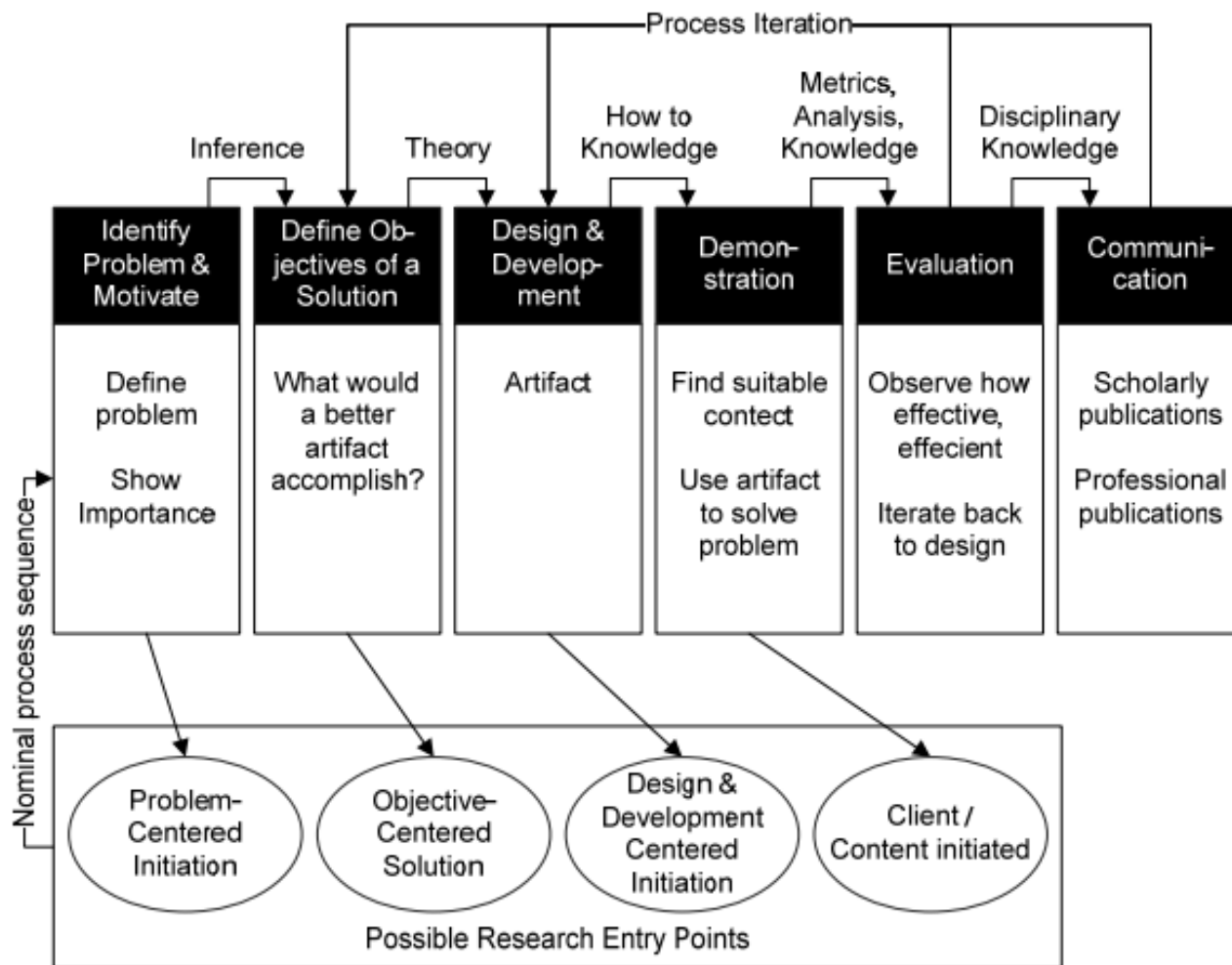


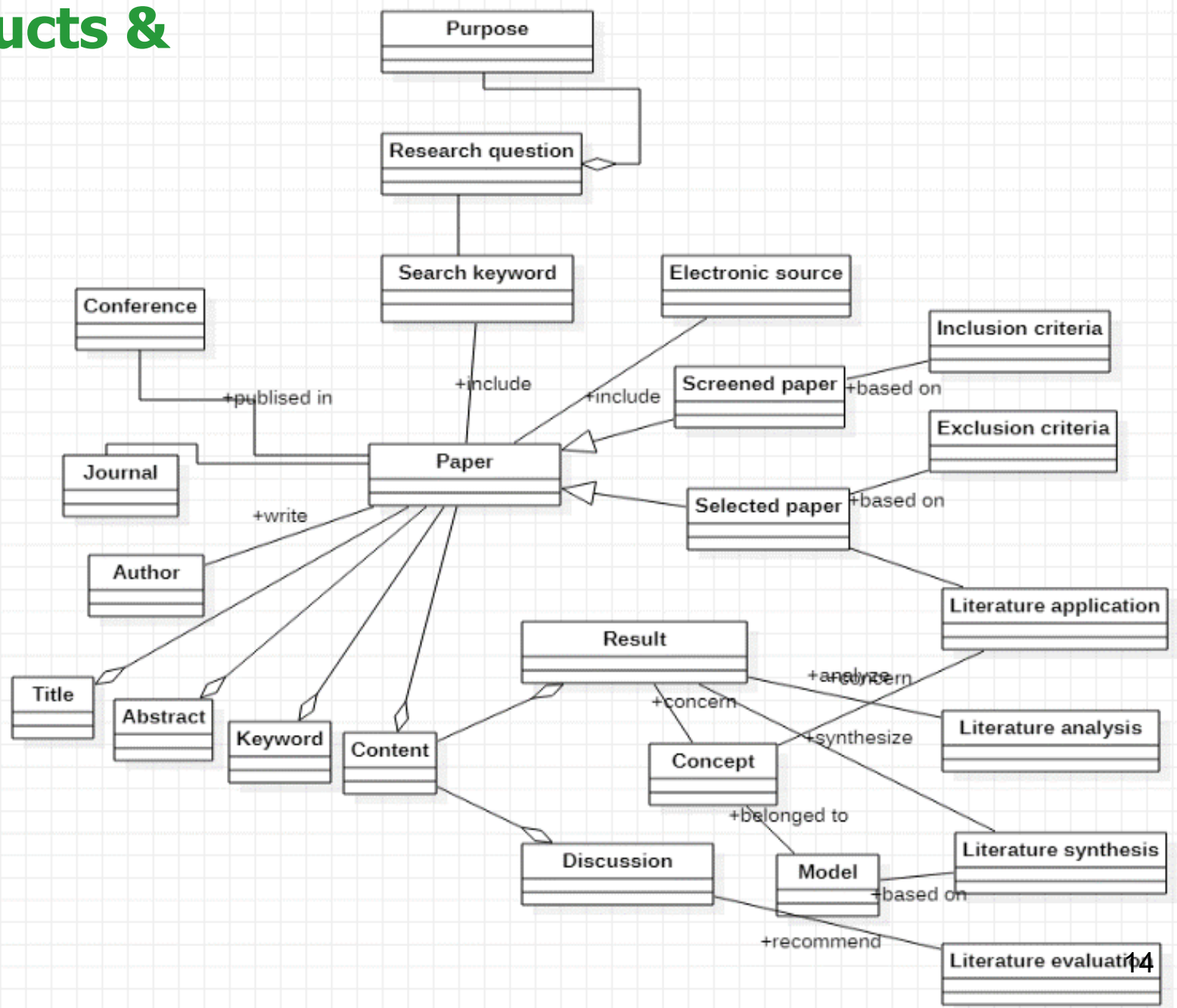
Figure 2. Design science research method [21].

[21] Peffers, K., Tuunanen, T., Rothenberger, M. A. and Chatterjee, S. 2007. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24, 3, 45-77

Artefacts of HCAI-SLR

- » The **HCAI-SLR framework** is presented on the basis of design science research, including the following artifacts:
 - **Concepts (constructs)**: form the vocabulary of a domain, constitute a conceptualization used to describe knowledge within the domain.
 - A **model**: a set of proposals or statements expressing the relationships between constructs.
 - A **method**: a set of steps used to perform the research, which is based on a set of concerned constructs (language) and a representation (model) of the solution space.
 - An **instantiation**: operationalize the constructs, the model and the method, is the concretization of an artefact in its environment.

Constructs & Model



Literature analysis



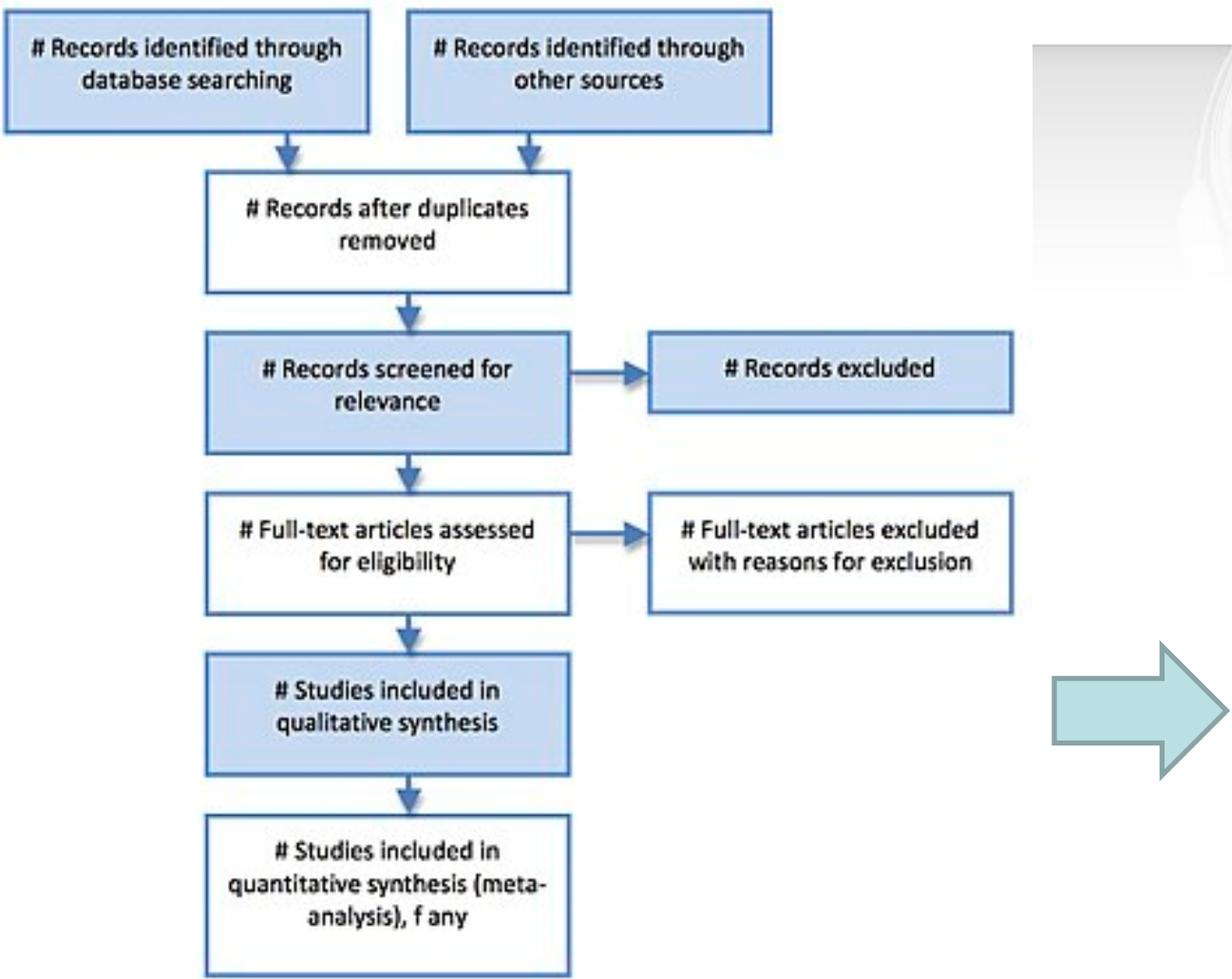
Table 1. Approaches to Literature Reviews

Concept-centric	Author-centric
Concept X ... [author A, author B, ...]	Author A ... concept X, concept Y, ...
Concept Y ... [author A, author C, ...]	Author B ... concept X, concept W, ...

Table 2. Concept Matrix

Articles	Concepts				
	A	B	C	D	...
1		✘	✘		✘
2	✘	✘			
...			✘	✘	

Method



1. Identification (S1)
2. Protocol and Training (S2)
3. Research in the literature (S3)
4. Practical screening (S4)
5. Quality Assessment (S5)
6. Data Extraction (S6)
7. Summary of studies (S7)
8. Writing (S8)

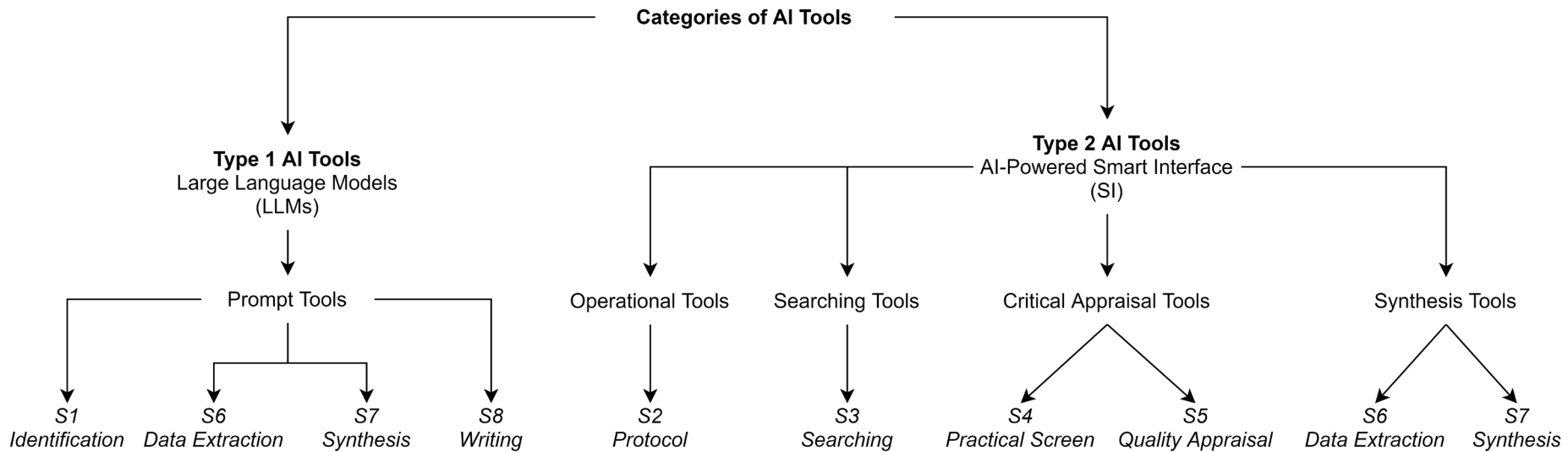
Method

<i>Step</i>	<i>Objective</i>	<i>Constructs</i>
Identification (S1)	Identify the purpose, goals, title, keywords, research questions of the review	Purpose, Research question, Keyword
Protocol and training (S2)	Identify the protocol of review process. More specifically, if there is more than one reviewer	Protocol
Searching for the literature (S3)	Find the related papers in different databases	Electronic sources, Keyword, Title, Paper, Journal/Conference
Practical screen (S4)	Identify what studies were considered for review based on the following criteria: content, publication language, journals, authors, setting, participants or subjects, program or intervention, research design and sampling methodology, date of publication or of data collection, source of financial support	Abstract, Title, Inclusion criteria, Exclusion criteria, Screening, Screened paper
Quality appraisal (S5)	Identify the exclusion criteria for judging which articles are of insufficient quality to be included	Exclusion criteria, Screening, Paper full-text, Selected paper

Méthode



Step	Objective	Constructs
<p>Data Extraction (S6)</p>	<p>Extract the applicable information related to selected research papers</p>	<p>Paper, Paper full-text, Selected paper, Data extraction, AI-powered tools, Human-AI interaction</p>
<p>Synthesis of studies (S7)</p>	<p>Combine the facts extracted from the studies carried out by selected research papers</p>	<p>Literature synthesis, AI-powered tools, Human-AI interaction</p>
<p>Writing the Review (S8)</p>	<p>Present the results of the review in a systematic way. This step is based on the DIKW hierarchy (data-information-knowledge-wisdom). Data is for gathering of parts. Information is for connecting parts. Knowledge is for forming a whole, and wisdom is for joining the wholes</p>	<p>AI-powered tools, Human-AI interaction, Literature synthesis</p>



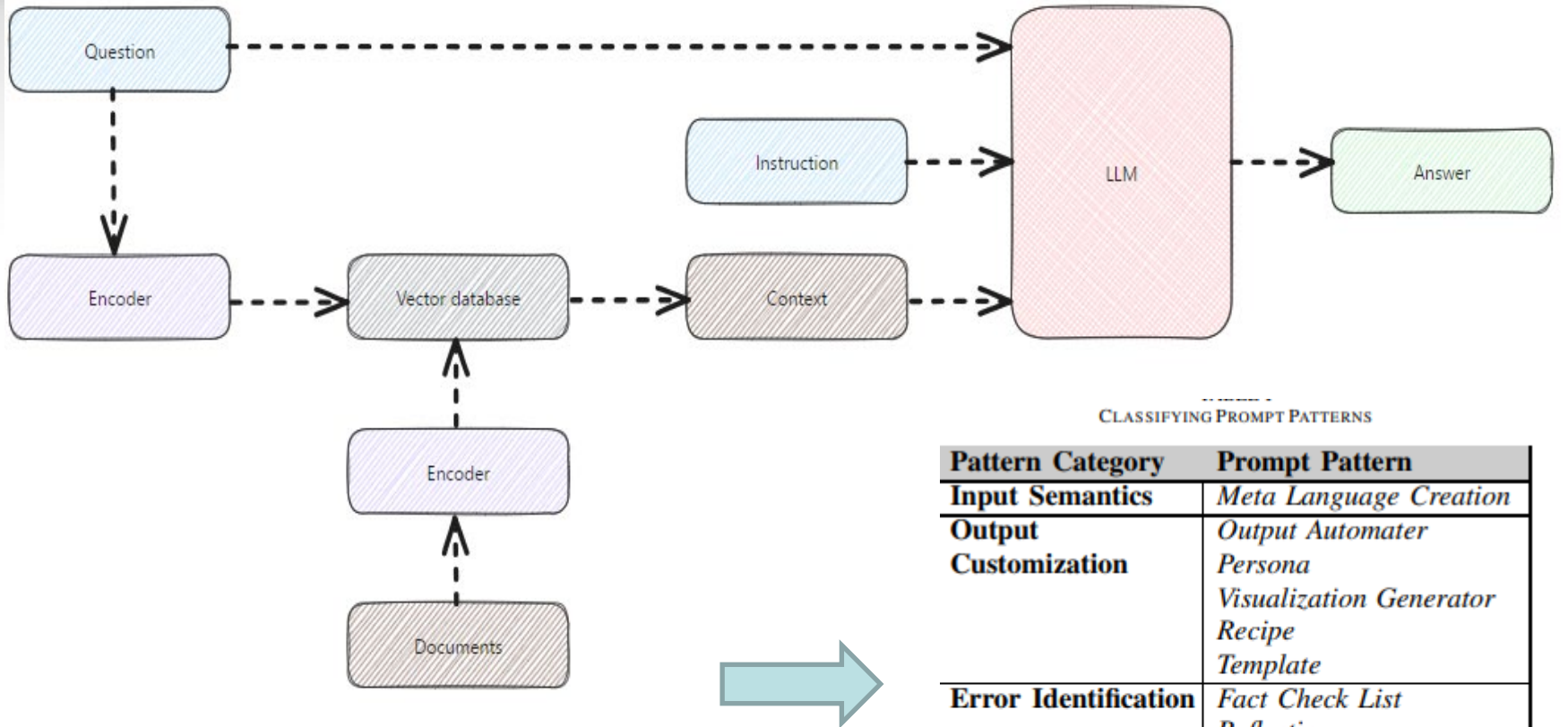
Type 1 AI Tools - Large Language Models (LLMs): Language Model-based Chatbots, also known as Large language models (LLMs) like ChatGPT, Anthropic, Bing Chat, and Google Bard, are AI tools that utilize advanced language models to understand and respond to user prompts

Type 2 AI Tools - Smart Interface (SI): AI-powered SI-based tools offer a more interactive and user-friendly approach to utilize AI in literature reviews. These tools provide a graphical user interface that allows users to navigate and utilize the tool's features easily in an interactive way.

Example of AI-powered tools

Cluster	AI Tool	Main Steps in A Systematic Literature Review							
		S1	S2	S3	S4	S5	S6	S7	S8
Type 1 (LLMs)	ChatGPT	**		*			**	**	**
	Bing Chat	*					*		*
	ClaudeAI	**					*	*	**
	Google Bard	*		*					*
	Mirrorthink	**		*			*	*	**
	Theb.AI								
	POE	*							*
	Perplexity	*		*					*
	ChatSonic	*							*
	HuggingChat	*							*
	PI AI	*							*
	Dante-ai	*							*
Type 2 (Smart Interface)	2dSearch			*					
	Semantic Scholar			*					
	Article Galaxy			*					
	CADIMA			*	*	*	*	**	
	Carrot2	*		**					
	Citationchaser			*					
	Rayyan		*		*	**			
	DistillerSR				*	*	*		*
	Nvivo	*					*		
	Atlas.ti	*					*		
	Covidence		*		*				
	EPPI-Reviewer		*			*			
	RobotReviewer						*	**	
	Iris.ai	**		*			*	*	
	Research Rabbit			*					
Scispace			**			**	*	*	

Type 1 – Prompt engineering



CLASSIFYING PROMPT PATTERNS

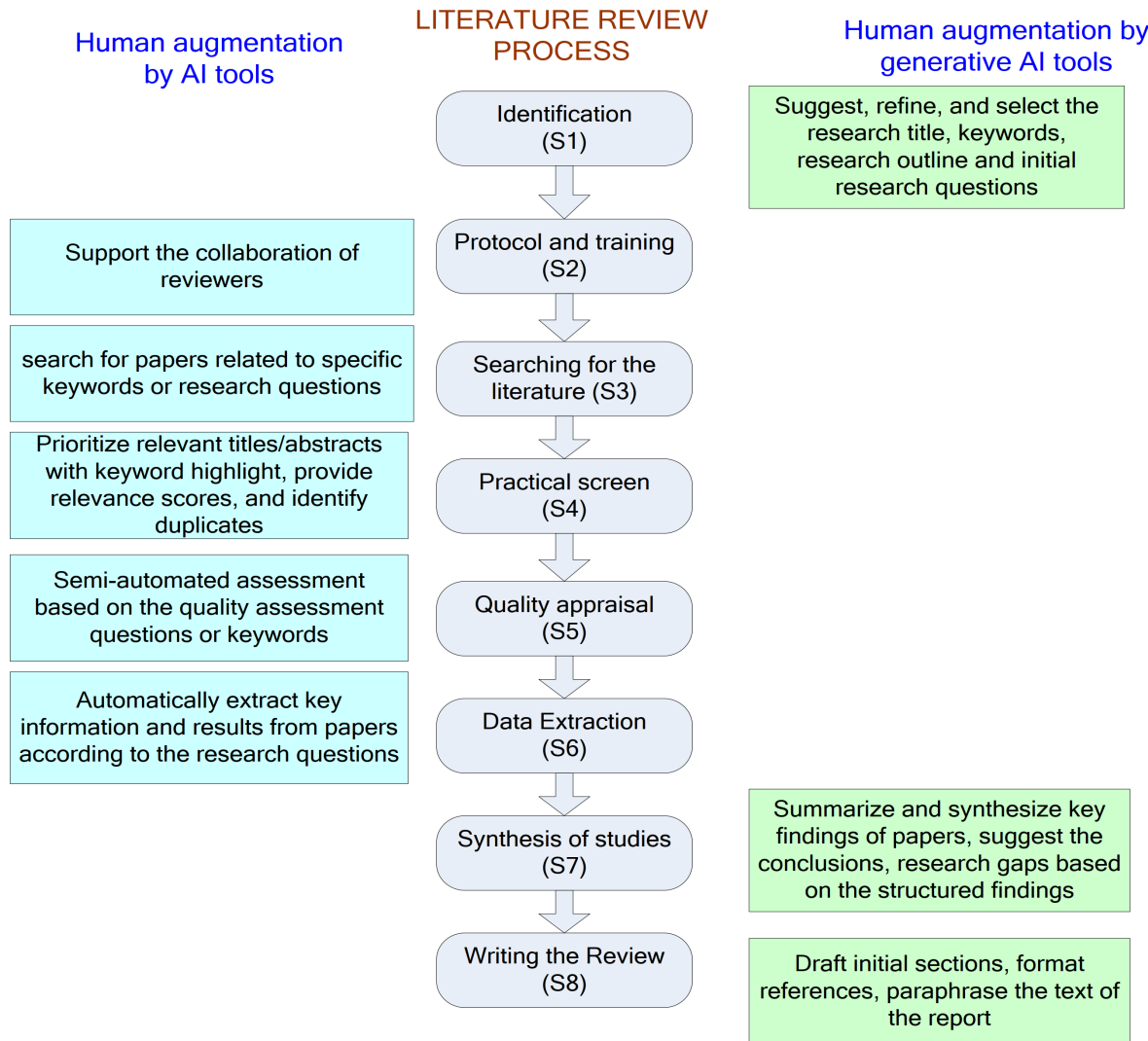
Pattern Category	Prompt Pattern
Input Semantics	<i>Meta Language Creation</i>
Output Customization	<i>Output Automater Persona Visualization Generator Recipe Template</i>
Error Identification	<i>Fact Check List Reflection</i>
Prompt Improvement	<i>Question Refinement Alternative Approaches Cognitive Verifier Refusal Breaker</i>
Interaction	<i>Flipped Interaction Game Play Infinite Generation</i>
Context Control	<i>Context Manager</i>

[[White et al., 2023](#)]

Type 1 – Prompt engineering

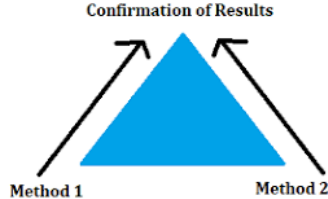
Pattern Category	Description	Prompt Pattern	Description
Input Semantics	Defines custom languages or input formats to communicate more effectively	Meta Language Creation	Establishes custom languages or notations that the LLM can interpret
Output Customization	Focuses on constraining or tailoring the types, formats, structure, or other properties of the LLM output	Output Automater	Generates scripts to automate any steps suggested in the LLM's output
		Persona	Gives the LLM a persona or role to influence the types of outputs generated
		Visualization Generator	Generates text that can be fed into other tools to create visualizations
		Recipe	Provides a sequence of steps to accomplish a goal using partially known information or constraints
		Template	Requires the LLM to follow a precise template for formatting its output
Error Identification	Focuses on identifying and resolving errors in the LLM's output	Fact Check List	Requires the LLM to list key facts from its output that should be verified
		Reflection	Asks the LLM to explain its reasoning and identify potential errors
Prompt Improvement	Aims to improve the quality of prompts and outputs	Question Refinement	Requires the LLM to suggest better versions of the user's questions
		Alternative Approaches	Makes the LLM list alternative ways to accomplish the user's task
		Cognitive Verifier	Forces the LLM to subdivide questions to provide more accurate answers
		Refusal Breaker	Rewords questions when the LLM refuses to answer
Interaction	Focuses on customizing the interaction between the user and LLM	Flipped Interaction	Makes the LLM ask questions instead of the user
		Game Play	Generates games centered around specific topics
		Infinite Generation	Generates output indefinitely without reentering the prompt
Context Control	Controls contextual information used by the LLM	Context Manager	Allows users to specify or remove context from the conversation

Literature Review Process and AI-powered tools

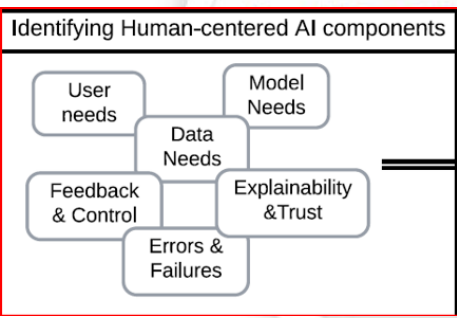


Horizontal flow: Intelligence augmentation process

Generative / Specific AI



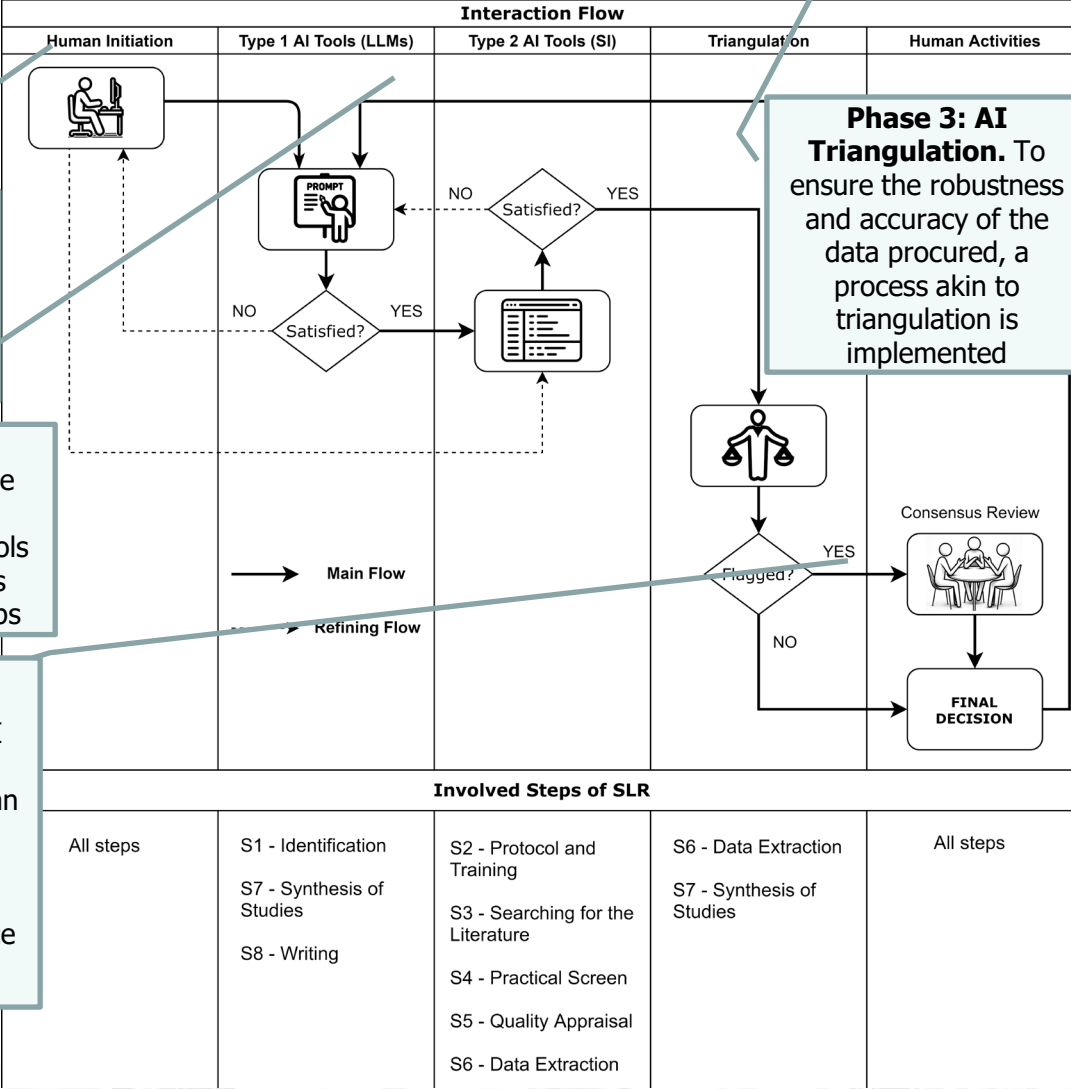
Interaction Human-IA



Phase 1: Human Initiation. The process begins with human experts who set the direction of the review.

Phase 2: AI Augmentation. Once the human researcher has initiated the re-view, AI tools can augment the process with two kinds of AI groups

Phase 4: Human Activities. After the AI has screened and procured the data, human intervention - the most important part - is reintroduced to ensure the validity and relevance of the findings



Intelligence augmentation process

Table 1: Intelligence augmentation process.

Step	Phase	Human initiation	AI augmentation (Generative AI tools)	AI augmentation (Traditional AI tools)	AI Triangulation	Human decision
Identification (S1)		X	X		X	X
Protocol and training (S2)		X		X		X
Searching for the literature (S3)		X		X		X
Practical screen (S4)		X		X		X
Quality appraisal (S5)		X		X	X	X
Data extraction (S6)		X	X	X	X	X
Synthesis of studies (S7)		X	X		X	X
Writing the review (S8)		X	X			X

GitHub repository: <https://github.com/tranducle/HCAI-SLR>

HCAI-SLR Framework Phase	User Needs	Model Needs	Data Needs	Feedback & Control	Explainability & Trust	Error & Failure
Human Initiation	✓✓	✓		✓		
AI Augmentation		✓✓	✓		✓	
AI Triangulation				✓	✓✓	✓
Human Activities	✓			✓✓	✓	✓

HCAI-SLR framework

Involved SLR steps with *Type 1* AI tools

Step	Role of AI Tools	Role of Humans
Identification (S1)	<p>Suggest, refine, and select the research title, keywords, research outline and initial research questions from input data</p>	<ul style="list-style-type: none"> - Define the review's scope, objectives, and critical keywords based on expertise and research needs - Prepare or refine the appropriate prompts - Determine the search strategy - Shortlist the keywords and research questions
Synthesis of Studies (S7)	<ul style="list-style-type: none"> - Summarizing and synthesizing key findings of papers through prompted queries - Identify and cluster recurring themes, patterns, or insights - Suggest the conclusions, research gaps based on the structured findings 	<ul style="list-style-type: none"> - Choose appropriate methods (quantitative or qualitative) to synthesize data from the selected studies - Draw insightful conclusions from aggregated findings
Writing (S8)	<ul style="list-style-type: none"> - Draft initial sections, format references, and ensure consistency throughout the review - Paraphrase the text of the report with an academic and concise tone 	<ul style="list-style-type: none"> - Write the draft of report - Craft the narrative, ensuring that interpretations align with evidence

HCAI-SLR framework

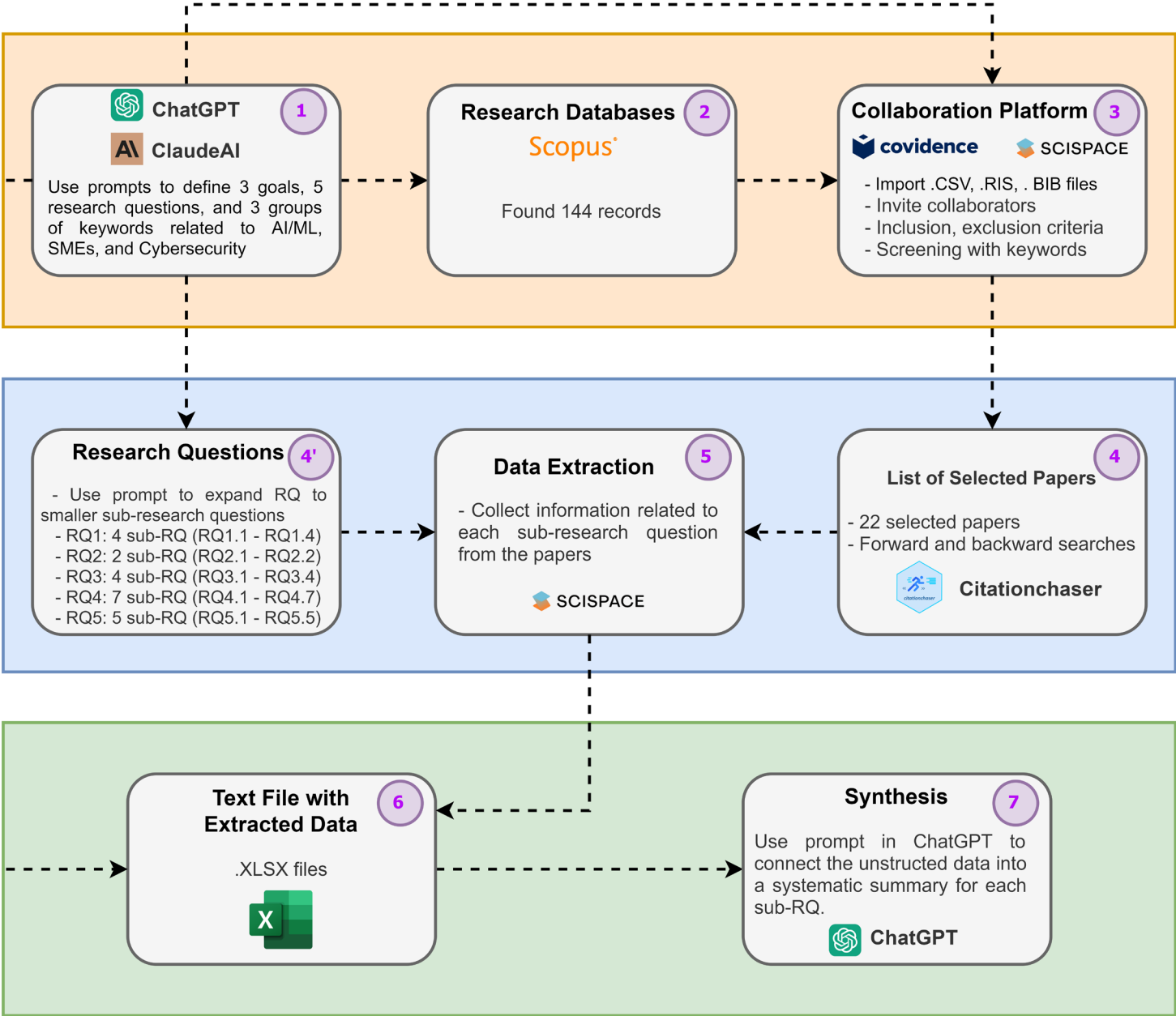
Involved SLR steps with Type 2 AI tools

Step	Role of AI Tools	Role of Humans
Protocol and Training (S2)	AI tools have a limited role	Choose a supported platform and define the review protocol
Searching for the Literature (S3)	<ul style="list-style-type: none"> - The capability to search for papers related to specific keywords or research questions - AI search engine cannot cover all databases 	Ensure comprehensive search across databases and refine search strategy for systematic coverage
Practical Screen (S4)	Prioritize relevant titles/abstracts with keyword highlight and provide relevance scores; duplicate detection	Validate and decide the list of screened papers
Quality Appraisal (S5)	<ul style="list-style-type: none"> - AI tools have a limited role - Semi-automated assessment based on the quality assessment questions or keywords 	Manually verify with full-text screening
Data Extraction (S6)	Automatically extract key information such as study characteristics, outcomes, contributions, and results from papers according to the research questions	<ul style="list-style-type: none"> - Verify AI-extracted data for accuracy - Interpret results

Outline

- » Introduction
- » HCAI-SLR Framework
- ➔ » **Operationalization of the HCAI-SLR framework**
- » Demonstration of HCAI-SLR system
- » Discussions & Conclusions

Example




Subject of demonstration:
Artificial Intelligence and Machine Learning (AI/ML) in Cybersecurity in SMEs: A Systematic Literature Review



Step 1, the identification phase

Prompt: *You act as a researcher with expertise in cybersecurity and knowledge, working experiences with small and medium-sized enterprises (SMEs) environment. I am going to provide a research title for conducting a systematic literature review. Your task is to refine the title if needed, then suggest the research goals, research questions, and related keywords. Ensure that your suggested keywords can cover all the aspects of the research topic.*

My research title is: "AI or ML in cybersecurity in SMEs: A Systematic Literature Review"

CHATGPT	CLAUDE AI
<p> Your research title is a good start, but it could benefit from a slight refinement for clarity and focus.</p> <p>Refined Research Title: "Applications of Artificial Intelligence (AI) and Machine Learning (ML) in Cybersecurity for Small Medium-sized Enterprises (SMEs): A Systematic Literature Review."</p> <p>Research Goals:</p> <ol style="list-style-type: none"> 1. To understand the extent and nature of AI and ML applications in cybersecurity specifically for SMEs. 2. To identify the advantages, challenges, and potential risks of using AI and ML tools in cybersecurity within the SME environment. 3. To provide a comprehensive synthesis of existing literature on the topic, identifying gaps and suggesting areas for future research. 4. To offer recommendations and best practices for SMEs looking to integrate AI and ML in their cybersecurity strategies. 	<p>Here are my suggestions for refining the research title, goals, questions, and keywords:</p> <p>Research Title: "The application of artificial intelligence and machine learning for cybersecurity in small and medium-sized enterprises: A systematic literature review"</p> <p>Research Goals:</p> <ul style="list-style-type: none"> • To understand the current landscape of AI/ML technologies being applied for cybersecurity in SMEs • To identify the benefits and challenges of using AI/ML for cybersecurity in SMEs • To determine the most common and effective uses of AI/ML for cybersecurity in SMEs • To highlight gaps in the research and opportunities for further study

The researcher chooses the title: *"Applications of Artificial Intelligence (AI) and Machine Learning (ML) for Cybersecurity in Small Medium-sized Enterprises (SMEs): A Systematic Literature Review"*

The researcher defines the goals:

- *To understand the current landscape of AI/ML technologies being applied for cybersecurity in SMEs;*
- *To identify the advantages, challenges, and potential risks of using AI and ML tools in cybersecurity within the SME environment;*
- *To provide a comprehensive synthesis of existing literature on the topic, identifying gaps and suggesting areas for future research.*

Step 1, the identification phase

Prompt:

Find the synonyms for these keywords, then classify all the old and new keywords into three categories: Category 1: related to cybersecurity Category 2: related to AI and ML Category 3: related to SMEs "Keywords: Artificial Intelligence, Machine Learning, Cybersecurity, Cyber security, Small Medium-sized Enterprises, SMEs, Threat detection, Cyber threats, Risk assessment, Anomaly detection, Intrusion detection system (IDS), Intrusion prevention system (IPS), Automated threat response, network security, information security, deep learning".

Present in tabular format

Sure, here's a tabular format:

Category	Keywords & Synonyms
1. Related to Cybersecurity	Cybersecurity, Cyber security, Threat detection, Cyber threats, Risk assessment, Anomaly detection, Intrusion detection system (IDS), Intrusion prevention system (IPS), Automated threat response, Network security, Information security, Information assurance, Digital security, Computer security, Threat discovery, Threat identification, Threat spotting, Digital threats, Online threats, Electronic threats, Risk evaluation, Risk analysis, Threat assessment, Outlier detection, Deviation detection, IDS system, Unauthorized access detection, IPS system, Unauthorized access prevention, Automatic threat reaction, Automated threat mitigation, Net security, Network protection, InfoSec, Data security
2. Related to AI and ML	Artificial Intelligence, Machine Learning, Deep learning, AI, Computational intelligence, Intelligent systems, ML, Data mining, Predictive analytics, Neural networks, Deep neural networks
3. Related to SMEs	Small Medium-sized Enterprises, SMEs, SME, Medium-sized businesses, Small and medium business

Here is the categorization of old and new keywords related to cybersecurity, AI/ML, and SMEs presented in a table:

Category	Keywords
Category 1: Related to cybersecurity	Cybersecurity, Cyber security, Threat detection, Cyber threats, Risk assessment, Anomaly detection, Intrusion detection system (IDS), Intrusion prevention system (IPS), Automated threat response, Network security, Information security, Data breach prevention, Vulnerability assessment, Security analytics, Threat intelligence, Incident response, Malware detection, Phishing detection
Category 2: Related to AI and ML	Artificial Intelligence, Machine Learning, Deep learning, Neural networks, Natural language processing (NLP), Computer vision, Predictive modeling, Pattern recognition, Data mining
Category 3: Related to SMEs	Small medium-sized enterprises, SMEs, Small business, Medium business, Startups, Entrepreneurship, SMBs

The researcher defines the keywords:

- **Group 1:** *Cybersecurity, Cyber Security, Threat Detection, Cyber Threats, Risk Assessment, Anomaly Detection, Intrusion Detection System, Intrusion Prevention System, Automated Threat Response, Network Security, Information Security, Computer Security, Threat Discovery, Threat Identification, Risk Evaluation, Risk Analysis, Threat Assessment, Outlier Detection, Unauthorized Access, Threat Mitigation, Data Security, Malware Detection, Phishing Detection*
- **Group 2:** *Artificial Intelligence, Machine Learning, Deep Learning, AI, Computational Intelligence, Intelligent Systems, ML, Data Mining, Predictive Analytics, Neural Networks, Deep Neural Networks, Pattern recognition*
- **Group 3:** *Small Medium-sized Enterprises, SMEs, SME, Medium-sized businesses, Small and medium businesses, SMB, SMBs*

Example



Step 2, the searching phase

The screenshot shows the Scopus search interface. At the top left, there are logos for UQTR (Université du Québec à Trois-Rivières) and Scopus. A search bar contains a complex query: `TITLE-ABS-KEY (("Cybersecurity" OR "Cyber Security" OR "Threat Detection" OR "Cyber Threats" OR "Risk Assessment" OR "Anomaly Detection" OR "Intrusion Detection System" OR "Intrusion Prevention System" OR "Automated Threat Response" OR "Network Security" OR "Information Security" OR "Computer Security" OR "Threat Discovery" OR "Threat Identification" OR "Risk`. Below the search bar, there are options to 'Save search', 'Set search alert', and 'Edit in advanced search'. The search results section shows '144 documents found'. On the left, there are 'Refine search' and 'Filters' sections. The main results table has columns for 'Document title', 'Authors', 'Source', 'Year', and 'Citations'. The first result is 'The impact of public health emergencies on small and medium-sized enterprises: Evidence from China' by Liu, Q., Shi, C., Tse, Y., and Zhang, L., published in 'Global Finance Journal' in 2023. The second result is 'The European AI liability directives – Critique of a half-hearted approach and lessons for the future' by Hacker, P., published in 'Computer Law and Security Review' in 2023. A red circle highlights the 'Document title' column header in the table.

Search results in the SCOPUS database

Example



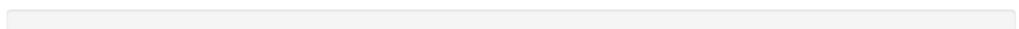
Step 3, the screening phase

Review settings Reviewers **Team settings** Eligibility criteria Study tags

Ⓢ This review is part of a trial and is restricted to screening 500 records. To remove this limit, [upgrade](#) to a paid plan.

Title and abstract screening

Team Progress



0 ● DONE 0 ● ONE VOTE 0 ● CONFLICTS 0 ● NO VOTES

REVIEWER	CONTRIBUTION
Antoine Dion	0
Tran Duc Le	0

Rules

Everyone can do anything Manage rules

ALL STUDIES MUST BE SCREENED BY EITHER

Anyone

Select a reviewer ▼ **Add**

CONFLICTS CAN BE RESOLVED BY

Tran Duc Le ✕

Select a reviewer ▼ **Add**

Full text review

Extraction

Plateforme Covidence

Manage Highlights

Inclusion

Add word or phrase

+ Add

- Cybersecurity
- Cyber Security
- Threat Detection
- Cyber Threats
- Risk Assessment
- Anomaly Detection
- Intrusion Detection System
- Intrusion Prevention System
- Automated Threat Response
- Network Security
- Information Security

Exclusion

Add word or phrase

+ Add

- survey
- review
- report

Example



Step 3, the screening phase

Review Summary Settings PRISMA Export

\$ This review is part of a trial and is restricted to screening 500 records. To remove this limit, [upgrade](#) to a paid plan.

Import references 0 total duplicates removed Import

IMPORT HISTORY

01 NOV 2023	144 studies added to Title and abstract screening	No duplicates found
-------------	---	---------------------

[VIEW DETAILS](#)

Title and abstract screening 0 irrelevant 144 studies to screen

TEAM PROGRESS

0 DONE 0 CONFLICTS

0 ONE VOTE 144 NO VOTES

[Team settings](#)

TRAN DUC, YOU CAN STILL

SCREEN

144

Continue

You've screened 0 studies so far

Reference import

Example



Step 3, the screening phase

Screen references 144 Resolve conflicts 0 Awaiting other reviewer 0 Irrelevant references 0

This review is part of a trial and is restricted to screening 500 records. To remove this limit, [upgrade](#) to a paid plan.

All Filter ▾ Tags ▾ Criteria ^ Hide highlights Hide abstracts Display: 25 ▾ Most relevant ▾

Include

- InC01. Studies published in the last ten years between 2013 to 2023
- InC02. Studies published in conferences and journals
- InC03. Studies that are written in English.

Exclude

- EXC01. Studies published before 2013
- EXC02. Studies that are published in non-peer-reviewed sources
- EXC03. Studies that are not written in English
- EXC04. Studies published in preprint platforms
- EXC05. The full text of the study is not available
- EXC06. None of the phrases/keywords from the two main search groups included in the title or abstract

[Edit criteria](#)

#57 - Petrariu 2022

A Comparative Study of Unsupervised **Anomaly Detection** Algorithms used in a Small and Medium-Sized Enterprise

Petrariu, I.; Moscaliuc, A.; Turcu, C.E.; Gherman, O.
International Journal of Advanced Computer Science and Applications 2022;(): 2022

Abstract

Anomaly detection finds application in several industries and domains. The **anomaly detection** market is growing driven by the increasing development and dynamic adoption of emerging technologies. Depending on the type of supervision, there are three main types of **anomaly detection** techniques: unsupervised, semi-supervised, and supervised. Given the wide variety of available **anomaly detection** algorithms, how can one choose which approach is most appropriate for a particular application? The purpose of this evaluation is to compare the performance of five unsupervised **anomaly detection** algorithms applied to a specific dataset from a small and medium-

No **Maybe** **Yes**

Example

<https://github.com/tranducle/HCAI-SLR>



Step 4: Full Text Screening, Backward & Forward Search

The screenshot displays the SCISPACE interface. On the left is a navigation sidebar with icons for home, search, and other functions. The main content area shows a paper titled "Cybersecurity Resilience in SMEs. A Machine Learning Approach" by Juan Carlos Fernandez de Arroyabe, Marta F. Arroyabe, Ignacio Fernandez, and Carlos F. A. Arranz. The abstract and introduction are visible. On the right, a chat interface with Copilot is open, showing a question: "Does the study specifically address the application of AI and/or ML for cybersecurity?" and a response: "Yes, the study specifically addresses the application of machine learning (ML) for cybersecurity. The study highlights the potential of statistical methods, particularly machine learning techniques, to identify the relationships between factors affecting cybersecurity resilience in small and medium-sized enterprises (SMEs).[1] The use of ML algorithms is considered appropriate in the field of cybersecurity, where there may be a lack of information on the part of firm managers, unbalanced databases, and correlation problems between variables. The study emphasizes the use of ML techniques to obtain robust models of the relationships between variables in the context of cybersecurity in SMEs. [2]"

The *Typeset* chat interface supports the formulation of quality assessment questions for full text screening

AI tools: Covidence, SCISPACE, typeset

Example



Step 4: Full Text Screening, Backward & Forward Search

citationchaser Home Article input **References** Citations Analysis Network

References from your articles (backward citation chasing)

Once you have loaded your input articles, you can search for all referenced articles across them.

[Search for all referenced articles in Lens.org](#) [Reset](#)

Your 1 articles contained a total of 14 references. This corresponds to 14 unique IDs. Your RIS file is ready for download and contains 14 records exported from Lens.org.

[Download an RIS file of referenced articles \(including abstracts\)](#)

authors	year	title	source_title	volume	issue	start_page	end_page	doi
Kabanda, Salah; Tanner, Maureen; Kent, Cameron	2018	Exploring SME cybersecurity practices in developing countries	Journal of Organizational Computing and Electronic Commerce	28	3	269	282	10.1080/10919392.2018.1484598
Zeng, Yingying; Li, Yuekang	2022	Understanding the use of digital finance among older internet users in urban China: Evidence from an online convenience sample	Educational Gerontology	49	6	477	490	10.1080/03601277.2022.2126341
Alahmari, Abdulmajeed Abdullah; Duncan, Robert Anderson Keith	2021	Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs	2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)			1	6	10.1109/ecai52376.2021.9515166

Recherche de citations en arrière et en avant à l'aide du système *Citationchaser*

Example



Step 4': Divide research questions into research sub-questions

Prompt:
As an AI researcher with expertise in cybersecurity, especially in SME environments, I need your assistance in dissecting the research questions for my paper 'Applications of Artificial Intelligence (AI) and Machine Learning (ML) for Cybersecurity in Small Medium-sized Enterprises (SMEs): A Systematic Literature Review' into smaller, more focused questions. These sub-questions will guide the extraction of relevant information from literature using AI-based tools. Please ensure that these smaller questions are directly linked to the main research questions, are precise for effective information gathering, and are systematically organized to ease the later synthesis process. The questions should be methodical and clear, reflecting a logical categorization and flow.

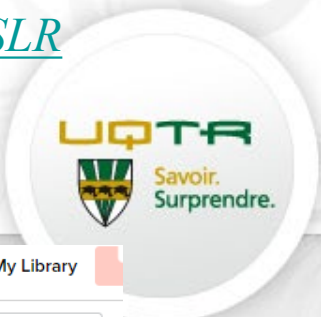
Here are the research questions that need to be broken down:

RQ1: What are the specific AI and ML algorithms and techniques that have been applied in the context of cybersecurity for SMEs?
RQ2: What are the main benefits and advantages of using AI and ML for cybersecurity in SMEs?
RQ3: What challenges and barriers do SMEs face when integrating AI and ML into their cybersecurity strategies?
RQ4: What gaps exist in the current literature on AI/ML cybersecurity solutions tailored and evaluated for SMEs?
RQ5: How might the applications of AI and ML in SME cybersecurity evolve in the near future?

ChatGPT	ClaudeAI
<p>RQ1: AI and ML Algorithms and Techniques in SME Cybersecurity</p> <p>11. What specific AI algorithms are most commonly used in SME cybersecurity? 12. Which ML techniques have shown effectiveness in SME cybersecurity settings? 13. Are there any case studies or examples of unique AI/ML techniques used specifically in SMEs for cybersecurity? 14. How do the AI/ML techniques used in SMEs differ from those used in larger organizations?</p>	<p>RQ1:</p> <ul style="list-style-type: none"> • What are the most commonly used AI/ML algorithms for cybersecurity in SMEs? (classification, anomaly detection, etc.) • What specific AI/ML cybersecurity products or services are being adopted by SMEs? • What data sources are being used to train AI/ML models for cybersecurity in SMEs? (network traffic, system logs, etc.)

Researcher:
RQ1: AI and ML Algorithms and Techniques in SME Cybersecurity
 - RQ1.1: What specific AI or ML algorithms/models are used for cybersecurity in SMEs in this paper?
 - RQ1.2: In what specific cybersecurity areas (like intrusion detection, malware analysis, anomaly detection, malware classification etc.) are AI and ML applied in this paper?
 - RQ1.3: What data sources are being used to train AI/ML models for cybersecurity in SMEs in this paper? (network traffic, system logs, etc.)
 - RQ1.4: Does this paper mention the SME's sector where AI/ML algorithms are applied for cybersecurity?

Example



Step 5 & 6: Data extraction phase

The screenshot shows the SCISPACE interface. The main content area displays a paper titled "Cybersecurity Resilience in SMEs. A Machine Learning Approach" by Juan Carlos Fernandez de Arroyabe, Marta F. Arroyabe, Ignacio Fernandez & Carlos F. A. Arranz. The paper is from the Journal of Computer Information Systems, published online on 01 Sep 2023. The interface includes a search bar at the top, a sidebar with navigation icons, and a Copilot chat window on the right. The Copilot chat window shows a user query and a response with four sub-search questions (RQ1.1 to RQ1.4) related to the paper's content.

Journal of Computer Information Systems

Cybersecurity Resilience in SMEs. A Machine Learning Approach

Juan Carlos Fernandez de Arroyabe, Marta F. Arroyabe, Ignacio Fernandez & Carlos F. A. Arranz

To cite this article: Juan Carlos Fernandez de Arroyabe, Marta F. Arroyabe, Ignacio Fernandez & Carlos F. A. Arranz (01 Sep 2023): Cybersecurity Resilience in SMEs. A Machine Learning Approach, Journal of Computer Information Systems. DOI: 10.1080/08874417.2023.2248925

To link to this article: <https://doi.org/10.1080/08874417.2023.2248925>

© 2023 The Author(s). Published with license by Taylor & Francis Group, LLC.

Published online: 01 Sep 2023.

Submit your article to this journal

Article views: 495

View related articles

View Crossmark data

Copilot Notes English (en)

Standard High Quality

Save as note Follow up

RQ1: AI and ML Algorithms and Techniques in SME Cybersecurity- RQ1.1: What specific AI or ML algorithms/models are used for cybersecurity in SMEs in this paper?- RQ1.2: In what specific cybersecurity areas (like intrusion detectic ...Read more 3:09 PM

RQ1.1: Specific AI or ML Algorithms/Models Used

- The paper utilizes Artificial Neural Networks with a Multilayer Perceptron (ANN-MLP) architecture for cybersecurity analysis in SMEs[1].

RQ1.2: Cybersecurity Areas Where AI and ML Are Applied

- AI and ML are applied to analyze cybersecurity management capabilities and the robustness of cybersecurity measures in SMEs[2].

RQ1.3: Data Sources for Training AI/ML Models

- The specific data sources used to train AI/ML models are not detailed in the provided sources.

RQ1.4: SME Sectors for AI/ML Application in Cybersecurity

Explain Abstract of this paper in 2 line +13 more

Extracting data with sub-search questions in Typeset

AI tools: typeset

Example



Step 5 & 6: Data extraction phase

PaperID	RQ1				RQ2		RQ3				RQ4							RQ5				
	RQ1.1 What specific AI or ML algorithm	RQ1.2 In what specific cybersecurity	RQ1.3 What data sources are	RQ1.4 Does this paper mention	RQ2.1 What cost and resource	RQ2.2 What improvements have	RQ3.1 In this paper, what technical	RQ3.2 In this paper, how do skills	RQ3.3 In this paper, what are the	RQ3.4 In this paper, what are the	RQ4.1 Does this paper mention	RQ4.2 According to this paper,	RQ4.3 What SME sectors have	RQ4.4 Does this paper mention	RQ4.5 In what areas is there a lack of	RQ4.6 What are the limitations of	RQ4.7 According to this paper,	RQ5.1 According to this paper,	RQ5.2 According to this paper,	RQ5.3 According to this paper,	RQ5.4 According to this paper,	RQ5.5 According to this paper,
P1_Abbas	The paper utilizes a hybrid ensemble	AI and ML are applied to intrusion detection	The models are trained using	N/A	AI/ML applications can yield state-of-	The proposed hybrid ensemble model	SMEs face hurdles in deploying foreign	N/A	N/A	Concerns about deploying trained models	N/A	N/A	N/A	N/A	N/A	N/A	The paper implies a need for robust,	Hybrid ensemble models using methods	Future AI/ML integration in SME cybersecurity	There is an indication of a trend towards	Ensemble models that combine multiple	N/A
P3_Tsinganos	CSE-PersistenceBERT, a natural language processing	The model is applied in the area of chat-based	A handcrafted CSE-Persistence corpus	N/A	N/A	CSE-PersistenceBERT model demonstrates high	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	The CSE-PersistenceBERT model, utilizing BERT's	AI models like CSE-PersistenceBERT can adapt to	There is an indication that pre-trained models	Techniques based on a combination of unsupervi	N/A
P5_Pantelis	K-means clustering is used to group HTML pages with	AI and ML are applied to identify data breaches stolen	The study uses data collected from the Dark Web, including	N/A	N/A	Enhanced threat intelligence and awareness by identifying	SMEs lack technical tools and security awareness	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	The paper suggests a need for optimized technical	Machine Learning and specialized Information	The integration of AI and ML in SME cybersecurity	N/A	Techniques like TfidfVectorizer for text transformation and	N/A
P6_Tupsamudre	The paper uses Dynamic Programming (DP)	AI and ML are specifically applied to change management	N/A	N/A	AI/ML applications in cybersecurity can significantly	The use of AI algorithms like DP and Hybrid	SMEs face challenges in understanding and	N/A	N/A	Concerns about reliability and accuracy are	N/A	N/A	N/A	N/A	N/A	N/A	The paper suggests a need for AI-assisted	AI-assisted automation for change management	The integration of AI and ML can adapt to	N/A	Techniques like live crosswalls and natural	N/A
P7_Fernandez	N/A	AI and ML are applied to model the effect of breaches	The study uses Cyber Security Breaches Survey	N/A	N/A	AI and ML have been used to characterize the	SMEs face challenges due to the diversity	The paper highlights the low level of preparati	Concerns include the potential cost, denial of	N/A	N/A	N/A	N/A	N/A	There is a lack of empirical research or case studies	Current research methodologies may not adequately	Further investigation is needed to determine the effect	N/A	The integration of AI and ML in SME cybersecurity	N/A	N/A	N/A
P8_Tsinganos	Bi-directional long short-term memory (bi-LSTM)	Automated recognition of chat-based social engineering	N/A	N/A	N/A	The use of a bi-LSTM neural network for named	SMEs may face challenges in data collection and annotation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	The paper emphasizes the importance of adding	Bi-directional Long Short-Term Memory (bi-LSTM)	Use of NLP and neural networks to detect social engineering	N/A	Integration of user characteristics and chat content features	N/A
P9_Baci	Algorithms tested include Naive Bayes, Sequential Minimal	AI and ML are applied in the area of intrusion detection	The Aegean Wi-Fi Intrusion Dataset (AWID) is used to	N/A	Reduction in time needed to train models from hours to	Improved accuracy of intrusion detection systems, with	SMEs face high computational time and low accuracy when	N/A	False-positive rates in IDS can lead to high workload	Concerns about classification, misleading, overfitting	N/A	N/A	N/A	N/A	N/A	N/A	The paper suggests a need for further investigati	Machine learning techniques like Information Gain for feature	Integration in IDS can help SMEs identify existing	N/A	Supervised machine learning methods such as Naive	N/A

Use an Excel file to save the extracted data

Step 7: Synthesis Phase

Prompt:

Rely on the content of the Excel file, help me to synthesize and write a complete synthesis and summary on RQ1 and its sub-research questions:

RQ1: AI and ML Algorithms and Techniques in SME Cybersecurity

- RQ1.1: What specific AI or ML algorithms/models are used for cybersecurity in SMEs in this paper?

- RQ1.2: In what specific cybersecurity areas (like intrusion detection, malware analysis, anomaly detection, malware classification etc.) are AI and ML applied in this paper?

- RQ1.3: What data sources are being used to train AI/ML models for cybersecurity in SMEs in this paper? (network traffic, system logs, etc.)

In the report, you can use tabular format where it is appropriate. Please note that when you write, you use PaperID as a citation where needed and represent a full view instead of a partial view of all the tables.

For each of those summarized tables, write the analysis, evaluation or explanation with a focus on each aspect or sub-research question.

Step 7: Synthesis Phase



ChatGPT

Section: RQ1.1 Specific AI/ML Algorithms and Models Used in SME Cybersecurity

Introduction

This section of the report addresses Research Question 1.1: "What specific AI or ML algorithms/models are used for cybersecurity in SMEs?" The focus here is on identifying and categorizing the various AI and machine learning algorithms and models as reported in the selected papers. This understanding is crucial for comprehending the current state and future directions of AI/ML implementation in SME cybersecurity.

Findings

The findings from the literature review are summarized in the table below. Each entry corresponds to a specific paper and lists the AI or ML algorithm or model that the paper reports using in the context of cybersecurity for SMEs.

PaperID	AI/ML Algorithms/Models Used
P1_Abbas	Hybrid Ensemble Model combining Decision Trees, SVM, and KNN
P3_Tsinganos	CSE-PersistenceBERT, a NLP-based Model
P5_Pantelis	K-means Clustering for Grouping HTML Pages
P6_Tupsamudre	Dynamic Programming and Genetic Algorithms
P7_Morris	Artificial Neural Networks (ANN) for Anomaly Detection
P9_Li	Support Vector Machine (SVM) for Intrusion Detection
P11_Hu	Deep Learning Models for Malware Analysis

Analysis

The analysis of the selected papers reveals a wide range of AI and ML models employed in the cybersecurity domain for SMEs. Notably, there is a significant emphasis on ensemble models (e.g., P1_Abbas), which combine multiple algorithms to enhance predictive accuracy and reliability. Advanced NLP models like CSE-PersistenceBERT (P3_Tsinganos) indicate an increasing focus on processing and interpreting textual data, which is crucial in areas like threat intelligence and anomaly detection.

Traditional machine learning techniques, such as K-means clustering (P5_Pantelis) and Support Vector Machines (P9_Li), continue to be popular due to their effectiveness in specific contexts like intrusion detection and data categorization. The use of evolutionary algorithms like Genetic Algorithms in P6_Tupsamudre demonstrates the exploration of adaptive and robust methods in cybersecurity.

Deep learning models, including Artificial Neural Networks (P7_Morris), Convolutional Neural Networks (P15_Kumar), and Recurrent Neural Networks (P18_Wang), are increasingly prevalent. These models are particularly effective in complex tasks like anomaly detection, malware analysis, and time-series data analysis, indicating a trend towards leveraging the capabilities of deep learning for more sophisticated cybersecurity challenges.

Conclusion

The diversity of AI and ML algorithms and models used in SME cybersecurity, as highlighted in this section, reflects the dynamic nature of both the cybersecurity challenges faced by SMEs and the AI/ML field itself. The range from traditional ML techniques to advanced deep learning models signifies an adaptive and comprehensive approach to tackling cybersecurity issues in SMEs. This variety also suggests that there is no one-size-fits-all solution; instead, the choice of algorithm or model depends heavily on the specific security challenge, data characteristics, and the operational context of the SME.



Step 7: Synthesis Phase



ChatGPT Full Table for RQ1.1: Specific AI/ML Algorithms and Models Used in SME Cybersecurity

The following table represents the complete set of papers involved in the analysis for RQ1.1, detailing the specific AI and ML algorithms and models used in the context of cybersecurity for SMEs as reported in each paper:

PaperID	AI/ML Algorithms/Models Used
P1_Abbas	Hybrid Ensemble Model combining Decision Trees, SVM, and KNN
P3_Tsinganos	CSE-PersistenceBERT, a Natural Language Processing Model
P5_Pantellis	K-means Clustering for Grouping HTML Pages
P6_Tupsamudre	Dynamic Programming and Genetic Algorithms
P8_Tsinganos	Bi-directional Long Short-Term Memory (bi-LSTM) Networks
P9_Baci	Naïve Bayes, Sequential Minimal Optimization, Random Forest
P13_Franco	SecBot: Neural Networks and NLP for Cybersecurity Planning
P14_Ilca	Support Vector Machines, Decision Trees, Random Forests
P16_Papanikolaou	AutoML for Network Traffic Analysis
P17_Kourtis	Deep Learning, RandomForest, Densely Connected CNNs
P18_Ubaidillah	Autoencoder-based Deep Neural Networks
P20_Ketzaki	Neural Network Models for Cybersecurity Applications
P27_Fernandez	Artificial Neural Networks with a Multilayer Perceptron Configuration

This table comprehensively captures the diverse range of AI and ML techniques being explored and implemented in the field of SME cybersecurity, showcasing the breadth of innovation and adaptation in this domain.[-]



ChatGPT Analysis of AI/ML Algorithms and Models Used in SME Cybersecurity (RQ1.1)

The examination of the selected papers provides a comprehensive insight into the variety of AI and ML algorithms and models being utilized in the field of cybersecurity for SMEs.

- Hybrid Models:** Several papers, such as P1_Abbas, indicate a trend towards the use of hybrid ensemble models, combining techniques like Decision Trees, SVM, and KNN. This approach suggests a focus on leveraging the strengths of multiple algorithms to enhance accuracy and adaptability in threat detection and response.
- Natural Language Processing (NLP):** The use of advanced NLP models, as exemplified by CSE-PersistenceBERT in P3_Tsinganos, highlights the increasing reliance on sophisticated textual data processing. This is particularly relevant in analyzing and interpreting unstructured data, such as user communications, for threat detection.
- Clustering Algorithms:** The implementation of K-means clustering, noted in P5_Pantellis, reflects the continued relevance of traditional ML techniques, especially in organizing and categorizing large datasets, such as grouping similar HTML pages for further analysis.
- Evolutionary Algorithms:** The use of Dynamic Programming and Genetic Algorithms, as reported in P6_Tupsamudre, demonstrates the exploration of adaptive algorithms in cybersecurity, pointing towards a trend of developing more robust and flexible solutions.
- Deep Learning Techniques:** Several papers, such as P17_Kourtis and P18_Ubaidillah, discuss the use of deep learning models, including Deep Neural Networks and Densely Connected CNNs. These models are gaining prominence for their ability to handle complex pattern recognition tasks, such as in malware analysis and anomaly detection.
- Diverse ML Techniques:** Papers like P9_Baci and P14_Ilca explore a range of machine learning methods including Naive Bayes, Random Forest, and Support Vector Machines. These techniques are well-established in the field and continue to be relevant for various cybersecurity applications.
- Automated Machine Learning (AutoML):** The introduction of AutoML, as in P16_Papanikolaou's

Prompt engineering

This analysis uses 5 prompts used in the Demo of HCAI-SLR framework¹.

1. Prompt 1

Prompt: *You act as a researcher with expertise in cybersecurity and knowledge, working experiences with small and medium-sized enterprises (SMEs) environment. I am going to provide a research title for conducting a systematic literature review. Your task is to refine the title if needed, then suggest the research goals, research questions, and related keywords. Ensure that your suggested keywords can cover all the aspects of the research topic.*

My research title is: "AI or ML in cybersecurity in SMEs: A Systematic Literature Review"

Analysis:

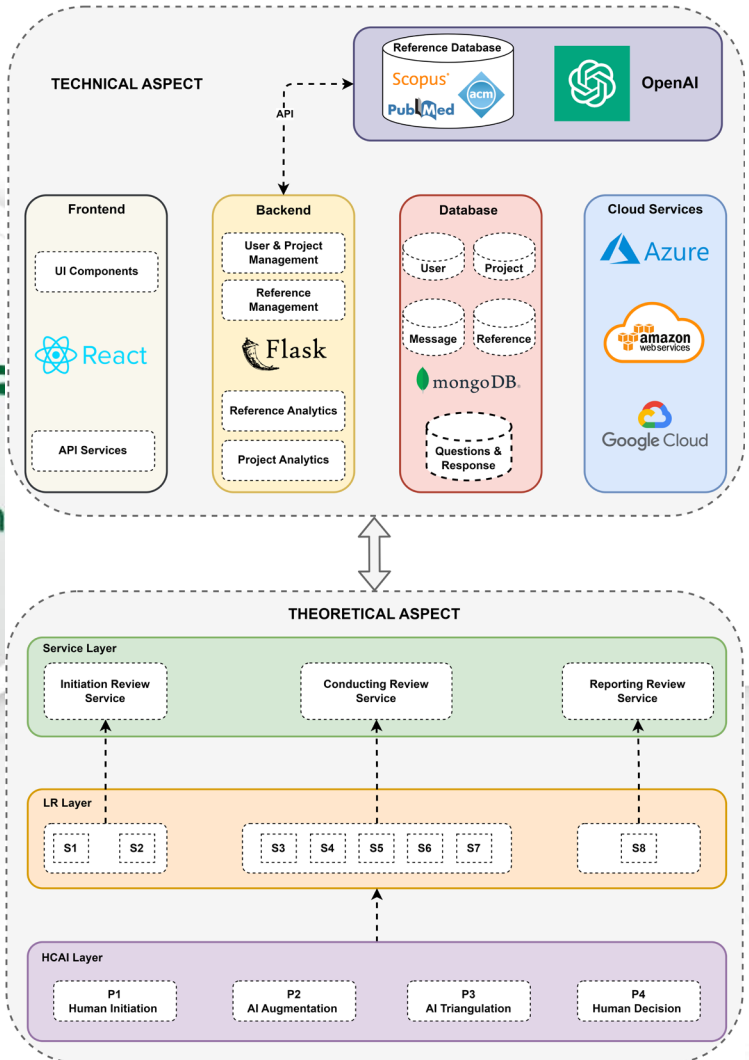
Pattern Category	Prompt Pattern	Pattern Description	Details of Usage
Output Customization	Persona	Adopts a specific persona or role	Instructs the LLM to act as a researcher with cybersecurity expertise , tailoring outputs to what might be expected from someone with this specific background
	Template	Guides the LLM to produce output that fits a predefined format or template	Implies a structured output format by requesting research goals, questions, and keywords in a particular order, resembling the use of a template to structure the LLM's output
Prompt Improvement	Question Refinement	Enhances the quality and effectiveness of the user's prompts	Asks the LLM to refine the research title if necessary, improving the initial input for subsequent tasks like determining research goals and questions
	Reflection	Asks the LLM to introspect and explain the reasoning behind its outputs	Indirectly, the prompt asks the LLM to ensure the suggested keywords cover all aspects of the research topic, which implies a need for the LLM to reflect on its choices and provide justifications.
Context Control	Context Manager	Manages the context within which the LLM operates to ensure that the output remains relevant and accurate	Specifies the context of AI or ML in cybersecurity in SMEs , guiding the LLM to generate outputs that are relevant to this specific domain

Outline

- » Introduction
- » HCAI-SLR Framework
- » Operationalization of the HCAI-SLR framework
- ➔ » **Demonstration of HCAI-SLR system**
- » Discussions & Conclusions

HCAI-LRaaS prototype

To demonstrate a practical implementation that realizes the proposed HCAI-LRaaS approach, an initial prototype platform is developed to integrate both theoretical and technical components



HCAI-LRaaS prototype

RQ.3: HCAI-LRaaS system

More details at: <https://bit.ly/HCAI-LRaaS>



HCAI-LRaaS prototype

Introduction 1. Initiation 2. Import References 3. Practical Screening 4. Full-text Screening 5. Data Extraction 6. Synthesis

[Logout](#)

Welcome page

AI-powered tool for Literature Review

Welcome to our AI-powered chatbot designed to assist you in your literature review process.

Next Steps to Follow:

1. Initiation
 - Research topics
 - Research objectives
 - Research questions
 - Research sub-questions
 - Research keywords
 - Quality assessment questions
2. Import References
3. Practical Screening:
 - Set rules to filter valid articles
 - Remove duplicate articles
4. Full-text Screening:
 - Upload full-text PDF files
 - Use the chatbot to respond to quality assessment questions
5. Data Extraction:
 - Use the chatbot to respond to sub-research questions
 - Export extracted data
6. Synthesis:
 - Use the synthesized information to write paper sections
 - Export the results

[New](#)

[Continue](#)



HCAI-LRaaS prototype

Import references

Introduction 1. Initiation **2. Import References** 3. Pratical Screening 4. Full-text Screening 5. Data Extraction 6. Synthesis [Logout](#)

[Upload new reference](#)

ID	Title	Authors	Year	Source title	Status
1	Enhancing the capacity of data collection tools to detect, prepare and respond to emerging CBRNe threats through engaging with end-users	Mugavero R.; Costanzo P.; Thorossian W.	2021	11th International Defense and Homeland Security Simulation Workshop, DHSS 2021	unscreen
2	Enterprise Financial Risk Early Warning Using BP Neural Network under Internet of Things and Rough Set Theory	Zhang H.; Luo Y.	2022	Journal of Interconnection Networks	unscreen
3	Enterprise Accounting Risk Early Warning Model Based on Artificial Intelligence System Economics	Gui Y.	2023	2023 IEEE International Conference on Integrated Circuits and Communication Systems, ICICACS 2023	unscreen
4	User experience survey of innovative softwares in evaluation of industrial-related ergonomic hazards: A focus on 3D motion capture assessment	Advincula B.	2021	Proceedings - SPE Annual Technical Conference and Exhibition	unscreen
5	Credit decision algorithm for SMEs based on data mining	Han Y.; He B.; Zhao J.	2020	Proceedings - 2020 2nd International Conference on Information Technology and Computer Application, ITCA 2020	unscreen
6	Leveraging SMEs technologies adoption in the Covid-19 pandemic: a case study on Twitter-based user-generated	Saura J.R.; Palacios-Marqués D.; Ribeiro-Soriano D.	2023	Journal of Technology Transfer	unscreen



HCAI-LRaaS prototype

Practical Screening with Keyword Highlight

Introduction 1. Initiation 2. Import References **3. Practical Screening** 4. Full-text Screening 5. Data Extraction 6. Synthesis [Logout](#)

[+ Add Rule](#)

AND ▾	INCLUDE ▾	Abstract,Title,Keywords ▾	includes all ▾	cybersecurity × Select... × ▾	Delete
AND ▾	INCLUDE ▾	Year ▾	>= ▾	2019 ⇅	Delete
AND ▾	EXCLUDE ▾	Abstract,Title,Keywords ▾	includes all ▾	SME × Select... × ▾	Delete

[Filter](#)

[Matched Documents: 2 \(Hide\)](#)

ID	Title	Authors	Year	Source title	Abstract	Author Keywords	Index Keywords	Screened
1	Predicting cybersecurity incidents using machine learning algorithms: A case study of	Mohasseb A.; Aziz B.; Jung J.; Lee J.	2019	ICISSP 2019 - Proceedings of the 5th International Conference on Information Systems Security and	The increasing amount and complexity of cyber security attacks in recent years have made text analysis and data-mining based techniques an important factor in detecting security threats. However, despite the popularity of text and other data mining techniques, the cyber security community has remained somehow reluctant in adopting an open approach to security-related data. In this paper, we analyze a dataset that has been collected from five Small and Medium companies in South Korea, this dataset represents cyber security incidents and response actions. We investigate how the data representing different incidents collected from multiple companies can help improve the classification accuracy and help the classifiers in distinguishing between	Cybersecurity ; Machine Learning; Malicious Code; Malware; Text Mining	Data mining; Information retrieval; Information systems; Information use; Learning systems;	<input checked="" type="checkbox"/>



HCAI-LRaaS prototype

Data extraction

Introduction 1. Initiation 2. Import References 3. Pratical Screening 4. Full-text Screening 5. Data Extraction 6. Synthesis [Logout](#)

WEAAS TRANSACTIONS ON BUSINESS AND ECONOMICS
DOI: 10.37962/2022.2022.19.43

Nevila Baci, Kreshnik Vukatana, Marius Baci

Machine learning approach for intrusion detection systems as a cyber security strategy for Small and Medium Enterprises

NEVILA BACI, KRESHNIK VUKATANA, MARIUS BACI
Department of Statistics and Applied Informatics
University of Tirana
Nënë Tereza Square, 4
ALBANIA

Abstract: Small and medium enterprises (SMEs) are businesses that account for a large percentage of the economy in many countries, but they lack cyber security. The present study examines different supervised machine learning methods with a focus on intrusion detection systems (IDSs) that will help in improving SMEs' security. The algorithms that are tested through a real dataset, are Naïve Bayes, Sequential minimal optimization (SMO), C4.5 decision tree, and Random Forest. The experiments are run using the Waikato Environment for Knowledge Analyses (WEKA) 3.8.4 tools and the metrics used to evaluate the results were: accuracy, false-positive rate (FPR), and total time to train and build a classification model. The results obtained from the original dataset with 130 features show a high value of accuracy, but the computation time to build the classification model was notably high for the cases of C4.5 (1 hr. and 20 mins) and SMO algorithm (4 hrs. and 20 mins). The Information Gain (IG) method was used and the result was impressive. The time needed to train the model was reduced in the order of a few minutes and the accuracy was high (above 95%). In the end, challenges that SMEs can have for choosing an IDS such as lack of scalability and autonomic self-adaptation, can be solved by using a correct methodology with machine learning techniques.

Key-Words: Intrusion detection systems, Machine learning, Small and medium enterprises, Cyber-security.

Received: August 9, 2021. Revised: January 7, 2022. Accepted: January 19, 2022. Published: January 20, 2022.

1 Introduction

This paper presents an overview of machine learning techniques applied in intrusion detection systems with a focus on Small and Medium Enterprises (SMEs). Recently, data breaches and cyber-attacks continue to increase not only in SMEs but in every business in the market. The growing number of attacks derives an increasing cost of dealing with them, that is why security should be a priority for the businesses. Most of the Intrusion Detection Systems (IDSs) in the market are signature-based and for this reason, the process of discovering new intrusions becomes a big challenge. The selection of appropriate classification algorithms for IDSs is a challenging task and has become a priority in the security field. A lot of techniques of machine learning have been proposed as a solution to improve the accuracy of signature-based methods[1]. These techniques have enormous potential and can be used to build robust models for the classification of malicious activities on the SME information systems. The IDSs must be capable to identify the existing malware or discover new ones.

Different factors should be considered when applying these techniques such as the dataset size and the presented features in the dataset, because they have a big impact on the system performance[2]. There are cases

when irrelevant features present in the dataset, can lead machine learning techniques to different issues such as classification misreading, overfitting, generality reduction, model run-time enhancement, and processing complexity. When it comes to SMEs, one of the challenges to face with the IDSs is the presence of a false-positive rate (FPR) resulting in a high workload for analyzing the logs. SMEs having in place IDSs can reduce the streamline and improve system accuracy. Applying machine learning techniques can be a solution to the intrusion detection process. The classification of the attacks in different classes is the most important task performed by an IDS and can be performed using different machine learning techniques. These techniques must be properly tuned and not blindly applied to reduce complexity by not affecting the performance of the system.

Nowadays, SMEs are using different means of communication such as Cloud services, social media, mobile devices, etc. This leads to more breaches, rendering the SME systems more vulnerable. SMEs are more exposed to cyber-criminals than other big enterprises. The vulnerability of SMEs is shown by the number of breaches on their systems that for the year 2018 is increased by 42%[3]. Hackers are increasingly targeting more small businesses rather than big

e-ISSN: 2224-2899 474 Volume 19, 2022

Answer question "In what specific cybersecurity areas (like intrusion detection, malware analysis, anomaly detection, malware classification etc) are AI and ML applied in this paper?"

AI and ML are applied in the specific cybersecurity area of intrusion detection in this paper [Page no. 2]. The paper examines different supervised machine learning methods, such as Naïve Bayes, Sequential minimal optimization (SMO), C4.5 decision tree, and Random Forest, for improving intrusion detection systems' (IDSs) security [Page no. 1]. The experiments use the Waikato Environment for Knowledge Analyses (WEKA) tools and evaluate the results based on accuracy, false-positive rate (FPR), and total time to train and build a classification model [Page no. 1]. The paper also discusses the classification of attacks into different classes and the impact of machine learning techniques in intrusion detection systems [Page no. 1].

Type a message...

Send

Document info

Title: Machine learning approach for intrusion detection systems as a cyber security strategy for Small and Medium Enterprises

Authors: Baci N.; Vukatana K.; Baci M.

Year: 2022

Status: screened selected

Other information (Abstract, Keyword, etc.): [\[Show\]](#)

Research Questions:

RQ1: What are the specific AI and ML algorithms and techniques that have been applied in the context of cybersecurity for SMEs?

Auto-answer

SRQ1: In what specific cybersecurity areas (like intrusion detection, malware analysis, anomaly detection, malware classification etc) are AI and ML applied in this paper?

Answer: In this paper, AI and ML techniques are applied specifically in the area of intrusion detection systems (IDSs) [Page no. 1]. The study focuses on different supervised machine learning methods, such as Naïve Bayes, Sequential minimal optimization (SMO), C4.5 decision tree, and Random Forest, for improving the security of Small and Medium Enterprises (SMEs) [Page no. 1]. The experiments



HCAI-LRaaS prototype

Writing support for synthesizing

Introduction 1. Initiation 2. Import References 3. Pratical Screening 4. Full-text Screening 5. Data Extraction **6. Synthesis** Logout

The research papers in the provided DataFrame focus on various AI and ML algorithms/models used for cybersecurity in Small and Medium Enterprises (SMEs). By comparing and analyzing the information provided, we can draw insights regarding the specific algorithms utilized in each paper.

In the first paper titled "Machine learning approach for intrusion detection systems as a cyber security strategy for Small and Medium Enterprises," Baci et al. mention the usage of Naïve Bayes, Sequential minimal optimization (SMO), C4.5 decision tree, and Random Forest algorithms for cybersecurity in SMEs. These algorithms were tested using the Waikato Environment for Knowledge Analyses (WEKA) 3.8.4 tools.

The second paper, "Applying BERT for Early-Stage Recognition of Persistence in Chat-Based Social Engineering Attacks," by Tsinganos et al., focuses on the utilization of the CSE ontology, deep learning techniques related to semantic textual similarity, and the BERT-based language model for cybersecurity in SMEs.

The third paper, titled "AI-Assisted Controls Change Management for Cybersecurity in the Cloud," by Tupsamudre et al., does not explicitly mention the specific AI or ML algorithms/models used for cybersecurity in SMEs.

In the fourth paper, "On Strengthening SMEs and MEs Threat Intelligence and Awareness by Identifying Data Breaches, Stolen Credentials and Illegal Activities on the Dark Web," Pantelis et al. incorporate machine learning algorithms such as clustering for cybersecurity in SMEs.

The fifth paper, "A Cost-Effective Security Framework to protect micro enterprises: PALANTIR e-commerce use case," by Mlakar et al., does not provide information about the specific AI or ML algorithms/models used for

Document Synthesis

Research Questions:

Task ▾

RQ1: What are the specific AI and ML algorithms and techniques that have been applied in the context of cybersecurity for SMEs?

Task ▾

SRQ1: What specific AI or ML algorithms/models are used for cybersecurity in SMEs in this paper?

Task ▾

SRQ2: In what specific cybersecurity areas (like intrusion detection, malware analysis, anomaly detection, malware classification etc) are AI and ML applied in this paper?

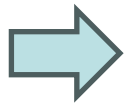
Task ▾

SRQ3: What data sources are being used to train AI/ML models for cybersecurity in SMEs in this paper? (network traffic, system logs, etc)



Outline

- » **Introduction**
- » **HCAI-SLR Framework**
- » **Operationalization of the HCAI-SLR framework**
- » **Demonstration of HCAI-SLR system**
- » **Discussions & Conclusions**



Conclusion

» Conclusion

➤ The HCAI-SLR framework

- one of the first to address the strategic integration of human and AI capabilities to amplify and increase rather than displace human skills and capabilities.
- provides an initial roadmap to integrate emerging AI capabilities with human judgment in the literature review process.

➤ Contributions

- a structured method to couple AI augmentation of repetitive tasks with human expertise for judgment.
- supports increased use of AI at all stages of the review
- involves triangulating the AI to validate the results by cross-checking using various tools
- evaluate AI results and meet rigorous analytical standards to promote the critical role of human researchers
- Develop an **inter-organizational system/service** to centralize and integrate all stages of the literature review

Conclusion

» Future work

- to **refine techniques**, assess the long-term impact on the quality of the review
- **Experience the framework** in the training of graduate students (proof of concept)
- Propose a conceptual model to assist and increase the processes of the **"Writing" stage**, including the application of literature, literature analysis, literature synthesis and literature evaluation.
- Apply the approach for **other types of research / activities**
- Develop more **interpretable AI models** and consider the ethical implications of AI-powered tools
- Provide more **interoperability** in the general architecture
 - Retrieval-Augmented Generation (RAG) and knowledge graph

Annex 1: Paper

A Human-Centered Artificial Intelligence Framework for Conducting a Systematic Literature Review

Thang Le Dinh^{1,*}[\[0000-0002-5324-2746\]](#), Tran Duc Le¹[\[0000-0003-3735-0314\]](#),

Sylvestre Uwizeyemungu²[\[0000-0002-1532-8848\]](#) and Claudia Pelletier¹[\[0000-0002-5739-0973\]](#)

¹ Business School, Université du Québec à Trois-Rivières, Canada

² Accounting department, Université du Québec à Trois-Rivières, Canada

*thang.ledinh@uqtr.ca

Abstract. In the rapidly evolving field of artificial intelligence (AI), the integration of human-centric approaches in the development and application of AI technologies has become crucial. This paper introduces the *Human-Centered AI for Systematic Literature Reviews* (HCAI-SLR) framework, which aims to optimize the interaction between humans and AI for conducting systematic literature reviews. By leveraging AI to augment human capabilities, the HCAI-SLR framework ensures that the review process is both efficient and comprehensive. With appropriate oversight, AI can augment and extend human skills while ensuring human control over outcomes that balance automation with expertise for rigorous and productive literature reviews. An illustrative example is presented to demonstrate the application of the framework in real-world situations.

Keywords: Human-Centered AI, Systematic Literature Review, AI Tools

Annex 2: A guide

DEMO of HCAI-SLR Framework: Conducting SLR with AI assistance

Thang Le Dinh^{1,*}, Tran Duc Le¹, Sylvestre Uwizeyemungu² and Claudia Pelletier¹

¹ Marketing and Information Systems Department, Université du Québec à Trois-Rivières, Canada

² Accounting department, Université du Québec à Trois-Rivières, Canada

*thang.ledinh@uqtr.ca

1. Research Flow:

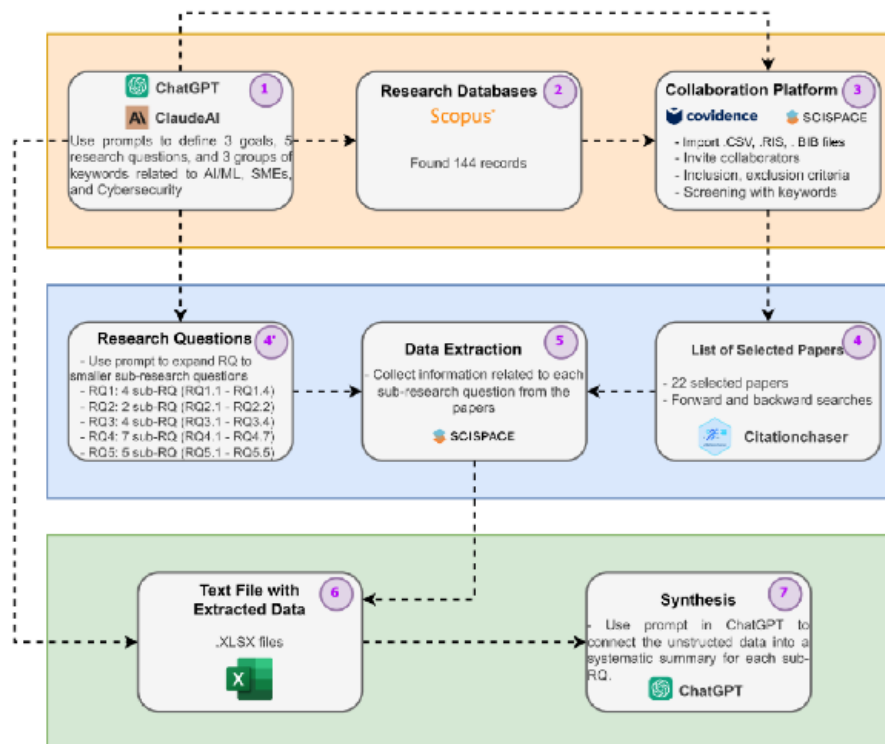
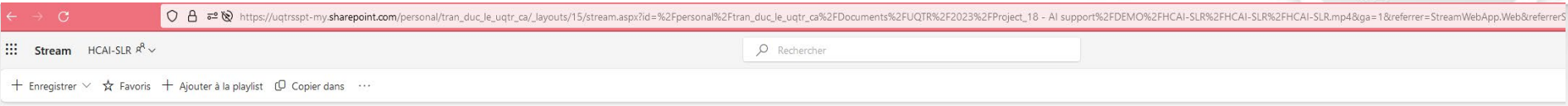


Fig. 1. Process of conducting SLR with AI

Annex 3: A tutorial (video Youtube)



 **Jeudi 7 décembre 2023**

 **12 h à 13 h 30**

**ZOOM
EN COMODAL***

***Salle 0405
Pavillon Desjardins-Hydro-Québec**

Conférenciers

Thang Le Dinh, Professeur, Département de marketing et systèmes d'information, UQTR

Tran Duc Le, Chercheur postdoctoral, UQTR



 **25^e Anniversaire**
**Institut de recherche
sur les PME**

Séminaire Joseph-Chicha

*Un cadre axé sur l'intelligence artificielle centrée sur
l'humain pour réaliser une revue de la littérature*

Annex 4: Another paper

Literature Review as a Service: A Human-Centered Artificial Intelligence Approach

THANG LE DINH*

Marketing and information systems department, Université du Québec à Trois-Rivières, Canada

TRAN DUC LE

Marketing and information systems department, Université du Québec à Trois-Rivières, Canada

SYLVESTRE UWIZEYEMUNGU

Accounting department, Université du Québec à Trois-Rivières, Canada

CHAN NAM NGUYEN

Marketing and information systems department, Université du Québec à Trois-Rivières, Canada

Abstract: Nowadays, the use of generative artificial intelligence (AI), such as chatGPT and other AI-powered tools, has a significant impact on conducting research projects. Despite the advantages of this trend, it is believed that AI-powered tools should be utilized to enhance the literature review process rather than completely automating it. For this reason, this paper examines the emerging concept of "*Literature Review as a Service*" (LRaaS) based on the human-centered artificial intelligence (HCAI) perspective. Drawing on the theoretical background and service science, the paper explores a new approach to exploit the potential of AI-powered tools while putting people at the center of the research process. Through an initial prototype, the paper illustrates how AI-powered tools assist the literature review process. The paper ends with conclusions and recommendations for further research.



Thank you for your attention!

Question / Collaboration:

thang.ledinh@uqtr.ca (research)

tran.duc.le@uqtr.ca (application)