KEAMANAN INFORMASI

APPLYING ARTIFICIAL INTELLIGENCE IN SECURE SOFTWARE DEVELOPMENT LIFECYCLE PLANNING

KELOMPOK 7

OUR TEAM

AJI SUPRIYATNO
2110512004

RADITYO AGRAPRANA S
2110512007

HARI AGUNG MERDEKA
2110512019

BIMA PUTRA EFENDI
2110512027

INTRODUCTION

With the growing reliance on software applications for critical operations, ensuring their security is becoming a pressing concern. Secure software planning plays an important role in identifying and addressing potential security risks throughout the software development lifecycle.

The advent of artificial intelligence (AI) offers promising opportunities to improve the effectiveness and efficiency of secure software planning. By leveraging AI techniques, organizations can proactively identify vulnerabilities, mitigate risks, and develop robust software applications with a better security posture. The integration of AI in secure software planning offers several advantages.

First, AI algorithms can analyze code bases, architectural designs, and software requirements, enabling early detection of potential security vulnerabilities. By identifying these vulnerabilities at an early stage of development, software planners can implement timely remedial actions, reducing the risk of exploitation at later stages. Secondly, AI can contribute to the generation of secure code writing guidelines and best practices. By analyzing large amounts of code and security-related data, AI models can identify patterns, common mistakes in code writing, and potential security holes. Developers can then receive recommendations in real-time to ensure secure code writing practices, minimizing the chances of security vulnerabilities occurring during the development process.

INTRODUCTION

Furthermore, AI can facilitate the automation of the security testing process. AI-powered tools can perform automated penetration testing, simulate various attack scenarios, and identify weaknesses in software defenses. This automation accelerates the identification of potential vulnerabilities, improves the accuracy of security assessments, and allows developers to focus on addressing critical security issues. However, the integration of AI in secure software planning also poses challenges that need to be addressed. Ethical considerations such as algorithm bias, fairness, and transparency must be addressed to ensure the responsible use of AI in software security.

In addition, the availability of high-quality training data and the need for skilled personnel who master both AI and software security are important factors for successful implementation. This paper aims to explore the application of artificial intelligence in secure software development lifecycle planning, focusing on secure software planning with AI techniques. The paper will discuss the potential benefits and challenges associated with applying AI in this context, as well as provide insights into how organizations can effectively leverage AI to improve the security of their software applications.

RELATED WORKS

In this subchapter, it discusses related research that has existed before. For example, an article with the title AI Governance in the System Development Life Cycle: Insights on Responsible Machine Learning Engineering which discusses the importance of AI (Artificial Intelligence) management and responsible implementation in the system development life cycle such as security and privacy [5].

RESEARCH METHOD

Systematic mapping or scoping studies are conducted to provide an overview of a research domain through classification. These studies mainly explore the existing literature to investigate the coverage of multiple topics, the frequency of publications, the research trends, and the publication venues where relevant studies have been published [1].

The essential process steps of the current systematic mapping study were defining the research questions, searching for relevant papers, screening the papers, keywording the abstracts, extracting the data, and mapping, as shown in Fig. 1. Each process step has an outcome and the outcome of the complete process is the systematic map, which is explained as follows [1]:

RESEARCH METHOD

- Definition of Research Questions (Research Scope) - The primary goal of a systematic mapping study is to provide an overview of a research area and identify the quantity and type of research and results available within this area.

- Conduct Search for Primary Studies (All Papers) - Primary studies were identified using search strings on scientific databases or browsing manually through relevant conference proceedings or journal publications.

- Screening of Papers for Inclusion and Exclusion (Relevant Papers) - Inclusion and exclusion criteria were used to exclude studies that were not relevant for answering the research questions.

- Keywording of Abstracts (Classification Scheme) - Keywording is a way to reduce the time needed to develop the classification scheme and ensure that the method considers the existing studies.

- Data Extraction and Mapping of Studies (Systematic Map) - Once the classification scheme was in place, the relevant articles were sorted into the scheme, i.e The actual data extraction took place.

RESEARCH QUESTION

No	Research Question	Motivation
RQ1	What types of AI techniques have been used in Software Planning?	To identify the most common AI techniques that have been used in Software Planning.
RQ2	What is the contribution of each artificial intelligence (AI) technique in secure software planning?	To understand the contribution of each artificial intelligence technique in secure software planning.

RESEARCH QUESTION

No	Research Question	Motivation
RQ3	What are the demographics of the primary studies?	To highlight the distribution of primary studies based on the type and year.

DATA SOURCES

No	Data Source	Link
1	Mendeleey	https://www.mendeley.com
2	IEEE Xplore	https://ieeexplore.ieee.org/
3	ScienceDirect	https://www.sciencedirect.com/
4	MDPI	https://www.mdpi.com/

SEARCH TERMS

Identifying the relevant search terms is essential for an adequate search of the relevant studies. Kitchenham et al. [2] suggested population, intervention, comparison, and outcome (PICO) viewpoints in this regard. These viewpoints have been extensively used by several SLRs.
Here, the relevant PICO terms are listed:

- Population: Primary studies using AI in secure software planning?
- Intervention: AI techniques?
- Comparison: AI techniques.
- Outcome: AI comparison results in secure software planning.

On the basis of the PICO structure, a generic search string was constructed to maintain the consistency of the search across multiple databases: (“Secure Software Planning” OR “*Artificial intelligence*” *OR* “*Software Development*” *OR* “*Software Planning*” *OR* ''*Secure Software*”).

INCLUSION CRITERIA

Inclusion Criteria	
IC1	Articles published in (2019-2023)
IC2	Articles specifically focused on software development life cycle
IC3	Articles related to the application of artificial intelligence in software development life cycle

EXCLUSION CRITERIA

Exclusion Criteria	
EC1	Articles that do not meet the inclusion criteria
EC2	Studies in languages other than english and indonesian
EC3	Articles without using artificial intelligence techniques

SOFTWARE DEVELOPMENT LIFE CYCLE

1. Requirement Analysis

This stage involves understanding and documenting the needs of users and stakeholders. The development team interacts with the users and gathers the necessary information to design a suitable software solution.

2. Design

The design stage involves designing the system architecture, user interface design, and software component design. At this stage, decisions about the technology, platform, and infrastructure to be used are also taken. The goal is to produce a detailed plan that can be implemented in later stages.

3. Development

The development stage is the stage where the development team begins to implement the software design. Program code is written, components are developed, and software functionality is constructed. The development team works according to the chosen development methodology, such as waterfall, agile, or DevOps methods.

SOFTWARE DEVELOPMENT LIFE CYCLE

4.Testing

The testing stage involves verifying and validating the software to ensure that it works according to expectations and meets user needs. Various types of testing, including unit testing, integration testing, functional testing, and performance testing, are performed in this stage. The goal is to identify and correct errors and deficiencies that may exist before the software is implemented.

5.Implementation (Deployment)

The implementation stage involves rolling out the software to the actual production environment. The software is installed and configured according to user requirements. If required, data can also be imported or converted into the new system. In addition, user and stakeholder training can also be carried out in this stage.

6.Maintenance

The maintenance stage involves supporting and maintaining the software after it has been launched. Maintenance includes bug fixes, updates, upgrades, and customization of the software according to needs and environmental changes. In this stage, feedback from users and stakeholders is also considered to improve the quality and performance of the software

RESULT AND DISCUSSION

A. RQ1: WHAT TYPES OF AI TECHNIQUES HAVE BEEN USED IN SOFTWARE PLANNING?

Referring to Table 4, there are seven AI techniques that have been widely used to facilitate activities in the SDLC: Machine Learning (ML), Deep Learning (DL), Data Driven (DD), Natural Language Processing (NLP), Heuristic Algorithm (HA) + Deep Learning (DL), Machine Learning (ML) + Deep Learning (DL), Deep Learning (DL) + Machine Learning (ML) + Natural Language Processing (NLP). Each AI technique has its own AI capabilities (see Fig. 1).

Current analysis shows that Machine Learning in SDLC is getting more and more attention. There is a growing interest in applying Machine Learning. Findings show that Machine Learning has attracted greater interest among researchers and practitioners than other techniques. other techniques

B. RQ2: WHAT IS THE CONTRIBUTION OF EACH AI TECHNIQUE IN SECURE SOFTWARE PLANNING?

Artificial intelligence (AI) techniques can make a significant contribution to secure software planning. Here are some of the key contributions of AI in secure software planning:

- Risk Analysis: AI can be used to perform more effective risk analysis in software development.
- Automated Testing: AI can be used to automate software testing to a great extent, including security testing.
- Attack Detection: AI can be used to detect attacks that attempt to exploit software.
- Security Analysis: AI can be used to analyze software security by identifying vulnerabilities and loopholes that may exist in the code or configuration.
- Threat Management: AI can help in security threat management by learning about attack trends, attack tactics, and techniques used by attackers.

C. RQ3: WHAT ARE THE DEMOGRAPHICS OF THE PRIMARY STUDIES?

To answer this RQ, two aspects of the primary studies were examined: the publication year and the publication type.

1) PUBLICATION YEAR

From that period (2019-2023), 15 publications were extracted from the literature. Figure 2 shows the evolution of AI technique publications in the literature. Research activities involving AI techniques used in SDLC are progressive and active. In 2019, there were 3 publications. Then, in 2020, research activities involving AI techniques increased, with 6 publications. then in 2021, research activities decreased, with 3 publications. In addition, in 2022, research activities again decreased to 2 published journal articles. And in 2023, it still amounted to 1 publication. In general, the number of AI engineering research publications changes from year to year.

2) PUBLICATION TYPES

In this mapping study, the authors covered 15 different publications. As shown in Figure 3, most of the main studies were journals (12), and papers (3).

GRAPHS

TECHNIQUES AI FOR SP

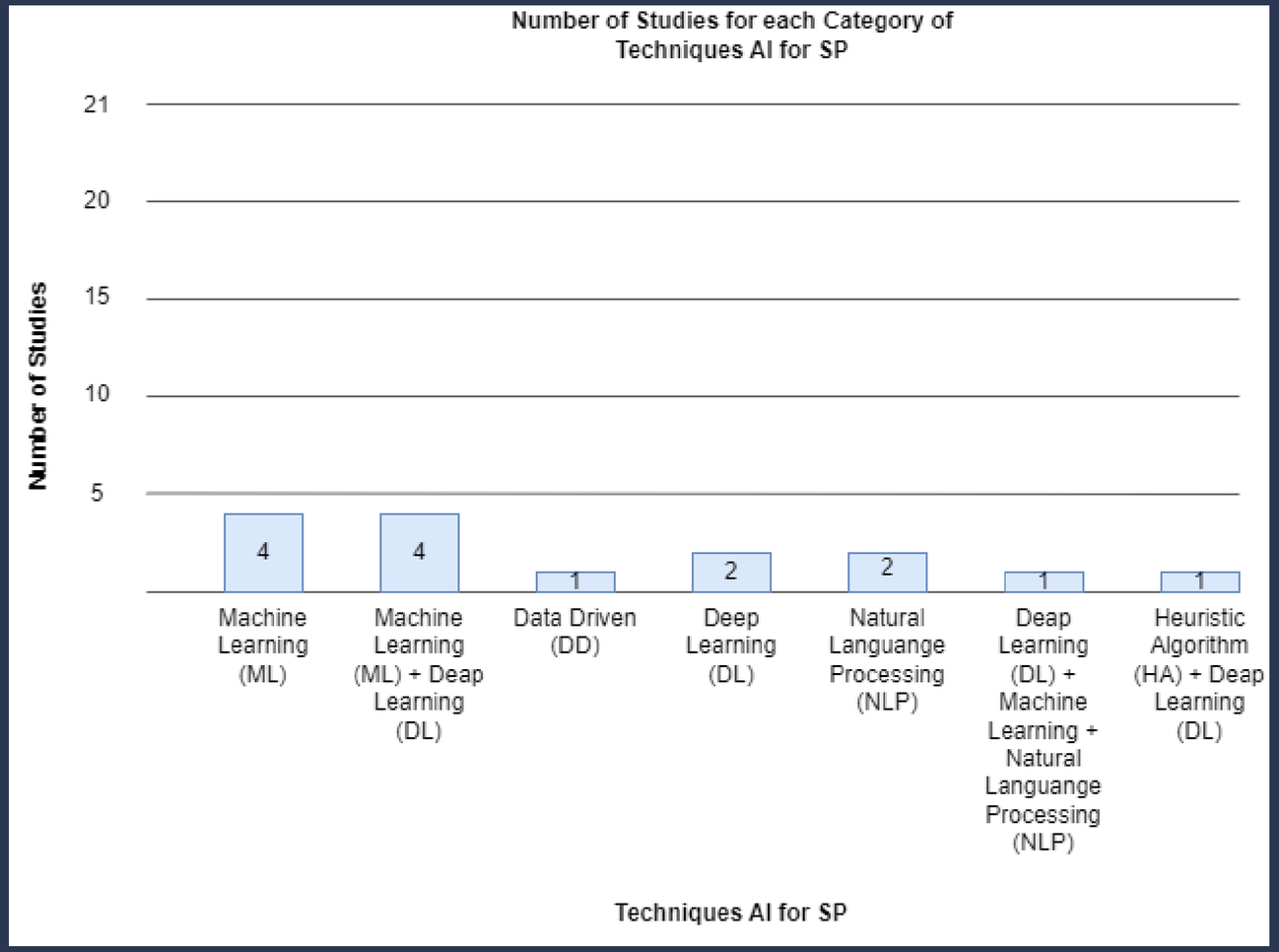

FIGURE 1. Number of studies for each category of AI techniques.

PUBLICATION YEARS

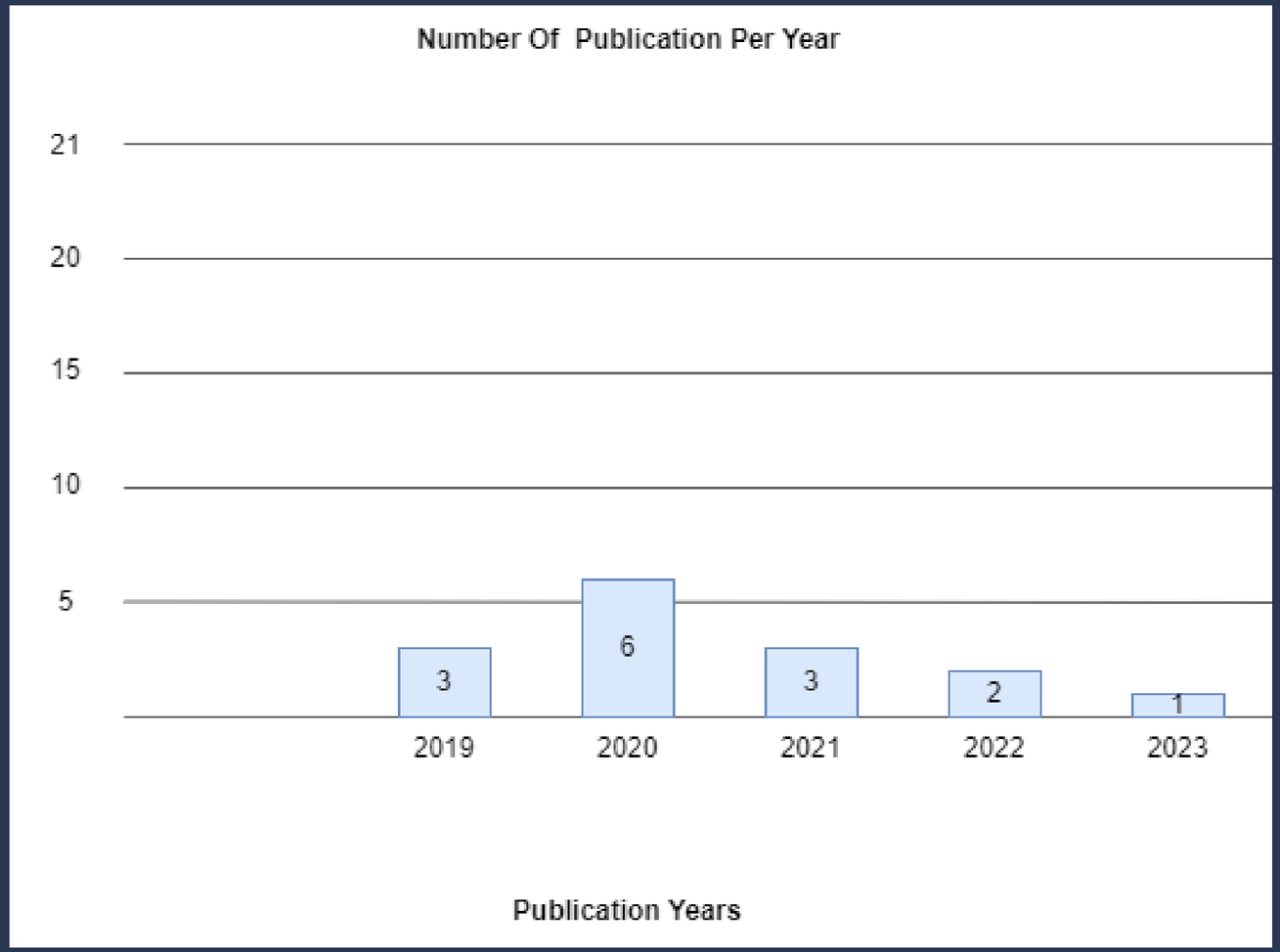

FIGURE 2. Number of publications per year.

PAPER DISTRIBUTIN IN SOFTWARE PLANNING

	Categories of AI Techniques							
	ML	DL	DD	NLP	HA + DL	ML + DL	DL + ML + NLP	Number of papers
Secure Software Planning	4	2	1	2	1	4	1	15

TABLE 4. Paper distribution in software planning.

TECHNIQUES IN THE PRIMARY STUDIES

Artificial Intelligence Techniques	Primary Studies	Number of Papers
ML	PS1, PS2, PS3, PS4	4
DL	PS5, PS6	2
DD	PS7	1
NLP	PS8, PS9	2
HA + DL	PS10	1
ML + DL	PS11, PS12, PS13, PS14	4
DL + ML + NLP	PS15	1

TABLE 5. AI Techniques in the primary studies.

THANK YOU