Journal of Theoretical and Applied Information Technology
31st January 2025. Vol.103. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SYSTEM ARCHITECTURE OF DIGITAL ASSET MANAGEMENT WITH AI TRISM

PINYAPHAT TASATANATTAKOOL[1], PANITA WANNAPIROON[2], PRACHYANUN NILSOOK[3]

[1,2,3]Division of Information and Communication Technology for Education, The Faculty of Technical Education, King Mongkut's University of Technology North Bangkok (KMUTNB), Bangkok, Thailand

E-mail: [1]s6502052956012@email.kmutnb.ac.th, [2]panita.w@fte.kmutnb.ac.th, [3]prachyanun.n@fte.kmutnb.ac.th

ABSTRACT

This scholarly investigation seeks to devise the architectural framework of a digital asset management system utilizing Artificial Intelligence-based Trust, Risk, and Security Management (AI TRiSM). The architecture is evaluated through the insight of nine specialists in the domain of information technology, employing five principal inquiries as follows: 1) Data about the characteristics and components of digital asset management 2) Devices & Connections 3) Methodology 4) Technology with AI TRiSM 5) Reports arising from architecture and supporting the university's governance principles. The findings from this evaluative process will be instrumental in advancing a digital asset management platform. The evaluation outcomes are commendable, exhibiting a mean score of 4.53 and a standard deviation (S.D.) of 0.49. In the context of this research, the investigator has meticulously synthesized the technologies employed to ensure that this system is dependable, mitigates risks, and guarantees operational safety. The findings presented in this report facilitate informed decision-making regarding digital asset management, emphasizing the fostering of robust governance within higher education institutions. This approach enhances the efficiency of managing digital resources and aligns with best practices in data security and compliance, ultimately contributing to a more sustainable and accountable educational environment.

Keywords: *Digital Asset Management, Artificial Intelligence, AI-TRiSM*

1. INTRODUCTION

Digital assets refer to the digital information and content that an organization or institution obtains via its production, operational, and management operations, which are considered valuable to that body. Conversely, digital asset management pertains to the systematic organization, preservation, and retrieval of digital assets to facilitate their adequate accessibility and utilization [1], [2]. Employing information and communication technologies supports developments meant to improve information management practices [3]. This innovative methodology helps asset managers to successfully manage and enhance asset operations. It underlines the need to combine data from reported asset-related issues to increase decision-making and operational efficiency. Stringent standards and data governance rules are established, allowing enterprises to improve their data's accuracy, consistency, and completeness [4]. It enables the organized storage, production, distribution, and management of digital assets in a regulated manner, seamlessly connected with existing enterprise systems, and includes services such as creation, rights management, data accessibility, and security. It enhances the organization and retrieval of digital information while reducing operational costs [5]. As a business grows, this system becomes essential for improving operational efficiency and enhancing performance across multiple divisions, promoting development throughout the institution. It guarantees the company can deploy assets sustainably [6], [7]. The rapid advancement of information technology has profoundly influenced digital security, compelling organizations to explore innovative strategies to mitigate more complex risks. The proliferation of digitized academic knowledge has underscored the necessity of safeguarding these digital assets, which are essential to contemporary educational pursuits. Integrating artificial intelligence (AI) is a crucial strategy for mitigating escalating security concerns. Artificial Intelligence provides an extensive array of sophisticated functionalities [8]. AI's inherent potential is demonstrated by the new opportunities it creates for

interactive communication in digital situations. However, developing critical thinking, technology literacy, and a responsible and informed attitude toward users' interactions with AI products calls for a sophisticated and fair teaching strategy [9]. As AI's capabilities permeate various domains of activity, it concurrently introduces potential hazards that raise concerns among users and those impacted by its deployment. Proficient risk management is indispensable for organizations intending to implement AI in applications characterized by high risk [10]. As a result, AI-driven models and frameworks have been developed to optimize digital asset management processes, providing more sophisticated methodologies for overseeing trust, risk, and security. AI TRiSM has been introduced within this framework to alleviate concerns about deploying AI technologies. This progressive methodology underscores the significance of transparency, accountability, and ethical considerations in the development of AI, ensuring that stakeholders can adeptly navigate the complexities entailed in adopting artificial intelligence. These principles foster trust among users and encourage a collaborative environment where innovation can thrive while maintaining ethical standards and compliance with regulatory requirements.

AI TRiSM, or AI Trust, Risk, and Security Management, is a framework that addresses the issues of trustworthiness, risk management, and security of AI systems. This concept is of great importance for integration into various sectors. AI TRiSM emphasizes building trust in predictions and decision-making [11]. AI TRiSM impacts decision-making and knowledge management in education, such as personalized learning and automation [12]. The applications of AI TRiSM include three main areas: 1) Digital Asset Management: AI TRiSM enhances organizational efficiency by AI-powered management systems, helps track digital asset usage, and ensures security [13] 2) Education Industry: AI TRiSM helps decision-making and knowledge management, improves student engagement, and reduces teacher workload through AI-powered tools [12] 3) Industries: AI TRiSM has been applied in the financial, healthcare, and metaverse industries, contributing to innovation and trust in AI systems [14]. This research paper aims to design a digital asset management architecture using AI TRiSM and evaluate it to ensure that it is reliable, risk-reducing, and secure, leading to continued organizational sustainability. The proposed framework aims to integrate advanced AI methodologies with traditional asset management practices, ensuring a comprehensive approach that addresses current challenges and future demands in digital governance.

2. OBJECTIVES OF RESEARCH

This descriptive research study reviews the relevant literature and analyzes and synthesizes the process with a focus on the architecture of the digital asset management system with AI TRiSM. The study consists of the following steps:

- Review trends, research and literature related to the systems architecture of digital asset management with AI TRiSM.
- Analyze and synthesize related research.
- Design the architecture system of digital asset management with AI TRiSM.
- Evaluate the system architecture of digital asset management with AI TRiSM.

3. RESEARCH HYPOTHESIS

The evaluation of the system architecture of digital asset management with AI TRiSM was excellent.

4. SCOPE OF THE RESEARCH

4.1 Digital Asset Management

Digital asset management relates to organizational systems and processes that study deal with the entire lifecycle of digital assets, from creation, processing, storage, and retrieval through to providing tailored solutions for each step. The benefits of digital asset management in an organization are timesaving, collaboration, and corporate image enhancement. Digital asset management is defined as the safe and scalable storage of digital assets, including storage capacity, backup and recovery, and access control mechanisms to ensure data integrity [6]. Digital asset management is divided into three parts: asset acquisition, management, and disposal [15]. To cover the entire organization clearly, it can be divided into six components: (1) Planning, (2) Procurement, (3) Usage, (4) Controlling, (5) Maintenance, and (6) Disposal [13], [16], [17]. The acquisition of assets necessitates a comprehensive understanding of the current asset landscape, its organizational structure and attributes, and a meticulous evaluation of the assets to ascertain their usage duration and maintenance requirements [18]. Implementing digital asset management systems is instrumental in diminishing the overall expenditures associated with asset operations and investments, mitigating potential failure risks, and enhancing

asset availability [16]. This strategy offers several benefits for the organization, including (1) enhanced interdepartmental collaboration through access to and real-time review of shared information, fostering teamwork and improving communication; (2) data centralization, which effectively reduces redundant information; (3) decreased risk of unauthorized asset usage; (4) the ability to make informed decisions regarding asset utilization, incremental asset development, and performance evaluation; (5) scalability and flexibility that correspond with the organization's growth; (6) the establishment of data backup, recovery, and access control measures that protect confidentiality, availability, and other security vulnerabilities, thereby ensuring long-term organizational confidence [4]. An antiquated system which does not incorporate digital asset management presents considerable challenges in terms of oversight; therefore, it is recommended that digital technologies that integrate web-based and mobile applications be implemented to streamline the operational process [19]. Comprehensive monitoring and tracking of an organization's assets—including their quantities, operational conditions, maintenance statuses, and depreciation rates—facilitates effective asset management [20]. The management framework encompasses strategic planning, the acquisition and upkeep of organizational assets, and their eventual disposal [21]. The created technique utilizes Application Programming Interfaces (API) to integrate the fundamental components of data, processes, and algorithms. The application programming interface (API) enhances dynamic data management by enabling the integration and interoperability of diverse data sources and knowledge domains, thereby supporting data-driven methodologies that are advantageous for asset management in constructed environments. Consequently, this encourages the creation of both adaptive and scalable solutions, which in turn enhances innovation in crucial asset management services [22]. An agile digital asset management system considerably improves operational efficiency by enabling quick access to data that has been saved. This, in turn, results in significant time and cost savings [6].

4.2 AI TRiSM

The primary variable is an e-portfolio format for digital universities using smart contracts on intelligence blockchain technology.

AI TRiSM (Trust, Risk, and Security Management) constitutes a comprehensive framework developed to guarantee the robustness, fairness, reliability, effectiveness, privacy, and protection of data about AI models. The primary objective of AI TRiSM is to cultivate trust in artificial intelligence systems through enhancing transparency, accountability, and equity [14]. Numerous scholarly investigations forecast that AI TRiSM will emerge as a prevalent technological paradigm in the forthcoming years, augmenting AI models efficiency and fostering user acceptance. It is posited that this framework will exert a considerable influence on the educational sector by facilitating administrators in acquiring knowledge and making informed decisions while simultaneously enhancing student engagement and academic outcomes [12]. The advantages conferred by this framework include the provision of a digital asset management platform that meticulously monitors usage, engenders trust in the outputs, mitigates risks associated with digital asset management by establishing a more secure and transparent system, and contributes to the promotion of heightened safety within the workplace [13]. As previously indicated, AI TRiSM encompasses 1) Trust Management, 2) Risk, and 3) Security, rendering it imperative to comprehend these foundational concepts.

The keywords used included (TITLE-ABS-KEY ("artificial intelligence") OR TITLE-ABS-KEY ("ai") OR TITLE-ABS-KEY ("AI TRiSM") AND TITLE-ABS-KEY ("trust") AND TITLE-ABS-KEY ("risk") AND TITLE-ABS-KEY ("security")) AND (LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2023) OR LIMIT-TO (PUBYEAR , 2024)) AND (LIMIT-TO (PUBSTAGE , "final") OR LIMIT-TO (PUBSTAGE , "aip")) AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar"))

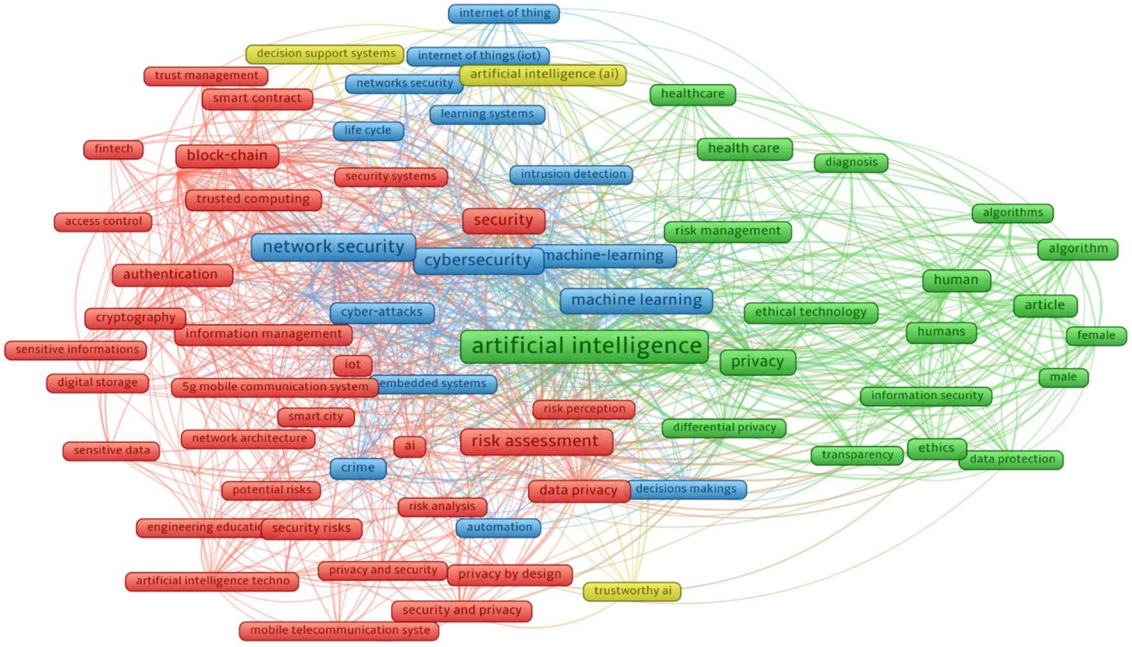

Figure 1. The bibliometrics from AI TRiSM queries in Scopus database

The studies included in review for Meta-Analysis were 210 research papers shown in Figure 2.

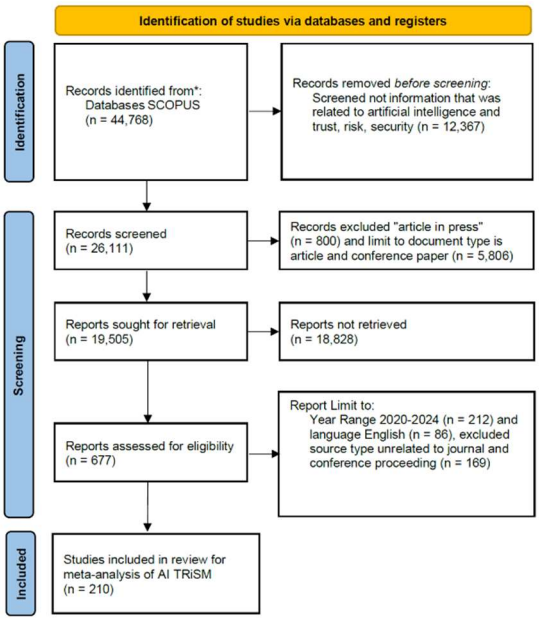

Figure 2. The Systematic reviews and Meta-Analyses (RRISMA) of AI TRiSM

After querying results with Communities of Practice keywords published in Scopus, the 44,768 research papers were analyzed using a bibliometric analysis. The results are shown in Figure 2. Therefore, 44,768 research papers from the Scopus database were used to systematically review the literature and meta-analysis. According to the research selection criteria,

Step 1 : filter out irrelevant information and screened information that was related to "artificial intelligence" and "trust", “risk”, “security” research, there were 26,111 research papers remained,

Step 2: excluded "article in press" research, there are 800 research papers and limit to document type is "article" and "conference paper" research, there are 5,806 research papers, there were 19,505 research papers remained,

Step 3: reports assessed for eligibility there are 677 research papers remained,

Step 4 : limit research document type published rang 2020 to 2024, there were 212 research papers, and English language there were 86 research papers, excluded source type unrelated to journal and conference proceeding there were 169 research paper, there were 210 research papers remained.

4.3 AI Trust Management

Trust management in artificial intelligence requires the development of comprehensive frameworks and regulations that allow users to predict and employ AI systems securely, highlighting the necessity to examine and rectify unexpected errors that may occur in AI applications [23]. A systematic methodology is implemented to ensure that performance and reliability are maintained by user expectations and standards [24]. The primary objective is to enhance metrics that assess security and privacy in artificial intelligence

technologies, especially those characterized by automated processes and interconnected hierarchical systems [25]. The implementation of this framework denotes an improvement in reliability. This approach integrates both direct and indirect trust assessments, and the results of these evaluations are synthesized to determine trustworthiness. Establishing trust mechanisms, facilitating secure interactions between persons and autonomous digital entities, and guaranteeing that systems can respond to agents that cannot be trusted all contribute to enhancing safety and security. Establishing trust governance results in creating a safe framework that protects human-machine interactions from any potential safety risks [26]. The advantages can be encapsulated as follows: Functional commitments establish benchmarks applicable across various applications and industries. The non-human-centric approach permits performance-based evaluations and adherence to functional requisites. They facilitate compliance with operational standards and commitments predicated on the capacity to fulfill designated functions. Safety and equity are critical components in cultivating trust with users. The design and dedication to trustworthiness in designated tasks can be analyzed and assessed regarding the efficacy of performance obligations to enhance duty execution [27].

Table 1: Synthesis of trust management component for artificial intelligence

Components	Trustworthy	Transparency	Accountability	Robustness	Security	Ethical	Privacy	Fairness
[28]	✓	✓	✓	✓	✓	✓		✓
[29]	✓	✓	✓		✓	✓	✓	✓
[30]	✓	✓	✓	✓	✓		✓	✓
[31]	✓	✓	✓	✓	✓	✓		✓
[32]	✓	✓	✓	✓	✓	✓		✓
[33]	✓	✓	✓	✓	✓	✓	✓	✓
[34]	✓	✓	✓	✓	✓	✓	✓	
[35]	✓	✓	✓	✓	✓		✓	✓
[36]	✓	✓	✓	✓	✓	✓	✓	✓
[37]	✓	✓	✓	✓	✓	✓	✓	✓
[38]	✓	✓	✓	✓	✓	✓	✓	✓
Conclude	✓	✓	✓	✓	✓	✓	✓	✓

Table 1 shows the synthesis of trust management elements relevant to artificial intelligence. The essential constituents include trustworthy, transparency, accountability, robustness, security, ethical, privacy, and equity.

After querying results with Communities of Practice keywords published in Scopus, the 22,100 research papers were analyzed using a bibliometric analysis. The results are shown in Figure 3. Therefore, the 22,100 research papers from the Scopus database were used to systematically review the literature and meta-analysis. According to the research selection criteria,

Step 1 : filter out irrelevant information and screened information that was related to "artificial intelligence" and "trust" research, there were 15,491 research papers remained,

Step 2: excluded "article in press" research, there are 490 research papers and limit to document type is "article" and "conference paper" research, there are 3,349 research papers, there were 11,652 research papers remained,

Step 3: reports assessed for eligibility there are 480 research papers remained,

Step 4 : limit research document type published rang 2020 to 2024, there were 361 research papers, and English language there were 42 research papers, excluded source type unrelated to journal and conference proceeding there were 35 research paper, there were 42 research papers remained.

The studies included in review for Meta-Analysis were 42 research papers.

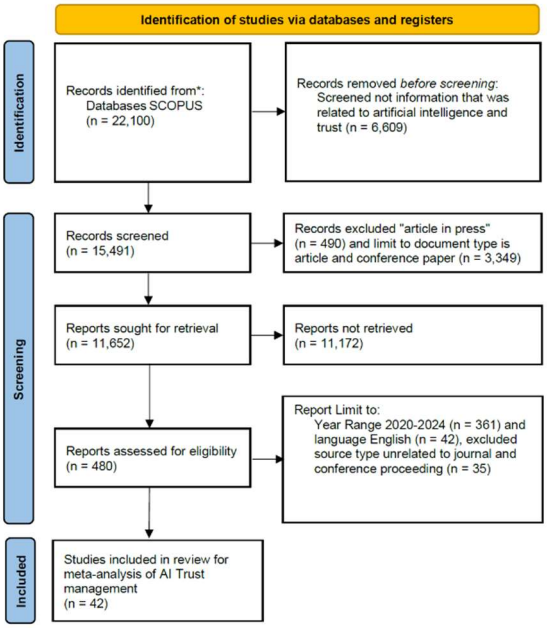

Figure 3. The Systematic reviews and Meta-Analyses (RRISMA) of AI Trust management

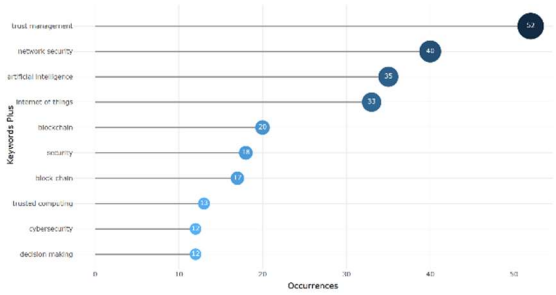

Figure 4. The bibliometrics analysis of AI Trust management

As shown in Figure 4, The keywords of AI trust management from queries in Scopus database with sort most frequent words to least searched as follows: trust management, network security, artificial intelligence, internet of thing, blockchain, security, trusted computing, cybersecurity, and decision making.

4.4 AI Risk Management

In AI risk management, machine learning can improve risk identification, assessment, and mitigation in an enterprise. Real-time analysis of large data sets allows modern technologies to identify trends and anomalies that may indicate threats. Organizations may use AI to improve risk predictions, monitoring, and threat prevention. A consistent, objective, and data-driven risk assessment improves operational efficiency and stakeholder confidence [39]. The application must display its capacity to minimize hazards to an acceptable threshold by delivering technical data, covering behavioral, cognitive, and developmental indicators, to evidence that the model performs safely and as designed [40]. It is essential to methodically monitor AI applications and implement governance frameworks during development, operation, and procurement. Organizations must evaluate and manage the risks linked to AI systems, implement appropriate risk mitigation strategies using personnel, processes, and technology, establish redundancy mechanisms, adhere to governance frameworks, and delineate risk acceptance criteria. Continuous monitoring and enhancement of stakeholder competencies are essential for sustaining confidence and adeptly navigating the intricacies related to the application [41]. Incorporating security and safety viewpoints is crucial for efficient risk reduction. This necessitates a comprehensive understanding of the interplay between security measures aimed at threat prevention and those that mitigate vulnerabilities and adversarial threats [42]. The advantages encompass enhanced identification of emerging risks, the capacity to analyze potential events, real-time monitoring and alerts, improved decision-making through actionable insights, automation of routine tasks to minimize human error, reduced costs related to risk mitigation, and increased adaptability and scalability [43].

Table 2: Synthesis of risk management component for artificial intelligence

Components	Analysis	Identification	Evaluation	Management	Response Planning	Control
[44]	✓	✓	✓	✓	✓	
[45]	✓	✓	✓	✓	✓	✓
[46]	✓	✓	✓	✓	✓	✓
[47]	✓	✓	✓	✓		✓
[48]	✓	✓	✓	✓	✓	✓
[49]	✓	✓	✓	✓	✓	✓
[50]	✓	✓	✓		✓	✓
[51]	✓	✓	✓	✓	✓	✓
[52]	✓	✓	✓	✓	✓	✓
[53]	✓	✓	✓	✓	✓	✓
[54]	✓	✓	✓	✓	✓	✓
Conclude	✓	✓	✓	✓	✓	✓

Table 2 presents the synthesis of risk management components for artificial intelligence consists of key principles that help reduce risk: risk analysis, risk identification, risk evaluation, risk management, risk response planning, and risk control.

After querying results with Communities of Practice keywords published in Scopus, the 28,223 research papers were analyzed using a bibliometric analysis. The results are shown in Figure 5. Therefore, the 28,223 research papers from the Scopus database were used to systematically review the literature and meta-analysis. According to the research selection criteria,

Step 1 : filter out irrelevant information and screened information that was related to "artificial intelligence" and "risk" research, there were 19,326 research papers remained,

Step 2: excluded "article in press" research, there are 567 research papers and limit to document type is "article" and "conference paper" research, there are 4,706 research papers, there were 14,053 research papers remained,

Step 3: reports assessed for eligibility there are 608 research papers remained,

Step 4: limit research document type published rang 2020 to 2024, there were 319 research papers, and English language there were 71 research papers, excluded source type unrelated to journal and conference proceeding there were 78 research paper, there were 140 research papers remained.

The studies included in review for Meta-Analysis were 140 research papers.

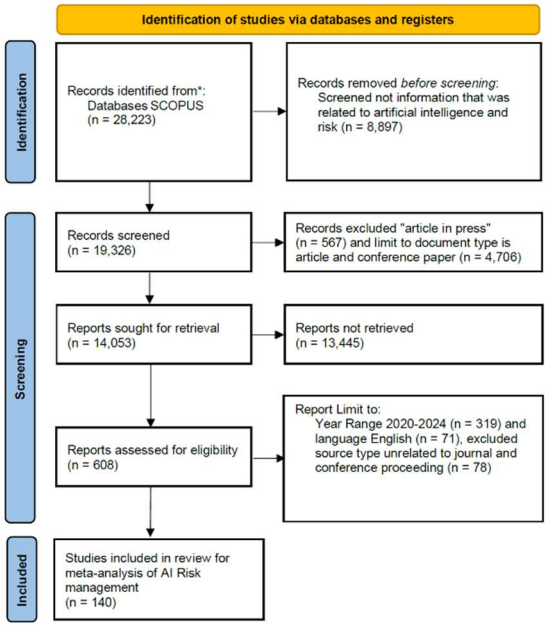

Figure 5. The Systematic reviews and Meta-Analyses (RRISMA) of AI Risk management

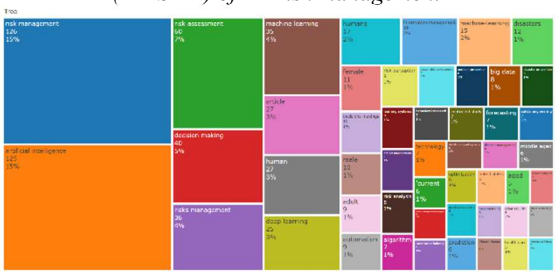

Figure 6. The bibliometrics analysis of AI Risk management

As shown in Figure 6, The keywords of AI risk management from queries in Scopus database with TreeMap most frequent top 5 rankings as follows: risk management, artificial intelligence, risk assessment, decision making, machine learning etc.

4.5 AI Security Management

AI security management constitutes a systematic framework for addressing an organization's security requirements, which encompasses the formulation and execution of policies, procedures, and strategies aimed at safeguarding informational assets against various threats while concurrently ensuring the integrity, confidentiality, and availability of data. This framework includes components such as risk assessment, the formulation of security policies, access control mechanisms, and incident response processes [55]. It performs real-time data analysis, detects threats, and autonomously responds to security issues, thereby reducing human error and lessening the burden on workers [56]. This process also entails identifying, evaluating, and mitigating risks to protect an organization's assets, encompassing personnel, data, and physical infrastructure [57]. Furthermore, it addresses contemporary security threats emanating from mobile applications and third-party vulnerabilities, thereby safeguarding organizational processes and data [58]. The advantages can be encapsulated as follows: It automates repetitive procedures and processes data at a velocity surpassing human capability, hence lowering the possibility of human mistake in threat detection and response, anticipating and mitigating possible hazards before their manifestation, and boosting the organization's resilience. Specific events trigger the automation of security measures. The capability for real-time threat mitigation enables an organization to respond promptly to emerging threats, thereby reducing the probability of data breaches. It effectively narrows existing security vulnerabilities, fortifying the organization against evolving threats [59], [60].

Table 3: Synthesis of security management component for artificial intelligence

Components	Policies	Access Control	Protection and Privacy	Trust	Assessment	Response	Monitoring
[58]	✓	✓	✓		✓	✓	✓
[61]	✓	✓	✓	✓	✓	✓	✓
[62]	✓	✓	✓	✓	✓	✓	✓
[63]	✓	✓	✓	✓	✓	✓	✓
[64]	✓	✓	✓	✓	✓	✓	✓
[65]	✓	✓	✓	✓	✓	✓	✓
[66]	✓	✓	✓	✓	✓	✓	✓
[67]	✓	✓	✓		✓	✓	✓
[68]	✓	✓	✓	✓	✓	✓	✓
[69]	✓	✓	✓	✓	✓	✓	✓
[70]	✓	✓	✓	✓	✓	✓	✓
Conclude	✓	✓	✓	✓	✓	✓	✓

Table 3 summarizes the synthesis of security management components for artificial intelligence, which includes critical components such as security policies and procedures, access control, data protection and privacy, trust management models,

risk assessment and management, incident response and management, monitoring and auditing.

After querying results with Communities of Practice keywords published in Scopus, 25,623 research papers were analyzed using a bibliometric analysis. The results are shown in Fig 7. Therefore, 25,623 research papers from the Scopus database were used to systematically review the literature and meta-analysis. According to the research selection criteria,

Step 1 : filter out irrelevant information and screened information that was related to "artificial intelligence" and "security" research, there were 17,343 research papers remained,

Step 2: excluded "article in press" research, there are 479 research papers and limit to document type is "article" and "conference paper" research, there are 3,816 research papers, there were 13,048 research papers remained,

Step 3: reports assessed for eligibility there are 602 research papers remained,

Step 4 : limit research document type published rang 2020 to 2024, there were 435 research papers, and English language there were 60 research papers, excluded source type unrelated to journal and conference proceeding there were 47 research paper, there were 60 research papers remained.

The studies included in review for Meta-Analysis were 60 research papers.

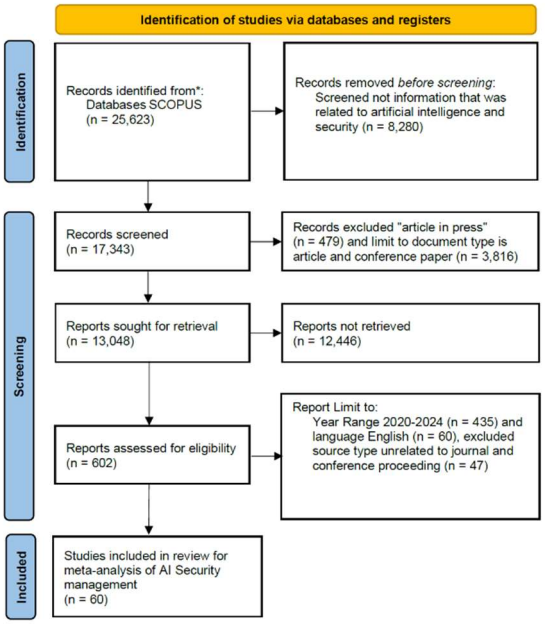

Figure 7. The Systematic reviews and Meta-Analyses (RRISMA) of AI Security management

Figure 8. The bibliometrics analysis of AI Security management

As shown in Figure 8, The keywords of AI security management from queries in Scopus database with WordCloud most frequent top 5 rankings as follows: artificial intelligence, information management, security management, network security, internet of thins etc.

The synthesis and related research are shown in Figure 1. It presents a bibliographic analysis of the system architecture of digital asset management with AI TRiSM.

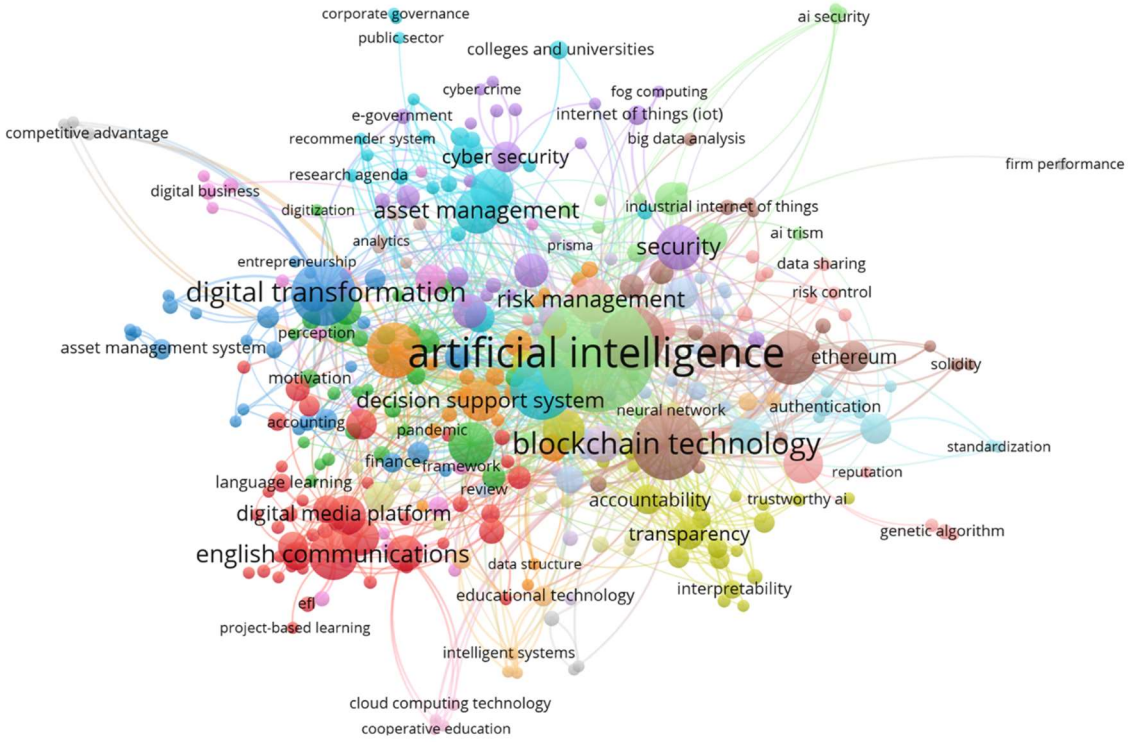

Figure 9. The bibliometrics from AI TRiSM queries in Scopus database

To write this section, you will need to do a thorough literature search on different studies that relate to the broad topic of your research. This will introduce the readers to the area of your research. It would be ideal to organize them thematically and discuss them chronologically so that readers are aware of the evolution and progress in the field. In other words, separate themes should be discussed chronologically to highlight how research in those fields has progressed over time. This will highlight what has been done and what are the future directions that need to be worked upon.

5. RESULT AND DISCUSSION

The synthesis of all related research shows the architecture of the digital asset management system with AI TRiSM, as shown in Figure 10.

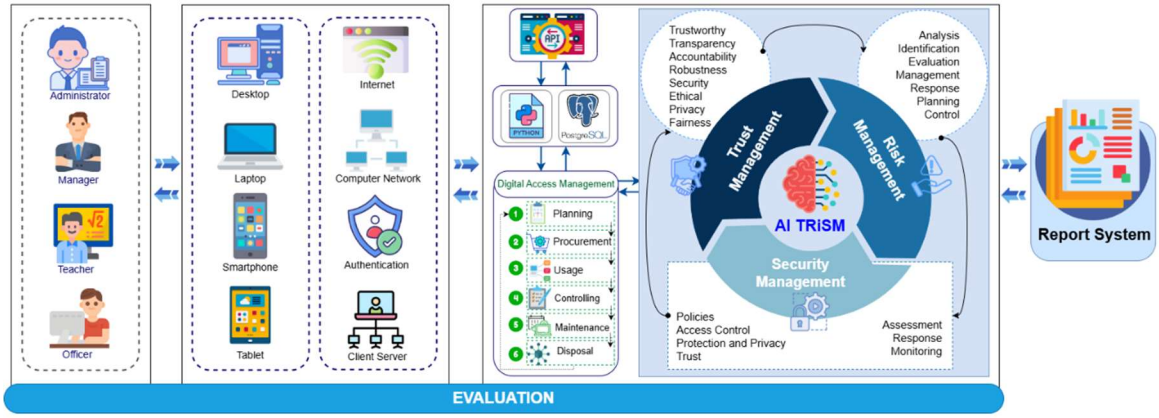

Figure 10. System Architecture of Digital Asset Management with AI TRiSM

Figure 10 shows this architecture is designed to be used in an organization that is a higher education institution. It consists of the following main modules:

1) The user base is categorized into four distinct groups: (1) University personnel or operational staff, whose function within this system entails the documentation of digital asset utilization, encompassing the importation of data about the date of utilization, duration of usage, quantity of assets, among other parameters. (2) Instructors or lecturers tasked with curricular responsibilities engage with the system when designated to acquire digital assets. They will employ this system to access reports on digital assets, thereby facilitating strategic planning for subsequent acquisitions of digital assets. (3) Executives at the university's junior, middle, and senior levels possess the capability to review reports concerning digital assets within the institution, allowing for an assessment of the utilization rates of each departmental unit. (4) System administrators are responsible for monitoring and rectifying any issues encountered within the system. This collaborative approach ensures that all stakeholders are well-informed and can make data-driven decisions to optimize the university's management and allocation of digital resources.

2) This platform is engineered to operate within a conventional network, accommodating various devices such as tablet, smartphone, laptop, and desktop. It ensures seamless connectivity and user experience by leveraging advanced protocols and technologies that optimize performance across all supported platforms.

3) Digital asset management encompasses six fundamental phases: 1) Planning: the strategic formulation for integrating digital asset management within the procurement system. 2) Procurement: the acquisition process necessitates data retrieval from the platform intended for purchasing activities. 3) Usage: the systematic data storage within the digital asset utilization framework. 4) Controlling: examining usage data to oversee digital asset management practices. 5) Maintenance: the preservation of digital assets that have attained their designated expiration date by established policies. 6) Disposal: the divestiture of digital assets upon expiration, adhering to the prescribed conditions. Each phase plays a crucial role in ensuring that digital assets are effectively managed throughout their lifecycle, maximizing value while minimizing data loss or non-compliance risks.

4) This digital asset management platform operates using an application programming interface (API) to connect the client and the server and act as a bridge between them. The platform's database is PostgreSQL, and the programming language used to develop it is Python. It offers a range of features, including advanced search capabilities, metadata management, and user access controls, ensuring that users can efficiently organize and retrieve their digital assets.

5) The technology used in this architecture to lead to the development of a digital asset management platform is called AI TRiSM, which is a framework designed from the synthesis of research consisting of: 1) Trust Management: Trustworthy, Transparency, Accountability, Robustness, Security, Ethical, Privacy, and Fairness. 2) Risk Management: Analysis, Identification, Evaluation, Management, Response, Planning, and Control. 3) Security Management: Policies, Access Control, Protection and Privacy, Trust, Assessment, Response, and Monitoring.

6) For all the above modules, the TRiSM AI digital asset management system architecture will be evaluated by nine experts in ICT or IT working in educational institutions due to their understanding of the context in which this research is conducted. Finally, the platform will produce a report to support asset management based on good governance practices in educational institutions, which is the next objective of this research. This report will outline best practices and recommendations for implementing effective digital asset management strategies that align with institutional goals and enhance overall operational efficiency.

The results of the assessment of the architecture by nine experts are presented in Table 4.

Table 4: The evaluate system architecture of digital asset management with AI TRiSM

Assessment list	Mean	S.D.	Opinions
1. Data			
1.1 Asset details include type, quantity, price, and duration of use.	4.67	0.50	Excellent
1.2 Digital asset management includes: 1) Planning 2) Procurement 3) Usage 4) Controlling 5) Maintenance 6) Disposal	4.56	0.53	Excellent
Overall evaluation results, Topic 1	**4.61**	**0.51**	**Excellent**

Assessment list	Mean	S.D.	Opinions
2. Device & Connection			
2.1 Device includes: 1) Computer Desktop 2) Computer Laptop 3) Smartphone 4) Tablet	4.67	0.50	Excellent
2.2 Connection includes: Internet, Computer Network, Authentication and Client Server.	4.78	0.44	Excellent
Overall evaluation results, Topic 2	**4.72**	**0.47**	Excellent
3. Methodology			
3.1 API connects between server and clients.	4.67	0.50	Excellent
3.2 Python Development Language and Database uses PostgreSQL.	4.67	0.50	Excellent
Overall evaluation results, Topic 3	**4.67**	**0.50**	Excellent
4. AI TRiSM			
4.1 Trust management includes: - Trustworthy - Transparency - Accountability - Robustness - Security - Ethical - Privacy - Fairness			
1) The components available for trust management to digital assets management are sufficient to operate.	4.33	0.50	Good
2) Organizations using trust management, a technology in AI TRiSM, will help make decisions about procurement about digital asset management within the organization.	4.56	0.53	Excellent
Overall evaluation results, Topic 4.1	**4.44**	**0.51**	**Good**
4.2 Risk management includes: - Analysis - Identification - Evaluation - Management - Response - Planning - Control			
1) The components available for risk management to digital assets management are sufficient to operate.	4.33	0.50	Good
2) Organizations using risk management, a technology in AI TRiSM, will help make reduce risk about digital asset management within the organization.	4.44	0.53	Good
Overall evaluation results, Topic 4.2	**4.39**	**0.51**	**Good**
4.3 Security management includes: - Policies - Access Control - Protection and Privacy - Trust - Assessment - Response - Monitoring			
1) The components available for security management to digital assets management are sufficient to operate.	4.22	0.44	Good
2) Organizations using security management, a technology in AI TRiSM, it will help prevent unauthorized access to data in managing the organization's digital assets management.	4.44	0.53	Good
Overall evaluation results, Topic 4.3	**4.33**	**0.48**	**Good**
Overall evaluation results, Topic 4.1-4.3	**4.39**	**0.50**	**Good**
5. Report			
5.1 This architecture can promote the image of the organization's management.	4.33	0.50	Good
5.2 This architecture can help manage digital assets with good governance university principles.	4.22	0.44	Good
Overall evaluation results, Topic 5	**4.28**	**0.47**	**Good**
All evaluation results	**4.53**	**0.49**	**Excellent**

As listed in table 4, the results of the assessment of the system architecture of digital asset management with AI TRiSM, which is composed of five topic, are excellent overall (mean = 4.53, standard deviation (S.D.) = 0.49). When considering each topic, it was found that for Topic 1: About information is excellent mean = 4.61, S.D. = 0.51). Topic 2: The overall use of devices and connections is excellent (mean = 4.72, S.D. = 0.47). Topic 3: The overall use of methodology is excellent (mean = 4.67, S.D. = 0.50). Topic 4: The overall use of AI TRiSM include: 4.1) The overall evaluation results are good (mean = 4.44, S.D. = 0.51) 4.2) The overall evaluation results are good (mean = 4.39, S.D. = 0.51) 4.3) The overall evaluation results are good (mean = 4.33, S.D. = 0.48) and all three topics had good overall results (mean = 4.39, S.D. = 0.50). Topic 5: The overall use of report is good (mean = 4.28, S.D. = 0.47).

6. CONCLUSION

As a result of this research, The evaluate system architecture of digital asset management with AI TRiSM. The architecture was evaluated by nine experts as excellent overall (mean = 4.53, S.D. = 0.49). This observation aligns with the findings of numerous scholars who have determined that Artificial Intelligence Trust, Risk, and Security Management (AI TRiSM) can substantially enhance knowledge acquisition and decision-making processes for executives within the educational sector. Nevertheless, stakeholders must improve their awareness and comprehension of the capabilities of AI to leverage its advantages fully [12]. Advocating for implementing the AI TRiSM framework can facilitate the creation of a digital asset management system that actively monitors internal organizational practices, thereby leading to heightened trust, diminished risk, and enhanced safety within the workplace [13], [14]. The AI TRiSM digital asset management infrastructure assessment, which has yielded commendable outcomes, is poised to evolve into a comprehensive digital asset management platform tailored for educational institutions. The researchers aspire to amalgamate the findings derived from using this platform with the principles of sound governance applicable to universities, ensuring that all investments in digital asset management remain consistent with these governance standards. This integration will streamline the management of digital assets and promote accountability and transparency, fostering an environment conducive to innovation and compliance in educational settings.

7. ACKNOWLEDGMENTS

The researchers would like to thank the Rajamangala University of Technology Suvarnabhumi (RMUTSB), and King Mongkut's Institute of Technology North Bangkok (KMUTNB), Thailand, for supported this research.

8. DECLARATIONS

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES:

[1] C. Zhang, K. Xian, Q. Wu, H. Yang, & Lang, J., and X. Wang, "Blockchain-based Power Digital Asset Security Management Framework," Procedia Computer Science, vol. 208, pp. 354–360, 2022, doi: 10.1016/j.procs.2022.10.050.

[2] B. Sicard, Y. Wu, and S. A. Gadsden, "Digital Twin Enabled Asset Management of Machine Tools," IEEE International Conference on Prognostics and Health Management, ICPHM 2024, Institute of Electrical and Electronics Engineers Inc., pp. 285–292, 2024, doi: 10.1109/ICPHM61352.2024.10626334.

[3] F. Re Cecconi, M. C. Dejaco, N. Moretti, A. Mannino, and J. D. Blanco Cadena, "Digital asset management," Research for Development, Springer, pp. 243–253, 2020, doi: 10.1007/978-3-030-33570-0_22.

[4] A. Alkhard, "Enhancing Asset Management Through Integrated Facilities Data, Digital Asset Management, and Metadata Strategies," Construction Economics and Building, vol. 24, no. 3, pp. 76–94, Jun. 2024, doi: 10.5130/AJCEB.v24i3.8741.

[5] M. Y. Zhou, "ROI Matters in the Digital Asset Management (DAM) World: How Real Estate Professionals Measure and Utilize ROI in Contribution to Company Success," Doctoral dissertation, Toronto Metropolitan University, 2022.

[6] Alqahtani, N. H., & Alqahtani, T. H., "Critical Assessment of Issues and Benefits of Digital Asset Management," Journal of Management and Strategy, vol. 13, no. 1, pp. 13–19, Apr. 2022, doi: 10.5430/jms.v13n1p13.

[7] A. Ammar, H. Nassereddine, and G. Dadi, "State departments of transportation's vision toward digital twins: Investigation of roadside asset data management current practices and future requirements," ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Copernicus GmbH, pp. 319–327, May. 2022, doi: 10.5194/isprs-Annals-V-4-2022-319-2022.

[8] M. Boujarra, A. Al Karkouri, Y. Fakhri, and S. Bourekkadi, "DIGITAL SECURITY IN MOROCCAN UNIVERSITIES IN THE ERA OF ARTIFICIAL INTELLIGENCE," J Theor Appl Inf Technol, vol. 15, no. 15, 2024, [Online]. Available: www.jatit.org

[9] O. Sytnyk, O. Hrozna, D. Filonenko, M. Konoplyannikova, and O. Serdiuk, "DEVELOPMENT OF INTERACTIVE FORMS OF COMMUNICATION THROUGH ARTIFICIAL INTELLIGENCE," J Theor Appl Inf Technol, vol. 15, no. 21, 2024, [Online]. Available: www.jatit.org

[10] D. Lau Keat Jin et al., "A FRAMEWORK FOR ARTIFICIAL INTELLIGENCE RISK MANAGEMENT," J Theor Appl Inf Technol, vol. 31, no. 16, 2024, [Online]. Available: www.jatit.org

[11] S. Ochella and M. Shafiee, "Performance metrics for artificial intelligence (AI) algorithms adopted in prognostics and health management (PHM) of mechanical systems," Journal of Physics: Conference Series, IOP Publishing Ltd, Mar. 2021.

[12] M. El Khatib, M. Al Sharif, and H. Mohamad, "Impact of AI TRiSM on Knowledge and Decision Making for Business Executives in the Education Industry," International Journal of Theory of Organization and Practice (IJTOP), vol. 3, no. 2, pp. 1–15, Jan. 2024, doi: 10.54489/ijtop.v3i2.290.

[13] P. Tasatanattakool, & Wannapiroon, P., and P. Nilsook, "Digital Asset Management Process using AI TRiSM," International Conference on Cybernetics and Innovations, ICCI 2024, Institute of Electrical and Electronics Engineers Inc., pp. 1–6, 2024, doi: 10.1109/ICCI60780.2024.10532376.

[14] A. Habbal, & Ali, M. K., and M. A. Abuzaraida, "Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions," Expert Syst Appl, vol. 240, pp. 1–14, Apr. 2024, doi: 10.1016/j.eswa.2023.122442.

[15] F. Re Cecconi, M. C. Dejaco, N. Moretti, & Mannino, A., and J. D. Blanco Cadena, "Digital asset management," Digital transformation of the design, construction and management processes of the built environment, pp. 243–253, 2020,[Online].Available:http://www.springer.com/series/13084.

[16] D. Wongarsa, S. Sinthupuan, A. Changkamanon, and S. Sitti, "Asset Management System on Somsri.io," in 2021 Joint 6th International Conference on Digital Arts, Media and Technology with 4th ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunication Engineering, ECTI DAMT and NCON 2021, Institute of Electrical and Electronics Engineers Inc., pp. 120–123, Mar.2021,doi:10.1109/ECTIDAMTNCON51128.2021.9425706.

[17] J. Mattioli, P. Perico, and P. O. Robic, "Artificial Intelligence based Asset Management," SOSE 2020 - IEEE 15th International Conference of System of Systems Engineering, Proceedings, Institute of Electrical and Electronics Engineers Inc., pp. 151–156, Jun. 2020, doi: 10.1109/SoSE50414.2020.9130505.

[18] M. Mirhosseini and F. Keynia, "Asset management and maintenance programming for power distribution systems: A review," John Wiley and Sons Inc., Aug. 01, 2021, doi: 10.1049/gtd2.12177.

[19] H. Jo, J. Ryu, and J. Shin, "Sewerage infrastructure asset management based on a consumer-centric approach," Environmental Science and Pollution Research, vol. 29, no. 35, pp. 53009–53021, Jul. 2022, doi: 10.1007/s11356-022-19347-z.

[20] K. Panjom, C. Chayanitivuth, N. Leepreecha, and V. Rujivorakul, "Asset Management System with Digital Technology: A Case Study of Government Agencies," 7th International Conference on Digital Arts, Media and Technology, DAMT 2022 and 5th ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering, NCON 2022, Institute of Electrical and Electronics Engineers Inc., pp. 472–476, 2022,doi:10.1109/ECTIDAMTNCON53731.2022.9720329.

[21] A. T. Joseph Kurien, S. A. Mathew, and S. C. Mana, "Development of PHP and MySQL based Digital Asset Management System for Secure Organizations," 2022 6th International Conference on Trends in Electronics and Informatics, ICOEI 2022 - Proceedings, Institute of Electrical and Electronics Engineers Inc., pp. 1859–1863, 2022, doi: 10.1109/ICOEI53556.2022.9776698.

[22] J. Wang, "The Development and Application of Enterprise Asset Lifecycle Management System Based on Big Data Technology," Proceedings of the 2nd International Conference on Big Data Economy and Digital Management, BDEDM 2023, European Alliance for Innovation n.o., Jun. 2023, doi: 10.4108/eai.6-1-2023.2330342.

[23] N. Moretti, X. Xie, J. Merino Garcia, J. Chang, and A. Kumar Parlikad, "Digital Twin based built environment asset management services development," IOP Conference Series: Earth and Environmental Science, Institute of Physics, 2022, doi: 10.1088/1755-1315/1101/9/092023.

[24] T. W. Um, J. Kim, S. Lim, and G. M. Lee, "Trust Management for Artificial Intelligence: A Standardization Perspective," Applied Sciences (Switzerland), vol. 12, no. 12, Jun. 2022, doi: 10.3390/app12126022.

[25] H. Bangui, B. Buhnova, and M. Ge, "Social Internet of Things: Ethical AI Principles in Trust

Management," Procedia Computer Science, Elsevier B.V., pp. 553–560, 2023 doi: 10.1016/j.procs.2023.03.070.

[26] M. Mylrea and N. Robinson, "Artificial Intelligence (AI) Trust Framework and Maturity Model: Applying an Entropy Lens to Improve Security, Privacy, and Ethical AI," Entropy, vol. 25, no. 10, Oct. 2023, doi: 10.3390/e25101429.

[27] B. Buhnova, "Trust Management in the Internet of Everything," European Conference on Software Architecture, pp. 123–137, Dec. 2022, [Online].Available:http://arxiv.org/abs/2212.14688

[28] M. Simion and C. Kelp, "Trustworthy artificial intelligence," Asian Journal of Philosophy, vol. 2, no. 1, Jun. 2023, doi: 10.1007/s44204-023-00063-5.

[29] Jyothi, V., T. Sreelatha, T. M. Thiyagu, & Sowndharya, R., and N. Arvinth, "A Data Management System for Smart Cities Leveraging Artificial Intelligence Modeling Techniques to Enhance Privacy and Security," Journal of Internet Services and Information Security, vol. 14, no. 1, pp. 37–51, Feb. 2024, doi: 10.58346/JISIS.2024.I1.003.

[30] P. Robles and D. J. Mallinson, "Artificial intelligence technology, public trust, and effective governance," Review of Policy Research, 2023, doi: 10.1111/ropr.12555.

[31] B. Li et al., "Trustworthy AI: From Principles to Practices," Association for Computing Machinery,Sep. 30, 2023, doi: 10.1145/3555803.

[32] M. Langer, C. J. König, C. Back, and V. Hemsing, "Trust in Artificial Intelligence: Comparing Trust Processes Between Human and Automated Trustees in Light of Unfair Bias," J Bus Psychol, vol. 38, no. 3, pp. 493–508, Jun. 2023, doi: 10.1007/s10869-022-09829-9.

[33] S. C. H. Hoi, "Responsible AI for Trusted AI-powered Enterprise Platforms," WSDM 2023 - Proceedings of the 16th ACM International Conference on Web Search and Data Mining, Association for Computing Machinery, Inc, pp. 1277–1278, Feb. 2023, doi: 10.1145/3539597.3575784.

[34] A. van Wynsberghe, "Sustainable AI: AI for sustainability and the sustainability of AI," AI and Ethics, vol. 1, no. 3, pp. 213–218, Aug. 2021, doi: 10.1007/s43681-021-00043-6.

[35] R. De Brito Duarte, "Towards Responsible AI: Developing Explanations to Increase Human-AI Collaboration," Frontiers in Artificial Intelligence and Applications, IOS Press BV, pp. 470–482, Jun. 2023, doi: 10.3233/FAIA230126.

[36] Prof. V. Patil, "Tourist Guide AI," International Scientific Journal of Engineering and Management, vol. 02, no. 12, pp. 1–7, Dec. 2023, doi: 10.55041/ISJEM01330.

[37] C. Sanderson, Q. Lu, D. Douglas, X. Xu, L. Zhu, and J. Whittle, "Towards Implementing Responsible AI," Proceedings - 2022 IEEE International Conference on Big Data, Big Data 2022, Institute of Electrical and Electronics Engineers Inc., pp. 5076–5081, 2022, doi: 10.1109/BigData55660.2022.10021121.

[38] Conitzer, V., & Oesterheld, C., "Foundations of Cooperative AI," Proceedings of the AAAI Conference on Artificial Intelligence, pp. 15359–15367, 2023, [Online]. Available: www.aaai.org

[39] J. Manyika, "Getting AI Right: Introductory Notes on AI & Society," Daedalus, vol. 151, no. 2, pp. 5–27, May 2022, doi: 10.1162/DAED_e_01897.

[40] B. E. Abikoye, W. Adelusi, S. C. Umeorah, A. O. Adelaja, and C. Agorbia-Atta, "Integrating Risk Management in Fintech and Traditional Financial Institutions through AI and Machine Learning," Journal of Economics, Management and Trade, vol. 30, no. 8, pp. 90–102, Aug. 2024, doi: 10.9734/jemt/2024/v30i81236.

[41] A. R. Wasil, J. Clymer, D. Krueger, E. Dardaman, & Campos, S., and E. R. Murphy, "Affirmative safety: An approach to risk management for high-risk AI," arXiv preprint arXiv:2406.15371., Apr. 2024, [Online]. Available: http://arxiv.org/abs/2406.15371

[42] B. Sateli, & Del Castillo, F., and R. Moshtagi, "Towards determining the criticality of AI applications: A model risk management perspective.," The 36th Cannadian Conference on Artificial Intelligence, Canadian AI, pp. 1–12, Jun. 2023.

[43] X. Qi et al., "AI Risk Management Should Incorporate Both Safety and Security," arXiv preprint arXiv:2405.19524., May 2024, [Online]. Available: http://arxiv.org/abs/2405.19524

[44] J. Schuett, "Risk Management in the Artificial Intelligence Act," European Journal of Risk Regulation, vol. 1, pp. 1–19, 2023, , doi: 10.1111/rego.12094.

[45] N. Cheptanari, S. Adauji, and M. Brumarel, "Risk management -component part of the quality assurance system of pharmaceutical

care," Moldovan Journal of Health Sciences, no. 4, pp. 52–60, Dec. 2022, doi: 10.52645/mjhs. 2022.4.09.

[46] P. Biolcheva, "The place of artificial intelligence in the risk management process," SHS Web of Conferences, vol. 120, p. 02013, 2021, doi: 10.1051/shsconf/202112002013.

[47] Ivanov, R., & Atanasov, D., "Risk management in agriculture," Agricultural Sciences/Agrarni Nauki, vol. 15. no. 37, 2023 doi: 10.22620/ agrisci.2023.37.005.

[48] G.-I. Țîrcovnicu and C.-D. Hațegan, "Integration of artificial intelligence in the risk management process: an analysis of opportunities and challenges," Journal of Financial Studies, vol. 15, no. 8, pp. 198–214, 2023.

[49] B. Leslie Appiah, "Risk Management Processes and Analysis in Projects Construction Industry," Journal of Civil, Construction and Environmental Engineering, vol. 5, no. 4, p. 92, 2020, doi: 10.11648/j.jccee.20200504.14.

[50] A. Shrestha and M. J. Thaheem, "Risk Management as a Tool for Sustainability," Apr. 01, 2022, doi: 10.3390/su14074331.

[51] Suraj Gupta, Shivanjali Mohite, S. Nisarga, and Muskan Shaikh, "A Study on Risk Management Strategies," REST Journal on Banking, Accounting and Business, vol. 2, no. 2, pp. 118–126, Jun. 2023, doi: 10.46632/jbab/2/2/18.

[52] A. samimi, "Risk Management in Information Technology," Progress in Chemical and Biochemical Research, vol. 3, no. 2, pp. 130–134, May 2020, doi: 10.33945/sami/pcbr.2020.2.6.

[53] G. Illangakoon, "Risk Management and Performance of Microfinance Industry," South Asian Journal of Social Studies and Economics, vol. 21, no. 3, pp. 1–17, Jan. 2024, doi: 10.9734/sajsse/2024/v21i3779.

[54] I. Makarova, G. Yakupova, P. Buyvol, A. Abashev, and E. Mukhametdinov, "Risk Management Methodology for Transport Infrastructure Security," Infrastructures (Basel), vol. 7, no. 6, Jun. 2022, doi: 10.3390/ infrastructures7060081.

[55] K. Jaszczyk, "Risk management in public-private partnership through management control," Annual Center Review, no. 12–13, pp. 40–44, 2020, doi: 10.15290/acr.2019-2020.12-13.07.

[56] Nguyen, K. D., & Duong, X. T., "Application of artificial intelligence to build a security control software system in local military units," Hong Bang International University Jour of Science, vol. 4, pp. 117–124, Jun. 2023, doi: 10.59294/ hiujs.vol.4.2023.394.

[57] H. Sun and S. Bai, "Enterprise Information Security Management Using Internet of Things Combined with Artificial Intelligence Technology," Comput Intell Neurosci, vol. 2022, no. 1, 2022, doi: 10.1155/2022/7138515.

[58] A. Andreou, "e-Securing the EU Borders: AI in European Integrated Border Management," Journal of Politics and Ethics in New Technologies and AI, vol. 2, no. 1, Apr. 2023, doi: 10.12681/jpentai.34287.

[59] S. Anđelić, N. Dedić, and V. Dedić, "Machine Learning-Based Information Systems Security Management," in Sinteza 2024-International Scientific Conference on Information Technology, Computer Science, and Data Science, Singidunum University, pp. 156–161, Jul. 2024, doi: 10.15308/sinteza-2024-156-161.

[60] P. R. J. Trim and Y. I. Lee, "Combining Sociocultural Intelligence with Artificial Intelligence to Increase Organizational Cyber Security Provision through Enhanced Resilience," Big Data and Cognitive Computing, vol. 6, no. 4, Dec. 2022, doi: 10.3390/bdcc6040 110.

[61] K. Lisovskyi and G.-D. Rochenovich, "Artificial Intelligence in the security system of enterprise," Grail of Science, no. 27, pp. 308–316, May 2023, doi: 10.36074/grail-of-science.12.05.2023.049.

[62] P. Wang, "Research on Key Technology of Network Security Management Based on Artificial Intelligence," 2023 IEEE 3rd International Conference on Data Science and Computer Application, ICDSCA 2023, Institute of Electrical and Electronics Engineers Inc., pp. 208–212, 2023, doi: 10.1109/ICDSCA59871. 2023.10393663.

[63] S. A. Alawadhi, A. Zowayed, H. Abdulla, M. A. Khder, and B. J. A. Ali, "Impact of Artificial Intelligence on Information Security in Business," 2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2022, Institute of Electrical and Electronics Engineers Inc., pp. 437–442, 2022, doi: 10.1109/ICETSIS55481.20 22.9888871.

[64] S. Dambe, S. Gochhait, and S. Ray, "The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit," 2023 3rd International Conference on Advancement in Electronics and Communication Engineering,

AECE 2023, Institute of Electrical and Electronics Engineers Inc., pp. 88–93, 2023, doi: 10.1109/AECE59614.2023.10428353.

[65] K. Andrzejewski, "Security information management systems," Management Sciences, vol. 24, no. 4, pp. 1–9, 2020, doi: 10.15611/ms.2019.4.01.

[66] D. Yadlapati, N. Siddhartha, M. Seelamneni, A. Y. Nali, H. R. Sangaraju, and P. S. V. S. Sridhar, "Security Management Approaches Over the Cloud," 2nd International Conference on Sustainable Computing and Data Communication Systems, ICSCDS 2023 - Proceedings, Institute of Electrical and Electronics Engineers Inc., pp. 1277–1282, 2023, doi: 10.1109/ICSCDS56580.2023.10105026.

[67] J. Marquez-Tejon, M. Jimenez-Partearroyo, and D. Benito-Osorio, "Integrated security management model: a proposal applied to organisational resilience," Security Journal, vol. 37, no. 2, pp. 375–398, Jun. 2024, doi: 10.1057/s41284-023-00381-6.

[68] A. Raffaj and K. Kampová, "Increasing Competencies of Security and Safety managers in the Risk Assessment Process," Proceedings of CBU in Social Sciences, vol. 1, pp. 201–205, Nov. 2020, doi: 10.12955/pss.v1.72.

[69] R. Yu, "Security Framework of Artificial Intelligence System," Journal of Physics: Conference Series, IOP Publishing Ltd, May 2021, doi: 10.1088/1742-6596/1927/1/012011.

[70] W. Villegas-Ch and J. García-Ortiz, "Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence," Electronics (Switzerland), vol. 12, no. 18, Sep. 2023, doi: 10.3390/electronics12183786.

[71] H. Jing, W. Wei, C. Zhou, and X. He, "An Artificial Intelligence Security Framework," in Journal of Physics: Conference Series, IOP Publishing Ltd, Jun. 2021, doi: 10.1088/1742-6596/1948/1/012004.