ABNUS JOURNAL
Your Research Partner

Financial Analytics and Economic Innovation Journal (FAEIJ)
E-ISSN: 3164-337X | Vol. 1, No. 4 (2026) | pp. 227-242

AI Literacy and Critical Thinking in Strengthening Students' Fraud Detection Capability in a Cashless Society

Dita Nur Affandi Saputri[1*], Tsabita Inas Fathina Rahma[2]

Universitas Muhammadiyah Surakarta, Surakarta, Indonesia[1,2]

***Corresponding author:** f100240338@student.ums.ac.id |

Received: 28 August 2026 | Revised: 9 September 2026 | Revised: 26 September 2026 | Published: 29 October 2026

Abstract

Purpose: This study analyzes the effect of Artificial Intelligence (AI) literacy on critical thinking and fraud detection capability, and the effect of critical thinking on fraud detection capability, among university students in Indonesia's cashless society.

Research Methodology: A quantitative cross sectional survey was conducted with 120 active students on the island of Java who had used digital transaction services. Participants were selected through purposive sampling. Data were collected using an online questionnaire with a five point Likert scale and analyzed with simple linear regression in Jamovi.

Results: AI literacy had a positive and significant effect on critical thinking (β=0.688, p<0.001, R^2=0.473) and on fraud detection capability (β=0.689, p<0.001, R^2=0.474). Critical thinking also had a positive and significant effect on fraud detection capability (β=0.691, p<0.001, R^2=0.478). All three hypotheses were supported.

Conclusions: The ability to understand and use AI, accompanied by critical thinking, helps students recognize and detect fraud in digital transactions.

Limitations: The sample was limited to 120 students in Java, the design was cross sectional, and the hypotheses were tested with separate simple regressions based on self reported data.

Contributions: The study links AI literacy, critical thinking, and fraud detection capability in one framework and supports integrating both competencies into higher education to prepare students for digital financial fraud risks.

Keywords: *AI Literacy, Cashless Society, Critical Thinking, Digital Financial Fraud, Fraud Detection Capability*

How to Cite: Saputri, D. N. A., & Rahma, T. I. F. (2026). AI Literacy and Critical Thinking in Strengthening Students' Fraud Detection Capability in a Cashless Society. *Financial Analytics and Economic Innovation Journal (FAEIJ)*, 1(4), 227-242.

1. Introduction

The shift toward a cashless society has changed the way people, including university students, conduct transactions. The use of digital wallets, the Quick Response Code Indonesian Standard (QRIS), mobile banking, and various online transaction services continues to increase because these methods are considered more practical and efficient than cash payments (Bank, 2025). Digital finance can expand financial inclusion and support economic stability when users trust and understand digital channels (Ozili, 2018), and the fintech revolution has transformed the design and delivery of financial services (Gomber, Kauffman, Parker, & Weber, 2018). Behind this convenience, however, the risk of cybercrime is also increasing. The National Criminal Information Center of the Indonesian National

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co | DOI:10.52909/faeij.v1i4.466

Police recorded 10,583 online fraud cases from January to March 2026, or about 3.000 to 3,700 cases each month, involving schemes such as phishing, fraudulent investments, and social engineering (Pusiknas, 2026). This shows that the growth of digital transactions is followed by rising fraud risk (Prasetya, Mohamed, & Shuhidan, 2023). Erbuğa and Ünal (2026) similarly explain that the rapid expansion of digital payment methods increases the risk of financial fraud, especially among individuals with low digital financial literacy. Increasing users' awareness and knowledge of digital finance is therefore an important component in reducing fraud risk in a cashless society.

As the need to detect and avoid digital payment fraud grows, the use of Artificial Intelligence (AI) has become an increasingly prominent approach. AI can increase productivity and effectiveness through its capacity to process large amounts of data and support decision making (Jarrahi, 2018). In the context of fraud detection, AI is applied to identify suspicious transactions and potentially fraudulent activities (Hilal, Gadsden, & Yawney, 2022). However, the development of AI also carries risks, because it allows perpetrators to use AI to develop new fraud methods such as AI powered scams and deepfakes (Gambín, Yazidi, Vasilakos, Haugerud, & Djenouri, 2024). AI therefore has two sides. It can support fraud detection, but it can also strengthen the methods of digital crime. The use of AI thus depends not only on technology but also on users' ability to understand and evaluate the information that AI provides.

In education, AI is increasingly used by students to support academic activities. Despite this growing use, there remains a gap in students' ability to understand, evaluate, and use AI responsibly. Gökçe, Topal, Geçer, and Eren (2025) showed that students' AI literacy varies and is influenced by learning experience, the intensity of AI use, and the field of study. Previous research in higher education also explains that AI literacy is needed so that students are not only able to use AI but also understand how AI works, recognize its limitations and potential biases, and use it responsibly (Pinski & Benlian, 2024). The high level of AI use among students is therefore not necessarily accompanied by the ability to understand, evaluate, and use AI generated information critically.

The increasing use of AI in academic activities requires students not only to use AI as a source of information but also to evaluate its output critically. Bećirović, Polz, and Tinkel (2025) showed that the quality of results obtained from AI depends strongly on users' ability to understand, assess, and evaluate AI output critically, which in turn affects academic performance. Effective use of AI therefore depends not only on access to technology but also on users' ability to evaluate the accuracy, relevance, and credibility of information before using it as a basis for decisions. Research also warns that excessive reliance on AI tools may reduce independent reasoning through cognitive offloading (Gerlich, 2025; Zhai, Wibowo, & Li, 2024). Strengthening the ability to evaluate AI generated information is therefore important so that students can use AI responsibly, including in recognizing various forms of fraud in a cashless society.

Along with the need for AI literacy, critical thinking has become an important competence in the use of AI. According to Biagini, Cuomo, and Ranieri (2024), AI literacy includes not only the ability to use AI but also an understanding of how AI works, its limitations, and the risks that can arise from its use. With this understanding, students are expected not to accept AI output directly but to think critically when analyzing the information produced. Although AI can help develop critical thinking, users need to be aware of the limitations of AI in providing accurate information (Darwin, Rusdin, Mukminatien, Suryati, Laksmi, & Marzuki, 2024). Critical thinking is very important in helping students recognize signs of fraud, analyze information produced by AI, and identify various forms of digital fraud more accurately. Research on misinformation shows that people who engage in more analytical reasoning are better able to distinguish false from true information (Pennycook & Rand, 2019).

Previous studies have focused mainly on the development of AI technology for fraud detection, while educational research has examined AI literacy or critical thinking separately. Studies that examine the relationships among AI literacy, critical thinking, and fraud detection capability among students, particularly in a cashless society, remain limited. Meanwhile, the effectiveness of AI in supporting

fraud detection is determined not only by technological sophistication but also by users' ability to understand, evaluate, and use AI generated information critically. Human factors such as awareness and the ability to evaluate suspicious messages also determine susceptibility to online fraud (Whitty, 2019). This study therefore analyzes the effect of AI literacy on critical thinking and fraud detection capability, and the effect of critical thinking on fraud detection capability, among students in a cashless society. The study is expected to show the importance of AI literacy and critical thinking in supporting students' ability to recognize and respond to fraud risks in digital financial transactions.

2. Literature Review and Hypothesis/es Development

2.1 Cashless Society

A cashless society is a condition in which people use noncash payment methods more than cash in their transactions. The development of digital technology has encouraged a shift in transaction patterns toward various digital payment methods that are more practical, fast, and efficient. Bank Indonesia positions the payment system as the foundation for the development of an efficient, inclusive, and integrated national digital economy and finance (Bank Indonesia, 2025). Efendi and Yazid (2026) explain that the development of a cashless society in Indonesia has changed consumer behavior, as shown by the growing use of digital payment methods that are regarded as practical, efficient, and accessible. Research on mobile payment adoption also shows that trust, perceived risk, and anxiety strongly influence whether consumers adopt digital payments (Patil et al., 2020).

The cashless society in Indonesia has grown significantly with the digitalization of the payment system, marked by the widening use of noncash payment methods such as QRIS, digital wallets, and mobile banking. Bank Indonesia continues to promote the transformation of the payment system by developing QRIS as the national standard for payments based on QR codes in order to create a payment system that is safe, efficient, accessible, and integrated. Although the cashless society provides various benefits, its implementation still faces several challenges. Khoiroh and Agustianto (2025) show that the main challenges include limited digital infrastructure, low digital and financial literacy, public habits that still depend on cash, and concerns about data security and the misuse of digital transactions. At the same time, the growing use of digital payment systems increases opportunities for cybercrime. The success of a cashless society therefore depends not only on payment technology but also on strengthening digital literacy, security systems, and public readiness for digital transactions.

2.2 Digital Financial Fraud

Digital financial fraud is intentional deception that uses technology and electronic financial systems in online transactions to manipulate or misuse financial systems in order to obtain illegal gains or unauthorized access (Udeh, Amajuoyi, Adeusi, & Scott, 2024). The development of technologies such as the internet and mobile computing has driven the growth of digital finance while increasing the likelihood of financial fraud in digital transactions (Udeh et al., 2024). The wider use of electronic payment methods and innovations in financial technology has expanded digital financial interactions and created new opportunities for perpetrators to exploit weaknesses in systems and users (Aicha, 2025). Reviews of financial fraud detection show that fraud schemes are constantly evolving and that static rules can no longer keep pace with them (Hilal, Gadsden, & Yawney, 2022). Digital financial fraud exploits digital technology and the vulnerability of users through various schemes, ranging from the manipulation of information to the use of AI based technology. The relevant types of digital financial fraud are described in the following paragraphs.

Phishing is a type of fraud that aims to illegally obtain personal data and information from users, such as user identification (ID), passwords, Personal Identification Number (PIN), account numbers, and credit card numbers (Yuspin, Putri, Fauzie, & Pitaksantayothin, 2024; Oyegoke, Amoo, & Aigberua, 2024). Phishing is carried out by impersonating a credible entity or organization through fake emails or other communication channels in order to convince victims to provide personal and financial

information (Yuspin et al., 2024). Perpetrators may also direct victims to fake websites that resemble official sites, and the information obtained can then be misused (Naqvi, Perova, Farooq, Makhdoom, Oyedeji, & Porras, 2023).

Social engineering is an approach of psychological manipulation that aims to persuade people to voluntarily provide personal data or take actions that benefit the perpetrator, such as handing over passwords, PINs, one time password codes, or account information (Sonia, Salsabila, Oktaviani, Nurullah, & Wahyudi, 2026). Unlike cyberattacks that exploit technical weaknesses in systems, social engineering focuses on exploiting the psychological side of individuals, such as trust, panic, or a lack of vigilance toward digital threats. Gehl and Lawson (2022) describe social engineering as a form of communicative manipulation that uses media to gather information about targets, create false identities, and spread messages that combine truth with misleading information in order to influence victims' views and actions. Social engineering takes various forms, such as phishing through unofficial links or websites, smishing through text messages or messaging applications, vishing through telephone calls, and impersonation (Sonia et al., 2026).

QRIS is the national QR code standard designed by the authorities together with the Indonesian Payment System Association to create a safe and efficient digital payment system (Tara & Sudiro, 2023). This development has triggered a new fraud scheme, namely fake QRIS codes, which are used to divert transaction funds to accounts controlled by perpetrators, so that payments intended for legitimate merchants or recipients are redirected (Tara & Sudiro, 2023). In practice, perpetrators often place fake QRIS stickers over a merchant's original QRIS code so that the victim's payment is diverted without being noticed. Because this scheme exploits a combination of technical weaknesses and predictable user behavior, fraud using fake QRIS codes can still occur despite multiple security layers (Alpaullivarez & Fajar, 2026).

Fake marketplaces are a type of digital fraud carried out by creating websites or online stores that resemble official platforms. Perpetrators offer goods to attract consumers and receive payments, but the promised goods never arrive or are replaced with counterfeit or poor quality items. After obtaining money from victims, perpetrators often close the accounts used, which makes it difficult for victims to demand accountability or refunds (Dasarraju, 2024). Perpetrators also try to build trust through various methods, such as clear product descriptions, shipping or return policies, and convincing language (Degeneve, Longhi, & Rossy, 2024). Various studies have developed approaches based on machine learning to detect suspicious financial transactions so that unusual activities can be identified earlier (Byrapu, Kanagala, Ravichandran, Pulimamidi, Sivarambabu, & Polireddi, 2024).

AI voice scams are a development of voice phishing, or vishing, which is a type of social engineering that uses voice communication by telephone to trick victims into revealing personal or financial information. Through AI voice technology, perpetrators can impersonate trusted parties such as banks, customer service, or official institutions, so that victims more easily believe the information conveyed. According to Fakieh and Akremi (2022), AI makes these attacks more difficult to detect, because perpetrators can use fake telephone numbers, voice changers, or social engineering techniques to convince victims, and the information obtained is then misused for identity theft, account takeover, or financial gain.

Deepfakes are synthetic content created with AI to alter or generate faces, expressions, voices, and identities so that they appear similar to a real person. According to Akhtar (2023), deepfakes are generated through methods such as identity swap, face reenactment, attribute manipulation, and entire face synthesis, which produce images, videos, and audio that are difficult to distinguish from authentic content. Deepfakes have increasingly become a tool for digital fraud. Gambín, Yazidi, Vasilakos, Haugerud, and Djenouri (2024) explain that deepfakes can be used to spread hoaxes, commit fraud, sabotage, and even undermine the stability of the financial sector. Deepfakes allow perpetrators to create highly convincing visual and vocal identities, which increases the effectiveness of social engineering and the likelihood that victims will be deceived.

2.3 AI Literacy

AI literacy is the ability of individuals to understand, use, evaluate, and interact with AI technology actively and responsibly. AI literacy is not only related to the skills of using AI but also includes an understanding of how AI works, its benefits, limitations, potential biases, and the consequences of its use. AI literacy is therefore a competence that allows users to make optimal use of AI while anticipating the risks that the technology may cause (Pinski & Benlian, 2024). Ng et al. (2021) conceptualize AI literacy as consisting of knowing and understanding AI, using and applying AI, evaluating and creating AI, and considering AI ethics. Measurement studies also confirm that AI literacy includes awareness, usage, evaluation, and ethical dimensions (Wang et al., 2023, Carolus et al., 2023).

In higher education, AI literacy has become increasingly important because students are among the most active users of AI. Strengthening AI literacy is needed so that students not only use AI as a learning aid but also understand how it works, evaluate the information it produces, and use the technology responsibly. This competence is important for students in facing the challenges of digital transformation, including the growing misuse of AI in various forms of fraud (Mahadewi et al., 2025). A systematic review of AI literacy scales shows that the competencies that need to be measured include knowledge of basic AI concepts, the ability to use AI effectively, the ability to evaluate AI output critically, an understanding of the potential biases and limitations of AI, and the ability to use AI responsibly (Lintner, 2024). Mastery of these competencies allows individuals not only to use AI as a tool but also to assess the quality of the information produced before using it as a basis for decisions. AI literacy is also closely related to broader digital skills, such as information management, critical evaluation, and problem solving with digital tools (van Laar et al., 2017, Oberländer et al., 2020).

For students, the ability to evaluate AI output is one of the most important components, because AI generated information is not always accurate, free from bias, or suited to the context required. AI literacy therefore focuses not only on mastering technology but also on encouraging users to verify, analyze, and evaluate AI generated information before using it. This ability is a basis for developing critical thinking, so that students can use AI responsibly and improve their ability to recognize various forms of digital financial fraud. Trust in AI also matters, because users who trust AI too much may accept its outputs uncritically, while users who understand its limitations can calibrate their trust (Glikson & Woolley, 2020). Explainable AI research shows that users' trust and acceptance improve when AI systems provide understandable explanations (Shin, 2021, Barredo Arrieta et al., 2020).

2.4 Critical Thinking

Critical thinking consists of several interrelated skills. Analytical skills are an important part of critical thinking that allow a person to understand and evaluate complex situations systematically. This ability involves breaking down problems or information into smaller parts and recognizing the characteristics of and relationships among those parts. Analytical skills help a person sort out important information, understand the basics of a problem, find appropriate answers, process information systematically, and draw conclusions based on evidence and structured reasoning (Wang et al., 2025).

Verification and evidential reasoning are the skills of identifying and assessing data by considering the quality of evidence and the accuracy of sources before the data are used as a basis for reasoning. Dawson et al. (2024) explain that the ability to identify accurate information in the process of evaluating information is very important. Sarıbaş (2023) shows that the skill of assessing information critically is closely related to evaluating the credibility of evidence and trust in sources of evidence.

Logical decision making is the skill of using critical thinking to make appropriate decisions when facing various challenges. Nag and Dwivedi (2024) show that decision making skills are related to critical thinking, with a significant positive relationship between critical thinking and decision making ability. In the context of digital financial fraud, critical thinking enables individuals to pause before acting, question the authenticity of messages and payment requests, and verify information through

independent channels. Research on misinformation also shows that analytical reasoning reduces susceptibility to false information (Pennycook & Rand, 2019).

2.5 Research Framework and Hypotheses

Based on the literature review and previous research, AI literacy is viewed as having a role in improving students' ability to understand, apply, and evaluate the use of AI. This ability can support critical thinking in analyzing and evaluating information obtained through AI, and critical thinking can help students identify information or transactions that may involve fraud. This study therefore examines the effect of AI literacy on critical thinking, the effect of AI literacy on fraud detection capability, and the effect of critical thinking on fraud detection capability.

AI literacy helps students improve their critical thinking because understanding AI and the skills to interact with it encourage students to be more critical in its use. Hanifatunnisa and Septiadi (2026) found that AI literacy has a significant positive effect on students' critical thinking. Xin et al. (2026) also found that AI literacy is related to critical thinking among medical students. Based on this description, H_1 states that AI literacy has a positive effect on critical thinking.

The use of AI in scams shows the importance of a person's expertise in understanding and identifying the possible misuse of AI. Aguilar (2026) emphasizes the need to improve AI literacy by providing students with knowledge about how AI can be misused by fraud perpetrators. This knowledge makes students more alert to types of fraud that use AI technology and supports their ability to identify and evaluate potential fraud in digital transactions. Based on this description, H_2 states that AI literacy has a positive effect on fraud detection capability.

Critical thinking plays an important role in helping students evaluate information more carefully before making decisions, especially when facing information or transactions that are suspected of fraud. Education can increase the likelihood that students will suspect an investment that may be fraudulent (Blackwell et al., 2024), and that study positions critical thinking as one of the abilities that higher education is expected to develop and that corresponds to vigilance toward potential fraud. With the ability to analyze and evaluate information critically, students can better recognize and assess types of fraud in digital transactions. Based on this description, H_3 states that critical thinking has a positive effect on fraud detection capability.

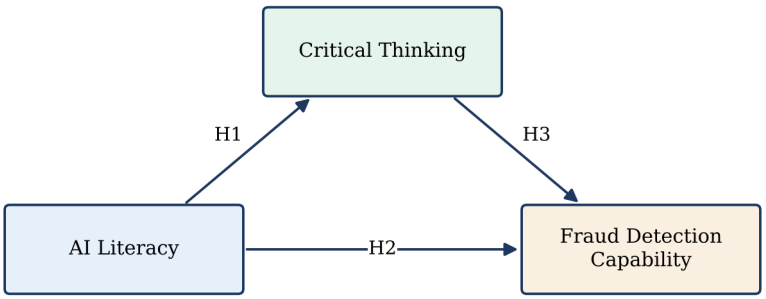


Figure 1. Research framework of AI literacy, critical thinking, and fraud detection capability

Figure 1 shows the research framework of this study. AI literacy is positioned on the left as the antecedent variable, critical thinking at the top, and fraud detection capability on the right as the outcome variable. The arrow from AI literacy to critical thinking represents H_1, the arrow from AI literacy to fraud detection capability represents H_2, and the arrow from critical thinking to fraud detection capability represents H_3. Each relationship was tested separately with simple linear regression. The figure was prepared by the authors in 2026.

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co | DOI:10.52909/faeij.v1i4.466

3. Research Methodology

3.1 Research Design and Participants

This study used a quantitative approach with a cross sectional survey design. The study aimed to examine the effects among AI literacy, critical thinking, and fraud detection capability among students in a cashless society. Data were collected in a single period through an online questionnaire using Google Forms. The participants were active students enrolled in higher education institutions on the island of Java. Participants were selected using purposive sampling with the following criteria, namely active diploma or undergraduate students aged at least 18 years who had used digital transaction services such as QRIS, mobile banking, and digital wallets, and who were willing to participate in the study. The number of participants was 120 students who met the criteria.

3.2 Instruments

The instrument was a questionnaire developed from the literature and consisting of three variables, namely AI literacy, critical thinking, and fraud detection capability. All items were measured on a five point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The AI literacy instrument was developed based on the Meta AI Literacy Scale (MAILS) proposed by Carolus et al. (2023), which covers four dimensions, namely understanding AI, applying AI, detecting AI, and AI ethics. The dimension of understanding AI was complemented by items adapted from Laupichler et al. (2023) to strengthen the measurement of conceptual understanding. The AI literacy instrument consisted of 10 items adapted from Carolus et al. (2023) and 2 items from Laupichler et al. (2023), and it has shown evidence of validity and reliability.

The critical thinking instrument was based on the dimensions developed by Payan-Carreira et al. (2022), which consist of analysis, evaluation, inference, explanation, and self regulation. The instrument consisted of 10 items and has shown evidence of validity and reliability. Fraud detection capability was adapted from Chen et al. (2026) using two of the four dimensions in the original instrument, namely threat awareness and anti fraud self efficacy, which were adjusted to the context of financial fraud among students. Threat awareness was developed into three indicators, namely the perceived existence of online fraud threats, the perceived severity of online fraud threats, and the perceived likelihood of becoming a victim of online fraud. Anti fraud self efficacy was developed into three indicators, namely the ability to identify digital fraud threats, the ability to verify suspicious information, and the ability to respond appropriately to digital fraud threats. The instrument consisted of 10 items, whose content validity was tested with Aiken's V and whose reliability was tested in Jamovi.

Table 1. Content validity of the fraud detection capability instrument

No	Item	Aiken V	Remark
1.	I am aware that internet users are at risk of online fraud	1.00	Valid
2.	I understand that technological developments can increase the emergence of various forms of online fraud	0.92	Valid
3.	I understand that online fraud can cause serious losses	1.00	Valid
4.	I am aware that I could also become a victim of online fraud	1.00	Valid
5.	I believe that a lack of vigilance can increase the risk of becoming a victim of online fraud	0.92	Valid
6.	I can identify signs of fraud in digital transactions	1.00	Valid
7.	I am able to distinguish safe digital activities from potentially fraudulent ones	0.92	Valid
8.	I can verify the truth of information before making a digital transaction	1.00	Valid
9.	I am able to check the authenticity of information before believing it	1.00	Valid

No	Item	Aiken V	Remark
10.	I am able to determine the appropriate action when I find indications of digital fraud	0.92	Valid

Table 1 shows the content validity of the ten items of the fraud detection capability instrument based on the judgment of three experts. Items 1, 3, 4, 6, 8, and 9 obtained an Aiken's V value of 1.00, while items 2, 5, 7, and 10 obtained a value of 0.92. All ten items were therefore declared valid and were retained for reliability testing. The first five items represent threat awareness and the last five items represent anti fraud self efficacy. The items were adapted from Chen et al. (2026), and the Aiken's V values were calculated by the authors in 2026.

Table 2. Reliability of the fraud detection capability instrument

Instrument	Number of Items	Cronbach Alpha	Remark
Fraud detection capability	10	0.819	Reliable

Table 2 shows that the fraud detection capability instrument, which consists of ten items, has a Cronbach's alpha of 0.819. This value indicates that the instrument has high internal consistency in measuring the research variable. The reliability coefficient was calculated by the authors in Jamovi in 2026.

3.3 Data Collection and Analysis

Data were collected online through Google Forms. The questionnaire was distributed through various digital platforms that were easily accessible to students on the island of Java. Before completing the questionnaire, participants received information about the purpose of the study and data confidentiality and gave informed consent to participate. Participation was voluntary, and the data obtained were used only for research purposes. The data were then checked for completeness and conformity with the participant criteria before analysis.

The data were analyzed using Jamovi. The analysis included checking data completeness, descriptive analysis, and testing the validity and reliability of the instruments. Statistical assumption tests were then conducted, including tests of normality, heteroscedasticity, autocorrelation, and multicollinearity. Hypotheses were tested using simple linear regression to examine the effect of AI literacy on critical thinking (H_1), the effect of AI literacy on fraud detection capability (H_2), and the effect of critical thinking on fraud detection capability (H_3).

4. Results and Discussions

4.1 Descriptive Statistics

Data from 120 respondents were analyzed to describe the research variables and test the relationships among AI literacy, critical thinking, and fraud detection capability. The analysis included descriptive statistics, classical assumption tests, and simple linear regression. Descriptive analysis was conducted to describe the minimum, maximum, mean, median, mode, and standard deviation of each variable.

Table 3. Descriptive statistics of the research variables

Statistic	AI Literacy	Critical Thinking	Fraud Detection Capability
N	120	120	120
Mean	49.7	42.7	43.4
Median	50	44	44
Mode	54	45	44
Standard deviation	6.05	4.86	4.28
Minimum	33	23	27
Maximum	60	50	50

Table 3 shows the descriptive statistics of the three variables for 120 respondents. AI literacy, measured with 12 items and a possible range of 12 to 60, had a mean of 49.7, a median of 50, a mode of 54, and a standard deviation of 6.05, with scores ranging from 33 to 60. Critical thinking, measured with 10 items and a possible range of 10 to 50, had a mean of 42.7, a median of 44, a mode of 45, and a standard deviation of 4.86, with scores ranging from 23 to 50. Fraud detection capability, also measured with 10 items, had a mean of 43.4, a median of 44, a mode of 44, and a standard deviation of 4.28, with scores ranging from 27 to 50. The means of all three variables are close to the upper end of their possible ranges, which indicates that respondents generally perceived themselves as having high AI literacy, critical thinking, and fraud detection capability. The table was compiled by the authors from data processed in Jamovi in 2026.

4.2 Classical Assumption Tests

Before hypothesis testing, classical assumption tests were conducted to ensure the suitability of regression analysis. The Kolmogorov Smirnov normality test produced p=0.587 (p>0.05), so the data met the assumption of normality. The Goldfeld Quandt heteroscedasticity test produced p=0.399 (p>0.05), which indicates no heteroscedasticity. The Durbin Watson autocorrelation test produced p=0.286 (p>0.05), which indicates no autocorrelation. The multicollinearity test produced a tolerance value of 0.527 for AI literacy and critical thinking, which indicates that the two variables did not show multicollinearity.

4.3 Hypothesis Testing

After all assumptions were met, simple linear regression was conducted to test the effect of AI literacy on critical thinking, the effect of AI literacy on fraud detection capability, and the effect of critical thinking on fraud detection capability.

Table 4. Results of simple linear regression

Hypothesis	Relationship	β	t	p	F	R^2
H_1	AI literacy to critical thinking	0.688	10.29	< 0.001	106	0.473
H_2	AI literacy to fraud detection capability	0.689	10.31	< 0.001	106	0.474
H_3	Critical thinking to fraud detection capability	0.691	10.39	< 0.001	108	0.478

Table 4 shows the results of the three simple linear regressions. AI literacy had a positive and significant effect on critical thinking (β=0.688, t=10.29, p<0.001, F=106, R^2=0.473), which means that AI literacy explained 47.3% of the variance in critical thinking. AI literacy also had a positive and significant effect on fraud detection capability (β=0.689, t=10.31, p<0.001, F=106, R^2=0.474), explaining 47.4% of its variance. Critical thinking had a positive and significant effect on fraud detection capability (β=0.691, t=10.39, p<0.001, F=108, R^2=0.478), explaining 47.8% of its variance. All three hypotheses were therefore supported. The table was compiled by the authors from data processed in Jamovi in 2026.

4.4 The Effect of AI Literacy on Critical Thinking

The regression results show that AI literacy had a positive effect on critical thinking, so H_1 was supported, which indicates that students' understanding of AI can support more critical thinking. This result is consistent with Xin et al. (2026), who showed that higher AI literacy is associated with stronger critical thinking among students. AI literacy is related not only to the ability to use AI but also to an understanding of how AI works, its limitations, its potential biases, and its responsible use (Lintner, 2024). When students understand that AI generated information is not always correct or relevant to their needs, they have a basis for evaluating that information before accepting it. The ability to evaluate AI generated information critically plays a role in identifying potential biases and supports the appropriate and effective use of AI (Aswan, 2025, Bećirović et al., 2025).

This evaluative ability can develop into students' reflective engagement in using AI, which is also an important part of AI literacy. Shapiro et al. (2026) consider that AI literacy involves reflective and

metacognitive thinking that allows a person to reflect critically on how they interact with AI. Consistent with this view, AI can serve as a cognitive tool that broadens the way students process information and encourages higher order critical thinking (Par, 2026). At the same time, research warns that heavy reliance on AI dialogue systems may weaken students' cognitive abilities when AI is used without reflection (Zhai et al., 2024), and that frequent AI use can reduce critical thinking through cognitive offloading (Gerlich, 2025).

These findings reinforce the view that the use of AI in education should not be directed only at technical skills. Students need the ability to assess information obtained from AI so that the technology is not used passively. This is consistent with Darwin et al. (2024), who explain that AI can support the development of critical thinking but that users still need to understand the limitations of AI in producing information. AI literacy therefore not only helps students understand and use AI but also encourages more active cognitive engagement in analyzing information, which in turn can support the development of critical thinking.

4.5 The Effect of AI Literacy on Fraud Detection Capability

The results show that AI literacy had a positive effect on fraud detection capability, so H_2 was supported. This finding shows that students' ability to understand and use AI is related to their ability to recognize potential fraud in digital transactions. Handayani et al. (2026) similarly show that students with better digital literacy tend to be more cautious in verifying information and better able to protect personal data when facing cybercrime. Umar and Dalimunthe (2024) reveal that digital literacy has an indirect effect on awareness of investment scams through cybercrime awareness among Indonesian students. This is supported by Istiqomah et al. (2025), who show that digital literacy helps people avoid phishing.

The relationship between AI literacy and fraud detection capability can be understood through students' ability to evaluate information obtained from technology. Dong et al. (2025) reveal that AI literacy includes critical appraisal, namely the ability to analyze information, technology, and applications related to AI in depth. AI can be used as a means of understanding and identifying fraud in digital financial transactions (Yang et al., 2026). Besides being a means of understanding and identifying fraud, AI is also used as a tool for detecting fraud, but its results still require human oversight and evaluation (Langer et al., 2025). Users who understand how AI works are better able to calibrate their trust in AI outputs and in AI generated content such as deepfakes (Glikson & Woolley, 2020). AI literacy can therefore help students use AI more appropriately while remaining aware of its limitations in providing information.

4.6 The Effect of Critical Thinking on Fraud Detection Capability

The results show that critical thinking had a positive effect on fraud detection capability, so H_3 was supported. This means that students with stronger critical thinking are better able to recognize and assess information that may lead to fraud in digital transactions. When facing suspicious information, students need not only to know the various forms of fraud but also to analyze information, weigh evidence, draw conclusions, and decide on appropriate actions. These abilities correspond to the dimensions of critical thinking used in this study, namely analysis, evaluation, inference, explanation, and self regulation.

This result is consistent with Orhan (2023), who found that critical thinking dispositions are positively related to students' ability to detect fake news and significantly predict this ability. The ability to analyze and evaluate information helps students distinguish trustworthy information from potentially misleading information. This ability is relevant for facing digital financial fraud, because fraudulent information can be made to resemble information from trusted sources. Research on misinformation also shows that people who think analytically are less likely to believe false content (Pennycook & Rand, 2019).

Niza et al. (2022) also found a relationship between critical thinking skills and information literacy in identifying fake news among social media users. Critical thinking is related to the ability to assess the credibility of sources and recognize untrustworthy information. This ability is also important in digital transactions, when students receive messages, links, payment information, or offers whose truth cannot yet be confirmed. Students need to check such information before believing it or taking action. Research on cyber fraud victimization shows that impulsive responses and a lack of verification increase susceptibility to fraud (Whitty, 2019).

The results also show that AI literacy and critical thinking play complementary roles in supporting fraud detection capability. AI literacy helps students understand and use AI appropriately, while critical thinking helps students assess the information obtained before making decisions. In the development of a cashless society, both abilities are increasingly important because students use various digital transaction services that carry fraud risks. The similar magnitude of the three coefficients also suggests that AI literacy, critical thinking, and fraud detection capability are closely interrelated, so future studies should test whether critical thinking mediates the effect of AI literacy on fraud detection capability.

5. Conclusions

Based on the results, AI literacy had a positive and significant effect on critical thinking and fraud detection capability among students, and critical thinking also had a positive and significant effect on fraud detection capability, so all three hypotheses were supported. AI literacy and critical thinking play complementary roles in supporting students' ability to detect fraud. AI literacy helps students understand and use AI appropriately, while critical thinking helps them analyze and evaluate information before making decisions. Both abilities are relevant for students as users of AI technology and of digital transaction services in a cashless society, so strengthening AI literacy and critical thinking in education can help prepare students to recognize and respond to the risks of digital financial fraud.

Educational institutions are advised to strengthen AI literacy and critical thinking through learning that teaches not only the use of AI but also the evaluation of information and the consideration of risks arising from AI generated content. This learning can be directed to the context of technology use and digital transactions so that students are better prepared to recognize information or activities that may lead to fraud. Fraud detection capability should also be trained through more realistic experiences so that students not only understand fraud in theory but can also recognize and respond to digital fraud in daily life.

This study has several limitations. The sample consisted of 120 students on the island of Java, the design was cross sectional, the data were self reported, and the three hypotheses were tested with separate simple regressions. Future research is advised to involve larger and more diverse samples so that the results can be generalized more widely, to test an integrated model in which critical thinking mediates the effect of AI literacy on fraud detection capability, and to consider other factors such as digital financial literacy, experience with digital transaction services, and previous experience with fraud.

Acknowledgement

The authors thank their supervisor and all parties at Universitas Muhammadiyah Surakarta who provided guidance and support during the preparation of this article, as well as the students who participated in the study.

Author Contributions

DNAS contributed to the conceptualization of the study, the development of the instruments, data collection, data analysis, and the writing of the original draft. TIFR contributed to the literature

review, data collection, the interpretation of the results, and the review and editing of the manuscript. Both authors read and approved the final manuscript.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

References

Aguilar, G. L. (2026). Increasing literacy on the scams targeting Latines: Generative artificial intelligence, digital technologies, and the Latine community. *Journal of Business and Technical Communication*, *40*(1), 1-23. https://doi.org/10.1177/10506519251372578

Aicha, F. (2025). Financial fraud in the era of digital transformation. *Revue Algérienne des Sciences Juridiques et Politiques*. Retrieved from https://asjp.cerist.dz/en/article/275999

Akhtar, Z. (2023). Deepfakes generation and detection: A short survey. *Journal of Imaging*, *9*(1). https://doi.org/10.3390/jimaging9010018

Alpaullivarez, A. A., & Fajar, A. N. (2026). Exploring factors influencing user avoidance behavior toward QR-based payment scams. *Journal of Information Systems Engineering and Business Intelligence*, *12*(2), 458-473. https://doi.org/10.20473/jisebi.12.2.458-473

Aswan, D. (2025). Hubungan antara literasi digital dan persepsi mahasiswa tentang etika penggunaan AI di kalangan akademik [The relationship between digital literacy and students' perceptions of the ethics of AI use in academia]. *Jurnal Ilmiah Wahana Pendidikan, 11(6.D), 283–294*. Retrieved from https://jurnal.peneliti.net/index.php/JIWP/article/view/12159/8510

Bank Indonesia. (2025). Laporan perekonomian Indonesia 2024 [Indonesian economic report 2024]. Retrieved from https://www.bi.go.id/id/publikasi/laporan/Pages/LPI_2024.aspx

Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58, 82–115*. https://doi.org/10.1016/j.inffus.2019.12.012

Bećirović, S., Polz, E., & Tinkel, I. (2025). Exploring students' AI literacy and its effects on their AI output quality, self-efficacy, and academic performance. *Smart Learning Environments*, *12*(1). https://doi.org/10.1186/s40561-025-00384-3

Biagini, G., Cuomo, S., & Ranieri, M. (2024). Less knowledge, more trust? Exploring potentially uncritical attitudes towards AI in higher education. *Italian Journal of Educational Technology. Advance online publication*. https://doi.org/10.17471/2499-4324/1337

Blackwell, C., Maynard, N., Malm, J., Pyles, M., Snyder, M., & Witte, M. (2024). *Who gets duped? The impact of education on fraud detection in an investment task* (Report No. 48).

Byrapu Reddy, S. R., Kanagala, P., Ravichandran, P., Pulimamidi, D. R., Sivarambabu, P. V., & Polireddi, N. S. A. (2024). Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics. *Measurement: Sensors, 33, Article 101138*. https://doi.org/10.1016/j.measen.2024.101138

Carolus, A., Koch, M. J., Straka, S., Latoschik, M. E., & Wienrich, C. (2023). MAILS: Meta AI literacy scale. *Development and testing of an AI literacy questionnaire based on well-founded competency models and psychological change- and meta-competencies. Computers in Human Behavior: Artificial Humans*, *1*(2). https://doi.org/10.1016/j.chbah.2023.100014

Chen, L., Li, H., Chua, Y. P., & Chen, J. (2026). When awareness is not enough: Online fraud susceptibility, threat awareness, anti-fraud self-efficacy and online scam prevention behavior among Chinese university students. *Frontiers in Psychology, 17, Article 1857855*. https://doi.org/10.3389/fpsyg.2026.1857855

Darwin, Rusdin, D., Mukminatien, N., Suryati, N., Laksmi, E. D., & Marzuki. (2024). Critical thinking in the AI era: An exploration of EFL students' perceptions, benefits, and limitations. *Cogent Education*, *11*(1). https://doi.org/10.1080/2331186X.2023.2290342

Dasarraju, V. K. (2024). E-commerce fraud: Understanding and mitigating fraudulent activities. *Journal of Artificial Intelligence, Machine Learning and Data Science*, *2*(1), 663-665. https://doi.org/10.51219/JAIMLD/vamshi-krishna-dasarraju/169

Dawson, C., Julku, H., Pihlajamäki, M., Kaakinen, J. K., Schooler, J. W., & Simola, J. (2024). Evidence-based scientific thinking and decision-making in everyday life. *Cognitive Research: Principles and Implications*, *9*(1). https://doi.org/10.1186/s41235-024-00578-2

Degeneve, C., Longhi, J., & Rossy, Q. (2024). Distinguishing sellers reported as scammers on online illicit markets using their language traces. *Languages*, *9*(7). https://doi.org/10.3390/languages9070235

Dong, Y., Xu, W., Huang, J., & Yann, K. (2025). Validating and refining a multi-dimensional scale for measuring AI literacy in education using the Rasch model. *Humanities and Social Sciences Communications*, *12*(1). https://doi.org/10.1057/s41599-025-05670-6

Efendi, A. R. S., & Yazid, M. (2026). Fenomena cashless society di Indonesia: Analisis deskriptif perkembangan dan dampaknya terhadap perilaku konsumen. https://doi.org/10.24929/feb.v16i1.5018

Erbuğa, G. S., & Ünal, C. (2026). Explainable artificial intelligence-driven fraud detection: Behavioral proxies of digital financial literacy in online payment models. *Borsa Istanbul Review, 26, Article 100840*. https://doi.org/10.1016/j.bir.2026.100840

Fakieh, A., & Akremi, A. (2022). An effective blockchain-based defense model for organizations against vishing attacks. *Applied Sciences*, *12*(24). https://doi.org/10.3390/app122413020

Gambín, Á. F., Yazidi, A., Vasilakos, A., Haugerud, H., & Djenouri, Y. (2024). Deepfakes: Current and future trends. *Artificial Intelligence Review*, *57*(3). https://doi.org/10.1007/s10462-023-10679-x

Gehl, R. W., & Lawson, S. T. (2022). *Social engineering: How crowdmasters, phreaks, hackers, and trolls created a new form of manipulative communication*.

Gerlich, M. (2025). AI tools in society: Impacts on cognitive offloading and the future of critical thinking. *Societies*, *15*(1). https://doi.org/10.3390/soc15010006

Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals*, *14*(2), 627-660. https://doi.org/10.5465/annals.2018.0057

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems*, *35*(1), 220-265. https://doi.org/10.1080/07421222.2018.1440766

Gökçe, A. T., Topal, A. D., Geçer, A. K., & Eren, C. D. (2025). Investigating the level of artificial intelligence literacy of university students using decision trees. *Education and Information Technologies*, *30*(5), 6765-6784. https://doi.org/10.1007/s10639-024-13081-4

Handayani, N. S., Prajawinanti, A., & Wasi'ah, D. A. (2026). Literasi digital sebagai strategi preventif cyber crime di kalangan mahasiswa [Digital literacy as a preventive strategy against cybercrime among university students]. *Jurnal Ilmu Perpustakaan (JIPER)*, *8*(1), 69-82. https://doi.org/10.31764/jiper.v7i1.37994

Hanifatunnisa, F. A., & Septiadi, J. (2026). The simultaneous influence of AI literacy and prompting skills on students' critical thinking disposition. *Journal of Educational Sciences*. Retrieved from https://jes.ejournal.unri.ac.id/index.php/JES/article/view/1685/1216

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications, 193, Article 116429*. https://doi.org/10.1016/j.eswa.2021.116429

Istiqomah, N. A., Lorenza, N. A., & Mutia, F. (2025). The impact of digital literacy on phishing prevention behaviour: A literature review. *Pustakaloka: Jurnal Kajian Informasi dan Perpustakaan*, *17*(2), 102-125. https://doi.org/10.21154/pustakaloka.v17i2.10495

Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, *61*(4), 577-586. https://doi.org/10.1016/j.bushor.2018.03.007

Khoiroh, S. F., & Agustianto, M. A. (2025). Tantangan dan peluang implementasi cashless society: Systematic literature review pada sektor UMKM. *Indonesian Journal of Management Science*, *4*(2), 109-122. https://doi.org/10.46821/ijms.v4i2.703

Langer, M., Baum, K., & Schlicker, N. (2025). Effective human oversight of AI-based systems: A signal detection perspective on the detection of inaccurate and unfair outputs. *Minds and Machines*, *35*(1). https://doi.org/10.1007/s11023-024-09701-0

Laupichler, M. C., Aster, A., & Raupach, T. (2023). Delphi study for the development and preliminary validation of an item set for the assessment of non-experts' AI literacy. *Computers and Education: Artificial Intelligence, 4, Article 100126*. https://doi.org/10.1016/j.caeai.2023.100126

Lintner, T. (2024). A systematic review of AI literacy scales. *npj Science of Learning*, *9*(1). https://doi.org/10.1038/s41539-024-00264-4

Mahadewi, M. P., Aysya, A. A. A., Sofiyani, Z., & Fahmi, F. (2025). The importance of literacy on artificial intelligence for the higher education students: A systematic literature review. *International Journal of Advances in Data and Information Systems*, *6*(1), 1-14. https://doi.org/10.59395/ijadis.v6i1.1350

Nag, S. K., & Dwivedi, S. K. (2024). Effect of critical thinking on decision making efficacy of students at senior secondary level. *International Journal of Indian Psychology*, *12*(3). https://doi.org/10.25215/1203.003

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security, 132, Article 103387*. https://doi.org/10.1016/j.cose.2023.103387

Ng, D. T. K., Leung, J. K. L., Chu, S. K. W., & Qiao, M. S. (2021). Conceptualizing AI literacy: An exploratory review. *Computers and Education: Artificial Intelligence, 2, Article 100041*. https://doi.org/10.1016/j.caeai.2021.100041

Niza, I. H., Mawarpury, M., Sulistyani, A., & Rachmatan, R. (2022). Critical thinking ability and information literacy in identifying fake news on social media users. *Jurnal Psikologi Terapan dan Pendidikan*, *4*(1), 1. https://doi.org/10.26555/jptp.v4i1.23357

Oberländer, M., Beinicke, A., & Bipp, T. (2020). Digital competencies: A review of the literature and applications in the workplace. *Computers & Education, 146, Article 103752*. https://doi.org/10.1016/j.compedu.2019.103752

Orhan, A. (2023). Fake news detection on social media: The predictive role of university students' critical thinking dispositions and new media literacy. *Smart Learning Environments*, *10*(1). https://doi.org/10.1186/s40561-023-00248-8

Oyegoke, T. O., Amoo, A. O., & Aigberua, J. (2024). An enhanced phishing detection system in online transactions. *TWIST*, *19*(3), 656-666. https://doi.org/10.5281/zenodo.10049652

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, *18*(4), 329-340. https://doi.org/10.1016/j.bir.2017.12.003

Par, E. (2026). The role of artificial intelligence literacy and learning motivation in enhancing students' critical thinking skills. *Edueksos*. Retrieved from https://syekhnurjati.ac.id/jurnal/index.php/edueksos

Patil, P., Tamilmani, K., Rana, N. P., & Raghavan, V. (2020). Understanding consumer adoption of mobile payment in India: Extending Meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal. *International Journal of Information Management, 54, Article 102144*. https://doi.org/10.1016/j.ijinfomgt.2020.102144

Payan-Carreira, R., Sacau-Fontenla, A., Rebelo, H., Sebastião, L., & Pnevmatikos, D. (2022). Development and validation of a critical thinking assessment-scale short form. *Education Sciences*, *12*(12). https://doi.org/10.3390/educsci12120938

Pennycook, G., & Rand, D. G. (2019). Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. *Cognition, 188, 39–50*. https://doi.org/10.1016/j.cognition.2018.06.011

Pinski, M., & Benlian, A. (2024). AI literacy for users: A comprehensive review and future research directions of learning methods, components, and effects. *Computers in Human Behavior: Artificial Humans*, *2*(1). https://doi.org/10.1016/j.chbah.2024.100062

Prasetya, M. E., Mohamed, I. S., & Shuhidan, S. M. (2023). Digital payment in mitigating traditional cash payment fraud risk: A systematic literature review. Paper presented at In European Proceedings of Social and Behavioural Sciences (pp. 723–738). European Publisher.

Pusiknas. (2026). Modus penipuan online kian canggih, ribuan kasus terjadi tiap bulan. Pusat Informasi Kriminal Nasional Polri. Retrieved from https://pusiknas.polri.go.id/detail_artikel/modus_penipuan_online_kian_canggih,_ribuan_kasus_terjadi_tiap_bulan

Sarıbaş, D. (2023). The impact of asynchronous reflection and discussion on pre-service teachers' evaluation of arguments about the COVID-19 pandemic. *Boğaziçi Üniversitesi Eğitim Dergisi*, *40*(1), 53-73. https://doi.org/10.52597/buje.1186711

Shapiro, H., Souto-Otero, M., & Watermeyer, R. (2026). Metacognitive AI literacy: Going beyond the AI skills gap agenda. *Learning, Media and Technology. Advance online publication*. https://doi.org/10.1080/17439884.2026.2652638

Sonia, D. G., Salsabila, N., Oktaviani, S., Nurullah, U. N., & Wahyudi, C. (2026). Social engineering dan fraud top-up e-wallet: Studi literatur pada pengguna dompet digital di Indonesia [Social engineering and e-wallet top-up fraud: A literature study of digital wallet users in Indonesia]. *Musytari: Jurnal Manajemen, Akuntansi, dan Ekonomi*, *25*(7). https://doi.org/10.2238/9erhjg61

Tara, I. K. K. B., & Sudiro, A. (2023). Perlindungan hukum konsumen terhadap pengguna QRIS dan penanganan penipuan dalam bertransaksi [Legal protection of consumers using QRIS and the handling of fraud in transactions]. *UNES Law Review*, *6*(2), 4581-4588. https://doi.org/10.31933/unesrev.v6i2.1498

Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The role of big data in detecting and preventing financial fraud in digital transactions. *World Journal of Advanced Research and Reviews*, *22*(2), 1746-1760. https://doi.org/10.30574/wjarr.2024.22.2.1575

Umar, S. O., & Dalimunthe, Z. (2024). Financial literacy and digital literacy to awareness of investment scams among Indonesian college students. *Eduvest: Journal of Universal Studies*, *4*(8), 7215-7227. https://doi.org/10.59188/eduvest.v4i8.1297

Wang, B., Rau, P. L. P., & Yuan, T. (2023). Measuring user competence in using artificial intelligence: Validity and reliability of artificial intelligence literacy scale. *Behaviour & Information Technology*, *42*(9), 1324-1337. https://doi.org/10.1080/0144929X.2022.2072768

Wang, M., Mohd Matore, M. E. E., & Rosli, R. (2025). A systematic literature review on analytical thinking development in mathematics education: Trends across time and countries. *Frontiers in Psychology, 16, Article 1523836*. https://doi.org/10.3389/fpsyg.2025.1523836

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277-292. https://doi.org/10.1108/JFC-10-2017-0095

Xin, Y., Yan, D., Shuren, L., Minyang, L., & Liuheng, L. (2026). AI literacy mediates AI assisted diagnosis participation and critical thinking among medical students under supervision. *npj Digital Medicine*, *9*(1). https://doi.org/10.1038/s41746-026-02521-9

Yang, H., Shukur, Z., & Sahran, S. (2026). A review of artificial intelligence for financial fraud detection. *Applied Sciences*, *16*(4). https://doi.org/10.3390/app16041931

Yuspin, W., Putri, A. O., Fauzie, A., & Pitaksantayothin, J. (2024). Digital banking security: Internet phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Safety and Security Engineering*, *14*(6), 1699-1706. https://doi.org/10.18280/ijsse.140605

Zhai, C., Wibowo, S., & Li, L. D. (2024). The effects of over-reliance on AI dialogue systems on students' cognitive abilities: A systematic review. *Smart Learning Environments, 11, Article 28*. https://doi.org/10.1186/s40561-024-00316-7