Journal of Advanced Research Design

Journal homepage:
https://akademiabaru.com/submit/index.php/ard
ISSN: 2289-7984

Evaluating and Modelling Artificial Intelligence and Emotional Intelligence to Improve Cybersecurity Employee Ethical Competence Model

Nor Hapiza Mohd Ariffin[1,*], Aida Wati Zainan Abidin[2], Zan Azma Nasruddin[2], Nurul Fadly Habidin[3], Marina Yusoff[1,2,4]

[1] MIS Department, Faculty of Business, Sohar University, Sohar 311, Oman
[2] College of Computing, Informatics and Mathematics, Kompleks Al- Khawarizmi, Universiti Teknologi MARA (UiTM), 40450 Shah Alam, Selangor, Malaysia
[3] Universiti Pendidikan Sultan Idris, 35900 Tanjoug Malim, Perak, Malaysia
[4] Institute for Big Data Analytics and Artificial Intelligence (IBDAAI) Kompleks Al-Khawarizmi, Universiti Teknologi MARA (UiTM), 40450 Shah Alam, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 6 January 2025
Received in revised form 14 February 2025
Accepted 7 April 2025
Available online 30 April 2025

ABSTRACT

Implementing an ethical competency model in a cybersecurity organisation is crucial for ensuring that employees are prepared to succeed in the complex ethical terrain of cybersecurity decision-making. The model comprises an ethical framework customised for cybersecurity, highlighting moral awareness across decision-making processes. This paper explores the integration of Artificial Intelligence (AI) and Emotional Intelligence (EI) to enhance ethical competence in cybersecurity professionals, highlighting the critical need for a balanced approach to technical efficiency and ethical decision-making**.** Through empirical research, including expert surveys and literature reviews, the study identifies critical AI and EI skills, develops a measurement instrument and proposes a model to assess and improve ethical competence in cybersecurity organisations**.** The research underscores the importance of AI in analysing cybersecurity threats and the role of EI in managing human factors, advocating for targeted training programs that combine AI capabilities with emotional and ethical awareness**.** Seven expert panels with an average of at least two years working as cybersecurity professionals were surveyed. The methodology involved applying exploratory factor analysis, reliability analysis and calculating the importance index with the developed questionnaire. EFA identified two constructs for each skill: AI in cybersecurity development and the integration challenges and EI in decision-making and leadership function in the operations. The instrument reliability was also consistent, with Alpha values ranging between 0.687 to 0.941. The findings suggest that developing an ethical competence model that integrates AI and EI can significantly contribute to establishing a cybersecurity environment that is both technologically advanced and ethically sound, addressing the complex ethical dilemmas faced by cybersecurity professionals**.**

Keywords:
Artificial intelligence; cybersecurity; emotional intelligence; ethical competence

[*] *Corresponding author*
E-mail address: nariffin@su.edu.om

https://doi.org/10.37934/ard.130.1.1325

1. Introduction

Implementing an ethical competency model in a cybersecurity organisation is critical for ensuring personnel are prepared to negotiate the complicated ethical landscape surrounding cybersecurity decision-making. The ethical competency model includes a normative framework customised to cybersecurity, emphasising moral awareness throughout decision-making processes [1]. This paradigm seeks to educate professionals who are not only technically adept but also ethically conscious, capable of recognising and resolving moral difficulties that may occur in their workplace. Tokat [2] defines ethical competence in cybersecurity as leadership approaches that prioritise ethical concerns and international cooperation to improve cybersecurity policy effectively. Integrating ethical principles such as beneficence, nonmaleficence, fairness, autonomy and explicability into training programs allows cybersecurity professionals to better comprehend and apply ethical priorities in decision-making processes [3]. This specialised course enables individuals to thoroughly understand ethical concepts and their practical applications in cybersecurity scenarios.

Furthermore, the ethical competence model includes the creation of conceptual frameworks for analysing ethical challenges in cybersecurity, such as those involving digital healthcare and well-being [4]. Organisations can address ethical difficulties in the digital environment in a comprehensive manner by taking into account numerous ethical factors such as biomedical ethics, ethics of care, core value clusters in cybersecurity and technical objectives.

Ethical competence also includes a psychological profile of hackers to improve long-term cybersecurity procedures, emphasising the need for ethical issues in privacy and bias while using personality profiling approaches [5]. Furthermore, research on cybersecurity investment decisions shows that managers' ethical views, attitudes and societal norms influence cybersecurity risk management [6]. To summarise, the ethical competence model in a cybersecurity organisation is multidimensional, including normative frameworks, leadership approaches, training programs, conceptual analyses and psychological considerations. By incorporating ethical concepts into all cybersecurity operations organisations may promote a culture of ethical awareness and responsibility among experts, ultimately improving cybersecurity practices and effectively mitigating risks.

In the rapidly evolving field of cybersecurity, integrating artificial intelligence (AI) and emotional intelligence (EI) into employee training programs has garnered significant attention. While AI provides technological efficiency, EI is crucial for maintaining ethical standards. Despite their recognised importance, the AI and EI skills necessary for fostering ethical competence remain underexplored. This paper reviews existing literature on AI and EI in professional settings, identifying a significant gap in comprehensive models that integrate both skill sets for cybersecurity professionals. Through empirical research, this study aims to:

i. Determine an importance index for AI and EI skills
ii. Develop and validate a measurement instrument for these skills
iii. Delineate the components of AI and EI that contribute to employee ethical competence model in cybersecurity organisations. The outcomes are expected to offer valuable insights for developing targeted training programs that enhance ethical decision-making in cybersecurity roles.

This study's primary objective is to determine employees' competency in artificial intelligence (AI) and emotional intelligence (EI) skills to propose an ethical competence model for evaluating their ethical competence in a cybersecurity organisation. This study aimed to fulfil the following objectives:

i. Determine the importance index for AI and EI skills features for the employee ethical competence model in cybersecurity organisations.
ii. Develop and validate a measurement instrument to identify the relationship between AI and EI skills for employee ethical competence models in cybersecurity organisations.
iii. Determine the components of AI skills and EI skills that contribute to AI and EI skills for the employee ethical competence model in cybersecurity organisations.

1.1 Ethical Competence in Cybersecurity

Developing an employee ethical competence model for cybersecurity organisations by integrating AI and EI is critical in the contemporary digital landscape. Integrating AI and EI aims to enhance professionals' abilities to navigate the ethical challenges of cybersecurity decision-making. By leveraging AI for data analysis and insights discovery, coupled with EI for understanding and managing emotions, cybersecurity professionals can develop a holistic approach to ethical decision-making.

The proposed model seeks to blend AI skills, such as machine learning techniques, with EI skills to equip cybersecurity employees with the necessary competencies to address moral dilemmas effectively [7]. This integration acknowledges the importance of technical proficiency, emotional awareness and ethical considerations in cybersecurity operations. By combining AI-driven cybersecurity intelligence with emotional resilience and ethical reasoning, professionals can make informed decisions that align with ethical principles and organisational values.

Ethical competence in cybersecurity is increasingly recognised as a critical component of effective security strategies. As cybersecurity threats evolve in complexity and sophistication, the ethical implications of defensive and offensive security measures become more pronounced [8]. Ethical competence involves understanding and applying ethical principles in decision-making, essential for maintaining trust and compliance in cybersecurity operations [9].

1.2 Role of Artificial Intelligence in Cybersecurity

AI has transformed the cybersecurity landscape, offering unprecedented capabilities in threat detection, response and prediction [10]. AI systems can analyse vast datasets rapidly, identifying patterns and anomalies that may indicate potential security threats [11]. However, integrating AI in cybersecurity raises ethical concerns, such as privacy issues, bias in algorithmic decision-making and potential unintended consequences [12].

1.3 Role of Emotional Intelligence in Cybersecurity

EI is the ability to perceive, use, understand and manage emotions effectively [13]. In cybersecurity, EI can enhance communication and collaboration among team members, improve leadership during crises and contribute to ethical decision-making processes [14]. EI is essential in managing the human factors in cybersecurity, such as stress, fatigue and ethical dilemmas [15].

1.4 Integration of AI and EI in Developing Ethical Competence

Integrating AI and EI to develop ethical competence involves leveraging the strengths of both to create a holistic approach to ethical decision-making in cybersecurity. AI can provide the technological tools necessary for effective and efficient data processing and decision support, while

EI can ensure that these decisions are made considering human values and ethics [16]. González *et al.,* [17] have explored models where AI systems are designed to recognise and respond to ethical concerns by incorporating ethical guidelines directly into algorithms. Meanwhile, studies by Nanda *et al.,* [18] have suggested frameworks for training cybersecurity professionals to enhance their EI, enabling them to interpret better and apply the ethical considerations that AI-generated solutions may lack.

1.5 Challenges and Future Directions

The main challenge in integrating AI and EI to develop ethical competence in cybersecurity is aligning technology with human ethical standards. AI systems must be transparent and accountable and their recommendations should be interpretable by humans who understand the broader ethical implications [19]. Additionally, there is a need for ongoing training and development programs to enhance EI among cybersecurity professionals, ensuring that they are equipped to make ethical decisions in rapidly changing scenarios [20].

2. Methodology

The study was segmented into three distinct phases. During Phase 1, the theoretical significance was emphasised by thoroughly examining the existing literature and a proposed Ethical Competence model.

Essential results and conclusions that can be drawn from Figure 1:

i. The model suggests that ethical competence in the context of AI requires a combination of AI skills and EI skills.
ii. AI skills encompass technical and analytical capabilities such as machine learning, security and algorithm optimisation.
iii. EI skills focus on human-centric attributes such as self-awareness, empathy and social skills, which are essential for understanding and interacting with others.
iv. Including both skill sets implies that a balanced approach is necessary for ethical decision-making in AI, highlighting the importance of technical expertise and emotional intelligence.

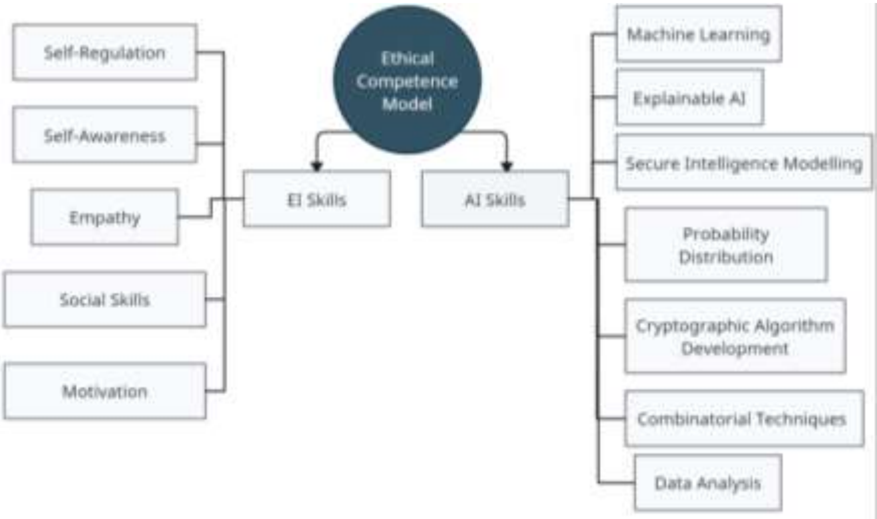

Fig. 1. Proposed ethical competence model

This model could be used to guide the development of training programs or educational curricula for professionals in the field of AI, ensuring they are equipped with the necessary skills to make ethically sound decisions.

During Phase 2, cybersecurity specialists will consult to determine the importance of AI capabilities and EI in cybersecurity organisations. Furthermore, a statistical analysis was performed to evaluate the construct validity and reliability of the items in the instrument. In Phase 3, the instrument utilises the designed and validated questions to assess. Meanwhile, in Phase 3, the instrument's designed and validated questions are used to evaluate the link between AI and EI regarding cybersecurity officer efficiency and credibility and the usefulness of the two bits of intelligence talents in the cybersecurity organisation. The study investigated the correlation between AI and EI regarding the efficiency and credibility of cybersecurity officers and the usefulness of the two intelligence skills within the cybersecurity organisation.

2.1 Procedure

This study was divided into four main phases as shown in Figure 2:

i. Literature search and review
ii. Assessing the order of importance of artificial intelligence skills and emotional intelligence skills based on the panel experts' survey
iii. Validating the constructs to finalise the instrument and checking for the internal consistency
iv. Analysing the relationship between artificial and emotional intelligence.

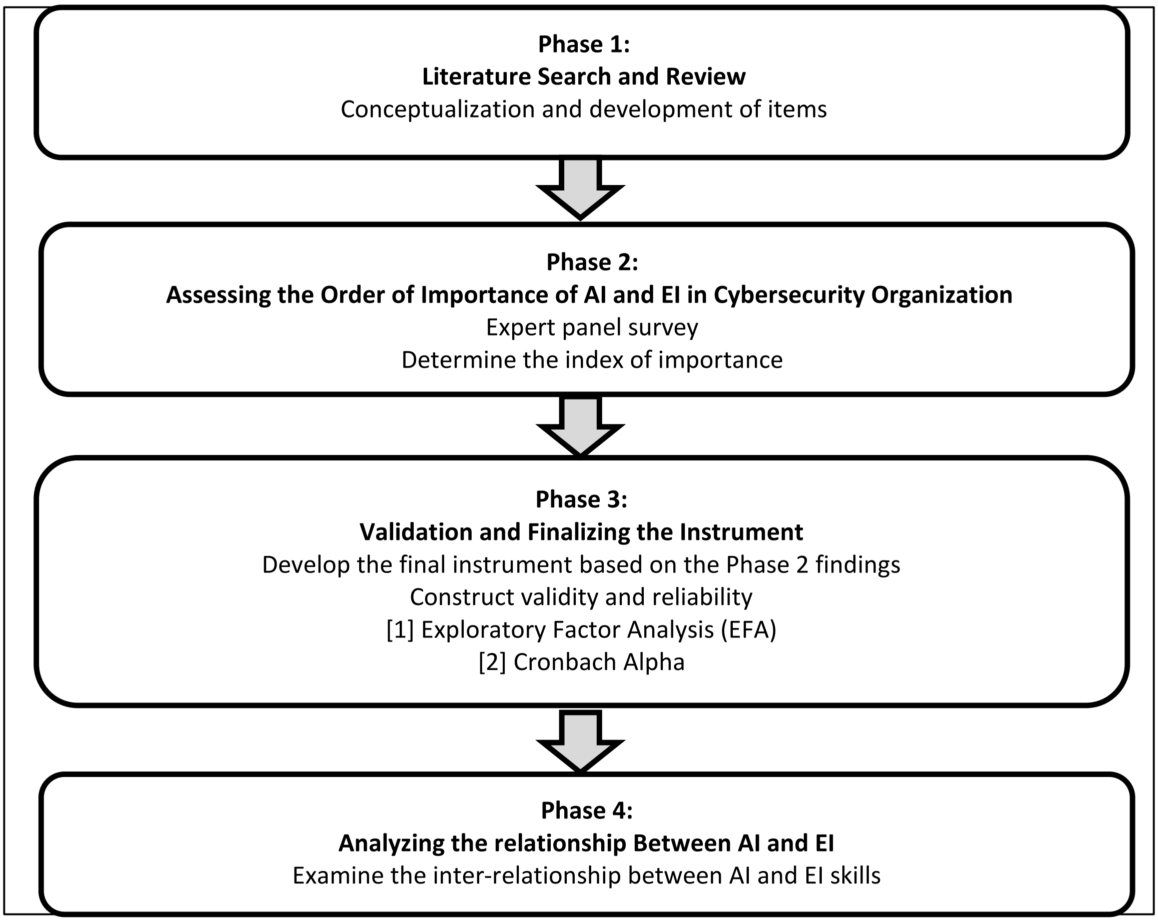
Phase 1:
Literature Search and Review
Conceptualization and development of items
Phase 2:
Assessing the Order of Importance of AI and EI in Cybersecurity Organization
Expert panel survey
Determine the index of importance
Phase 3:
Validation and Finalizing the Instrument
Develop the final instrument based on the Phase 2 findings
Construct validity and reliability
[1] Exploratory Factor Analysis (EFA)
[2] Cronbach Alpha
Phase 4:
Analyzing the relationship Between AI and EI
Examine the inter-relationship between AI and EI skills

Fig. 2. Proposed method flow

2.1.1 Phase 1: Literature search and review

During this phase, items were conceptualised and developed using inductive and deductive approaches. The findings of this phase are discussed in the earlier section.

2.1.2 Phase 2: Assessing the order of importance of artificial intelligence skills and emotional intelligence skills based on the panel experts' survey

An individual expert survey was conducted in March 2024. The survey was intended to get input on the importance of skills among cybersecurity employees from the seven expert panels from various government and private agencies in Malaysia who were invited to share their expert opinions and knowledge. Their say and suggestions are very beneficial as the primary findings support the findings from the literature search. From this survey, the order of importance of both artificial and emotional intelligence skills, which are crucial for cybersecurity professionals in cybersecurity organisations, is determined.

2.1.3 Phase 3: Validation and finalising the instrument

Based on the importance of the AI and EEI skills found in Phase 2, the researcher developed the final instrument. On top of the skills required, the components that contribute to both skills were also examined.

2.1.3.1 The instrument

The researchers developed the instrument based on the findings from the literature search. The instrument is divided into five main sections:

i. <u>Section 1:</u> Demographic profiles of the panel experts
ii. <u>Section 2:</u> Artificial Intelligence Skills in Cybersecurity Organisations.
iii. <u>Section 3:</u> The components of AI skills
iv. <u>Section 4:</u> Emotional Intelligence Skills in Cybersecurity Professionals
v. <u>Section 5:</u> The components of EI skills.

2.1.3.2 Construct validity and reliability

The exploratory factor analysis (EFA) was carried out to determine the instrument's construct validity. The number of factors selected will depend on several criteria, including Eigenvalue > 1 [21], factor loading coefficient > 0.4 [22] and the cumulative percentage of variance extracted [23]. The reliability of each factor was assessed by calculating Cronbach's Alpha. Kline [24] suggests that reliability coefficients ranging from 0.90 to 0.70 are acceptable. The Cronbach's Alpha coefficient of 0.90 and above indicates strong internal consistency and reliability in assessing intended constructs. The instrument's EFA and Cronbach's Alpha were obtained using IBM Statistics version 29.0.

2.1.4 Phase 4: Analysing the relationship between artificial and emotional intelligence

Pearson Product Moment Correlation analysis was also employed to examine the inter-relationship between the AI and EI skills. Besides overall AI and EI skills, the correlation of each dimension suggested during EFA is also determined.

3. Results

The acquired results are derived from the study's methodology. Initially, a questionnaire was developed and distributed to the panel experts. Following this, the constructed instrument underwent validation, encompassing face validity, content validity, construct validity and reliability assessment. Lastly, the study evaluated the critical skills crucial to cybersecurity professionals in cybersecurity organisations by calculating the importance index for each instrument item.

Table 1 summarises the panel experts' backgrounds and profiles and provides information on the importance of AI and EI skills in cybersecurity organizations.

Table 1
Demographic profile of the respondents

Expert		Frequency	Mean (SD)	Median
Gender	Male	6		
	Female	1		
Position	Developer	2		
	Engineers	2		
	Technical Support	2		
	Academician	1		
Qualification	Bachelor Degree	5		
	Masters and above	2		
Salary	RM3000-RM4999	3		
	RM4000 – RM9999	2		
	More than RM10000	2		
Age (years)			36.1 (10.3)	36
Number of years in the current organisation			6.7 (7.9)	3
Number of years in current position			5.7 (5.0)	3
Number of years in cybersecurity sector			3.6 (3.4)	2

The index of importance for both AI skills and EI skills required by cybersecurity professionals working with cybersecurity organisations based on the survey by the panel experts are shown in Tables 2 and 3. All experts agreed that applying AI in cybersecurity could help detect Android malware or vulnerable source code. This opinion indicates that all cybersecurity professionals should be knowledgeable about the application of artificial intelligence. On top of that, the combination of AI and machine learning (ML) is essential in developing cybersecurity solutions, particularly in detecting malware and vulnerable source code.

Table 2
Index of importance for AI skills

Items	Index of Importance	Order of Importance
AI Skills are crucial in cybersecurity organisations.	80	4
AI skills contribute to the protection of Internet-connected systems from cyber threats, attacks, damage or unauthorised access	82.8	2
The integration of AI and the Internet of Things (IoT) in critical infrastructure sectors presents opportunities and challenges, particularly in the area of cybersecurity	71.4	9
AI and machine learning (ML) are indeed essential in the development of cybersecurity solutions, particularly for detecting malware and vulnerable source code	82.8	2
Cybersecurity risks are associated with AI	77.2	8
The application of AI in cybersecurity helps to detect Android malware or vulnerable source code	85.8	1
AI-driven cybersecurity helps to protect computing systems, devices, networks, programs and data from cyber-attacks	80	4
AI and machine learning skills are crucial for mitigating (weakening) cyber-attacks, with a focus on the technical ability, knowledge and experience required to implement information systems (IS) security for cyber-attack mitigation	80	4
AI and machine learning skills are essential for designing a cybersecurity curriculum for universities	80	4

As for the importance of emotional skills, the experts agreed that emotional intelligence skills should combine knowledge experts, technical skills and capabilities in cybersecurity competence. These skills are essential to managing the human capital involved in cybersecurity operations. Though EI skills are essential when deciding on incident response, the experts believe that the skills are not crucial in the general decision-making processes.

Table 3
Index of importance for EI skills

Items	Index of Importance	Order of Importance
EI in cybersecurity organisations could enhance decision-making processes	71.4	8
EI in cybersecurity organisations could enhance leadership qualities	77.2	5
EI in cybersecurity organisations could enhance individual and group decisions and outcomes	74.2	6
EI in cybersecurity organisations helps organisations achieve organisational goals	74.2	6
EI skills are a combination of knowledge, skills and abilities in cybersecurity competence	82.8	1
EI skills are relevant in cybersecurity in detecting threats and vulnerabilities	80	3
EI skills are essential for managing the human capital involved in cybersecurity operations	82.8	1
EI skills are essential in decision-making and incident response	80	3

3.1 Exploratory Factor Analysis and Reliability Analysis

The survey has two main sections: artificial intelligence skills and emotional skills, with nine and eight items each. Two factors were extracted after the construct validity was conducted for each skill. Based on Table 4, the factor loading for all items is greater than 0.4, ranging from 0.743 to 0.949. The first dimension in AI Skills accounted for 62.72% and the second dimension accounted for 23.72%, which accounted for 86.44%. In the emotional intelligence section, the first dimension extracted accounted for 44.82%, while the second dimension accounted for 33.38%, with a total variation of 78.2%. The eigenvalues for all two dimensions in the EI skills range surpass the threshold value 1.0.

The reliability of all three dimensions, ranging from 0.687 to 0.864, suggests that internal consistency is acceptable. Dimension 1 in AI skills has a Cronbach value of 0.941, suggesting strong internal consistency when assessing intended constructs. However, two items from each section (in total, four) were excluded from the final instrument as the factor loading value was less than 0.4 and had an indecisive dimension.

Table 4
The results of exploratory factor analysis (EFA) and reliability testing

Items	Factor Loading		Dimension
	1	2	
Item 1	.788		Dimension 1 – Artificial Intelligence Skills
Item 2	.904	-	
Item 3	.960		
Item 4	.960		
Item 5		.909	Dimension 2 – Artificial Intelligence Skills
Item 6		.849	
Item 7		.949	
Item 8	-	-	
Item 9	-	-	
Total % of the variance	62.72	23.72	
Eigenvalue	4.39	1.66	
Cronbach’s Alpha (* excluded)	.941	.864	
Item 10	.847		Dimension 1 – Emotional Intelligence Skills
Item 11	.942		
Item 12	.834		
Item 13		.788	Dimension 2 – Emotional Intelligence Skills
Item 14		.778	
Item 15		.743	
Item 16	-	-	
Item 17	-	-	
Total % of the variance	44.82	33.38	
Eigenvalue	2.69	2.00	
Cronbach’s Alpha (* excluded)	.888	.687	

Note: *Item excluded in the final instrument

All the items were renamed to represent each dimension better. Table 5 lists the details of the items for each dimension with its proposed dimension name.

Table 5
The Final Dimensions with its associated name

Items	Dimension Name
AI Skills are crucial in cybersecurity organisations. AI and machine learning (ML) are essential in developing cybersecurity solutions, particularly for detecting malware and vulnerable source code. AI and machine learning skills are crucial for mitigating (weakening) cyber-attacks, with a focus on the technical ability, knowledge and experience required to implement information systems (IS) security for cyber-attack mitigation. AI and machine learning skills are essential for designing a university cybersecurity curriculum.	Artificial Intelligence Skills in Cybersecurity Development

Integrating AI and the Internet of Things (IoT) in critical infrastructure sectors presents opportunities and challenges, particularly cybersecurity. The application of AI in cybersecurity helps to detect Android malware or vulnerable source code. AI-driven cybersecurity helps to protect computing systems, devices, networks, programs and data from cyber-attacks	Artificial Intelligence Integration and Cybersecurity Challenges
EI skills are essential in decision-making for incident response EI in cybersecurity organisations could enhance individual and group decisions and outcomes. EI in cybersecurity organisations helps organisations achieve organisational goals.	Emotional Intelligence in Cybersecurity Decision-Making
EI skills are essential for managing the human capital involved in cybersecurity operations. EI in cybersecurity organisations could enhance decision-making processes. EI in cybersecurity organisations could enhance leadership qualities.	Emotional Intelligence and Leadership in Cybersecurity Operations

3.2 Analysing the Relationship between Artificial and Emotional Intelligence

A correlation analysis using The Pearson Product Moment Correlation Coefficients was calculated to identify whether AI and EI skills correlate. The results are shown in Figure 3 and Table 6 below.

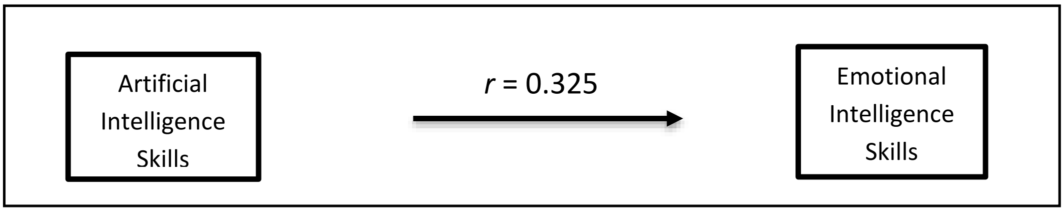

Fig. 3. Correlations of AI skills and EI skills

Figure 3 depicts a correlation between AI and EI skills. The two circles represent two different skill sets: AI skills on the left and EI skills on the right. An arrow connects the two circles, with r=0.325 written above it, indicating the correlation coefficient between these skills. The correlation coefficient r of 0.325 suggests a positive but weak relationship between AI and EI skills. This implies that as AI skills increase, there is a tendency for EI skills to increase as well, but the strength of this association is not strong. The research may explore how skills in technology and human interaction are related, which could have implications for educational programs and hiring practices.

Table 6 presents the correlations between different dimensions of AI skills and EI skills in cybersecurity. The table is structured to show how each dimension correlates with the others. The four dimensions include: “AI Skills in Cybersecurity Development”, “AI Integration and Cybersecurity Challenges”, “EI in Cybersecurity Decision-Making” and “EI and Leadership in Cybersecurity Operations”. It was found that only the dimensions’ A integration and cybersecurity challenges’ and ‘EI and Leadership in Cybersecurity Operations’ are significantly related at a 5% significance level.

A negative correlation (r = −0.296) is observed between AI Integration and Cybersecurity Challenges and EI in Cybersecurity Decision-Making, suggesting that challenges in AI integration might reduce EI’s ability to make decisions. A significant positive correlation (r = 0.579) is noted between AI Integration and Cybersecurity Challenges and EI and Leadership in Cybersecurity Operations, indicating that challenges in AI integration are associated with higher EI in leadership roles within cybersecurity operations. The correlation is moderate and the significance of this correlation implies that this finding is unlikely to be due to chance.

Table 6
Correlations of AI skills dimensions and EI skills dimensions

Dimensions	AI Skills in Cybersecurity Development	AI Integration and Cybersecurity Challenges	EI in Cybersecurity Decision-Making	EI and Leadership in Cybersecurity Operations
AI Skills in Cybersecurity Development	-	.324	.243	.054
AI Integration and Cybersecurity Challenges	.324	-	-.296	.579*
EI in Cybersecurity Decision-Making	.243	-.296	-	.118
EI and Leadership in Cybersecurity Operations	.054	.579*	.118	-

Note: * Significance at 5% level of significance

This paper identifies a significant gap in existing models by integrating AI and EI skills to enhance ethical competence in cybersecurity professionals, aiming to create a balanced approach to ethical decision-making in the field. It contributes by developing and validating a measurement instrument for AI and EI skills, which is crucial for assessing and improving the ethical competence of employees in cybersecurity organisations. The study also proposes a model that delineates the components of AI and EI contributing to ethical competence, offering a novel framework for analysing ethical challenges in cybersecurity, thereby guiding the development of targeted training programs. By investigating the relationship between AI and EI skills, the paper provides empirical evidence on how these skills correlate, significantly contributing to understanding how technical efficiency and emotional intelligence can be integrated to foster ethical decision-making in cybersecurity roles.

There are links between AI and EI skills in cybersecurity, such as malware detection, which function alongside EI skills, which aid in incident decision-making, demonstrating that both skills are critical in effectively dealing with cybersecurity difficulties. The study discovered a significant relationship between AI integration and cybersecurity difficulties and EI in leadership within cybersecurity operations, implying that technical AI skills and emotional intelligence-powered leadership traits are inextricably tied in the cybersecurity industry. Emotional intelligence abilities, particularly in leadership and decision-making, are highly regarded in cybersecurity, indicating that recognising and controlling emotions is critical in guiding teams and making ethical decisions.

One major limitation of this paper is the challenge of aligning AI technology with human ethical standards [25,26]. It requires AI systems to be transparent and accountable and their recommendations to be understandable by humans who grasp the broader ethical implications. The biggest challenge is making sure AI can work well with human ethical rules, meaning AI needs to be transparent and responsible and its advice should be straightforward for people to understand, especially when it comes to right and wrong decisions. Additionally, the paper highlights the need for ongoing training and development programs to enhance EI among cybersecurity professionals, ensuring they are equipped to make ethical decisions in rapidly changing scenarios. This suggests a gap in current training frameworks. There's also a need for continuous learning and training to improve EI among cybersecurity professionals to be better prepared to make good choices when things quickly change.

4. Conclusions

This study achieved its aims by determining employees' competency in artificial intelligence (AI) and emotional intelligence (EI) skills and proposing an ethical competence model for evaluating their ethical competence in a cybersecurity firm. Developing an employee ethical competence model that includes AI and EI in cybersecurity organisations is a realistic approach to addressing cybersecurity's technology and human factors. According to this study, the proposed model will be combined with 60% AI and 40% EI components. Future research should focus on creating robust frameworks that enable the efficient integration of AI capabilities with human ethical judgement, resulting in a cybersecurity environment that is both technologically sophisticated and ethically sound. To recap, developing an employee ethical competence model for cybersecurity organisations through the integration of AI and EI is a key step towards promoting an ethical awareness and responsibility culture in cybersecurity. Professionals who combine technological expertise with emotional intelligence and ethical reasoning can help to solve complex ethical quandaries and develop ethical cybersecurity policies.

Acknowledgement

We want to extend our utmost gratitude for the financial assistance provided by the RMC Grant - FRGS/1/2021/SS02/UITM/02/20 and the College of Computing, Informatics and Mathematics at Universiti Teknologi MARA, Selangor, MALAYSIA, which has greatly supported our research and publications.

References

[1] Formosa, Paul, Michael Wilson and Deborah Richards. "A principlist framework for cybersecurity ethics." *Computers & Security* 109 (2021): 102382. https://doi.org/10.1016/j.cose.2021.102382

[2] Tokat, Yasin. "Towards a Safe and Secure Global Information Technology Ecosystem." *Multidiszciplináris kihívások, sokszínű válaszok-Gazdálkodás-és Szervezéstudományi folyóirat* 2 (2023): 239-269. https://doi.org/10.33565/MKSV.2023.02.09

[3] Sadeghi, Bakhtiar, Deborah Richards, Paul Formosa, Mitchell McEwan, Muhammad Hassan Ali Bajwa, Michael Hitchens and Malcolm Ryan. "Modelling the ethical priorities influencing decision-making in cybersecurity contexts." *Organizational Cybersecurity Journal: Practice, Process and People* 3, no. 2 (2023): 127-149. https://doi.org/10.1108/OCJ-09-2022-0015

[4] Rajamäki, Jyri and Heikki Hämäläinen. "Ethics of Cybersecurity and Biomedical Ethics: Case SHAPES." (2021). https://doi.org/10.11610/isij.5002

[5] Hani, Umema, Osama Sohaib, Khalid Khan, Asma Aleidi and Noman Islam. "Psychological profiling of hackers via machine learning toward sustainable cybersecurity." *Frontiers in Computer Science* 6 (2024): 1381351. https://doi.org/10.3389/fcomp.2024.1381351

[6] Fleischman, Gary M., Sean R. Valentine, Mary B. Curtis and Partha S. Mohapatra. "The influence of ethical beliefs and attitudes, norms and prior outcomes on cybersecurity investment decisions." *Business & Society* 62, no. 3 (2023): 488-529. https://doi.org/10.1177/00076503221110156

[7] Ariffin, Nor Hapiza Mohd and Ruhaila Maskat. "A proposal of ethical competence model for cyber security organization." *Indonesian Journal of Electrical Engineering and Computer Science* 24, no. 3 (2021): 1711. https://doi.org/10.11591/ijeecs.v24.i3.pp1711-1717

[8] Lourens, Melanie, Amar Prakash Dabral, Durgaprasad Gangodkar, Navjot Rathour, Cs Nagabhushanam Tida and Anupama Chadha. "Integration of AI with the Cybersecurity: A detailed Systematic review with the practical issues and challenges." In *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 1290-1295. IEEE, 2022. https://doi.org/10.1109/IC3I56241.2022.10073040

[9] Sinha, Ekta. "Integrating Human and Artificial Intelligence Within Organizations: A Conceptual Framework Based on Artistry and Scientific HR Elements." In *Managing Technology Integration for Human Resources in Industry 5.0*, pp. 48-67. IGI Global, 2023. https://doi.org/10.4018/978-1-6684-6745-9.ch004

[10] Mendes, Carlos and Tatiane Nogueira Rios. "Explainable artificial intelligence and cybersecurity: A systematic literature review." *arXiv preprint arXiv:2303.01259* (2023).

[11] Aaltola, Kirsi, Harri Ruoslahti and Jarmo Heinonen. "Desired cybersecurity skills and skills acquisition methods in the organizations." In *European Conference on Cyber Warfare and Security*, vol. 21, no. 1, pp. 1-9. 2022. https://doi.org/10.34190/eccws.21.1.293

[12] Markevych, Michal and Maurice Dawson. "A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai)." In *International conference Knowledge-based Organization*, vol. 29, no. 3, pp. 30-37. 2023. https://doi.org/10.2478/kbo-2023-0072

[13] Salovey, Peter and John D. Mayer. "Emotional intelligence." *Imagination, cognition and personality* 9, no. 3 (1990): 185-211. https://doi.org/10.2190/DUGG-P24E-52WK-6CDG

[14] Hamburg, Ileana and Kira Rosa Grosch. "Ethical aspects in cyber security." *Archives of Business Research* 5, no. 10 (2017). https://doi.org/10.14738/abr.510.3818

[15] Saxena, Parul, Shivani Sharma and Rachna Bansal Jora. "Impact of Emotional Intelligence and Artificial Intelligence on Employee Retention: A Review of the Service Industry." In *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 1, pp. 819-823. IEEE, 2023. https://doi.org/10.1109/ICACCS57279.2023.10113017

[16] Sadiku, Matthew NO, Omobayode I. Fagbohungbe and Sarhan M. Musa. "Artificial intelligence in cyber security." *International Journal of Engineering Research and Advanced Technology* 6, no. 05 (2020): 01-07. https://doi.org/10.31695/IJERAT.2020.3612

[17] González, Ariel López, Mailyn Moreno, Ariadna Claudia Moreno Román, Yahima Hadfeg Fernández and Nayma Cepero Pérez. "Ethics in Artificial Intelligence: an Approach to Cybersecurity." *Inteligencia Artificial* 27, no. 73 (2024): 38-54. https://doi.org/10.4114/intartif.vol27iss73pp38-54

[18] Nanda, Mahima and Gurpreet Randhawa. "Emotional intelligence, well-being and employee behavior: A proposed model." *Journal of Management Research* 19, no. 3 (2019): 157-172.

[19] Kumar, Manish and Harsha Kundan Patil. “Challenges And Solutions of Artificial Intelligence in Cyber Security.” (2022). https://doi.org/10.46610/RTAIA.2022.v01i02.006

[20] Kolini, Farzan and Lech J. Janczewski. "Exploring incentives and challenges for cybersecurity intelligence sharing (CIS) across organizations: A systematic review." *Communications of the Association for Information Systems* 50, no. 1 (2022): 2. https://doi.org/10.17705/1CAIS.05004

[21] Kaiser, Henry F. "The application of electronic computers to factor analysis." *Educational and psychological measurement* 20, no. 1 (1960): 141-151. https://doi.org/10.1177/001316446002000116

[22] Stevens, James. *Applied multivariate statistics for the social sciences*. Vol. 4. Mahwah, NJ: Lawrence Erlbaum Associates, 2002.

[23] Williams, Brett andrys Onsman and Ted Brown. "Exploratory factor analysis: A five-step guide for novices." *Australasian journal of paramedicine* 8 (2010): 1-13. https://doi.org/10.33151/ajp.8.3.93

[24] Kline, Rex B. "Structural equation modeling." *New York: Guilford* 33 (1998).

[25] Morshidi, Azizan, Noor Syakirah Zakaria, Mohammad Ikhram Mohammad Ridzuan, Rizal Zamani Idris, Azueryn Annatassia Dania Aqeela and Mohamad Shaukhi Mohd Radzi. "Artificial Intelligence and Islam: A Bibiliometric-Thematic Analysis and Future Research Direction." *Semarak International Journal of Machine Learning* 1, no. 1 (2024): 41-58. https://doi.org/10.37934/sijml.1.1.4158

[26] Hashim, Mohd Ekram Alhafis, Nur Safinas Albakry, Wan Azani Mustafa, Banung Grahita, Miharaini Md Ghani, Hafizul Fahri Hanafi, Suraya Md Nasir and Catherina ana Ugap. "Understanding the Impact of Animation Technology in Virtual Reality: A Systematic Literature Review." *International Journal of Computational Thinking and Data Science* 1, no. 1 (2024): 53-65. https://doi.org/10.37934/CTDS.1.1.5365