Indonesian Journal of Electrical Engineering and Computer Science
Vol. 24, No. 3, December 2021, pp. 1711~1717
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v24.i3.pp1711-1717

A proposal of ethical competence model for cyber security organization

Nor Hapiza Mohd Ariffin, Ruhaila Maskat
Faculty of Computer and Mathematical Sciences, Universiti Teknologi Mara (UiTM), Shah Alam, Malaysia

Article Info

Article history:

Received Jul 14, 2021
Revised Oct 20, 2021
Accepted Oct 27, 2021

Keywords:

Artificial intelligence
Cyber security
Emotional intelligence
Ethical competence

ABSTRACT

A proactive cyber security plan to safeguard confidential information and privacy still lacks initiatives to avoid frequent harmful attacks. Cybersecurity professionals must possess ethical competence and prove worthy of overseeing valuable information for efficient decision-making since ethical competence is fundamental for daily practice. There is a need to define what it means to be ethically competent in the era of IR4.0. The previous competence models still lack consideration of both artificial intelligence (AI) and emotional intelligence (EI) skills. AI brings new opportunities to cyber security organizations that focus on AI skills related to cognitive Intelligence or intelligent quotient (IQ). EI, which refers to emotional quotient (EQ), is a good predictor of ethical competence as it can perceive and express emotions precisely to facilitate thought to understand and manage emotions. However, practically, most cyber security organizations focused on AI skills and disregarded EI skills' roles. This research proposes a cyber artemotional model that blends AI skills and EI skills for cyber security employees. This research would benefit cyber security organizations with cyber artemotional model as employees ethical competence assessment, and it is in line with the demand of IR4.0.

Corresponding Author:

Nor Hapiza Mohd Ariffin
Faculty of Computer and Mathematical Sciences
Universiti Teknologi Mara
Shah Alam, 40450, Selangor, Malaysia
Email: hapiza@tmsk.uitm.edu.my

1. INTRODUCTION

Cyber security has come to the forefront of the political and diplomatic agenda due to the increasing risks for the fundamental functioning of societies. At the same time, it is creating the potential for economic growth through the development of new markets and industries, such as hardware and software solutions, cyber security insurance, and education and research. The pace of development of technology and trends and the multidisciplinary nature of the problem requires a comprehensive approach to developing competencies with professionals in industry and government services that go beyond traditional education and simple training for institutions and companies. Over the past few years, cyber-attacks have left no industry unscathed. For example, in the United States (US), about 78,617 business and email account compromise scams 41,058 occurred. The costs resulted in companies suffering $2.9 billion in losses from October 2013 to May 2018. Globally, cyber-crime is expected to cost the world $6 trillion per year by 2021. Damaging attacks such as NotPetya in Ukraine, which is estimated to have cost companies $1.2 billion, underscores that cybercrime is a serious concern for every industry worldwide. Information technology (IT) was the most intensely targeted industry for web application cyber-attacks in 2017; an average of 1,014 attacks occurred

each day. These frequent attacks emphasize the need to take an active approach to prevent a damaging data breach.

A deloitte report on the technology sector noted that high tech companies usually have a higher risk appetite than counterparts in other sectors. It can be concerning without proper cyber security measures, especially since some tech companies provide key infrastructure components for other organizations. With many high-tech companies exhibiting riskier practices regarding cyber security, more technology firms must implement security protocols to protect their business and clients. IR 4.0 invites tremendous advantages for companies towards business sustainability. It has nine pillars: the internet of things, big data, supply chain, cloud computing, horizontal and vertical integration, autonomous robot, additive manufacturing, cyber security, simulation, and augmented reality. However, the major challenge facing this digitalization era is cyber security [1], [2].

Cyber security is moving towards a more holistic focus, considering its environment and a more human dimension. Above all, it is becoming more proactive. Rather than waiting for a cyber-attack to happen, the key is prediction and prevention. Now, artificial intelligence (AI) comes into the picture, and it can be used to detect patterns in the data and take action when alerts arise. Privacy and security of the data will always be the top security measures that cyber security organizations should take. Lack of monitoring and protection against unauthorized changes or alterations will create unwanted changes in data information. Moreover, most companies face a preliminary development phase [3], thus limiting the risk of application-related assaults or attacks.

2. LITERATURE REVIEW

Ethics is a very subjective concept, but it depends on one thing, choice. An individual chooses to do the right thing even if other options benefit them. As a society, we have an unconscious expectation from others in society to behave a certain way. Therefore, it keeps the social fibre of the community together and promotes a deeper sense of harmony. Ethical refers to a science or study of morals, ethical principles and decision-making skills [4].

Meanwhile, ethical competence is closely associated with the concept of emotional competence, which determines how well we handle ourselves and each other [5]. At its root, ethical competence resides in the human quest for knowledge and action that defines right and wrong behaviour, the touchstone of ethics. Thus, an ethically competent person is one who, through innate or learned behaviour, can distinguish between right and wrong and act accordingly [6].

This study aims to construct an ethical competence Model for cyber security organizations. The terms competency and competence are used similarly to describe the ability to do something successfully or effectively. Nonetheless, we can differentiate it as competency is "an important skill that is needed to do a job"." In contrast, competence is "the ability to do something well". Another similar word related is competencies, which are statements about the knowledge and skills required for success (competence) in a work or professional role [7]. From a business view of points, competence indicates sufficiency of knowledge and skills that enable someone to act in a wide variety of situations. Table 1 shows the difference between competence and competency [8].

In a cyber-security organization, ethical competence is a fundamental qualification or capacity that cyber security professionals need in daily practice to identify the ethical dimensions inherent in their decision-making. Cyber security professionals must behave ethically and prove to their managers that they are worthy of overseeing valuable information that is, in reality, laidback to practical due to lack of regulation [8]. Conversely, there is a cyber security competency model designed to represent the competencies needed by individuals whose activities impact the security of their organization's cyberspace [9]. The model is depicted as a pyramid consisting of five tiers divided into two categories of competencies: foundation competencies and industry-specific competencies. The foundational competencies, which comprises Tier 1 through 3, represents the "soft-skills" and work readiness skills that most employers demand, and each tier covers a different group of competencies. For Tier 1, one of the components is integrity which refers to displaying strong moral principles and work ethic. Therefore, it exposed that ethics was one of the elements considered important in a cyber security organization.

Table 1. Differences between competence and competency

Competence	Competency
Skill-based	Behaviour-based
Standard attained	Manner behaviour
What is measured	How the standard is achieved

3. EMOTIONAL INTELLIGENCE (EI) AS A NEW SKILL IN CYBER SECURITY ORGANIZATION

According to an article [10], emotional intelligence (EI) ranked in the top 10 most in-demand skills necessary to thrive in 2020 by the World Economic Forum. It is expected that there will be a greater bidding war for employees with social abilities, including persuasion and emotional intelligence, due to the new demand for interpersonal skills involving the ability to communicate and build relationships with others or otherwise called "people skills". Currently, most organizational models in cyber security organizations focus on technical skills such as numerical, scientific and technological, which is limited to programming or equipment operation and control. Moreover, the application of artificial intelligence (AI) is bringing new opportunities and greater efficiencies to cyber security organizations that solely focus on AI skills related to cognitive intelligence or IQ. Examples of AI skills are programming languages, linear algebra, calculus, statistics, signal processing techniques, applied math algorithms and neural network architectures [11]. However, as AI and automation accelerate, emotional intelligence (EI) is becoming a must-have skill. Due to a recent report from the Capgemini Research Institute that stated, EI is an essential skill for the age of AI. Therefore, EI will be a must-have skill in the future, with demand likely to rise six-fold within the next five years, with 74% of executives believing that EI will become a "must-have" skill [9]. The research concludes that companies need to embed EI into their various practices and take bottom-up and top-down approaches to build a high EI workforce through modifications to existing processes. Organizations will also need to create a culture that values EI and strives for continuous improvement. It highlights four key areas on which organizations should focus to build a more emotionally intelligent workforce:

- Customize existing learning programs to integrate EI and make them accessible to all
- Modify recruitment processes to include the evaluation of EI
- Apply an EI lens when promoting and rewarding talent
- Use technology and data for building a high EI culture

Furthermore, AI comes closest to human society since it is a replication of the human mind. Intelligent devices have become an integral part of our lives and hence need to adhere to the principles that hold society together. For businesses to invest in AI, they would need to trust it. IBM's Watson is a great example of an ethical AI that targets firms that want to use AI to help them work. Privacy, transparency, and accountability are very important for any business to indulge in technology. Emotional intelligence will be increasingly significant as automation, and artificial intelligence replaces all or part of many jobs. Humans in the workplace become increasingly differentiated by their unique human characteristics and skills [12]. We need to nurture human assets and consider how skills and competencies such as emotional intelligence, management, leadership, operating culture, skills and processes work individually and together to generate value. EI involves two critical abilities. First, it consists of the ability to recognize, understand, and control our own emotions. Second, it includes the ability to identify, understand, and influence others' emotions. Those that will emerge on top in the age of AI will almost certainly score high in terms of EI [13]. Harvard business review (HBR) explains, ″those that want to stay relevant in their professions will need to focus on skills and capabilities that artificial intelligence has trouble replicating — understanding, motivating, and interacting with human beings". Therefore, it can be concluded that there is a need for EI skills which indicates the importance of blending AI skills and EI skills for employees' competencies in cyber security organizations.

Intelligence refers to the unique human mental ability to handle and reason information, while intelligent quotient (IQ) refers to cognitive intelligence. IQ is the intelligence that people are generally most familiar with, as it is the type that is most often referred to when the word "intelligence" is used. It is also the type most often measured through testing and estimated through grade-point averages [9]. On the other hand, cognitive intelligence is an important part of AI that encompasses the technologies and tools that allow our apps, websites and bots to see, hear, speak, understand and interpret a user's needs in a natural way [14]. Therefore, we can conclude that IQ or cognitive intelligence is a subset of AI. In other words, we can refer to IQ as part of AI. The Encyclopedia Britannica defines the concept of AI as "the ability of a digital computer or computer-controlled robots to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from experience". The problem with the term artificial is that it gives the connotations of a lack of authenticity, robotic-like and unnatural when it aims to be quite the opposite.

To summarize this rather lengthy explanation in fewer words, one could simply describe AI as creating a computer that can solve complex problems as a human would. As an application, it allows machines to learn their users' language so that they don't have to learn the language of machines. AI is a much wider concept that includes technology and innovations such as robotics, machine learning, deep learning, neural networks, and natural language processing (NLP). Additionally, AI is closely linked to the

four pillars of innovation and digital transformation: cloud computing, mobility, social analytics and big data as it powers some of the main accelerators of this transformation; including cloud computing, cognitive systems, the internet of things (IoT), cyber security and big data technologies. As AI gradually seeps into more industries, its need for an emotional quotient (EQ) becomes more pronounced. Monitoring artificial intelligence by setting an ethical framework is the way forward [15].

On the other hand, being emotionally intelligent requires us to pay attention to what we are thinking and feeling (self-awareness) and direct our attention to what others may be thinking and feeling (empathy). The evidence is strong that a high level of EI is a key differentiator in many successful people. A framework of EI be built by describing some specific competencies:

- Self-awareness: Knowing your emotions, your competencies, your capacity, what you are thinking, and how you can listen to the signals your body is sending.
- Self-management: Emotional self-control, adaptability, achievement & positive outlook.
- Social awareness: Empathy & organizational awareness.
- Relationship management: Inspiring leadership, influence, conflict management, teamwork and collaboration.

Table 2 shows the differences between EI/EQ and IQ in skills or capabilities [16]. The benefits of IQ capabilities are well known and relatively obvious. It has helped people achieve practical goals through linear thinking and execution. In contrast, the benefits of the EI/EQ capabilities are less well known and more difficult to measure because they are holistic skills that cannot be easily quantified.

Meanwhile, Peter Salovey and John D. Mayer, in their influential article "emotional intelligence," defined EI as the subset of social intelligence [17]. Later, Daniel Goleman's book on EI described that to be successful, EI/EQ is more important than traditional IQ measures [18]. According to [19], based on her almost three decades of research, EI results from the interaction of intelligence and emotion and can be defined as "the ability to carry out accurate reasoning about emotions and the ability to use emotions and emotional knowledge to enhance thought". It is also referring to an individual's capacity to understand and manage emotions [20]. EI impacts many aspects of our daily lives, such as how people behave and interact with their colleagues, customers, seniors, and family. EI/EQ matters more than our Intellectual ability (IQ) to effectively deal with these stakeholders as it helps build stronger relationships, achieve career goals, and succeed at work. A study by [21] explored how EI and cognitive intelligence positively affect performance and social interactions. While IQ is a strong predictor of success, they found that EI/EQ also contributes. Furthermore, EI/EQ is a significant factor in social interactions, while IQ does not have many roles in social life. Thus, from the previous study discussed, it can be concluded that AI can be referred to as cognitive Intelligence or IQ. Hence, there is a relationship between AI and EI. Therefore, blending AI skills and EI skills for an ethical competence framework for an organization can be a suitable approach.

Table 2. Differences between EI/EQ and IQ

EI/EQ	IQ
Self-awareness	Logic thinking
Self Management	Mathematical reasoning
Responsible Decision Making	Spatial reasoning
Relationship skills	Verbal reasoning
Social Awareness	Memory and recall

4. DEVELOPMENT OF ETHICAL COMPETENCE MODEL

The new ethics measures are grounded in the age-old concept of ethics, which is the study of human conduct, emphasizing right and wrong. They have been the gold standard for human behaviour for millennia. But their application in modern economic industrialized society has been twisted and tangled in pursuit of another less noble principle—expediency: grasping for advantage rather than for what is right [21]. Hence, the ethical rules of the past acquire a new and urgent prominence in the present, especially in the era of IR4.0. We are challenged as individuals, organizations and society to become ethically competent. To be competent means having an ability in sufficient measure that one can perform at an acceptable standard. Thus, there is a need to define what it means to be ethically competent in the era of IR4.0.

Based on Goleman's study towards EI, he mentioned that the concept of ethical intelligence gives rise to ethical competence beyond showing how EI determines success in the workplace and society [4]. Additionally, Goleman defined emotional competence as ″a learned capability based on EI that results in an outstanding performance at work". Though difficult to measure, Goleman suggested that EI is observable as the quality that distinguishes successful performance beyond training and expertise and high cognitive intelligence as measured by IQ tests. An ethical competence framework builds on the emotional competence

framework presented by Goleman in Working with EI. The ethical competence framework incorporates three dimensions of competence, beginning with the personal and moving through social competence to global competence. Each dimension of the ethical competence framework is further divided into descriptive components that generate in total 30 items that are grouped into the ethical competence scale. By assigning values from 1 to 10 for each of the 30 items, a score can be obtained, which, expressed as a percentage, becomes the ethical quotient (EthQ), following the tradition of expressing cognitive intelligence as the Intelligence quotient or IQ.

However, no claim is made that the ethical quotient is an accurate or distinguishing measure between individuals or organizations on their level of ethical competence. Furthermore, based on another ethical competence framework from previous studies, Table 3 shows the description of AI and EI elements consisting in the framework [22]-[24]. Therefore, the previous study and Table 3 showed a lack of an ethical competence model or framework that blends AI and EI skills. This situation becomes a big challenge to cyber security organizations whose emphasis is on AI skills if they intend to implement ethical competence for their cyber ethics purposes. Hence, this proposed project is to construct an ethical competence for cyber security employees or potential employees using a new model proposed as cyber artemotional model. Furthermore, based on the previous ethical competence model, it can be divided into three components which are knowledge, skills and attitudes [23], [25]-[28]. Therefore, Figure 1 shows the proposed ethical competence model for cyber security organizations, namely as cyber artemotional model.

Table 3. Research on ethical competence framework

Researchers	Ethical Competence Framework Elements	AI elements	EI elements
Maesschalck and Schrijver [22]	Rule abidance Moral sensitivity Moral Moral motivation Moral reasoning	NO	YES
Pohling *et al.* [23]	Empathy Personal values Five-factor model for Personality	NO	YES
Kulju *et al.* [24]	Character Strength Ethical awareness Moral Judgment Skills Willingness to do Good	NO	YES

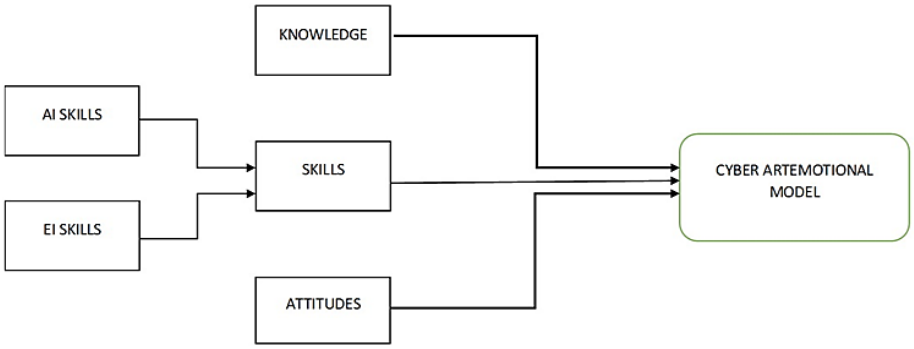


Figure 1. Cyber artemotional model

5. CONCLUSION

The urge for more attention towards people skills such as EI has come into debate and research recently. In 2020, a study revealed that EI is a good predictor of ethical competence. It is the competency to perceive and express emotions precisely to facilitate thought to understand and manage emotions. As AI is referred to as cognitive Intelligence or IQ, it showed a relationship between AI and EI. Thus, blending AI skills and EI skills for an ethical competence framework for an organization can be a suitable approach. However, there is a lack of an ethical competence model or framework that blends AI and EI skills. This situation becomes a big challenge to cyber security organizations that emphasize AI skills if they intend to implement ethical competence for their cyber ethics purposes. In addition, most cyber security organizations focused on AI skills and disregarded EI skills. Many overlooked the roles of EI skills, which are about personal ethical competencies and abilities. To date, there is a lack of any model that includes EI skills and

AI skills as an assessment for ethical competence in cyber security organizations. It showed that the concept of ethical competence has still not been sufficiently researched in the cyber security organization context. Therefore, there is a need for studies on modelling the blends of AI and EI skills for the cyber security organization's ethical competence model. Furthermore, cyber artemotional model is a proposed model for the ethical competence of employees in the cyber organization, particularly for assessment tools. It will be a novel theory that provides good material as a guideline and references to cyber security organizations, government, IR4.0 consultants, and local and international academicians.

REFERENCES

[1] J. Lee, B. Bagheri, and C. Jin, "Introduction to cyber manufacturing," *Manufacturing Letters*, vol. 8, pp. 11-15, 2016, doi: 10.1016/j.mfglet.2016.05.002.

[2] M. A. Mokhtar and N. Noordin, "An exploratory study of industry 4.0 in Malaysia: a case study of higher education institution in Malaysia," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 2, pp. 978-978, 2019, doi: 10.11591/ijeecs.v16.i2.pp978-987.

[3] I. Yaqoob *et al.,* "The rise of ransomware and emerging security challenges in the Internet of Things," *Computer Networks: The International Journal of Computer and Telecommunications Networking,* vol. 129, pp. 444-458, 2017, doi: 10.1016/j.comnet.2017.09.003.

[4] D. Goleman, "Emotional Intelligence: Why it can matter more than IQ," *London, UK: Bloomsbury Publishing*, 2020.

[5] M. Issah, "Change leadership: The role of emotional intelligence," SAGE Open, vol. 8, no. 3, 2018, doi: 10.1177/2158244018800910.

[6] A. Farazmand, "Global Encyclopedia of Public Administration, Public Policy, and Governance," *AG, Switzerland: Springer International Publishing,* 2019, doi: 10.1007/978-3-319-20928-9.

[7] R. Moghabghab, A. Tong, A. Hallaran, and J. Anderson, "The Difference between Competency and Competence: A Regulatory Perspective," *Journal of Nursing Regulation*, vol. 9, no. 2, pp. 54-59, 2018, doi: 10.1016/S2155-8256(18)30118-2.

[8] S. Sanghi, "Developing competency models," *The Handbook of Competency Mapping: Understanding, Designing and Implementing Competency Models in Organizations*, pp. 20-41, 2007, doi: 10.4135/9788132108481.n2.

[9] C. Creed and R. Beale, "Emotional intelligence: Giving computers effective emotional skills to aid interaction," *Studies in Computational Intelligence*, pp. 185-230, 2008, doi: 10.1007/978-3-540-78293-3_5.

[10] J. Hess and A. Bacigalupo, "Applying emotional intelligence skills to leadership and decision making in non-profit organizations," *Administrative Sciences,* vol. 3, no. 4, pp. 202-k220, 2013, doi: 10.3390/admsci3040202.

[11] J. C. G. Salamanca, O. L. Agudelo, and J. Salinas, "Key competences, education for Sustainable Development and strategies for the development of 21st Century skills. A systematic literature review," *Sustainability*, vol. 12, no. 24, 2020, doi: 10.3390/su122410366.

[12] M. A. Rahim, C. Psenicka, P. Polychroniou, and J.-H. Zhao, "A model of Emotional Intelligence and Conflict Management Strategies: A study in seven countries," *SSRN Electronic Journal*, vol. 10, no. 3, 2003, doi: 10.2139/ssrn.429760.

[13] A. A. Behbahani, "A comparative study of the relation between emotional intelligence and employee's performance," *Procedia - Social and Behavioral Sciences*, vol. 30, pp. 386-389, 2011, doi: 10.1016/j.sbspro.2011.10.076.

[14] K. Ramchandran, D. Tranel, K. Duster, and N. L. Denburg, "The role of emotional vs. Cognitive Intelligence in economic decision-making amongst older adults," *Frontiers in Neuroscience*, vol. 14, 2020, doi: 10.3389/fnins.2020.00497.

[15] V. Dignum, "Ethics in artificial intelligence: Introduction to the special issue," *Ethics and Information Technology*, vol. 20, no. 1, pp. 1-3, 2018, doi: 10.1007/s10676-018-9450-z.

[16] C. MacCann, "Further examination of Emotional Intelligence as a standard intelligence: A latent variable analysis of fluid intelligence, crystallized intelligence, and emotional intelligence," *Personality and Individual Differences,* vol. 49, no. 5, pp. 490-496, 2010, doi: 10.1016/j.paid.2010.05.010.

[17] J. D. Mayer, R. D. Roberts, and S. G. Barsade, "Human Abilities: Emotional Intelligence," *Annual Review of Psychology*, vol. 59, no. 1, pp. 507-536, 2008, doi: 10.1146/annurev.psych.59.103006.093646.

[18] W. Pan, T. Wang, X. Wang, G. Hitchman, L. Wang, and A. Chen, "Identifying the core components of emotional intelligence: Evidence from amplitude of low-frequency fluctuations during resting state," *PLoS ONE*, vol. 9, no. 10, 2014, doi: 10.1371/journal.pone.0111435.

[19] A. Lawton, "Ethics in public policy and management: a global research companion," London: *Routledge*, 2016, doi: 10.4324/9781315856865.

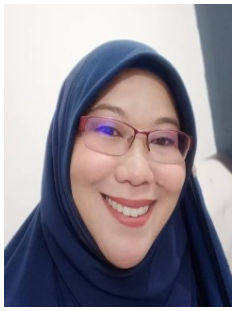
[20] L. J. Song, G.-Hua Huang, K. Z. Peng, K. S. Law, C.-S. Wong, and Z. Chen, "The differential effects of general mental ability and emotional intelligence on academic performance and social interactions," *Intelligence*, vol. 38, no. 1, pp. 137-143, 2010, doi: 10.1016/j.intell.2009.09.003.

[21] J. B. Butts and K. L. Rich, "Nursing ethics: across the curriculum and into practice," *Burlington, MA, Canada: Jones & Bartlett Learning*, 2020.

[22] J. Maesschalck and A. D. Schrijver, "Researching and Improving the Effectiveness of Ethics Training," *Ethics in Public Policy and Management*, pp. 197-211, 2015, doi: 10.4324/9781315856865-12.

[23] R. Pohling, D. Bzdok, M. Eigenstetter, S. Stumpf, and A. Strobel, "What is Ethical Competence? The Role of Empathy, Personal Values, and the Five-Factor Model of Personality in Ethical Decision-Making," *Journal of Business Eth*ics, vol. 137, no. 3, pp. 449-474, 2015, doi: 10.1007/s10551-015-2569-5.
[24] K. Kulju, M. Stolt, R. Suhonen, and H. Leino-Kilpi, "Ethical competence," *Nursing Ethics*, vol. 23, no. 4, pp. 401-412, 2015, doi: 10.1177/0969733014567025.
[25] M. A. Hogg and G. M. Vaughan, "Social psychology," *Harlow, England: Pearson*, 2018.
[26] C. Guo, N. Peng, and L. Wu, "Research on the Construction of Ethical Competence Model of Corporate Top Manager," *Proceedings of the Third International Conference on Economic and Business Management (FEBM 2018),* 2018, doi: 10.2991/febm-18.2018.64.
[27] S. Berhil, H. Benlahmar, and N. Labani, "A review paper on Artificial Intelligence at the service of Human Resources Management," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 1, pp. 32-40, 2020, doi: 10.11591/ijeecs.v18.i1.pp32-40.
[28] F. S. Jamaludin and R. K. Ramasamy, "Systematic review on event prediction models," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 19, no. 3, pp. 1490-1496, 2020, doi: 10.11591/ijeecs.v19.i3.pp1490-1496.

BIOGRAPHIES OF AUTHORS



Dr. Nor Hapiza Mohd Ariffin received her BSc Hons in Computer Science (1994), MSc in Information Technology (IT) (2001) and PhD in Information System (2010). Her research interests include Strategic Relationship Management (CRM), Strategic Information System Planning (SISP), Human Capital, Spiritual Information systems, Online Distant Learning and Blockchain. She is currently working as Senior Lecturer in UiTM Malaysia since 1995.
Email: hapiza@tmsk.uitm.edu.my

Dr. Ruhaila Maskat is an academician at the Universiti Teknologi MARA Shah Alam Malaysia. She received her PhD in Computer Science from the University of Manchester, United Kingdom. Her research interest includes data science, text analytics, dataspaces and databases. Email: ruhaila@tmsk.uitm.edu.my