© Universiti Tun Hussein Onn Malaysia Publisher's Office

IJSCET

http://publisher.uthm.edu.my/ojs/index.php/ijscet

ISSN : 2180-3242 e-ISSN : 2600-7959

International Journal of Sustainable Construction Engineering and Technology

Mediating Role of Organizational Learning in the Relationship between Use of Artificial Intelligence Security Technology and Community Security

Amna Ali Abdulla Mohammed Almakki Alhajeri[1,2], Edie Ezwan Mohd Safian[1*]

[1]Faculty of Technology Management and Business,
Universiti Tun Hussein Onn Malaysia, MALAYSIA

[2]Ministry of Interior, UNITED ARAB EMIRATES

*Corresponding Author

DOI: https://doi.org/10.30880/ijscet.2023.14.03.012
Received 27 August 2023; Accepted 27 August 2023; Available online 21 September 2023

Abstract: This study focuses on developing a robust model to augment community security through the implementation of AI, while simultaneously investigating the mediating influence of organizational learning within the context of vital AI factors in the UAE. The model examines the interplay among key AI elements, such as compatibility (COMPAT), complexity (COMPLEX), management support (MS), ethics (ETH), and staff capabilities (SC), concerning their impact on the effectiveness of Community Security (ESC). Data collection was conducted via a questionnaire survey utilizing the Abu Dhabi Police as a representative case study for public organizations in the UAE, involving 138 participants spanning both managerial and operational roles, with responses acquired through randomized distribution using online tools. The amassed data was employed to construct the model using SmartPLS software, and its evaluation adhered to assessment criteria encompassing measurement and structural components. A goodness-of-fit score of 0.751 indicated a high level of overall predictive performance for the model. The study's findings revealed that organizational learning (OL) serves as a partial mediator in the relationship between the complexity construct (COMPLEX) and the effectiveness of Community Security (ESC), with no observed mediation effects in other relationships. The research outcomes culminated in the creation of a versatile model that enhances community security through AI technology, applicable across diverse scenarios, and benefiting individuals invested in AI and community security, such as academics, researchers, and practitioners. The study's methodology provides valuable insights for practitioners and researchers in the UAE and related fields, affording opportunities for replication or adaptation to suit specific investigative contexts.

Keywords: Mediation role, use of AI security technology

1. Introduction

Artificial intelligence (AI) plays a pivotal role in security intelligent systems, making it a central focus with profound societal implications, particularly for enhancing community security in the coming decades (Jia et al., 2019; Injadat et al., 2021). AI is a versatile, general-purpose technology (Vannuccini & Prytkova, 2021) capable of addressing diverse challenges across various application contexts. Its core capabilities hold the potential to integrate community-focused research into processes, essential for fostering positive advancements in security and interventions for community security (Klinger et al., 2018). AI not only improves efficiency but also has the potential to detect and deter security interventions that go beyond enhancement (Simon, 2019). Implementing AI in security intervention settings, however,

*Corresponding author: edie@uthm.edu.my

requires researchers to consider a broad spectrum of challenges, including those related to community security (Klinger et al., 2018). Artificial Intelligence differs from human responses, lacking judgment, intention, and contemplation. It's defined as machines consistently responding to stimuli, holding significance in national security (Hurley, 2018). AI processes vast surveillance data adaptively and intelligently, while human analysts discern patterns and identify suspicious activities, ultimately enhancing community security (Acemoglu & Restrepo, 2019).

Artificial intelligence is not a mere futuristic concept; it's actively being integrated into various fields, including security intelligence systems, with a focus on detecting and deterring security interventions to enhance community security (Bryson & Winfield, 2017). AI's impact on the world poses significant challenges and opportunities, demanding continuous investigation into critical factors that could weaken the effectiveness of AI security technologies (Carter & Nielsen, 2017). In essence, ongoing research is necessary to identify the key elements facilitating the optimal use of these security technologies for the benefit of community security. The centrality of artificial intelligence in shaping perspectives and confronting critical challenges within security intelligence systems is crucial for enhancing community security (Ramos, 2007). While AI systems possess decision-making capabilities (Klinger et al., 2018), emphasizing critical factors is essential to maximize the effective utilization of these AI security technologies. Despite the many benefits of security technologies, concerns arise in AI networks, including potential technology abuse due to flaws in IA security tools (Pan, 2016). Users might also face dissatisfaction, as malicious programs used by criminals can diminish the efficiency of AI systems' communication channels and technologies, making it harder for hackers to breach data (Pesapane et al., 2018). Addressing these concerns with AI security technology is vital for the overall security of the community, particularly regarding technology use (Abubakar, 2019).

Numerous challenges confront Artificial Intelligence in its role in maintaining community security and effective policing of its impacts. The success of AI in this field hinges on the collaboration of researchers and scientists who contribute perspectives and identify critical factors in security intelligent systems (Quiggin, 2007). Research focused on AI security technologies is imperative, demanding careful attention from researchers. This study seeks to delve into the perspectives surrounding the challenges faced in exploring security intelligent systems. Its primary objective is to uncover the key factors that enhance the effective utilization of AI security technologies to enhance community security. Consequently, this research aims to scrutinize the critical aspects of AI security systems, leading to recommendations for optimizing the utilization of these technologies to bolster community security. Previous literature has highlighted essential factors and challenges in security technologies, encompassing aspects such as standardization, interoperability, data management, trust, identity, confidentiality, integrity, availability, security, and privacy, all of which are critical in various IoT applications (Mohanta et al., 2020). Nonetheless, much of the existing literature lacks empirical evidence to pinpoint which factors are most crucial for community security in the context of AI security technologies.

People from around the world, including tourists and expats, find the United Arab Emirates, particularly Dubai and Abu Dhabi, appealing due to luxurious accommodations, expansive shopping malls, pleasant climate, and the strong emphasis on protection and security. The country experiences relatively low rates of traditional crimes like burglaries and robberies, with outdated security measures contributing to a significant portion of serious offenses. However, the UAE faces challenges in the form of increasing cybercrime, evidenced by a 300% rise in computer hacking incidents in a six-month period in 2014, making it vulnerable to hacker attacks. This underscores the importance of leveraging AI technologies to bolster community security (Ammar et al., 2012). The use of AI security technologies plays a crucial role in enhancing community security, helping anticipate issues and making decisions that typically require human expertise (Haider et al., 2020; Zuiderveen Borgesius, 2018). In line with this, the UAE government introduced the "UAE Strategy for Artificial Intelligence (AI)" in 2017, heralding a future driven by technology and aiming to achieve the UAE Centennial 2071 objectives. These efforts aim to improve government performance, establish a robust digital communication infrastructure for addressing problems effectively, and position the UAE as a leader in AI investments across various sectors, including community security (Ahmed et al., 2017).

The UAE government strongly backs the integration of AI technologies across all sectors, aligning with the Vision 2030 plan for full automation by 2030 (UAE 2031, 2018). AI security technologies are pivotal in achieving this goal by ensuring community security. Despite this, the essential determinants of AI technology effectiveness within the UAE context remain unexplored. Thus, the present research aims to fill this gap by specifically identifying these crucial factors within the realm of AI security technologies and their impact on community security in the UAE. This study intends to conduct a comprehensive investigation, highlighting the key factors influencing the success or failure of AI security technologies, particularly within the UAE, with insights gleaned from professionals actively involved in AI security technology.

2. Literature Review

2.1 Use of Artificial Intelligence Security Technology

The technological context encompasses all technologies relevant to the firm, both internal and external, and investigates their impact on technology adoption (Tornatzky & Fleischer, 1990). As highlighted by Collins et al. (1988), the current internal technology within the firm plays a pivotal role in defining the limits of the firm's capacity to handle technological change. Similarly, an external technology not yet present within the firm can be characterized in terms of the capabilities required by the firm to enhance the likelihood of adoption. External technologies, as identified by Hage (1980) and Tushman and Nadler (1986), introduce incremental, synthetic, or discontinuous changes, each of which places distinct demands on the organization's capabilities. Incremental changes entail the lowest level of disruption and risk, involving the addition of new functionality or a new version of existing technology. Synthetic change, on the other hand, involves the amalgamation of existing technology and ideas to drive change, carrying a higher level of risk compared to incremental change. Lastly, discontinuous change represents the most significant and risky type of transition, describing scenarios where new product and process development have occurred.

2.1.1 Compatibility

The compatibility factor highlights the significance of technology aligning with an organization's existing workflow, along with softer aspects such as values and norms. It is defined as the "degree to which an innovation is perceived as consistent with existing values, cultural norms, experiences, and needs of potential users" (Rogers 2003). While compatibility can encompass a range of elements, this study specifically examined the alignment of AI security technologies with employee needs and skills. Therefore, it is postulated that the Compatibility of Artificial Intelligence security technologies has a positive impact on the effectiveness of community security.

2.1.2 Complexity

Complexity is characterized as the "degree to which innovation is perceived as somewhat difficult to comprehend and apply" (Rogers, 2003). This attribute is believed to negatively impact the adoption of innovation, as more intricate technologies require personnel to acquire new skills and knowledge (Tidd & Bessant, 2009). AI should be recognized as a complex technology (Alsheibani et al. 2020); however, different AI applications may vary in complexity, making it a critical factor that could impede the adoption of AI security technologies. Hence, it is hypothesized that a low level of complexity in Artificial Intelligence security technologies has a positive impact on the effectiveness of community security

2.1.3 Ethics of Artificial Intelligence

According to Sun et al. (2018), prior TOE research has had limited coverage of critical concerns such as security, privacy, and ethics, although this trend is changing. While Sun et al. (2018) argued for placing ethical considerations within an environmental framework, Mittelstadt (2019) demonstrates that ethics should be viewed as integral organizational processes. Although AI ethics encompasses a wide range of subjects, this study narrows its focus to three aspects of the black box dilemma: bias, integrity, and transparency. The study aims to restrict the examination of these factors to how the organization operates in relation to them, thereby embedding the component of AI ethics within the organizational context. This encompasses how employees interact with data and processes to address the ethical challenges presented by these facets. The potential for biases in pre-trained datasets for existing language models (Sahlgren & Olsson, 2019) underscores the significance of preventing these biases from leading to discrimination against citizens, especially for authorities. Therefore, ethics plays a pivotal role in enhancing the effective use of AI technologies for community security improvement. Consequently, it is hypothesized that the Ethics of Artificial Intelligence security technologies has a positive impact on the effectiveness of community security.

2.1.4 Staff Capability

As per Scaccia et al. (2015), staff capability encompasses the general abilities, education, and competence possessed by the workforce. Having individuals with the requisite knowledge and skills is crucial for the successful implementation of innovations. It is advisable that individuals with programming proficiency in languages conducive to AI development and a solid understanding of the organization work on AI-related projects (Pumplun et al., 2019). Given the growing demand for programmers in the job market, companies may encounter difficulties in attracting personnel with the necessary skills. Additionally, research indicates that organizations often prioritize technology over the essential expertise and implementation methods (Alsheibani et al., 2018). Consequently, the skills and capabilities of the staff play a significant role in optimizing the use of AI to bolster community security. Thus, it is hypothesized that the staff's capability in Artificial Intelligence security technologies has a positive impact on the effectiveness of community security.

2.1.5 Management Support

According to Scaccia et al. (2015), management support is characterized as the extent to which authoritative figures articulate and endorse organizational operations. Often referred to as top management support, it stands as a frequently mentioned component in the TOE (Technology, Organization, and Environment) literature (Alsheibani et al. 2020). Key metrics highlighted for the deployment of new technologies, such as AI or cloud-based computing, include the presence of a manager with a favourable attitude toward change (Yang et al. 2015), a sound understanding of the technology

(Pumplun et al. 2019), and active participation in the project, all considered vital aspects in grasping the concept of management support. Furthermore, Alsheibani et al. (2018) emphasize that a lack of management support not only affects an organization's competitive position but also increases the likelihood of new technology adoption failures. Therefore, top management support is pivotal in enhancing the effectiveness of AI security technologies, particularly in augmenting community security. Therefore, it is can be hypothesised that Management support for Artificial Intelligence security technologies positively affect the effectiveness of community security.

2.2 Artificial Intelligence and Organizational Learning

Organizations fostering a culture of organizational learning can expect improved employee proficiency in utilizing current technological advancements, including artificial intelligence (Terziyan et al., 2018; Dalenogare et al., 2018). However, there remains substantial uncertainty surrounding the impact of Technology 4.0 on sociocultural aspects, such as the integration of organizational learning among employees. Previous research has indicated that improper implementation or inadequate integration of Industry 4.0 technology can negatively influence organizational practices and employee behaviour, potentially impacting the future adoption of technology within the organization (Shamim et al., 2016). Therefore, the variable of organizational learning has the potential to either facilitate or hinder technology adoption within the organization, significantly influencing the relationship between IT technologies and community security.

The organizational context encompasses internal elements that influence the adoption of technology, including resources and organizational characteristics that can either facilitate or impede effective technology utilization (Aboelmaged 2014). Depending on the type of organization, the framework can incorporate various theoretical approaches. As demonstrated by Karahanna et al. (1999), work networks play a significant role in shaping subjective norms among individuals within an organization both before and after the adoption of technology. Similarly, Rogers (2015) identifies this as a component of the social system, a pivotal factor in disseminating new ideas. Rogers highlight’s structure, opinion leadership, and the type of innovation-decision as key areas within the social system. Establishing and maintaining internal linking processes in such social systems, transcending boundaries, and connecting distinct units, can enhance technology utilization (Tushman and Nadler 1986). According to Weyer et al. (2015), the anticipated technology-driven, highly automated movement resulting from current technological breakthroughs will not lead to reduced human interaction or completely workerless production facilities. However, Dworschak and Zaiser (2014) as well as Beneová and Tupa (2017) emphasize that advanced technology such as artificial intelligence in the context of the Fourth Industrial Revolution 4.0 will likely demand specific skills and knowledge for successful adoption in the 4.0 era. Furthermore, the inherent complexity of artificial intelligence within the Industry4.0 technological era may drive the enhancement of particular learning capabilities within organizations (Schuh et al., 2015), suggesting a synergistic relationship with the development of organizational learning (Faller & Feldmüller, 2015).

Indeed, certain research streams indicate that the level of organizational learning development is directly related to an organization’s process design and workplace management, supporting the assumption of a positive relationship between current advanced technologies and organizational learning (Beneová & Tupa, 2017). Furthermore, as current technological advancements, such as artificial intelligence, enable a faster and clearer understanding of the status quo of products, processes, and services within a company or throughout the value chain (Terziyan et al., 2018), organizations that foster organizational learning development can expect their learning and information sharing to be catalysed by these technologies (Fang et al., 2016; Dalenogare et al., 2018).

However, there remains uncertainty about Industry 4.0 technology's interaction with sociocultural elements, such as organizational learning growth. Previous research suggests that misinterpretation or insufficient integration of Industry 4.0 technologies could negatively impact organizational routines and human habits, potentially impeding future digital automation projects (Erol et al., 2016; Shamim et al., 2016; Hecklau et al., 2016). Similar impacts were observed during the Computer-Integrated Manufacturing period (Tamás et al., 2016). Furthermore, Pirvu et al. (2015) argue that companies choosing to participate in the Fourth Industrial Revolution and utilizing advanced technologies like artificial intelligence must revisit, adapt, and update their communication and information sharing processes to align with the implications of such technologies. However, the absence of organizational tools and methodologies that integrate these technologies into conventional organizational learning processes may negatively affect operational performance (Mittal et al., 2018). Consequently, misalignment with current organizational learning skills may undermine the successful adoption of artificial intelligence and other advanced technologies, leading to resistance and undermining envisioned benefits.

2.3 Artificial Intelligence Enhanced Community Security

Cities are rapidly adopting AI technologies for public safety and defence purposes, with a projected full reliance on these technologies by 2030 in North American cities. Implementations include surveillance cameras detecting potential crimes, drones, and predictive policing apps, offering advantages and disadvantages that require earning public trust. While concerns about AI-assisted policing becoming intrusive exist, the potential for focused, necessity-driven usage exists, with AI's ability to reduce human bias under proper implementation (Srivastava et al., 2017). AI analytics show promise in detecting white-collar crimes, such as credit card fraud, impacting cybersecurity, and aiding commanders in resource allocation. Although not fully automated yet, AI advancements, especially in machine and transfer learning, could enable more feasible automation. Cameras play a greater role in crime investigation than prevention, but AI's progress could enhance incident classification and video analysis, leading to more significant surveillance. Drones are already utilized for surveillance in various cities, likely expanding to maintain security in key areas, raising concerns about privacy and safety (Srivastava et al., 2017).

Predictive policing, a technique pioneered by the New York Police Department, is already in use by many police forces. Machine learning enhances the ability to forecast where and when crimes are likely to happen, as well as identifying potential perpetrators. The strategic deployment of AI prediction tools could mitigate human bias, aiming to ensure a positive impact. AI can be utilized to create intelligent simulations for training law enforcement officers in effective communication, addressing challenges in international collaborations among police forces. Initiatives like the European Union's Horizon 2020 and projects such as LAW-TRAIN aim to foster such cooperation, progressing from simulation to real investigations with the necessary resources. AI tools are employed to scan social media platforms like Twitter for specific events that may impact security. For instance, AI can aid social network research to safeguard individuals at risk of radicalization by violent groups. While law enforcement agencies are increasingly leveraging social media to identify disruptive event plans and monitor large gatherings for security assessment, concerns about potential privacy invasions are valid. Security agencies like the US Transportation Security Administration (TSA) and Coast Guard are likely to expand their use of AI to significantly enhance productivity and effectiveness. Techniques like vision, speech analysis, and gait analysis using AI can be applied by interviewers, interrogators, and security personnel to detect potential deception and criminal behaviour. The TSA is working on a comprehensive airport security project, including DARMS, a personalized protection system based on risk categories and flight details (Koch, 2014).

2.4 Conceptual Model

This study seeks to analyse the impact of specific factors related to artificial intelligence security technologies on the overall performance of public organizations with respect to community security. Five independent variables, namely compatibility, complexity, management support, ethics of artificial intelligence, and staff capabilities, are examined for their influence on the dependent variable of security effectiveness within the community. Additionally, organizational learning is incorporated as a mediator between these independent variables and the dependent variable, as illustrated in Figure 1, which presents the conceptual model for this research.

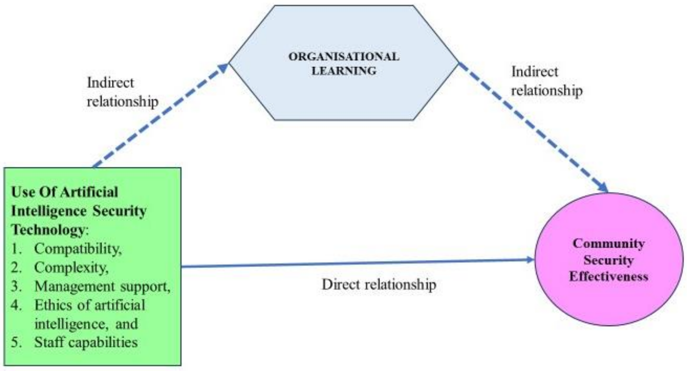

Fig 1 - Conceptual model of this study

3. Data Collection

This study utilized a questionnaire survey to collect data, focusing on the Abu Dhabi Police as a case study to represent public organizations in the UAE. The survey was directed at both managerial and operational staff within the organization. The survey research design involved a sample size of 138 participants, with the questionnaire distributed randomly to individuals accessible through various online tools and applications. Ultimately, 138 individuals from the intended target respondents provided responses to the survey.

The analysis of respondents' backgrounds in terms of age revealed the following distribution: 35 (25.4%) were in the 21-30 age group, 45 (32.6%) in the 31-40 age group, 33 (23.9%) in the 41-50 age group, and 25 (18.1%) were over 50 years old. The gender breakdown indicated that there were 103 (74.6%) male respondents and 35 (25.4%) female respondents. In terms of educational level, the analysis showed that 20 (14.5%) had a certificate/diploma, 80 (57.9%) held a bachelor's degree, 33 (23.9%) had a master's degree, and 5 (3.7%) had a Ph.D. Regarding work experience, 8 (5.8%) respondents had less than 1 year of experience, 28 (20.3%) had 2-5 years of experience, 52 (37.6%) had 6-10 years of experience, and 32 (23.2%) had 11-15 years of experience.

To ensure the reliability of multiple-item architectures, internal consistency is essential. Pallant (2011) highlights that reliability is determined by the extent to which research measurements are free from random errors and the scale's ability to produce consistent results upon repeated measurement of the same variable. The widely utilized measure of reliability is Cronbach's alpha, which evaluates the consistency of the measurement scale (Hair et al., 2011; Wong, 2013). Table 1 below presents the values for the Cronbach's Alpha reliability assessment on this study collected data.

Table 1 - Cronbach's Alpha reliability test

No.	Constructs/group	Code	No. of factors	Cronbach's Alpha
1	Ethics of Artificial Intelligence	ETH	5	0.840
2	Compatibility	COMPAT	6	0.821
3	Complexity	COMPLEX	5	0.836
4	Efficiency of Community Security	ESC	6	0.828
5	Management support	MS	6	0.836
6	Organizational Learning	OL	5	0.833
7	Staff Capability	SC	5	0.836

Table 1 indicates that the internal consistency as defined as Cronbach's alpha exceeding 0.7. The overall perception scale showed satisfactory internal consistency with alpha values ranging from 0.821 to 0.840 across all dimensions.

4. Modelling PLS-SEM Technique

Partial Least Squares Structural Equation Modelling (PLS-SEM) is a statistical technique used for analysing complex relationships among multiple variables. It's particularly useful when dealing with small sample sizes or highly dimensional data. PLS-SEM focuses on both predicting the dependent variables and understanding latent constructs by modelling the relationships between observed indicators and latent variables, making it a versatile approach in various research fields. It combines components of regression analysis and factor analysis, allowing researchers to assess direct and indirect effects while providing flexibility in model specification. Hence, the PLS-SEM model of this study was constructed using the SmartPLS software, encompassing three primary processes: the PLS Algorithm, Blindfolding, and bootstrapping, as elaborated in the subsequent subsection.

4.1 PLS Algorithm

After creating the conceptual model in SmartPLS software and assigning the data, we proceeded with the modelling process using the PLS Algorithm function. Following this, the resulting measurement values were analysed to ensure they met specific criteria. In cases where these criteria were not met, factors were removed, and the modelling process with the PLS Algorithm was iterated until the measurement component criteria were satisfied.

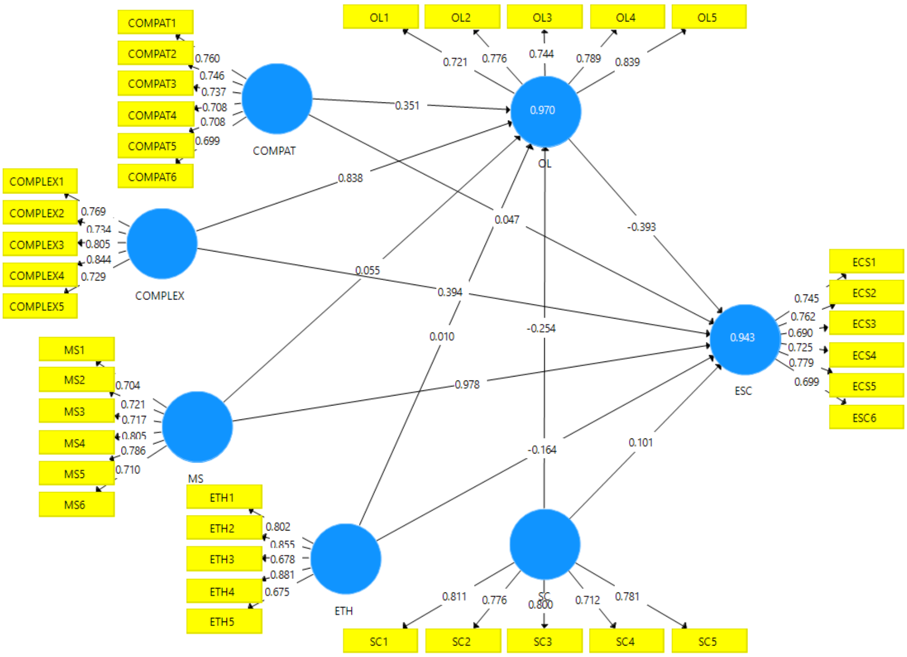

Fig 2 - Model after First modelling using PLS Algorithm

4.1.1 Checking Collinearity Statistics [VIF]

In regression analysis, collinearity of two variables means that strong correlation exists between them, making it difficult or impossible to estimate their individual regression coefficients reliably.

Table 3 - Generated VIF values

First modelling		**Second modelling**	
FACTORS	**VIF**	**FACTORS**	VIF
COMPAT1	2.039	COMPAT1	1.996
COMPAT2	2.076	COMPAT2	2.072
COMPAT3	1.757	COMPAT3	1.622
COMPAT4	1.807	COMPAT4	1.771
COMPAT5	**10.714**	COMPLEX1	1.702
COMPAT6	**10.462**	COMPLEX2	1.609
COMPLEX1	1.702	COMPLEX3	2.138
COMPLEX2	1.609	COMPLEX4	2.331
COMPLEX3	2.138	COMPLEX5	1.704
COMPLEX4	2.331	ECS1	1.655
COMPLEX5	1.704	ECS2	1.778
ECS1	1.655	ECS3	1.927
ECS2	1.778	ECS4	1.827
ECS3	1.927	ECS5	1.973
ECS4	1.827	ESC6	1.751
ECS5	1.973	ETH1	1.978
ESC6	1.751	ETH2	2.71
ETH1	1.978	ETH3	1.464
ETH2	2.71	ETH4	2.629
ETH3	1.464	ETH5	1.63
ETH4	2.629	MS1	1.849
ETH5	1.63	MS2	2.016
MS1	1.849	MS3	2.087
MS2	2.016	MS4	2.059
MS3	2.087	MS5	2.359
MS4	2.059	MS6	1.63
MS5	2.359	OL1	1.785
MS6	1.63	OL2	1.81
OL1	1.785	OL3	1.673
OL2	1.81	OL4	2.221
OL3	1.673	OL5	2.297
OL4	2.221	SC1	1.963
OL5	2.297	SC2	2.1
SC1	1.963	SC3	1.887
SC2	2.1	SC4	1.833
SC3	1.887	SC5	1.852
SC4	1.833		
SC5	1.852		

Generally, a VIF above 4 or tolerance below 0.25 indicates that multicollinearity might exist, and further investigation is required. When VIF is higher than 10 or tolerance is lower than 0.1, there is significant multicollinearity that needs to be corrected. Hence, based on table 3 COMPAT5 and COMPAT6 factors have to be deleted and the model was again run by PLS Algorithm function and the final model is as figure 3.

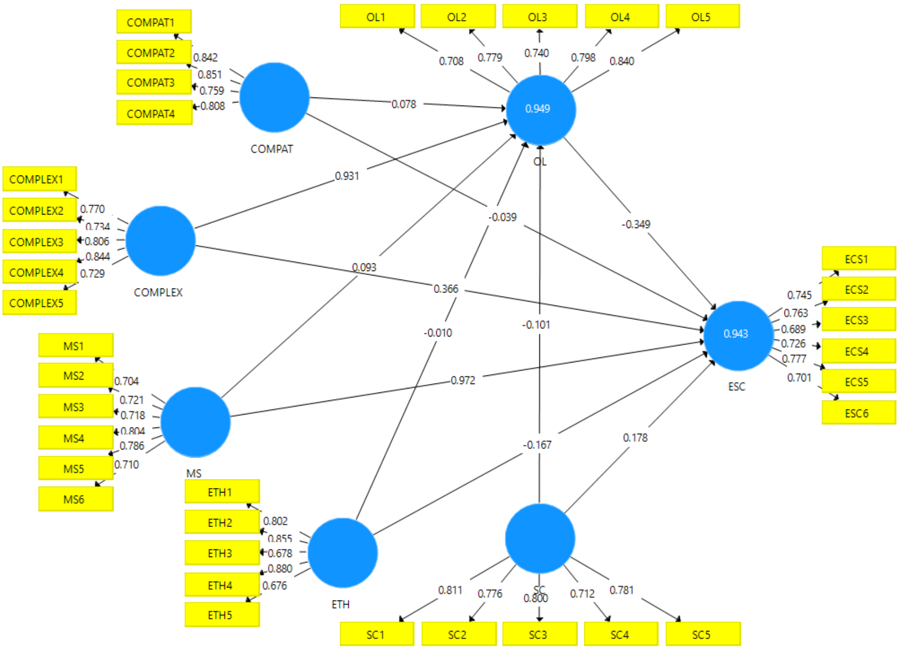

Fig 3 - Model after second modelling using PLS Algorithm

4.1.2 Outer Loading

Outer loading represents a fundamental idea within factor analysis, especially concerning confirmatory factor analysis (CFA) and structural equation modelling (SEM). It quantifies how robustly an observable variable (indicator or item) connects with its associated latent construct. Elevated outer loadings, usually presented as standardized factor loadings, suggest that the observable variable effectively reflects the underlying construct, supporting the legitimacy of the measurement model.

Table 4 - Outer loading

	COMPAT	COMPLEX	ESC	ETH	MS	OL	SC
COMPAT1	0.842						
COMPAT2	0.851						
COMPAT3	0.759						
COMPAT4	0.808						
COMPLEX1		0.770					
COMPLEX2		0.734					
COMPLEX3		0.806					
COMPLEX4		0.844					
COMPLEX5		0.729					
ECS1			0.745				
ECS2			0.763				
ECS3			0.689				
ECS4			0.726				
ECS5			0.777				
ESC6			0.701				
ETH1				0.802			
ETH2				0.855			
ETH3				0.678			
ETH4				0.880			
ETH5				0.676			
MS1					0.704		
MS2					0.721		
MS3					0.718		
MS4					0.804		
MS5					0.786		

MS6	0.710		
OL1		0.708	
OL2		0.779	
OL3		0.740	
OL4		0.798	
OL5		0.840	
SC1			0.811
SC2			0.776
SC3			0.800
SC4			0.712
SC5			0.781

Table 4 displays the strength of relationships (outer loadings) between latent variables and their indicators in a factor analysis. Each latent variable has several indicators, with loadings ranging from 0.676 to 0.88, indicating the extent to which each indicator contributes to measuring the latent construct. Higher loadings signify a stronger association. This information is crucial for evaluating the validity of the latent variables and understanding the measurement properties of the model.

4.1.3 Construct Reliability and Validity

Construct reliability signifies the consistency and stability of measurements across repeated tests, often evaluated using metrics like Cronbach's alpha, indicating the correlation between items within a construct. High construct reliability indicates consistent measurement of the same underlying construct. Conversely, construct validity ensures that a measurement tool effectively captures the intended theoretical construct. It encompasses elements such as content validity (item coverage), criterion validity (external correlation), and convergent/divergent validity (consistent correlations with similar/different constructs). Ensuring both reliability and validity is crucial for meaningful and accurate research results, providing a strong foundation for data analysis and interpretation. Results of construct reliability and validity from the model of this study are generated as in table 5

Table 5 - Construct reliability and validity

Constructs	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
COMPAT	0.832	0.839	0.888	0.665
COMPLEX	0.836	0.846	0.884	0.605
ESC	0.828	0.831	0.875	0.539
ETH	0.84	0.866	0.887	0.613
MS	0.836	0.844	0.88	0.55
OL	0.833	0.845	0.882	0.6
SC	0.836	0.843	0.884	0.603

Table 5 summarizes key metrics for assessing the quality of the measurement model in a study involving several constructs. It includes Cronbach's Alpha, a measure of internal consistency, which ranges from 0.828 to 0.84 across the constructs. Another reliability measure, rho_A, falls between 0.831 and 0.866. Composite Reliability, indicating the overall reliability of the latent construct, ranges from 0.875 to 0.888. The Extracted Average Variance (AVE), a measure of convergent validity, varies from 0.539 to 0.665. Overall, these metrics collectively suggest that the measurement model is well-constructed with consistent and reliable indicators for each construct, providing a solid foundation for the research analysis.

4.1.4 Discriminant Validity

Discriminant validity is a critical concept in the field of research, especially in the context of construct measurement and validation. It assesses the extent to which distinct constructs, which are supposed to measure different underlying concepts, are indeed distinct from one another. One common way to demonstrate discriminant validity is by examining the correlations between constructs and ensuring that they are lower than the square root of the average variance extracted (AVE) for each construct. Demonstrating discriminant validity is essential because it ensures that the measurement instrument can accurately differentiate between the intended constructs, preventing issues of construct overlap or confusion in statistical analyses. This is particularly important when constructing multi-dimensional scales or using latent variables in techniques like structural equation modelling.

Table 6 - Discriminant validity

	COMPAT	COMPLEX	ESC	ETH	MS	OL	SC
COMPAT	0.816						
COMPLEX	0.623	0.778					
ESC	0.75	0.713	0.734				
ETH	0.666	0.569	0.735	0.783			
MS	0.744	0.709	0.96	0.813	0.741		
OL	0.625	0.973	0.704	0.574	0.72	0.774	
SC	0.945	0.665	0.826	0.732	0.818	0.661	0.777

Table 6 presents a symmetric matrix of correlation coefficients between different constructs: COMPAT, COMPLEX, ESC, ETH, MS, OL, and SC. The diagonal entries are all 1.0, indicating perfect correlation of each construct with itself. Off-diagonal entries show the strength of correlation between pairs of constructs, ranging from 0.569 to 0.973. Notably, the highest correlation is between OL and COMPLEX (0.973), while the lowest is between ETH and COMPLEX (0.569). These correlation coefficients offer valuable insights into the interrelationships among the constructs, helping to understand potential associations and dependencies in the research context.

4.1.5 Model Fit [R Square Values]

R-squared (R^2) is a statistical metric commonly used to assess the goodness of fit of a regression model. It measures the proportion of the total variation in the dependent variable that is explained by the independent variables in the model. A higher R-squared value indicates that the model can explain a larger portion of the variability in the data, suggesting a better fit. However, it's essential to consider the context and the nature of the data; a high R-squared doesn't necessarily imply a meaningful or predictive model, and other factors such as model complexity and theoretical relevance should also be evaluated. R-squared is particularly useful when comparing different models to select the one that best explains the variation in the data.

Table 7 - R Square values

Constructs	Name	R Square	R Square Adjusted
Dependent	ESC	0.943	0.94
Mediator	OL	0.949	0.947

4.1.6 Model Fit [Goodness of Fit]

In contrast to covariance-based structural equation modelling, PLS-SEM lacks a universally accepted global goodness of fit metric (Vinzi et al., 2010). To address this issue, Tenenhaus et al. (2004) introduced the "GoF" index, a comprehensive criterion for evaluating model fit. This index combines the geometric mean of the average communality (AVE) and the average coefficient of determination (R2), and it can be computed using the following formula:

$$GoF = \sqrt{\overline{AVE}\ X\ \overline{R^2}}$$

The purpose of the GoF index is to assess the performance of the PLS model, encompassing both the measurement and structural aspects, with a specific emphasis on the overall predictive capability of the model (Memon & Rahman, 2013). In the formula, the R2 component pertains to the structural model, while the AVE assesses the quality of the index's measurement models. When the calculated GoF index takes values of 0.1, 0.25, or 0.36, it is interpreted as small, medium, or large, respectively (Akter et al., 2011). The values of the averaged AVE and averaged R2 for this study's model are provided in Table 8.

Table 8 - Averaged values

Constructs	Average Variance Extracted (AVE)	R square
COMPAT	0.665	
COMPLEX	0.605	
ESC	0.539	0.943
ETH	0.613	
MS	0.550	
OL	0.600	0.949

SC	0.603	
Average values	**0.596**	**0.946**

After substituting the values from Table 8 into the formula, the resulting calculated GoF index for the model is as follows:

$$GoF = \sqrt{\mathbf{0.596}x\ \mathbf{0.946}}$$

$$GoF = \sqrt{0.564}$$

$$GoF = 0.751$$

Above is a formula for calculating the goodness of fit index. The GoF of the model was 0.751. which according to Akter et al. (2011), the GoF value indicates a high level of goodness of fit, suggesting that the research model is of high quality.

4.2 Bootstrapping

Bootstrapping is a versatile statistical technique used in both hypothesis testing and structural equation modeling. In hypothesis testing, it helps assess the significance of statistics like mean differences, while in structural equation modelling, it's used to evaluate the significance and stability of path coefficients representing relationships between variables. Bootstrapping provides robust inferences, especially when assumptions about data distribution or sample size are uncertain. It creates resampled distributions, allowing the construction of confidence intervals and the assessment of statistical significance without relying on traditional assumptions. By addressing these challenges, bootstrapping enhances the reliability of results in both contexts.

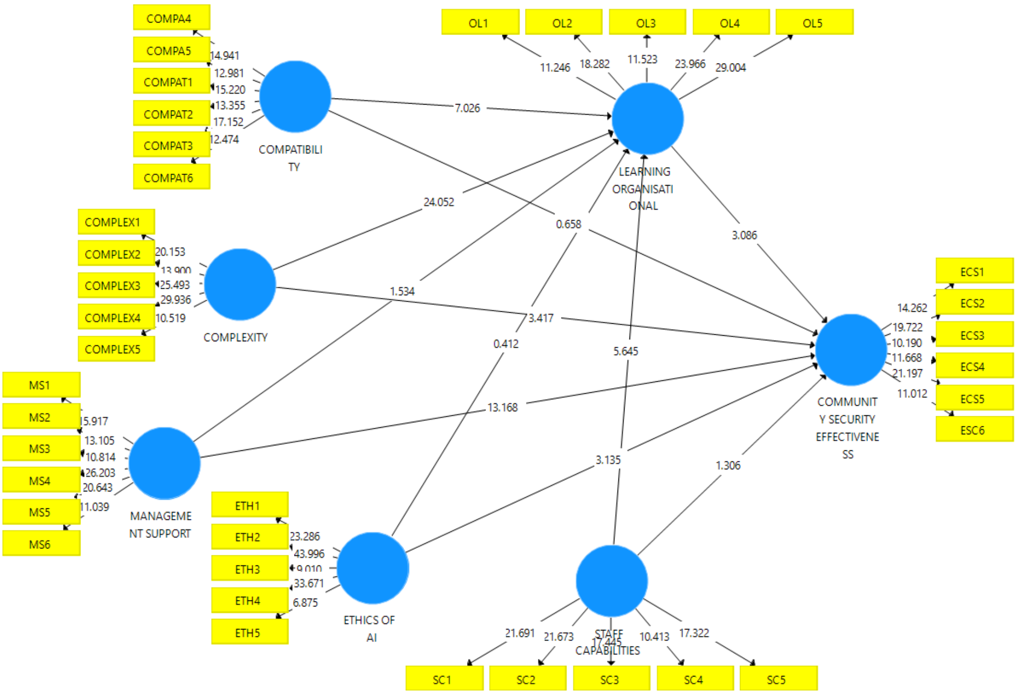

Fig 4 - Model after bootstrapping process

4.2.1 Indirect [Hypothesis Testing and Path Coefficient]

In a Partial Least Squares (PLS) model, the path coefficient shows the intensity and direction of the association between components inside the model. It illustrates how much change in the dependent construct corresponds to a unit change in the independent construct when all other variables are held constant. In PLS models, path coefficients are generally displayed as arrows indicating the direction of influence. PLS is a useful strategy for dealing with complex models with latent variables since these coefficients are calculated using data and reflect the underlying latent constructs. Understanding and interpreting path coefficients is critical for finding causal linkages and determining their significance in a PLS model.

Table 9 - Indirect relationship

Relationship	Path coefficient/beta values	Significant/Not significant	Rank
COMPAT -> ESC	-0.039	Not significant	-NA-
COMPAT -> OL	0.078	Not significant	-NA-
COMPLEX -> ESC	0.366	Significant	3
COMPLEX -> OL	0.931	Significant	2
ETH -> ESC	-0.167	Significant	5
ETH -> OL	-0.01	Not significant	-NA-
MS -> ESC	0.972	Significant	1
MS -> OL	0.093	Not significant	-NA-
OL -> ESC	-0.349	Significant	4
SC -> ESC	0.178	Not significant	-NA-
SC -> OL	-0.101	Not significant	-NA-

Table 9 provides path coefficients, significance levels, and ranks for relationships between different constructs in a model. Notably, the relationship between MS and ESC is the most influential with a highly significant positive path coefficient of 0.972, ranking first. COMPLEX also has significant positive relationships with both ESC and OL, ranking second and third, respectively, with path coefficients of 0.366 and 0.931. COMPAT has non-significant relationships with both ESC and OL, while ETH have a significant negative relationship with ESC but a non-significant relationship with OL. SC does not exhibit significant relationships with either ESC or OL.

4.2.2 Direct [Hypothesis Testing and Path Coefficient]

Hypothesis testing in the context of a model involves the systematic evaluation of specific conjectures (hypotheses) about the relationships between variables or the parameters of the model. It aims to determine whether the observed data provides sufficient evidence to support or reject these hypotheses based on statistical significance criteria. This process helps researchers draw meaningful conclusions about the validity and significance of proposed relationships or model parameters, enhancing the understanding of the underlying phenomena. While, A path coefficient in a structural equation model (SEM) is essential as it reveals the strength and direction of the connection between latent or observed variables. It measures how an independent variable (predictor) influences a dependent variable (outcome) within the larger model, with positive or negative effects. The magnitude and statistical significance of these coefficients offer valuable insights into the underlying causal relationships and the theoretical framework under examination within the SEM.

Table 10 - Direct relationship

Relationships	Path coefficient	T Statistics	P Values	Remarks
COMPAT -> ESC	-0.039	0.512	0.609	Not significant
COMPAT -> OL	0.078	0.97	0.332	Not significant
COMPLEX -> ESC	0.366	3.252	0.001	Significant
COMPLEX -> OL	0.931	34.382	0	Significant
ETH -> ESC	-0.167	3.423	0.001	Significant
ETH -> OL	-0.01	0.22	0.826	Not significant
MS -> ESC	0.972	13.086	0	Significant
MS -> OL	0.093	1.908	0.057	Not significant
OL -> ESC	-0.349	3.038	0.003	Significant
SC -> ESC	0.178	1.664	0.097	Not significant
SC -> OL	-0.101	1.018	0.309	Not significant

# significant p-values<0.05

Table 10 shows results of eleven direct relationships with OL. as a mediator and ESC dependent construct. However, only five of the relationships are significant. These relationships are COMPLEX -> ESC; COMPLEX -> OL; ETH -> ESC; MS -> ESC; and OL -> ESC. The following is the generated results of indirect relationships of the model from bootstrapping process as in table 11.

Table 11 - Indirect relationship

Relationships	Original Sample (O)	T Statistics	P Values	Remarks
MS -> OL -> ESC	-0.032	1.688	0.092	Not significant
SC -> OL -> ESC	0.035	1.005	0.315	Not significant
COMPLEX -> OL -> ESC	-0.325	2.966	0.003	**Significant**
COMPAT -> OL -> ESC	-0.027	0.988	0.324	Not significant
ETH -> OL -> ESC	0.003	0.250	0.802	Not significant

# significant p-values<0.05

Table 11 shows results of five indirect relationships with OL as a mediator. It indicates that only one of the relationships is significant with T and P values comply with the criteria values. The significant indirect relationship is COMPLEX -> OL -> ESC.

4.2.3 Mediation Effect

A mediating effect within a PLS structural model takes on the form of a dynamic driving force, propelled by the involvement of a third variable termed the mediator. This mediator operates as a catalyst, unveiling the intricate mechanisms that lie beneath the surface of the relationship between an independent variable (IV) and a dependent variable (DV). Positioned as an intermediary, the mediator not only brings the primary causal pathway to light but also uncovers indirect routes, enriching our understanding of the model's multifaceted interplay. When the mediating impact demonstrates statistical significance, it not only validates but also accentuates the mediator's pivotal role in tightly linking the IV and the DV.

The mediating effect in a PLS structural model, is assessed through statistical tests and theoretical considerations. Firstly, the total effect between the independent variable (IV) and the dependent variable (DV) is examined to establish their relationship. Then, the direct effect of the IV on the DV, controlling for the mediator, is evaluated. If the indirect effect through the mediator is significant and the direct effect becomes insignificant, this indicates mediation. The mediating role is supported by both statistical evidence and theoretical plausibility in understanding the complex relationships within the model. Table 12 demonstrates the criteria for considering the mediating effect.

Table 12 - Mediation status

Relationships		T Statistics	P Values	Remarks	Mediation effects
Direct	COMPAT -> ESC	0.512	0.609	Not significant	No
Indirect	COMPAT -> OL -> ESC	0.988	0.324	Not significant	
Direct	COMPLEX -> ESC	3.252	0.001	Significant	Partial effect
Indirect	COMPLEX -> OL -> ESC	2.966	0.003	Significant	
Direct	MS -> ESC	13.086	0.000	Significant	No
Indirect	MS -> OL -> ESC	1.688	0.092	Not significant	
Direct	SC -> ESC	1.664	0.097	Not significant	No
Indirect	SC -> OL -> ESC	1.005	0.315	Not significant	
Direct	ETH -> ESC	3.423	0.001	Significant	No
Indirect	ETH -> OL -> ESC	0.250	0.802	Not significant	

Table 12 presents results from a statistical analysis of relationships in a model. It highlights significant direct effects from COMPLEX and MS to ESC, with partial and strong relationships, respectively. In most other cases, including COMPAT -> ESC, SC -> ESC, and ETH -> ESC, the effects are not significant, suggesting limited mediation or no mediation in these instances.

4.3 Blindfolding

Blindfolding, or cross-validation, is used to validate and assess the predictive performance of a model on new data, ensuring it doesn't overfit. It also evaluates the stability of the model's results and helps in selecting the optimal complexity for the model by testing its performance on subsets of the data. Additionally, blindfolding assists in identifying essential features, enhancing the model's reliability and generalizability. Results generated from blindfolding process is Construct Cross-Validated Redundancy (CCR) and Construct Cross-Validated Communality (CCV).

4.3.1 Construct Cross-Validated Redundancy (CCR)

CCR evaluates the extent of overlap or shared information among observed variables representing different constructs in a model, identifying issues like multicollinearity. It assesses the relationships between constructs in terms of redundancy. On the other hand, CCV measures how well observed variables capture the underlying latent construct's variance, considering shared variance with other constructs, and ensures its stability across different data subsets. It focuses on the adequacy of individual indicators in representing a specific latent construct.

Table 13 - Results of construct cross validated redundancy

Construct	**SSO**	**SSE**	**Q² (=1-SSE/SSO)**
COMPAT	552	552	
COMPLEX	690	690	
ESC	828	421.068	0.491
ETH	690	690	
MS	828	828	
OL	690	312.27	0.547

Table 13 presents SSO (Sum of Squares Observed), SSE (Sum of Squares Error), and Q² values for various constructs in a model. Notable findings include the constructs "ESC" and "OL," which have significant proportions of variance explained (Q² = 0.491 and 0.547, respectively) relative to their SSO values. It can be concluded that the constructs "ESC" and "OL" demonstrate substantial explanatory power, with Q² values indicating significant proportions of variance explained relative to their observed variance (SSO). This suggests that the model is effective in capturing meaningful relationships for these constructs, while other constructs may require further investigation due to their inability to explain a significant portion of the variance.

4.3.2 Construct Cross-Validated Communality (CCV).

The following is the results of construct cross validated communality (CCV) generated from blindfolding as table 14.

Table 14 - Results of construct cross validated communality

	SSO	SSE	Q² (=1-SSE/SSO)
COMPAT	552	310.464	0.438
COMPLEX	690	411.331	0.404
ESC	828	536.629	0.352
ETH	690	398.237	0.423
MS	828	521.888	0.37
OL	690	416.526	0.396
SC	690	417.643	0.395

Table 14 presents statistical results for several constructs, including SSO (total observed variance), SSE (unexplained variance), and Q² (proportion of variance explained by the model). Constructs like "ESC" and "ETH" have relatively higher Q² values, indicating better model fit and explanatory power. Lower Q² values for other constructs suggest they may need further investigation or refinement to improve their explanatory capabilities

5. Conclusion

This paper presents a study on developing a PLS-SEM model of community security through the implementation of AI, while simultaneously investigating the mediating influence of organizational learning within the context of vital AI factors in the UAE. Data collection was conducted via a questionnaire survey utilizing the Abu Dhabi Police as a representative case study for public organizations in the UAE, involving 138 participants spanning both managerial and operational roles, with responses acquired through randomized distribution using online tools. The collected data was employed to construct the model using SmartPLS software, and its evaluation adhered to assessment criteria encompassing measurement and structural components. It was found that a goodness-of-fit score of 0.751, suggested that the model performed well in terms of overall predictive performance. The study's findings also revealed that organisational learning (OL) acts as a partial mediator in the relationship between the complexity construct (COMPLEX) and the efficacy of Community Security (ESC), but no mediation effects were identified in other relationships. The research findings resulted in the development of a versatile model that improves community security using AI technology, is usable in a variety of circumstances, and benefits persons interested in AI and community security, such as academics, researchers, and practitioners. The approach of the study offers useful insights for practitioners and scholars in the UAE and adjacent sectors, allowing for replication or adaption to specific investigative situations.

Acknowledgement

The authors would like to thanks the university for allowing to conduct and publish this study.

References

Aboelmaged, M. G. (2014). Predicting e-readiness at firm-level: An analysis of technological, organizational and environmental (TOE) effects on e-maintenance readiness in manufacturing firms. International Journal of Information Management, 34(5), 639-651.

Abubakar, A. M., Behravesh, E., Rezapouraghdam, H., & Yildiz, S. B. (2019). Applying artificial intelligence technique to predict knowledge hiding behavior. International Journal of Information Management, 49, 45-57.

Acemoglu, D., & Restrepo, P. (2019). 8. Artificial Intelligence, Automation, and Work (pp. 197-236). University of Chicago Press.

Ahmed, M. A., & van der Schaar, M. (2017). Bayesian inference of individualized treatment efects using multi-task gaussian processes. NeurIPS 2017.

Akter, S., D'ambra, J., & Ray, P. (2011). An evaluation of PLS based complex models: the roles of power analysis, predictive relevance and GoF index.

Alsheibani, S., Cheung, Y., & Messom, C. (2018). Artificial Intelligence Adoption: AI-readiness at Firm-Level. In PACIS (p. 37).

AlSheibani, S., Messom, C., & Cheung, Y. (2020, January). Re-thinking the competitive landscape of artificial intelligence. In Proceedings of the 53rd Hawaii international conference on system sciences.

Ammar, H. H., Abdelmoez, W., & Hamdi, M. S. (2012, March). Software engineering using artificial intelligence techniques: Current state and open problems. In Proceedings of the First Taibah University International Conference on Computing and Information Technology (ICCIT 2012), Al-Madinah Al-Munawwarah, Saudi Arabia (Vol. 52).

Bene!ová A and Tupa J 2017 Procedia Manufacturing 11 2195-2202

Bryson, J., & Winfield, A. (2017). Standardizing ethical design for artificial intelligence and autonomous systems. Computer, 50(5), 116-119.

Carter, S., & Nielsen, M. (2017). Using artificial intelligence to augment human intelligence. Distill, 2(12), e9.

Collins, P. D., Hage, J., & Hull, F. M. (1988). Organizational and technological predictors of change in automaticity. Academy of Management Journal, 31(3), 512-543.

Dalenogare, L. S., Benitez, G. B., Ayala, N. F., & Frank, A. G. (2018). The expected contribution of Industry 4.0

Dworschak, B., & Zaiser, H. (2014). Competences for cyber-physical systems in manufacturing–first findings and scenarios. Procedia Cirp, 25, 345-350.

Erol, S., Jäger, A., Hold, P., Ott, K., & Sihn, W. (2016). Tangible Industry 4.0: a scenario-based approach to learning for the future of production. Procedia CiRp, 54, 13-18.

Faller, C., & Feldmüller, D. (2015). Industry 4.0 learning factory for regional SMEs. Procedia Cirp, 32, 88-91.

Hage, J. (1980). Theories of organizations: Form, process, and transformation. John Wiley & Sons.

Haider, N., Baig, M. Z., & Imran, M. (2020). Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends. arXiv preprint arXiv:2007.04490.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. Journal of Marketing theory and Practice, 19(2), 139-152.

Hecklau, F., Galeitzke, M., Flachs, S., & Kohl, H. (2016). Holistic approach for human resource management in Industry 4.0. Procedia Cirp, 54, 1-6.

Hurley, J. S. (2018). Enabling successful artificial intelligence implementation in the department of defense. Journal of Information Warfare, 17(2), 65-82.

Injadat, M., Moubayed, A., Nassif, A. B., & Shami, A. (2021). Machine learning towards intelligent systems: applications, challenges, and opportunities. Artificial Intelligence Review, 1-50.

Jia, Y., Liu, S., & Jiang, S. (2019, September). Analysis of the development status of artificial intelligence technology at home and abroad. In 2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS) (pp. 195-198). IEEE.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. MIS quarterly, 183-213.

Klinger, J., Mateos-Garcia, J. C., & Stathoulopoulos, K. (2018). Deep learning, deep change? Mapping the development of the Artificial Intelligence General Purpose Technology. Mapping the Development of the Artificial Intelligence General Purpose Technology (August 17, 2018).

Koch, W. (2014). Towards cognitive tools: systems engineering aspects for public safety and security. IEEE Aerospace and Electronic Systems Magazine, 29(9), 14-26.

Memon, A. H., & Rahman, I. A. (2013). Analysis of cost overrun factors for small scale construction projects in Malaysia using PLS-SEM method. Modern applied science, 7(8), 78

Mittal, S., Khan, M. A., Romero, D., & Wuest, T. (2018). A critical review of smart manufacturing & Industry 4.0 maturity models: Implications for small and medium-sized enterprises (SMEs). Journal of manufacturing systems, 49, 194-214.

Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, 1(11), 501-507.

Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, 100227.

Pallant, J. (2020). SPSS survival manual: A step by step guide to data analysis using IBM SPSS. Routledge.

Pan, Y. (2016). Heading toward artificial intelligence 2.0. Engineering, 2(4), 409-413.

Pesapane, F., Codari, M., & Sardanelli, F. (2018). Artificial intelligence in medical imaging: threat or opportunity? Radiologists again at the forefront of innovation in medicine. European radiology experimental, 2, 1-10.

Pirvu, B. C., Zamfirescu, C. B., & Gorecky, D. (2016). Engineering insights from an anthropocentric cyber-physical system: A case study for an assembly station. Mechatronics, 34, 147-159.

Pumplun, L., Tauchert, C., & Heidt, M. (2019). A new organizational chassis for artificial intelligence-exploring organizational readiness factors.

Quiggin, T. (2007). Seeing the invisible: national security intelligence in an uncertain age. World Scientific.

Ramos, C. (2007). Ambient intelligence–a state of the art from artificial intelligence perspective. In Progress in Artificial Intelligence: 13th Portuguese Conference on Aritficial Intelligence, EPIA 2007, Workshops: GAIW, AIASTS, ALEA, AMITA, BAOSW, BI, CMBSB, IROBOT, MASTA, STCS, and TEMA, Guimarães, Portugal, December 3-7, 2007. Proceedings 13 (pp. 285-295). Springer Berlin Heidelberg.

Sahlgren, M., & Olsson, F. (2019). Gender bias in pretrained Swedish embeddings. In Proceedings of the 22nd Nordic Conference on Computational Linguistics (pp. 35-43).

Scaccia, J. P., Cook, B. S., Lamont, A., Wandersman, A., Castellow, J., Katz, J., & Beidas, R. S. (2015). A practical implementation science heuristic for organizational readiness: R= MC2. Journal of community psychology, 43(4), 484-501.

Schuh, G., Gartzen, T., Rodenhauser, T., & Marks, A. (2015). Promoting work-based learning through industry 4.0. Procedia Cirp, 32, 82-87.

Shamim, S., Cang, S., Yu, H., & Li, Y. (2016, July). Management approaches for Industry 4.0: A human resource management perspective. In 2016 IEEE congress on evolutionary computation (CEC) (pp. 5309-5316). IEEE.

Simon, J. P. (2019). Artificial intelligence: scope, players, markets and geography. Digital Policy, Regulation and Governance.

Srivastava, S., Bisht, A., & Narayan, N. (2017, January). Safety and security in smart cities using AI—A review. In Cloud Computing, Data Science & Engineering-Confluence, 2017 7th International Conference on (pp. 130-133). IEEE.

Sun, S., Cegielski, C. G., Jia, L., & Hall, D. J. (2018). Understanding the factors affecting the organizational adoption of big data. Journal of Computer Information Systems, 58(3), 193-203.

Tamás, P., Illés, B., & Dobos, P. (2016, November). Waste reduction possibilities for manufacturing systems in the industry 4.0. In IOP Conference Series: Materials Science and Engineering (Vol. 161, No. 1, p. 012074). IOP Publishing.

Tenenhaus, M., Amato, S., & Esposito Vinzi, V. (2004, June). A global goodness-of-fit index for PLS structural equation modelling. In Proceedings of the XLII SIS scientific meeting (Vol. 1, No. 2, pp. 739-742).

Terziyan, V., Gryshko, S., & Golovianko, M. (2018). Patented intelligence: Cloning human decision models for Industry 4.0. Journal of manufacturing systems, 48, 204-217.

Tidd, J. and Bessant, J. (2009). Managing innovation: Integrating technological, market and organizational change. Wiley.

Tornatzky, Louis G. and Mitchell Fleischer, The processes of technological innovation. Lexington, Mass.: Lexington Books, 1990.

Tushman, Michael L. and David Nadler, "Organizing for innovation," California Management Review 28, 3 (Spring 1986): 74-92.

UAE 2031 (2018), "UAE artificial intelligence strategy", Retrieved from http://www.uaeai.ae/en

Vannuccini, S., & Prytkova, E. (2021). Artificial intelligence's new clothes? From general purpose technology to large technical system. From General Purpose Technology to Large Technical System (April 7, 2021). SWPS, 2.

Vinzi, V. E., Chin, W. W., Henseler, J., & Wang, H. (2010). Handbook of partial least squares (Vol. 201, No. 0). Berlin: Springer.

Weyer, S., Schmitt, M., Ohmer, M., & Gorecky, D. (2015). Towards Industry 4.0-Standardization as the crucial challenge for highly modular, multi-vendor production systems. Ifac-Papersonline, 48(3), 579-584.

Wong, K. K. K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. Marketing Bulletin, 24(1), 1-32.

Yang, Z., Sun, J., Zhang, Y., & Wang, Y. (2015). Understanding SaaS adoption from the perspective of organizational users: A tripod readiness model. Computers in Human Behavior, 45, 254-264.

Zuiderveen Borgesius, F. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy..