IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 16 June 2023, accepted 3 July 2023, date of publication 10 July 2023, date of current version 14 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3293480

RESEARCH ARTICLE

The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective

SYED ASAD ABBAS BOKHARI[1], (Member, IEEE), AND SEUNGHWAN MYEONG[2]
[1]Center of Security Convergence and e-Governance, Inha University, Incheon 22212, South Korea
[2]Department of Public Administration, Inha University, Incheon 22212, South Korea

Corresponding author: Seunghwan Myeong (shmyeong@inha.ac.kr)

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea under Grant NRF-2022S1A5C2A03093690.

ABSTRACT Artificial intelligence (AI) has been identified as a critical technology of Fourth Industrial Revolution (Industry 4.0) for protecting computer network systems against cyber-attacks, malware, phishing, damage, or illicit access. AI has potential in strengthening the cyber capabilities and safety of nation-states, local governments, and non-state entities through e-Governance. Existing research provides a mixed association between AI, e-Governance, and cybersecurity; however, this relationship is believed to be context-specific. AI, e-Governance, and cybersecurity influence and are affected by various stakeholders possessing a variety of knowledge and expertise in respective areas. To fill this context specific gap, this study investigates the direct relationship between AI, e-Governance, and cybersecurity. Furthermore, this study examines the mediating role of e-Governance between AI and cybersecurity and moderating effect of stakeholders involvement on the relationship between AI, e-Governance, and cybersecurity. The results of PLS-SEM path modeling analysis revealed a partial mediating impact of e-Governance between AI and cybersecurity. Likewise, moderating influence of stakeholders involvement was discovered on the relationship between AI and e-Governance, as well as between e-Governance and cybersecurity. It implies that stakeholders involvement has vital significance in AI and e-Governance because all stakeholders have interest in vibrant, transparent, and secured cyberspace while using e-services. This study provides practical implications for governmental bodies of smart cities for strengthening their cybersecurity measures.

INDEX TERMS Artificial intelligence, cybersecurity, e-Governance, stakeholder involvement, machine learning, computer crime, smart cities, data privacy.

I. INTRODUCTION

Cybersecurity has become a critical and vital topic that requires protecting the computer network from potential threats in today's modern world [1], [2]. A cyber-attack is a deliberate attack targeting computer networks, relevant data, programs, and electronic information, resulting in sub-national entities inciting violence towards non-combatant opponents. As technology develops, so do cyber threats, necessitating the development of new prevention strategies [3], [4]. It has been alleged that cyber-attacks have become more prevalent in the industrial sector, resulting in serious infrastructure damage and significant monetary loss. The rise of cyber-attacks among organizations is primarily due to the growing reliance on online technologies that enable the storage of personal and economic data [5].

Consequently, it is acknowledged as perhaps the most critical problem in the modern context because it creates economic loss and discloses confidential information. Cyber-attacks include phishing, denial of service, malware, and ransomware infestations, which can harm anybody in society [6]. Cyber-attacks also have a significant psychological impact on humans, producing unhappiness, tension, and stress among people [7].

The associate editor coordinating the review of this manuscript and approving it for publication was Bo Pu.

Artificial intelligence (AI) applications can positively influence the cyber capabilities and national security of the sovereign nation, regional government entities, and non-state organizations [8], [9]. AI is a reliable technique for mitigating cyber-attack effects [10]. AI is machine intelligence that executes activities connected with intelligence [11]. Human professionals' expertise is integrated for strategic planning and decision-making [12], including making medical diagnoses and getting insights from expertise in concluding. In terms of cybersecurity, Zarina et al., [10] have illustrated that AI has both beneficial and harmful effects, with the harmful effect of facilitating the instigation phase of cyber-attacks, resulting in quicker and more devastating attacks. Looking forward, AI has the potential to greatly improve cybersecurity by increasing security precautions and promoting security in cyberspace. Furthermore, AI assists security experts in detecting cyber hazard symptoms and has enhanced the machine learning applications for malware classification and networked intrusion detection [13]. Lastly, the modern phenomenon in AI has transformed innovative solutions and improved city external attacks against serious security threats [14].

A smart city provides multiple innovative solutions to several challenges that city administration faces. However, information and communication technology (ICT) has become a vital component of e-Government. Implementing ICT into a city's infrastructure introduces hazards and obstructions [15]. People frequently use insecure Wi-Fi networks to check their email messages, e-banking, and other digital services, uncovering themselves to cybercrimes including hacking, denials of service, and cracking. Cybersecurity applying technologies to protect e-Government services is among the most important distinctive features that can be utilized to categorize safe cities globally [16]. Somewhere in this tendency, the 'inclusive smart city' framework has triggered strong interest because it emphasizes the importance of interpersonal and social capital in urban initiatives that focus on stakeholders' inclusion in the Digital Realm and involving inhabitants in service improvement to implement appropriate government services that match citizens' necessities [17], [18]. Recent studies on e-services and technologies also have emphasized the importance of implementing a citizens-centered strategy for smart cities because it is expected to develop strong social ecologies that depend strongly on web technology. Consequently, web technologies and services can significantly impact stakeholder interactions [19].

Although previous literature demonstrated influence of AI in smart mobility [20], energy management [21], public services [22], climate change [23], and smart security [24] in smart cities, cybersecurity has widely been neglected, especially in the context of stakeholders who use online government services. To fill this contextual gap, this study formulated the following research question:

- How AI applications used in smart cities influence cybersecurity directly?
- How AI applications used in smart cities influence e-Governance and e-Governance impacts cybersecurity directly?
- Does e-Governance play a mediating role between the relationship of AI applications and cybersecurity?
- Additionally, this study examines the moderating role of stakeholders' involvement in the relationship between AI and e-Governance and on the relationship between e-Governance and cybersecurity.

These main research questions are attempted to address empirically in this study, based on the premise that the interactions are context-dependent. Figure 1 explains the channel of the study's proposed framework to classify cybersecurity level in a smart city. The moderating significance of stakeholder involvement was systematically examined by using structural equational modeling (SEM) in SmartPLS 4.0. PLS-SEM path modeling was selected as the analytical tool because of its widespread utilization in examining research frameworks in prior studies and its acknowledged appropriateness for analyzing complex research models.

Section II proceeds with a literature background on the relationships between artificial intelligence, e-Governance, stakeholder involvement, cybersecurity, and the key hypotheses under consideration. The data sampling, research framework, methodology, and analysis are described in Section III. The statistical findings are presented in Section IV. Section V summarizes the discussions, draws conclusions, and recommends future research possibilities.

II. LITERATURE REVIEW AND HYPOTHESES

A. CYBERSECURITY CHALLENGES IN SMART CITIES

Smart city is a captivating concept characterized by its intelligent features. Its scope extends beyond improving the level of urban economic efficiency and the reduction of costs and resource consumption. Rather, it encompasses the integration of different components of the city through intelligent gadgets and the application of digital technologies or information and communication technology (ICT) to enhance service delivery. The transformation of conventional urban areas into smart cities has resulted in a higher living standard for citizens [25].

An illustration of a smart city can be outlined by using several fundamental elements, as exemplified in Figure 2.

Smart government comprises various aspects such as smart office, smart supervision, smart services, and smart decision-making to enhance the performance of city governance and optimize the life standard of citizens by establishing a bilateral collaboration between the government and citizens [26]. Smart public services offer various electronic information and online services to enhance the standard of living and satisfaction of the public, thereby developing the perception of a service-oriented government. The evolution of a smart economy can facilitate the smooth development of resource driven cities, enhance the efficiency of urban economies, and generate sustainable employment opportunities [27]. Smart healthcare systems that utilize e-health

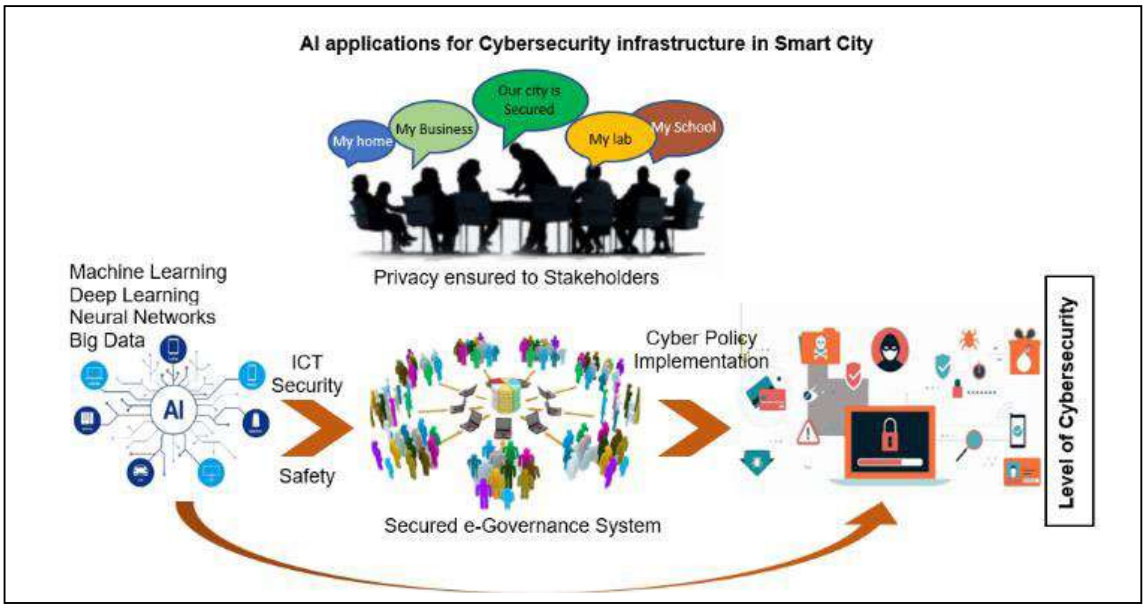

FIGURE 1. Channel of the proposed framework for classifying cybersecurity level in smart city.

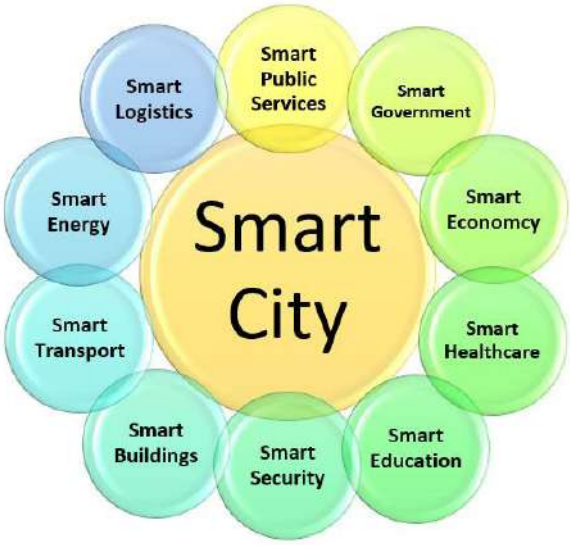

FIGURE 2. Fundamental elements of a smart city.

records to forecast the individual's health, like remote tracking of individuals with cardiac disease, has the potential to assess the state of vulnerability and furnish essential information for optimal treatment [28]. Smart education is a concept that involves using data-centric intelligent education in different contexts in smart cities to deliver individuals a smooth educational experience with customized individual assistance [29]. Smart buildings that effectively apply different information. The building is capable of satisfying the necessities of its users and residents, as well as identifying any defects in its operation. Buildings with features such as security, flexibility, ease of use, and efficiency are extremely attractive [30]. Smart transport systems are multifaceted and digitally managed to help with urban development and decision-making, thereby organizing smart transportation. Strategic travel scheduling can be achieved by the use of route projection and real-time roadway state monitoring [31]. Smart Security offers an assortment of benefits including detection, alarm, emergency assistance, and other functions pertaining to personal protection of individuals and safeguarding cybersecurity [32].

It is well-established that various infrastructure systems, including energies, grid system, healthcare, traffic, transportation, water distribution, and wastewater disposal, are furnished with computer networks. The use of Internet of Things has resulted in the emergence of smart cities, which aim at improving their facilities and developing more sophisticated, effective, and eco-friendly solutions. Nonetheless, a study ABI Research has projected that by 2024, barely 44% of the overall cybersecurity expenses for critical systems will be assigned to sectors such as healthcare, security, water, transport, and other related areas, leading to a significant lacking funding for protecting infrastructure against cybersecurity risks [33]. Consequently, there is a likelihood of various challenges involving cyber-attacks on crucial urban infrastructure, resulting in serious repercussions including the act of hijacking infrastructure communication and encrypting malware to disable computer systems has the potential to significantly impact the financial security of a city, resulting in substantial losses to both the finances and assets of inhabitants. Similarly, the disruption or destruction of communication systems, power grids, water conservation mechanisms, and other facilities can destroy the social system and cause an outbreak of a state of anxiety. Moreover, interfering with sensor data for creating a situation of chaos,

such as in disaster detection technologies, and stealing of crucial information such as people, healthcare, customers, and private information.

B. ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

Every nation on the planet necessitates security for economic progress and political stability. The advanced economies invest heavily in intelligence to safeguard their strategic interests and legitimacy in the face of terror threats. They confront high vulnerabilities, and new technologies may enhance security inside the state's sensitive zones [34], [35]. AI contributes to eliminating physical interaction, increasing the probability of operations detecting extremist threats at multiple stages. Different aspects of computation require security improvements from AI devices to monitor the specific regions' security, including technological infrastructure and data security. The US emphasizes the intelligence program's applications with the support of augmenting defense installations, and it has proved effective in counterterrorism. It is suggested that the usage of artificial intelligence is a significant point in enhancing security mechanisms in strategic industries, including public treasury centers and airport terminals [36]. The security challenges seem critical, driving the US to formulate a strategy toward future AI technologies that will support the elimination of all complications associated, including the curtailing of terrorist organizations' routine activities [37].

Several prior research has explored the significance of artificial intelligence in detecting and preventing cyberattacks [38], combating terrorism [39], enhancing security in strategic sectors [36], and building resilience in vulnerable sovereign places [34]. Soni [35] stated in his study that Information obtained from a broad selection of scientific and engineering specialists suggests that AI development depends on the United States capabilities to reconcile the advantages and disadvantages of AI, specifically in cybersecurity. AI is universally perceived among the most impressive technologies of the digital world, and cybersecurity is undoubtedly the domain that might benefit greatly from it. Optimization algorithms, strategies, devices, and companies providing AI-based solutions are evolving in international security markets [40]. It is emphasized that privacy and public security constitute critical concerns in smart cities which require additional legislative, technological, and administrative attention. Combating cybercrime in smart cities is essential for making this technology as advantageous and credible as possible for community acceptance. All stakeholders, particularly legislators, administrations, judicial systems, power companies, telecom firms, automobile manufacturers, cloud hosting, research institutes, and industries, will have to continue their assistance and endeavors [15]. Following previous literature, we propose our hypothesis:

Hypothesis 1: Artificial intelligence applications in smart cities affect cybersecurity positively

C. MEDIATING ROLE OF E-GOVERNANCE

E-governance is a revolutionary system implemented by a city government that applies AI and ICT to interconnect public bodies and corporate enterprises. To ensure maximum e-Government services and security for the public and other stakeholders, numerous governments have attempted to implement e-Governance [15]. Nonetheless, most citizens are anxious about their privacy and security while utilizing e-Government facilities, as per a 2014 UN e-Government survey [41]. Concerning security, the primary obstacles that e-Government should address are secrecy, integrity, and accessibility. Indeed, e-Governance security comprises standard security apparatus (verification, privacy, reliability, and accessibility), with a stronger reliance on information security and economic growth planning. The official statement of the European initiative, ''Security of eGovernment Systems,'' outlined 11 policies and procedures for security [20]. This initiative focused on security in e-Governance by developing a ''Privacy by Design'' technical expertise, encouraging professional and procedural measures to ensure privacy, and providing security effect evaluations of e-Government technology obligatory and accessible.

Artificial intelligence (AI) has revolutionized the way corporations work; several municipalities have begun to incorporate AI into everyday operations, yet there seem to be a substantial number of nations that would not get an advantage using Artificial intelligence and machine learning. E-voting, e-decision making, and e-participation are prominent phenomena. However, the level of adoption of e-services varies substantially across countries. Despite such advancements, governments may not benefit from e-decision making, yet the United Nations recognizes it as a critical concern [42]. AI adoption by government agencies is rising, with the United States of America and China gaining ground. Countries gain from AI in various domains, including healthcare, mobility, education, security, telecommunications, and defense services [43]. E-governance is categorized into four major brackets: governments, population, commerce, and workforce, all of which are interconnected. Every component can use one of several frameworks to incorporate e-Governance. Cybersecurity includes safeguarding network servers, storage systems, and software applications and employing appropriate technology [44]. The emergence of the e-Governance approach necessitates a complex and resilient cybersecurity strategy based on examining previous literature. Cybersecurity is therefore identified as one of the most critical domestic, regional, and national challenges. It restricts data breaches and promotes numerous users' security and privacy [15], [38], [45]. Hence, we propose our hypotheses based on previous literature as follows:

Hypothesis 2: Artificial intelligence applications in smart cities contribute to e-Governance positively

Hypothesis 3: E-Governance execution in smart cities affect cybersecurity positively

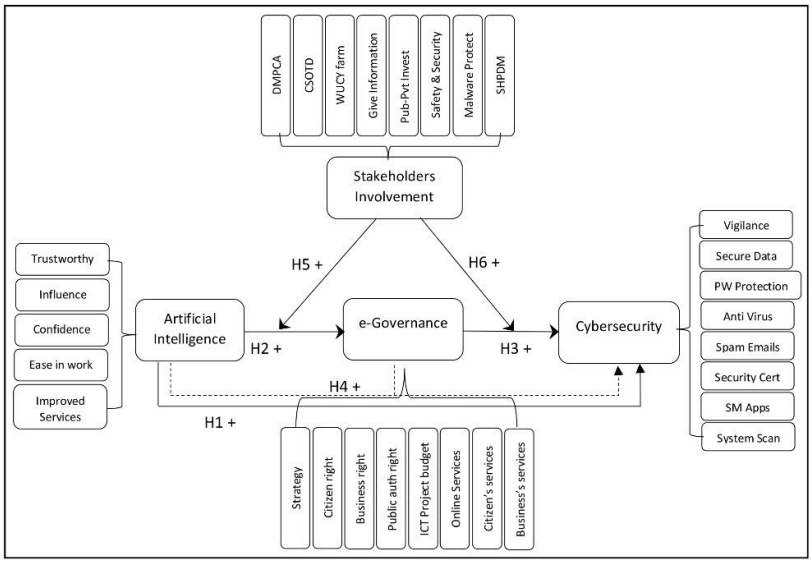

FIGURE 3. AI application in cybersecurity conceptual framework.

Hypothesis 4: E-Governance mediates between artificial intelligence and cybersecurity positively

D. MODERATING ROLE OF STAKEHOLDERS' INVOLVEMENT

As a policy matter, cybersecurity influences a wide spectrum of stakeholders who have various forms of expertise and competence on the issue [46]. It is mostly purely speculative solely within governments. The variety of stakeholders involved in attempts to secure a nation's cyberspace mental maturity necessitates active participation in executing every cybersecurity framework [47]. Nevertheless, mostly all cybersecurity policies incorporate segments on public-private collaborations, R&D financing, and awareness campaigns, which all entail private stakeholders [48]. The effective and sustainable execution of a cybersecurity policy is contingent on assuring that all stakeholders have complete confidence in the cybersecurity policy and the involvement of other stakeholders in its implementation. Stakeholders involved throughout the formulation of the cybersecurity policy may have a thorough knowledge of the strategies and whatever is desired, ensuring compliance activities are more efficient [49], [50]. Furthermore, multiple stakeholders' opinions and knowledge are essential whenever it refers to evaluating a cybersecurity policy. This opinion and knowledge are more likely to be constructive if such stakeholders were involved in the cybersecurity policy's formation and execution [51]. It also assures that transformation and adjustments improve the cybersecurity policy highly efficiently.

The concentration on involving stakeholders in the formation of technologies and workplace conditions was pioneered under participatory innovation in the Scandinavian research methodological approach [52], [53]. The participative conceptual model arose through 1970s socio-technical research designed to strengthen organizational democracy [53], [54], while subsequent legislative amendments granted personnel the freedom to affect the deployment of technologies in the corporation. The participative design method emphasizes stakeholder involvement in technical and political contexts [53]. The humanitarian perspective toward stakeholder involvement articulated by academics Mumford [55] demonstrates the sociopolitical foundations and concentration. The emphasis under this field of research is on participatory democracy and organizational satisfaction, as stakeholder involvement is considered a mechanism of assuring employees' performance and developing solutions to support the employees' demands. Such a technique offers a transparent, bottom-up approach to the institution's stakeholders and can potentially be applied to the e-Governance setting if emphasizing 'inhabitants' instead of 'employees.' This stakeholder involvement standpoint aligns nicely with enhanced accountability and transparency via proactive citizen involvement in formulating government e-services [56]. The technological method of stakeholder involvement can be observed in mainstream IS design research, where the emphasis is on developing information technology infrastructure [57]. Stakeholder involvement is considered a method of assuring the knowledge and expertise requiring higher IT architecture in the research [58]. It is often recognized as a means of growing consumer adoption of innovative technologies [59]. In this approach, the corporation's viewpoint is sometimes 'top-down,' even from an operations standpoint. The technological framework for stakeholder involvement is effective in e-Governance, as stakeholder involvement may provide the essential basic knowledge for enhancing community e-services that fulfill the requirements of their potential recipients [60]. Hence, we developed our hypotheses as follows:

Hypothesis 5: Stakeholders involvement moderates the relationship between artificial intelligence and e-Governance

Hypothesis 6: Stakeholders involvement moderates the relationship between e-Governance and cybersecurity

Figure 3 illustrates our research framework, in which artificial intelligence applications symbolize independence, dependency on cybersecurity, e-Governance as a mediating, and stakeholder involvement as moderating variables. Our empirical framework predicts that artificial intelligence applications significantly impact cybersecurity; however, when e-Governance and stakeholders' involvement are included in the equation, the direct linear trend transforms into a mediating and moderating interaction. A summary of developed research hypotheses is presented in Table 1. For the empirical mediation test, three main methodologies are employed: (1) causality processes, (2) coefficient variance, and (3) coefficient output [61].

TABLE 1. Summary of research hypotheses.

Hypotheses	Description
Hypothesis 1	Artificial intelligence applications in smart cities affect cybersecurity positively
Hypothesis 2	Artificial intelligence applications in smart cities contribute to e-Governance positively
Hypothesis 3	E-Governance execution in smart cities affect cybersecurity positively
Hypothesis 4	E-Governance mediates between artificial intelligence and cybersecurity positively
Hypothesis 5	Stakeholders involvement moderates the relationship between artificial intelligence and e-Governance
Hypothesis 6	Stakeholders involvement moderates the relationship between e-Governance and cybersecurity

III. RESEARCH METHODS

A. SAMPLING AND DATA COLLECTION

The primary objective of this study is to investigate the relationship between artificial intelligence and cybersecurity, performing e-Governance as a mediator and stakeholders' involvement as a moderator. A longitudinal research method is conducted to investigate the hypothesis derived from this study and ascertain the findings. It comprises a study into perceptions of the importance of AI in cybersecurity in smart cities. The primary data for this study was collected from 478 respondents through a survey questionnaire distributed via emails and online through several social media networks. Respondents were adequately explained about answers and were encouraged to respond to the questionnaire with utmost honesty, that may minimize issues about potential bias [62]. Lastly, participants might opt out of the survey at any moment.

This study's dataset includes an Asian country, Pakistan. The basic purpose of selecting this discrete nation to acquire samples is that Pakistan is in South Asia where regional cultures, norms, and values appear to be very important. Further, Pakistan is relatively less developed and striving to achieve its targets to implement AI across all urban cities for cybersecurity [63]. The study sample consists of civil servants, corporate personnel, representatives of the business sector, and citizens. We decided to approach private individuals and public officials; we attempted to obtain insights from both camps to minimize errors. The main study's data collection was conducted in April 2022. During the study period, 534 surveys were answered and retrieved from respondents employing an online survey questionnaire. The engagement was entirely voluntary, anonymous, and confidential. 478 surveys were meaningful after missing value responses were eliminated. The demographic characteristics of survey respondents are given in Figure 4, which include age, gender, and education. While considering about the gender, out of 478 respondents, 161 (33.7%) were females and 317 (66.3%) were males. The highest age percentage of participants 40.6% that was ranging from 18 to 35 years and 48.5% of the respondents were holding bachelor's degree.

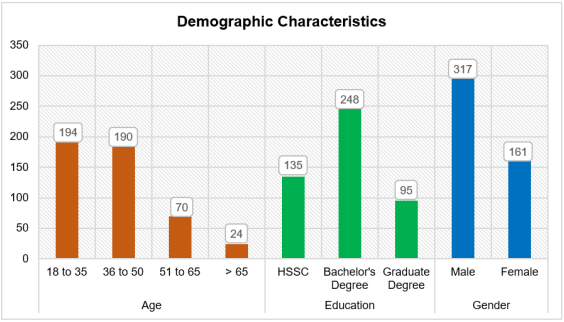

FIGURE 4. Demographic characteristics of survey respondents.

B. VARIABLE MEASUREMENT

A survey was administered to evaluate respondents' perceptions of using artificial intelligence to improve cybersecurity through e-Government and stakeholder involvement. All these components were modified from reputed scales and evaluated on a five-point Likert scale ranging from one "strongly disagree" to five "strongly agree". The survey questionnaire contained questions to measure the use of AI as an independent variable, cybersecurity as a dependent variable, e-Governance as a mediating variable, and stakeholder involvement as a moderating variable in this study. Survey questionnaire is given in Appendix's Table 6.

1) DEPENDENT VARIABLE

The probability of governments' willingness to use technology to prevent cyber-attacks was used to measure respondents' perceptions of cybersecurity. This item was adapted [64] with the input of 8 components.

2) INDEPENDENT VARIABLE

This paper incorporates a measurement scale of AI applications utilizing measurement questions from prior studies. This study adapted and employed a 05-item scale established to assess AI application [12].

3) MEDIATING VARIABLE

We adapted the OECD scales [65] to measure e-Governance. In this context, e-Governance is defined as "a local

TABLE 2. Measurement model results.

Constructs	Item Code	Loadings	t-values	VIF	α	CR	AVE	rho_A
Artificial Intelligence	AI1	0.811	35.932	2.641	0.856	0.897	0.635	0.767
	AI2	0.787	31.383	2.060				
	AI3	0.775	37.268	1.955				
	AI4	0.793	28.790	1.947				
	AI5	0.818	47.352	2.647				
e-Governance	EG1	0.933	193.032	0.572	0.950	0.959	0.746	0.712
	EG2	0.921	136.845	2.247				
	EG3	0.688	17.223	1.304				
	EG4	0.824	38.554	2.893				
	EG5	0.801	41.722	2.053				
	EG6	0.915	82.788	1.692				
	EG7	0.881	45.965	0.854				
	EG8	0.918	89.045	1.579				
Stakeholders' Involvement	SI1	0.757	34.199	1.430	0.947	0.957	0.737	0.723
	SI2	0.902	74.765	0.332				
	SI3	0.874	46.246	1.308				
	SI4	0.915	88.971	3.673				
	SI5	0.947	220.513	2.025				
	SI6	0.926	148.291	2.837				
	SI7	0.699	16.407	3.135				
	SI8	0.822	36.139	1.220				
Cybersecurity	CS1	0.924	95.671	4.601	0.934	0.947	0.690	0.709
	CS2	0.811	37.697	3.672				
	CS3	0.840	42.330	2.611				
	CS4	0.861	50.981	3.223				
	CS5	0.686	16.845	2.243				
	CS6	0.907	170.191	4.066				
	CS7	0.760	27.403	3.817				
	CS8	0.834	41.206	3.215				

Note: α = Cronbach's Alpha; CR = Composite Reliability; AVE = Average Variable Extracted

government e-Government strategy, a citizen's right to require digital communication, a business's right to require digital communication, a public authority's right to require digital communication from other parts of the public sector, the use of ICT project budget thresholds/ceilings to structure its governance processes, public services or procedures that are mandatory to use online, and a government priority to increase the number of online users."

4) MODERATING VARIABLE

Stakeholder involvement was used as moderating variable in this study. This construct was adapted [66] using 8 components.

C. ANALYSIS

Partial least square (PLS) path modeling, also referred to as "partial least square structural equation modeling" (PLS-SEM) was applied to analyze the acquired dataset for this study to investigate our hypotheses. Contemporary social science research has proven a considerable dependency on this method as one of the finest conventional methods for exploring mediating and moderating variables in social science topics [67]. Furthermore, because of several new advancements like confirmatory factor analysis, non-linear effects, and mediation and moderation influences, PLS-SEM is considered as one of the greatest modern solutions to conventional analytical techniques [68]. Several prior studies suggested multiple regression statistics to investigate moderating effect by employing quantitative and qualitative data [69]. Although numerous scholars [70] employed linear multiple regression to assess interaction effects between study variables, we believed that PLS-SEM employing SmartPLS would be the appropriate method for this study to determine our outcomes [68].

This study justifies the relevance of using PLS-SEM as a statistical method for data analysis based on the subsequent justifications. Firstly, the structural framework was developed to accurately reflect complexities, involving three different types of dependence interactions and emphasizing the relative effect of exogenous variables on endogenous variables [71]. Secondly, the theoretical framework was developed for formulating estimations and justifying the variability in vital target constructs [67]. Thirdly, This study examined the links between artificial intelligence, e-Governance, stakeholder involvement, and cybersecurity. This particular area was considered to be in an early phase of theoretical development, thereby offering the potential of exploring innovative phenomenon [71].

A convergent validity test was used to construct a measurement model of the complete self-ratings employing confirmatory factor analysis (CFA). After that, the modification index is performed to include items from the variables. The item with the highest modification index score was eliminated initially, followed by the next item until the acceptable goodness of fit was attained. Most of the goodness of fit indices exceeded the desired cutoff criterion, although a

TABLE 3. Descriptive statistics, mean, standard deviation, correlation and discriminant validity results.

	MEAN	S.D.	VIF	1	2	3	4	5	6
1. Artificial Intelligence	3.989	0.455	1.708	***0.797***	0.548	0.653	*0.312*	*0.134*	*0.250*
2. e-Governance	4.032	0.380	1.549	0.857**	***0.864***	0.634	*0.483*	*0.126*	*0.176*
3. Stakeholder's Involvement	3.908	0.830	3.030	0.867**	0.997**	***0.858***	0.627	0.514	*0.214*
4. Cybersecurity	3.918	0.799	3.693	0.916**	0.936**	0.941**	***0.831***	0.465	0.576
5. Gender	0.670	0.470	1.00	0.146**	0.109	0.175**	0.174**	1	0.556
6. Education	1.32	0.466	1.20	0.241**	0.293**	0.198**	0.223**	0.217**	1

Note: S.D. = Standard Deviation; Significance levels: P<0.05*; P<0.01**.
Diagonal, bold, and italicized factors are square root of average variance extracted (AVE).
The factors shown in the lower-left half are correlations between the constructs values.
The italicized factors shown in the upper-right half are HTMT values.

few factor loadings were less than the baseline level of 0.5. Consequently, we eliminated them to collect valid data for our model. The loadings of all variables items are affirmed to be higher than the alpha level of 0.5 [72]. The exact model fit indicator was determined utilizing goodness-of-fit analysis, which estimated if the data sample aligned the interconnect route map of the integrative framework. Cronbach's alpha coefficients were utilized to measure the observations' reliability, and correlation was employed to confirm the sample's validity. The items for each factor were constructed using prior findings. These indices can provide greater insights into construct reliability and validity. Cronbach's alpha's level of confidence should be greater than 0.50.

IV. STUDY FINDINGS

SmartPLS 4.0 software was applied to conduct PLS-SEM path modeling [73]. The standard setup for the PLS algorithm involved utilizing the basic approach (path weighting scheme and a maximum iteration limit of 300). The values of the beta coefficients, mean, standard deviations, t-values, p-values, and the corresponding 95% bias-correlated and accelerated confidence interval bootstrap were computed with the use of basic 5000 subsamples bootstrapping. The analytical and descriptive technique in PLS-SEM path modeling includes both the measurement and structural models. The measurement model was examined with reliability and validity analysis, by estimating each item and constructing reliability (CR), as well as convergent and discriminant validity. The validation of the structural model was confirmed according to the established guidelines presented by Hair et al. [68].

A. MEASUREMENT MODEL ASSESSMENT

1) RELIABILITY

The adoption criteria suggested for accepting each item exhibiting standardized factor loadings of 0.60 or higher was used [68]. The study conducted a standardized factor loadings analysis to evaluate the four developed variables: artificial intelligence, e-Governance, stakeholder's involvement, and cybersecurity. Initial analysis in Table 2 indicates that all standardized factor loadings exhibited a high level of significance. T-statistics values for the standard errors surpassed 1.96, with a two-tailed p-value of 0.05. Hence, each item reliability of all four constructs was considered acceptable.

2) CONVERGENT VALIDITY

The composite reliability (CR) approach was used to estimate the reliability of each construct. Table 2 displays the values of Cronbach's alpha (α) and CR indices. Both kinds of reliability indices outweighed the recommended threshold value of 0.70 for significance, hence confirming that all four constructs in the framework were considered reliable [61]. Moreover, Table 2 displays the average variance extracted (AVE) values for each of the four constructs included in the framework. The results of this study demonstrate that the values of AVE have exceeded the minimum threshold of 0.50 for significance, thereby suggesting that all constructs displayed necessary convergent validity.

3) DISCRIMINANT VALIDITY

Two dominant techniques were applied to determine the discriminant validity. Table 3 presents the confirmation of the Fornell-Larcker criterion through the evaluation to determine if the AVE of each construct exceeded its associations with other constructs in the framework, as measured by the square root of the AVE. The associations between the constructs are presented in the lower-left quadrant of Table 3. The HTMT (heterotrait–monotrait) ratio generated an outcome that confirmed all HTMT indices to be less than the critical threshold of 0.85 or 0.90 [74], as presented in the upper-right quadrant of Table 3.

4) MODEL FIT

Overall model fit was assessed applying the SRMR values (standardized root mean square residual) to validate the PLS-SEM path modeling [74]. The SRMR can be described as "the root means square discrepancy between the observed correlations and the model-implied correlation" [68]. A model fit is regarded as adequate if the SRMR value is below 0.080. The SRMR value of 0.072 in Table 4 suggests the PLS-SEM has an adequate overall model fit.

B. STRUCTURAL MODEL ASSESSMENT

The findings of the overall model indicate that the data is good fit the model adequately. Initially, the VIF values were computed to determine the existence of multicollinearity in the structural model. The findings indicate the absence of

TABLE 4. Structural model results.

Structural Path	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values	Supported or Not
Hypothesized Relationships (Direct Effects)						
Artificial Intelligence -> Cybersecurity	0.273	0.270	0.023	11.654	0.000	Supported
Artificial Intelligence -> e-Governance	0.027	0.027	0.107	3.917	0.000	Supported
e-Governance -> Cybersecurity	0.314	0.308	0.170	2.847	0.025	Supported
Stakeholders' Involvement x Artificial Intelligence -> e-Governance	0.511	0.511	0.014	3.317	0.001	Supported
Stakeholders' Involvement x e-Governance -> Cybersecurity	0.188	0.188	0.023	8.368	0.000	Supported
Non-Hypothesized Relationships (Control Variables)						
Stakeholders' Involvement -> Cybersecurity	3.743	3.756	0.238	15.72	0.000	Supported
Stakeholders' Involvement -> e-Governance	1.021	1.021	0.007	145.067	0.000	Supported
GEN -> Artificial Intelligence	-0.539	-0.54	0.099	5.419	0.000	Supported
GEN -> Cybersecurity	-0.226	-0.229	0.031	7.295	0.000	Supported
GEN -> Stakeholders' Involvement	-0.529	-0.531	0.114	4.621	0.000	Supported
GEN -> e-Governance	0.018	0.018	0.008	2.233	0.026	Supported
AGE -> Artificial Intelligence	-0.143	-0.14	0.064	2.217	0.027	Supported
AGE -> Cybersecurity	0.16	0.162	0.021	7.749	0.000	Supported
AGE -> Stakeholders' Involvement	0.077	0.078	0.064	1.209	0.227	NOT
AGE -> e-Governance	0.029	0.029	0.004	8.214	0.000	Supported
EDU -> Artificial Intelligence	-0.027	-0.03	0.072	0.371	0.711	NOT
EDU -> Cybersecurity	0.196	0.196	0.013	14.695	0.000	Supported
EDU -> Stakeholders' Involvement	-0.29	-0.29	0.057	5.084	0.000	Supported
EDU -> e-Governance	0.032	0.033	0.006	5.059	0.000	Supported
SRMR Composite Model = 0.072						
R^2 (Cybersecurity) = 0.940	Q^2 (Cybersecurity) = 0.280					
R^2 (e-Governance) = 0.995	Q^2 (e-Governance) = 0.255					

Note: R^2 = Determination Coefficients; Q^2 = Predictive Relevance of Endogenous; R^2 Value Threshold ≥0.25, ≥0.50, ≥0.75 (weak, moderate, and substantial respectively)

significant multicollinearity among the predictor variables in the structural model, as evidenced by the VIF values in Table 3, which were below the threshold of 5. Subsequently, the efficacy of PLS-SEM path modeling was examined through the adoption of the blindfolding approach, with an omission distance of 7. When the index of Q2 predictive relevance exceeds 0, it indicates that the structural model possesses adequate predictive relevance. the predictive accuracy of the PLS path model appears appropriate based on the findings presented in Table 4, particularly in terms of out-of-sample forecasting [68]. The R2 values provide additional support for the Q2 predictive relevance findings. Table 4 displays that the PLS-SEM path model exhibits suitable in-sample predicting capability [75].

C. CORRELATION ANALYSIS

Table 3 describes the correlation between factors, reliability, and descriptive analysis. The mean value for artificial intelligence was 3.989 (SD = 0.455), suggesting that participants believed to react to the AI application in smart cities for cybersecurity, and the mean value for e-Governance was 4.032 (SD = 0.380), denoting that most survey participants believed in e-Governance for cybersecurity with the use of technology.

The value for stakeholders' involvement was 3.908 (SD = 0.830), and the value for cybersecurity was 3.918 (SD = 0.799), demonstrating that participants agreed to cybersecurity with AI applications, e-Government, and stakeholder involvement in smart cities. The correlation between AI and cybersecurity was ($r = 0.865$ **; $p < 0.01$), between AI and e-Governance ($r = 0.973$ **; $p < 0.01$), between e-Governance and cybersecurity ($r = 0.878$ **; $p < 0.01$), and between stakeholder involvement and cybersecurity was ($r = 0.998$ **; $p < 0.01$), demonstrating a substantial correlation between all measures.

D. STRUCTRUAL EQUATIONAL MODELING RESULTS

1) DIRECT EFFECTS

The first issue that we investigated was how AI applications influence cybersecurity. Towards that objective, we formulated hypothesis H1 and analyzed it using PLS-SEM path modeling because the endogenous variable is evaluated on

TABLE 5. Mediation analysis results.

	Original sample (O)	Sample mean (M)	Std. deviation (STDEV)	T statistics (|O/STDEV|)	P values	Supported or Not
Artificial Intelligence -> Cybersecurity	0.273	0.270	0.023	11.654	0.000	Supported
Artificial Intelligence -> e-Governance -> Cybersecurity	0.320	0.315	0.074	2.838	0.036	Supported

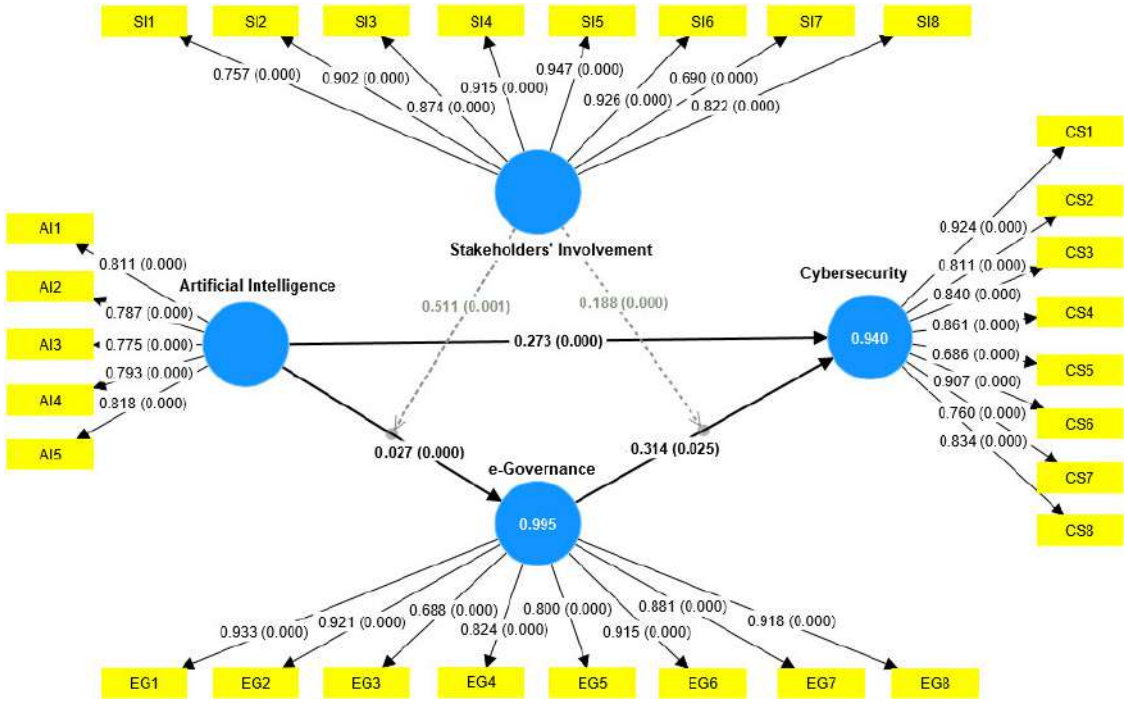

FIGURE 5. Structural model results.

an ordinal scale. Table 4 presents the findings. Our results demonstrated strong significant outcomes ($\beta = 0.273^{**}$, t = 11.564, p < 0.01); thus, we argue that the exogenous variable significantly impacts cybersecurity in smart cities.

Non-hypothesized relationships in Table 4 are the standard model that reflects the effects of the control variables such as gender, age, and education. Table 4 and Figure 5 were applied to examine the legitimacy of H2 and H3, which contend that there is a significant positive association between artificial intelligence and e-Governance, and between e-Governance and cybersecurity, respectively. The findings indicate that artificial intelligence had a substantial positive influence on e-Governance ($\beta = 0.27$ **, t = 3.927, p < 0.001), while e-Governance had a significant positive effect on cybersecurity ($\beta = 0.314^{**}$, t = 2.847, p < 0.05), thus providing support for H2 and H3, respectively. Generally, the effect size evaluates the proportional impact of an independent (exogenous) variable, on a dependent (endogenous) variable [68]. This approach facilitates the assessment of various hypotheses and the determination of whether a predictor variable significantly impacts the R^2 of the dependent variable.

2) MODERATING EFFECTS

Further, moderating hypotheses were examined thoroughly, and the outcomes in Table 4 showed that there is strong support for our assumptions. When stakeholders' involvement is included as a moderator in structural framework, the association between AI applications and e-Governance is intensified, and the results suggest considerable support for hypothesis 5 ($\beta = 0.511^{**}$, t = 3.317, p < 0.01) as verified in Figure 4. In hypothesis 6, we predicted that incorporating stakeholders' involvement as a moderator strengthens the association between e-Governance and cybersecurity, and we discovered significant evidence for our hypothesis ($\beta = 0.188^{**}$, t = 8.368, p < 0.01) validated in Figure 5 as well. Hence, these results indicate strong support for H5 and H6.

3) MEDIATING EFFECT

This study used the PLS-SEM path model (Figure 5) to indicate a partially mediated model. An analysis was performed to explore the extent to which e-Governance served as a mediator between artificial intelligence applications and cybersecurity in the framework. A nonparametric bootstrapping analysis was performed to assess the mediating effect's significance [68] using SmartPLS 4.0 software [76], following the method defined by [77]. The results reported in Table 5 suggest that there is a direct significant positive association between artificial intelligence applications and cybersecurity ($\beta = 0.273^{**}$, t = 11.654, p < 0.01),

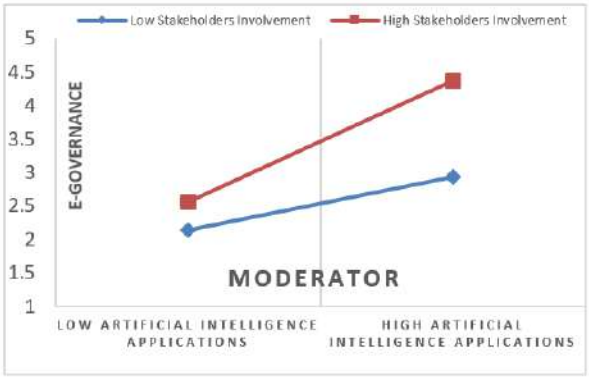

FIGURE 6. Moderating role of stakeholders' involvement on the relationship between AI applications and e-Governance.

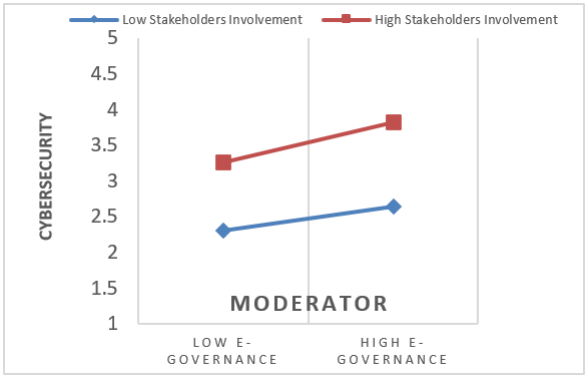

FIGURE 7. Moderating role of stakeholders' involvement on the relationship between e-governance and cybersecurity.

Additionally, the indirect effect of this association through e-Governance also proved to be significant ($\beta = 0.320^{**}$, t = 2.838, p < 0.05). The results indicate that a partial mediation effect of e-Governance on the association between artificial intelligence applications and cybersecurity exists. The findings further suggest that the influence of artificial intelligence applications on cybersecurity was partially mediated by e-Governance. Hence, hypothesis 4 is strongly supported as proposed.

4) CONTROL VARIABLES

The PLS-SEM path model exhibited significant positive impacts for various control variables, as reported in Table 4. The study found a significant negative association between gender and artificial intelligence (β = -0.539**, t = 5.419, p < 0.01), cybersecurity (β = -0.226**, t = 7.295, p < 0.01), and stakeholders involvement (β = -0.529**, t = 4.621, p < 0.01), whereas a positive association between gender and e-Governance (β = 0.018**, t = 2.233, p < 0.01). A significant positive association was found between age and e-Governance (β = 0.029**, t = 8.214, p < 0.01) and cybersecurity (β = 0.160**, t = 7.749, p < 0.01), whereas a significant negative association between age and artificial intelligence applications (β = -0.143**, t = 2.217, p < 0.05). No relationship was found between age and stakeholders involvement. Lastly, a negative association between education and stakeholder involvement (β = -0.290**, t = 5.084, p < 0.01), however, a positive association between education and e-Governance (β = 0.032**, t = 5.059, p < 0.01) and cybersecurity (β = 0.196**, t = 14.695, p < 0.01) was found. No relationship was found between education and artificial intelligence applications. The findings related to the control variables are consistent with previous studies conducted [78], [79], [80].

V. DISCUSSIONS

As summarized in this research, artificial intelligence (AI), recognized as one of the most important technologies in industry 4.0, may play an important part in cognitive cybersecurity systems and operations. Widely Implemented AI techniques, including machine learning, deep learning, computational linguistics, knowledge discovery and rationale, and the notion of knowledge or deterministic intelligent computer simulation may be utilized to rectify today's multiple cybersecurity threats through e-governance smartly, termed securing web-based systems from cyber-threats, malfunction, or security breaches. Nonetheless, various research challenges have been discovered within the domain of AI-driven cybersecurity. The main objective of this study was to explore the direct and indirect connections between artificial intelligence, e-governance, stakeholder involvement, and cybersecurity. We investigated the direct interactions of AI and cybersecurity, AI and e-governance, e-governance and cybersecurity, and stakeholder involvement and cybersecurity. Furthermore, we examined the indirect relationships: the mediating role of e-governance between AI and cybersecurity and the moderating role of stakeholders' involvement in the relationship between AI and e-governance, as well as e-governance and cybersecurity.

Table 4 represents a wide variety of outcomes. All the interactions between AI applications, e-governance, stakeholder involvement, and cybersecurity were pointedly positive. Table 4 suggests that multiple discrete AI features do not correspond with various outcome parameters. Another plausible explanation of such data is that contrasting outcome measurements might deteriorate from a positive bias, in which city administrators exaggerate the cybersecurity efficiency of their metropolises. Furthermore, AI technology applications are not only elements influencing cybersecurity, but other elements, including the city's e-governance framework and stakeholder involvement, may significantly affect cyber threat mitigation. The conceptual association between artificial intelligence, e-governance, stakeholders' involvement, and cybersecurity was found in several studies, but empirical support was insufficient. Therefore, according to this study's analysis, a city adept in applying artificial intelligence facets seems to be highly interested in e-governance and rather effective in cybersecurity with effective involvement of stakeholders. The insights reported in this study are remarkable because they suggest that all stakeholders must be involved in enhancing cybersecurity in smart cities employing

artificial intelligence technology. After all, such deployments will influence them.

Cities with sophisticated AI technology implementation strategies are more concerned about improving cybersecurity, which benefits in mitigating cyber-attacks and developing progressive e-governance systems that significantly complement our projected H1 and H2. Furthermore, cities with advanced e-governance structures are stronger determinants of better cybersecurity deployment to protect their inhabitants, government agencies, and business organizations from malware attacks, with e-governance mechanisms being vital in enhancing electronic services in smart cities utilizing internet connections that are susceptible to hacking, endorsing our assumption in H3. Our statistical findings demonstrate that AI applications positively and significantly impact e-governance. That e-governance substantially affects cybersecurity but indicated that AI applications have a statistically significant mediating influence on cybersecurity through e-governance, significantly sustaining our predicted H4, asserting that cities with better AI technology can strengthen cybersecurity by optimizing e-governance structure to provide e-services to their inhabitants.

Preceding academics asserted that while assessing complexities in city decision-making mechanisms and how they influence smart city outcomes, it is essential to consider stakeholders' perspectives [81]. Because smart cities involve stakeholders from public and private segments, it is essential to determine and comprehend the various stakeholders and respective interests in the city's security and protection. Further empirical investigation revealed that stakeholders' involvement significantly and positively influenced superior cybersecurity. The outcomes validated H5 and H6 by demonstrating that the direct interactions between AI applications and e-governance, as well as the relationship between e-governance and cybersecurity, are strengthened by the involvement of stakeholders, confirming those moderating associations as showed in Figure 6 and Figure 7. We explored the importance of stakeholders' involvement in enhancing cybersecurity to eliminate ransomware and the ramifications for stakeholders' satisfaction in the perspective of smart cities through e-governance. As per our study outcomes, involving stakeholders in the decision-making of implementing cybersecurity in smart cities has the potential to strengthen the relationship between AI applications and e-governance, as well as e-governance and cybersecurity. There is a massive difference in the beliefs and perceptions of various city stakeholders regarding cybersecurity, particularly those participating in electronic services, that has affected users' contentment over time. Despite the present detrimental effect of the current problem, there is an immediate requirement to develop cities that lack e-governance systems by implementing greater cybersecurity in all public institutions.

VI. STUDY IMPLICATIONS

The findings of this experimental study demonstrated that most city governments are rigorously adopting security strategies to effectively detect and identify cybersecurity breaches, establishing a conceptual framework. This study has broad practical implications because it concentrates on various topics such as hazards, financing, and the nature and consequence of cybersecurity incidents experienced. This research empirically indicated that most participants believe their cities conformed with policies and strategy and that the technologies implemented can detect, react to, and analyze a security issue appropriately. It was further asserted that in the absence of stakeholder involvement, respective cities could not prevent a security incident. It demonstrates the necessity of additional investigation.

The findings of this study can be utilized to influence legislation, governmental policies, and regulatory requirements in operation. The study findings indicated that city governments often must review decision-making strategies to decrease the number of cybersecurity threats through prevention strategies such as adopting AI applications and implementing an e-governance structure to deliver e-services. Effective security strategies must be adopted aggressively to eliminate cybersecurity hazards to all stakeholders.

VII. LIMITATIONS AND FUTURE RESEARCH

The findings of this experimental study serve as a framework for future research on developing a different framework to mitigate cybersecurity threats. This framework could be incorporated with existing community frameworks to enhance commercial and economic effectiveness by expanding the knowledge base in the field of cybersecurity. The limitations of this research, like those of other scientific studies, must be addressed when evaluating, broadening, and generalizing the outcomes. Although this study was conducted in an emerging Asian country, Pakistan, the qualities of the investigated participants may not apply to other countries and contexts. Consequently, more research on intercontinental variances in cultural forces geared to confront e-governance and stakeholders' involvement in cybersecurity is essential. Moreover, since involvement throughout this survey was voluntary, there was certain to be some variation in cognition. The Harman one-factor assessment was conducted to eliminate any underlying problems. The analysis showed that each primary structure reflects roughly similar variation, indicating that our datasets do not contain a substantial common method bias.

VIII. CONCLUSION

The current study examined artificial intelligence applications to overcome cybersecurity challenges. The research findings indicate that artificial intelligence is progressively converting into an indispensable technology to enhance information security performance. Individuals are not capable anymore of fully secure project-level cyberattacks, and artificial intelligence offers the desired analytics and threat intelligence that security practitioners might use to minimize the likelihood of an infringement and strengthen the security structure of an enterprise. Since more technologies

TABLE 6. Survey questionnaire to collect data sample.

Items	Source
Artificial Intelligence	
AI1: In my opinion, Information from the Artificial Intelligence science community is trustworthy AI2: In my opinion, the Artificial Intelligence science community has much influence on society AI3: I have very much confidence in the Artificial Intelligence science community AI4: In my opinion, Artificial intelligence has helped to ease working in the community AI5: In my opinion, Government services have improved with Artificial Intelligence	(Bokhari & Myeong, 2022)
E-Governance	
EG1: My local government has a strategy for digital government or e-Government EG2: It is a citizen's right to require digital communication with the public sector EG3: It is a business right to require digital communication with the public sector EG4: It is a public authority right to require digital communication from other parts of the public sector EG5: My government uses ICT project budget thresholds/ceilings to structure its governance processes EG6: There are many public services or procedures mandatory to use online EG7: It is a government priority to increase the number of mandatory online services aimed at citizens EG8: It is a government priority to increase the number of mandatory online services aimed at businesses	(OECD, 2015)
Stakeholders Involvement	
SI1: Smart cities are engaged in the development and management of privatized corporate activity SI2: City authorities focuses on cyber-attack security and optimizing technological deployment across all sectors SI3: Agriculture requests from farm owner groups involved in water usage crop yield are included in local administration SI4: The smart city admin's bureaus attempt to give Information SI5: Corporations from public-private investment can establish structures with the involvement of prospective entrepreneurs SI6: The main community union emphasizes the importance of technological applications in ensuring safety and security SI7: It is the responsibility of IT firms to provide antivirus software to protect against malware threats SI8: All pertinent stakeholders are involved in decision-making in a smart city	(Casadevall, 2016)
Cybersecurity	
CS1: I am vigilant about the private data I share in cyberspace CS2: I ensure that the necessary people can only view the data I share in cyberspace CS3: I use the phone verification service to protect my email password CS4: I use an up-to-date antivirus program on my devices CS5: I do not open spam mails sent to my email address CS6: I do not trust websites without a security certificate CS7: I use social media applications to share Information in cyberspace CS8: I regularly scan my devices with an antivirus program	(Arpaci & Sevinc, 2021)

are introduced into the usual human lifestyle, the impact of artificial intelligence on daily human life may intensify. Several scholars assert that AI will have a catastrophic influence on technological development, whereas others have a contradictory assumption of AI applications' positive effect on everyday human life. One of the major features of cloud computing in cybersecurity is the capacity to evaluate and eliminate risk faster. Several individuals are concerned about cybercriminals' capability to perform incredibly advanced cyber and technological attacks. Moreover, artificial intelligence can contribute to the detection and classification of hazards, the structuring of incident management, and the detection of cyberattacks before their occurrence. Consequently, despite potential negatives, artificial intelligence would contribute to the evolution of cybersecurity and support enterprises in establishing an enhanced security strategy.

This study further sought to investigate artificial intelligence and its ongoing development in offering e-government services and then highlight the need to accommodate strategies regarding cybersecurity for adopting innovative social and technical processes in government serving the community. The eventual objective of smart city governments is to establish and strengthen relationships with most stakeholders, as their involvement strengthens e-government efficacy which fortifies cybersecurity. Public services should be administered using innovative AI technologies and e-governance in convenient modes to eliminate the barriers between stakeholders and city governments, while state officials can still sustain the model for better support. While e-government is progressing, the citizens and those in authority or advocating mechatronics are lagging. That creates disparities in cybersecurity standards for something in the virtual environment, potentially turning performance into a much more difficult experience with several grooves to monitor. With an elevation in the initiatives identified in this research, stakeholders' involvement and awareness of e-governance and cybersecurity may rise, enabling benefits associated with the virtual environment.

APPENDIX

See Table 6.

REFERENCES

[1] B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry," *Mater. Today, Proc.*, vol. 531, pp. 1–6, 2021, doi: 10.1016/j.matpr.2021.02.531.

[2] M. Komar, V. Kochan, L. Dubchak, A. Sachenko, V. Golovko, S. Bezobrazov, and I. Romanets, "High performance adaptive system for cyber attacks detection," in *Proc. 9th IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl. (IDAACS)*, vol. 2, Sep. 2017, pp. 853–858.

[3] M. D. Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Evanston, IL, USA: Routledge, 2007.

[4] F. Fransen, A. Smulders, and R. Kerkdijk, "Cyber security information exchange to gain insight into the effects of cyber threats and incidents," *Elektrotechnik Informationstechnik*, vol. 132, no. 2, pp. 106–112, Mar. 2015.

[5] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the industrial Internet of Things: A systematic literature review," *Comput. Ind.*, vol. 137, May 2022, Art. no. 103614.

[6] G. A. Weaver, B. Feddersen, L. Marla, D. Wei, A. Rose, and M. Van Moer, "Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach," *Transp. Res. C, Emerg. Technol.*, vol. 137, Apr. 2022, Art. no. 103423.

[7] M. Bada and J. R. C. Nurse, "The social and psychological impact of cyberattacks," in *Emerging Cyber Threats and Cognitive Vulnerabilities*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 73–92.

[8] G. Allen and T. Chan, *Artificial Intelligence and National Security*. Cambridge, MA, USA: Belfer Center for Science and International Affairs, 2017.
[9] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K.-K. R. Choo, "Artificial intelligence in cyber security: Research advances, challenges, and opportunities," *Artif. Intell. Rev.*, vol. 55, pp. 1029–1053, Feb. 2022.
[10] Z. I. Khisamova, I. R. Begishev, and E. L. Sidorenko, "Artificial intelligence and problems of ensuring cyber security," *Int. J. Cyber Criminol.*, vol. 13, no. 2, pp. 564–577, 2019.
[11] J.-H. Li, "Cyber security meets artificial intelligence: A survey," *Frontiers Inf. Technol. Electron. Eng.*, vol. 19, no. 12, pp. 1462–1474, 2018.
[12] S. A. A. Bokhari and S. Myeong, "Use of artificial intelligence in smart cities for smart decision-making: A social innovation perspective," *Sustainability*, vol. 14, no. 2, p. 620, Jan. 2022.
[13] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101589.
[14] J. Singh, M. Sajid, S. K. Gupta, and R. A. Haidri, "Artificial intelligence and blockchain technologies for smart city," in *Intelligent Green Technologies for Sustainable Smart Cities*. Beverly, MA, USA: Scrivener Publishing, 2022, pp. 317–330.
[15] R. Khatoun and S. Zeadally, "Cybersecurity and privacy solutions in smart cities," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 51–59, Mar. 2017.
[16] K. Kourtit, M. M. M. Pele, P. Nijkamp, and D. T. Pele, "Safe cities in the new urban world: A comparative cluster dynamics analysis through machine learning," *Sustain. Cities Soc.*, vol. 66, Mar. 2021, Art. no. 102665.
[17] J. Engelbert, L. van Zoonen, and F. Hirzalla, "Excluding citizens from the European smart city: The discourse practices of pursuing and granting smartness," *Technol. Forecasting Social Change*, vol. 142, pp. 347–353, May 2019.
[18] C. Wang, E. Steinfeld, J. L. Maisel, and B. Kang, "Is your smart city inclusive? Evaluating proposals from the U.S. department of transportation's smart city challenge," *Sustain. Cities Soc.*, vol. 74, Nov. 2021, Art. no. 103148.
[19] J. Ju, L. Liu, and Y. Feng, "Citizen-centered big data analysis-driven governance intelligence framework for smart cities," *Telecommun. Policy*, vol. 42, no. 10, pp. 881–896, 2018.
[20] M. Weber, T. Weiss, F. Gechter, and R. Kriesten, "Approach for improved development of advanced driver assistance systems for future smart mobility concepts," *Auto. Intell. Syst.*, vol. 3, no. 1, p. 2, Feb. 2023.
[21] S. U. Khan, N. Khan, F. U. M. Ullah, M. J. Kim, M. Y. Lee, and S. W. Baik, "Towards intelligent building energy management: AI-based framework for power consumption and generation forecasting," *Energy Buildings*, vol. 279, Jan. 2023, Art. no. 112705.
[22] S. Myeong, M. J. Ahn, Y. Kim, S. Chu, and W. Suh, "Government data performance: The roles of technology, government capacity, and globalization through the effects of national innovativeness," *Sustainability*, vol. 13, no. 22, p. 12589, Nov. 2021.
[23] W. L. Filho, T. Wall, S. A. R. Mucova, G. J. Nagy, A.-L. Balogun, J. M. Luetz, A. W. Ng, M. Kovaleva, F. M. S. Azam, F. Alves, Z. Guevara, N. R. Matandirotya, A. Skouloudis, A. Tzachor, K. Malakar, and O. Gandhi, "Deploying artificial intelligence for climate change adaptation," *Technol. Forecasting Social Change*, vol. 180, Jul. 2022, Art. no. 121662.
[24] M. Alam and I. R. Khan, "Application of AI in smart cities," in *Industrial Transformation*. Boca Raton, FL, USA: CRC Press, 2022, pp. 61–86.
[25] H. Kumar, M. K. Singh, M. P. Gupta, and J. Madaan, "Moving towards smart cities: Solutions that lead to the smart city transformation framework," *Technol. Forecasting Social Change*, vol. 153, Apr. 2020, Art. no. 119281.
[26] A. Kankanhalli, Y. Charalabidis, and S. Mellouli, "IoT and AI for smart government: A research agenda," *Government Inf. Quart.*, vol. 36, no. 2, pp. 304–309, Apr. 2019.
[27] W. Li, P. Yi, D. Zhang, and Y. Zhou, "Assessment of coordinated development between social economy and ecological environment: Case study of resource-based cities in northeastern China," *Sustain. Cities Soc.*, vol. 59, Aug. 2020, Art. no. 102208.
[28] M. M. Aborokbah, S. Al-Mutairi, A. K. Sangaiah, and O. W. Samuel, "Adaptive context aware decision computing paradigm for intensive health care delivery in smart cities—A case analysis," *Sustain. Cities Soc.*, vol. 41, pp. 919–924, Aug. 2018.
[29] Z.-T. Zhu, M.-H. Yu, and P. Riezebos, "A research framework of smart education," *Smart Learn. Environ.*, vol. 3, no. 1, pp. 1–17, Dec. 2016.
[30] J. Al Dakheel, C. D. Pero, N. Aste, and F. Leonforte, "Smart buildings features and key performance indicators: A review," *Sustain. Cities Soc.*, vol. 61, Oct. 2020, Art. no. 102328.
[31] M.-P. Efthymiopoulos, "Cyber-security in smart cities: The case of Dubai," *J. Innov. Entrepreneurship*, vol. 5, no. 1, pp. 1–16, Dec. 2016.
[32] D. Gasper and O. A. Gómez, "Human security thinking in practice: 'Personal security', 'citizen security' and comprehensive mappings," *Contemp. Politics*, vol. 21, no. 1, pp. 100–116, Jan. 2015.
[33] D. Bonte, *Role of Smart Cities for Economic Development*. New York, NY, USA: ABI Research, 2018, pp. 1–16.
[34] H. Kolivand, M. S. Sunar, S. Y. Kakh, R. Al-Rousan, and I. Ismail, "Photorealistic rendering: A survey on evaluation," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 25983–26008, Oct. 2018.
[35] V. D. Soni, "Challenges and solution for artificial intelligence in cybersecurity of the USA," Social Sci. Res. Netw. (SSRN), USA, Tech. Rep. 3624487, 2020.
[36] M. Liu, J. Ma, L. Lin, M. Ge, Q. Wang, and C. Liu, "Intelligent assembly system for mechanical products and key technology based on Internet of Things," *J. Intell. Manuf.*, vol. 28, no. 2, pp. 271–299, Feb. 2017.
[37] A. L. Shoushtari, P. Dario, and S. Mazzoleni, "A review on the evolvement trend of robotic interaction control," *Ind. Robot, Int. J.*, vol. 43, no. 5, pp. 535–551, Aug. 2016.
[38] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, "Weaponized AI for cyber attacks," *J. Inf. Secur. Appl.*, vol. 57, Mar. 2021, Art. no. 102722.
[39] B. Heller, "Combating terrorist-related content through AI and information sharing," *Algorithms*. The Transatlantic Working Group, Apr. 2019, pp. 1–8. [Online]. Available: https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/05/Combating_Terrorist_Content_TWG_Heller_April_2019.pdf
[40] T. C. Truong, I. Zelinka, J. Plucar, M. Candík, and V. Šulc, "Artificial intelligence and cybersecurity: Past, presence, and future," in *Artificial Intelligence and Evolutionary Computations in Engineering Systems*. Singapore: Springer, 2020.
[41] I. Peña-López, *United Nations E-Government Survey 2014: E-Government for the Future We Want*. New York, NY, USA: United Nations, 2014.
[42] T. Kaya, "Artificial intelligence driven e-government: The engage model to improve e-decision making," in *Proc. 19th Eur. Conf. Digit. Government (ECDG)*. New York, NY, USA: Academic, Oct. 2019, pp. 43–50.
[43] W. G. D. Sousa, E. R. P. D. Melo, P. H. D. S. Bermejo, R. A. S. Farias, and A. O. Gomes, "How and where is artificial intelligence in the public sector going? A literature review and research agenda," *Government Inf. Quart.*, vol. 36, no. 4, Oct. 2019, Art. no. 101392.
[44] M. Sannigrahi, B. Sahoo, and R. N. Behera, "Introduction to cybersecurity in e-governance systems," in *Strategies for E-Service, E-Governance, and Cybersecurity*. New York, NY, USA: Academic, 2021, pp. 1–11.
[45] M. Grobler, J. J. van Vuuren, and L. Leenen, "Implementation of a cyber security policy in South Africa: Reflection on progress and the way forward," in *ICT Critical Infrastructures and Society*. Amsterdam, The Netherlands: Springer, Sep. 2012.
[46] J. M. Bauer and M. J. G. van Eeten, "Cybersecurity: Stakeholder incentives, externalities, and policy options," *Telecommun. Policy*, vol. 33, nos. 10–11, pp. 706–719, Nov. 2009.
[47] J. Alexander, B. Barlow, and D. Haskin, "National security personnel system (NSPS): An analysis of key stakeholders' perceptions during DoD's implementation of NSPS," Graduate School Bus. Public, Naval Postgraduate School, Monterey, CA, USA, Tech. Rep., 2010.
[48] T. Tropina, C. Callanan, and T. Tropina, "Public–private collaboration: Cybercrime, cybersecurity and national security," in *Self- and Co-Regulation in Cybercrime, Cybersecurity and National Security*. Cham, Switzerland: Springer, 2015, pp. 1–41.
[49] N. Gcaza and R. von Solms, "A strategy for a cybersecurity culture: A South African perspective," *Electron. J. Inf. Syst. Developing Countries*, vol. 80, no. 1, pp. 1–17, May 2017.
[50] R. Sabillon, V. Cavaller, and J. Cano, "National cyber security strategies: Global trends in cyberspace," *Int. J. Comput. Sci. Softw. Eng.*, vol. 5, no. 5, p. 67, 2016.
[51] *Commonwealth Approach for Developing National Cybersecurity Strategies: A Guide to Creating a Cohesive and Inclusive Approach to Delivering a Safe, Secure and Resilient Cyberspace*, Commonwealth Telecommun. Org. (CTO), London, U.K., 2015.

[52] P. J. Ågerfalk, K. Axelsson, and M. Bergquist, "Addressing climate change through stakeholder-centric information systems research: A Scandinavian approach for the masses," *Int. J. Inf. Manage.*, vol. 63, Apr. 2022, Art. no. 102447.
[53] J. Gregory, "Scandinavian approaches to participatory design," *Int. J. Eng. Educ.*, vol. 19, no. 1, pp. 62–74, 2003.
[54] O. Hanseth and N. Lundberg, "Designing work oriented infrastructures," *Comput. Supported Cooperat. Work*, vol. 10, nos. 3–4, pp. 347–372, 2001.
[55] E. Mumford, "A socio-technical approach to systems design," *Requirements Eng.*, vol. 5, no. 2, pp. 125–133, Sep. 2000.
[56] M. Ruus, I. Pappel, V. Tsap, and D. Draheim, "Enhancing public e-service delivery: Recognizing and meeting user needs of youngsters in Estonia," in *Digital Transformation and Global Society*. Saint Petersburg, Russia: Springer, Jun. 2019.
[57] A. Serrat-Capdevila, J. B. Valdes, and H. V. Gupta, "Decision support systems in water resources planning and management: Stakeholder participation and the sustainable path to science-based decision making," in *Efficient Decision Support Systems—Practice and Challenges From Current to Future*, vol. 3. London, U.K.: IntechOpen, 2011, pp. 423–440.
[58] R. Subramanyam, F. L. Weisstein, and M. S. Krishnan, "User participation in software development projects," *Commun. ACM*, vol. 53, no. 3, pp. 137–141, Mar. 2010.
[59] C. Bayley and S. French, "Designing a participatory process for stakeholder involvement in a societal decision," *Group Decis. Negotiation*, vol. 17, no. 3, pp. 195–210, May 2008.
[60] K. Axelsson, U. Melin, and I. Lindgren, "Public e-services for agency efficiency and citizen benefit—Findings from a stakeholder centered analysis," *Government Inf. Quart.*, vol. 30, no. 1, pp. 10–22, Jan. 2013.
[61] J. F. Hair, "Multivariate data analysis: An overview," in *International Encyclopedia of Statistical Science*. Berlin, Germany: Springer, 2010, pp. 904–907, doi: 10.1007/978-3-642-04898-2.
[62] P. E. Spector, "Method variance in organizational research: Truth or urban legend?" *Org. Res. Methods*, vol. 9, no. 2, pp. 221–232, Apr. 2006.
[63] N. N. Abbas, T. Ahmed, S. H. U. Shah, M. Omar, and H. W. Park, "Investigating the applications of artificial intelligence in cyber security," *Scientometrics*, vol. 121, no. 2, pp. 1189–1211, Nov. 2019.
[64] I. Arpaci and K. Sevinc, "Development of the cybersecurity scale (CS-S): Evidence of validity and reliability," *Inf. Develop.*, vol. 38, no. 2, pp. 218–226, Jun. 2022.
[65] *Government at a Glance 2015*, OECD Publishing, Paris, France, 2015.
[66] S. R. Casadevall, "Improving the management of water multi-functionality through stakeholder involvement in decision-making processes," *Utilities Policy*, vol. 43, pp. 71–81, Dec. 2016.
[67] J. F. Hair, M. Sarstedt, C. M. Ringle, and J. A. Mena, "An assessment of the use of partial least squares structural equation modeling in marketing research," *J. Acad. Marketing Sci.*, vol. 40, no. 3, pp. 414–433, May 2012.
[68] J. Hair, C. L. Hollingsworth, A. B. Randolph, and A. Y. L. Chong, "An updated and expanded assessment of PLS-SEM in information systems research," *Ind. Manage. Data Syst.*, vol. 117, no. 3, pp. 442–458, Apr. 2017.
[69] N. F. Richter, G. Cepeda, J. L. Roldán, and C. M. Ringle, "European management research using partial least squares structural equation modeling (PLS-SEM)," *Eur. Manage. J.*, vol. 34, no. 6, pp. 589–597, Dec. 2016.
[70] S. D. Li, "Testing mediation using multiple regression and structural equation modeling analyses in secondary data," *Eval. Rev.*, vol. 35, no. 3, pp. 240–268, Jun. 2011.
[71] A. K. Montoya, "Moderation analysis in two-instance repeated measures designs: Probing methods and multiple moderator models," *Behav. Res. Methods*, vol. 51, no. 1, pp. 61–82, Feb. 2019.
[72] D. Shi, T. Lee, and A. Maydeu-Olivares, "Understanding the model size effect on SEM fit indices," *Educ. Psychol. Meas.*, vol. 79, no. 2, pp. 310–334, Apr. 2019.
[73] M. Sarstedt and J.-H. Cheah, "Partial least squares structural equation modeling using SmartPLS: A software review," *J. Marketing Anal.*, vol. 7, no. 3, pp. 196–202, Sep. 2019.
[74] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *J. Acad. Marketing Sci.*, vol. 43, no. 1, pp. 115–135, Jan. 2015.
[75] H. U. R. Khan, M. Ali, H. G. T. Olya, M. Zulqarnain, and Z. R. Khan, "Transformational leadership, corporate social responsibility, organizational innovation, and organizational performance: Symmetrical and asymmetrical analytical approaches," *Corporate Social Responsibility Environ. Manage.*, vol. 25, no. 6, pp. 1270–1283, Nov. 2018.
[76] C. M. Ringle and M. Sarstedt, "Gain more insight from your PLS-SEM results: The importance-performance map analysis," *Ind. Manage. Data Syst.*, vol. 116, no. 9, pp. 1865–1886, Oct. 2016.
[77] A. F. Hayes and K. J. Preacher, "Conditional process modeling: Using structural equation modeling to examine contingent causal processes," in *Structural Equation Modeling: A Second Course*, vol. 2, G. R. Hancock and R. O. Mueller, Eds. Greenwich, CT, USA: Information Age, 2013, pp. 217–264.
[78] *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance*, World Health Org., Geneva, Switzerland, 2021. Accessed: Apr. 22, 2023.
[79] E. Bassey, E. Mulligan, and A. Ojo, "A conceptual framework for digital tax administration—A systematic review," *Government Inf. Quart.*, vol. 39, no. 4, Oct. 2022, Art. no. 101754.
[80] M. Hilowle, W. Yeoh, M. Grobler, G. Pye, and F. Jiang, "Users' adoption of national digital identity systems: Human-centric cybersecurity review," *J. Comput. Inf. Syst.*, pp. 1–16, Nov. 2022.
[81] K. Axelsson and M. Granath, "Stakeholders' stake and relation to smartness in smart city development: Insights from a Swedish city planning project," *Government Inf. Quart.*, vol. 35, no. 4, pp. 693–702, Oct. 2018.

SYED ASAD ABBAS BOKHARI (Member, IEEE) was born in Mandi Bahauddin, Punjab, Pakistan, in 1982. He received the M.B.A. degree from the Virtual University of Pakistan and the M.S.B.A. degree in strategic management from Ajou University, Republic of Korea, in 2020. He is currently pursuing the Ph.D. degree with the Center for Convergence Security and e-Governance, Inha University, Incheon, Republic of Korea, in 2023.

From 2014 to 2017, he was a Teaching Assistant with the Ajou Business School, Ajou University. Since 2021, he has been a Research Assistant with the Center for Convergence Security and e-Governance, Inha University. He is the author of 13 published articles in SSCI, SCI, Scopus, and KCI Journals. His current research interests include artificial intelligence applications, e-Governance, smart cities, innovations, technology adoption, political corruption, and CSR strategy.

SEUNGHWAN MYEONG was born in the Republic of Korea. He received the B.S. degree in public administration from the Hankuk University of Foreign Studies, South Korea, the M.P.A. degree in public administration, and the Ph.D. degree in social science from Syracuse University in 1996.

Since 2000, he has been a Professor with the Public Administration Department, Inha University, Incheon, Republic of Korea. He is the author of ten book and more than 100 articles. His current research interests include smart city, smart governance, e-government, block chain, government reform, industrial security, cyber security, policy decision process, policy analysis and evaluation, methodology Methods and techniques: social science methodology, policy analysis, big data, and interdisciplinary approach. Current projects are building models and methods for Industrial security governance issues, including technical, physical, and managerial perspectives. His research interests are electronic government and e-governance, information management in public organizations, and information and communication policy. He served as a President of the Korean Association for Policy Analysis and Evaluation (KAPAE) in 2016 and the Korea Association for Policy Studies (KAPS) in 2018. He currently serves as the Center for Security Convergence and eGovernance (CSCeG) Director. He was a Vice Chair of the Digital New-deal Committee in the Presidential Commission on Policy Planning (2021-2022). His work appeared in the Administration and Society, Korean Journal of Information Policy, Government Information Quarterly, Sustainability, and others.