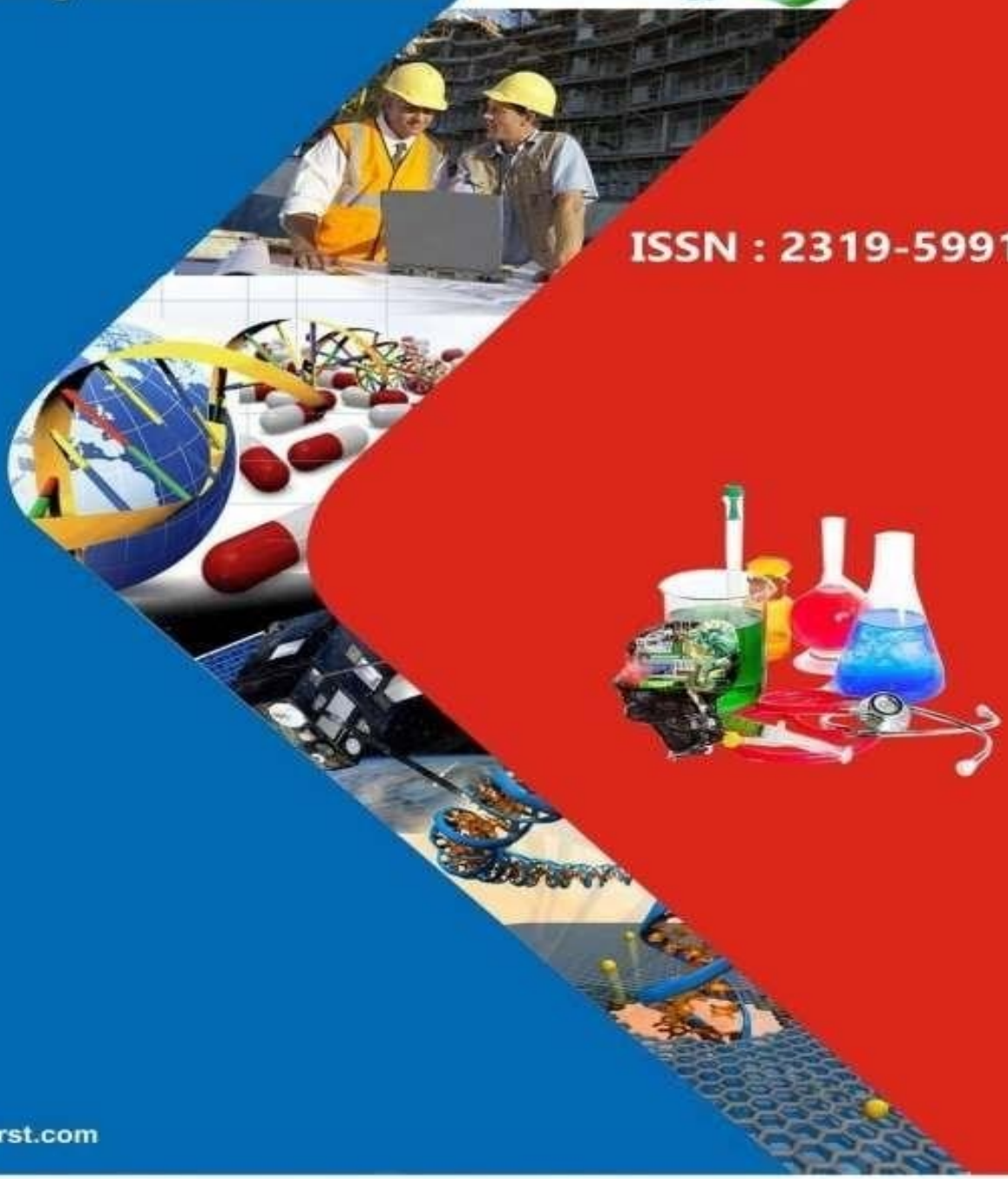
International Journal of Engineering Research and Science & Technology

IJERST



ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp589-598

Vol. 21, Issue 2, 2025

THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENHANCING E-GOVERNANCE AND CYBERSECURITY IN SMART CITIES: INSIGHTS FROM STAKEHOLDERS

[1]*Sesham, Kartik, MCA Student, Department Of MCA*

[2]*K Muddu Swamy, M.Tech, Assistant Professor, Department Of MCA*

[12]*Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool*

ABSTRACT

One crucial technology of the Fourth Industrial Revolution (Industry 4.0) is artificial intelligence (AI), which guards computer network systems against viruses, phishing, cyberattacks, damage, and unauthorised access. Through e-Government, AI has the ability to improve the cyber capabilities and security of nationstates, local governments, and non-state organisations. According to current research, there is a mixed link between cybersecurity, e-Government, and AI; however, this relationship is thought to be context-specific. Numerous stakeholders with diverse backgrounds and specialities in AI, e-Government, and cybersecurity impact and are influenced by these fields. This research examines the close connection between cybersecurity, e-Government, and AI in order to close this context-specific gap. Additionally, this research looks at how e-Government mediates the link between AI and cybersecurity as well as how stakeholder participation modifies that relationship. According to the findings of the PLS-SEM path modelling investigation, e-Government somewhat mediates the relationship between cybersecurity and artificial intelligence. Similar findings were made about the moderating effect of stakeholder participation on the link between cybersecurity and e-Government and AI. Since all stakeholders have an interest in a dynamic, open, and safe cyberspace while using e-services, it follows that stakeholder participation is crucial to AI and e-Government. This paper offers useful recommendations for enhancing cybersecurity measures for smart city government agencies.

1. INTRODUCTION

In the present world, cyber security has emerged as a crucial issue that demands safeguarding the computer network from any attacks [1], [2]. An intentional assault that targets computer networks, pertinent data, programs, and electronic information and causes subnational organisations to incite violence against noncombatant opponents is known as a cyberattack. Cyber risks are evolving along with technology, thus new preventative measures must be created [3], [4]. Cyberattacks are said to have increased in frequency in the industrial sector, causing major financial loss and damage to infrastructure. Organisations' increasing dependence on internet technologies that allow for the storing of financial and personal data is the main cause of the growth in cyberattacks [5].

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp589-598
Vol. 21, Issue 2, 2025

Because hacking causes financial loss and exposes private information, it is thus seen as maybe the most important issue in the contemporary setting. Any member of society may be harmed by cyberattacks such as ransomware infections, malware, phishing, and denial of service [6]. Humans are also significantly impacted psychologically by cyberattacks, which cause stress, anxiety, and dissatisfaction [7].

Applications of artificial intelligence (AI) have the potential to improve the national security and cyber capabilities of non-state organisations, regional governments, and sovereign nations [8], [9]. AI is a dependable method for reducing the impact of cyberattacks [10]. AI is machine intelligence that performs intelligence-related tasks [11]. Expertise from human experts is incorporated into strategic planning and decision-making [12], including diagnosing medical conditions and drawing conclusions based on expert observations. Zarina et al. [10] have shown that artificial intelligence (AI) has both positive and negative impacts on cyber security, with the latter being the ability to facilitate the instigation phase of cyberattacks, which leads to faster and more destructive assaults. By strengthening security measures and encouraging cyberspace security, AI has the potential to significantly enhance cyber security in the future. Additionally, AI has improved machine learning applications for malware categorisation and networked intrusion detection and helps security professionals identify the signs of cyber hazards [13]. Last but not least, the current AI phenomena has enhanced city exterior assaults against significant security risks and modified creative remedies [14].

A smart city offers a variety of creative answers to the problems that local government encounters. On the other hand, e-Government now relies heavily on information and communication technology (ICT). There are risks and challenges when integrating ICT into a city's infrastructure [15]. When people regularly check their email, e-banking, and other digital services over unprotected Wi-Fi networks, they expose themselves to cybercrimes including hacking, denial-of-service attacks, and cracking. One of the most significant distinguishing characteristics that may be used to classify safe cities worldwide is the use of cyber security technology to safeguard e-Government services [16]. Because it highlights the value of social and interpersonal capital in urban initiatives that centre on integrating stakeholders in the Digital Realm and involving residents in service improvement to implement appropriate government services that match citizens' necessities, the "inclusive smart city" framework has generated a lot of interest somewhere along this trend [17], [18]. Because smart cities are predicted to create robust social ecologies that heavily rely on web technology, recent research on e-services and technologies have also highlighted the significance of establishing a citizens-centered approach. As such, stakeholder relationships may be greatly

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp589-598
Vol. 21, Issue 2, 2025

impacted by online technology and services [19].

Cyber security has been largely overlooked, particularly when considering stakeholders who use online government services, despite prior research showing the impact of AI in smart mobility [20], energy management [21], public services [22], climate change [23], and smart security [24] in smart cities. This study developed the following research question to close this contextual gap:

• How can AI applications in smart cities directly affect cyber security?

• How can AI applications in smart cities affect e-Government, and how does e-Government directly affect cyber security?

• Does e-Government act as a mediator in the interaction between cyber security and AI applications? This research also looks at how stakeholders' engagement affects the link between e-Government and cyber security as well as the interaction between AI and e-Government.

This study aims to experimentally answer these primary research concerns, predicated on the idea that interactions vary depending on the setting. The study's suggested methodology for categorising the degree of cyber security in a smart city is shown in Figure 1. Stakeholder involvement's moderating relevance was extensively investigated using Smart PLS 4.0's structural equation modelling (SEM). Because of its well-established suitability for analysing complicated research models and its extensive usage in analysing research frameworks in previous studies, PLS-SEM route modelling was chosen as the analytical method. A review of the literature on the connections between artificial intelligence, e-Government, stakeholder participation, cyber security, and the main theories being discussed is covered in Section II. Section III describes the methodology, analysis, research strategy, and data sampling. Section IV presents the statistical results. In Section V, the talks are compiled, conclusions are made, and potential directions for further study are suggested.

2. LITERATURE SURVEY

"The ability of artificial intelligence techniques to effectively mitigate cyber security threats in the IT industry,"

I. Z. Chaloob, J. S. Ahmed, B. Alhayani, and H. J. Mohammed,

The researcher used primary data and a quantitative study approach in order to ascertain the efficacy of artificial intelligence methods in mitigating cyber security threats, specifically in the context of Iraq. Data was gathered by the researcher from workers in the IT sector. Confirmatory factor analysis, discriminant validity, basic model analysis, and hypothesis evaluation were performed on a sample of 468 people. All of the variables' P-values were found to be significant, with the exception of the expert system, which showed no discernible relationship to cyber security or artificial intelligence. The primary problems were accessibility, sample size, geographic location, and fewer variables.

"High performance adaptive system for detecting cyberattacks,"

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

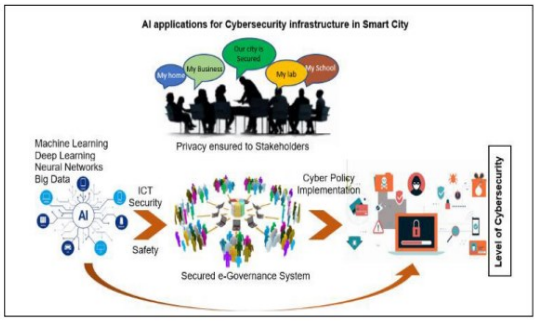
https://doi.org/10.62643/ijerst.2025.v21.i2.pp589-598

Vol. 21, Issue 2, 2025

S. Bezobrazov, I. Romanets, V. Kochan, L. Dubchak, A. Sachenko, V. Golovko, and M. Komar

A generalised framework of a highly performance adaptable system for cyberattack detection was created in order to improve the security of the intrusion detection system. Artificial intelligence techniques were suggested in order to increase its resilience. The primary instrument for detecting cyberattacks was neural immune detectors. These cyberattack detection and classification detectors, along with other susceptible subsystems, were put into practice using programmable logic arrays. High performance was achieved by developing pertinent subsystem structures and using the Mamdani fuzzy inference rules.

3. SYSTEM ARCHITECTURE



4. EXISTING SYSTEM

The idea of a "smart city" is intriguing because of its clever characteristics. Its reach goes beyond lowering expenses and resource consumption and raising the degree of urban economic efficiency. Instead, it includes the use of digital technologies, or information and communication technology (ICT), to improve service delivery and the integration of various city components via smart devices. Citizens now enjoy a greater level of life as a consequence of traditional metropolitan regions being transformed into smart cities [25].

Several basic components may be used to define an example of a smart city, as shown in Figure 2. By creating a bilateral partnership between the government and residents, smart government encompasses a number of elements, including smart offices, smart supervision, smart services, and smart decision-making, to improve municipal governance performance and maximise inhabitants' quality of life [26]. In order to raise the people's level of living and happiness and foster the idea that the government is service-oriented, smart public services provide a range of online services and electronic information. The creation of a smart economy has the potential to improve urban economies' efficiency, provide sustainable job possibilities, and enable the seamless growth of resource-driven cities [27].

Smart healthcare systems that use e-health data to predict a person's health, such as remote monitoring of people with heart disease, may determine a person's susceptibility and provide crucial information for the best possible care [28]. In order to provide people with a seamless educational experience and individualised support, smart education is a concept that uses data-centric intelligent education in

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp589-598
Vol. 21, Issue 2, 2025

many situations in smart cities [29]. intelligent structures that efficiently use many data sources. The structure is able to detect any malfunctions in its functioning and meet the needs of its occupants and users. Structures with attributes like efficiency, adaptability, security, and simplicity of use are very appealing [30]. In order to facilitate urban growth and decision-making, smart transport systems are digitally controlled and multidimensional. Real-time highway status monitoring and route forecast may be used to schedule trips strategically [31]. Detection, alarm, emergency support, and other features related to individual safety and cybersecurity protection are only a few of the advantages that smart security provides [32].

Numerous infrastructure systems, such as those related to energy, the grid, healthcare, traffic, transportation, water distribution, and wastewater disposal, are known to be equipped with computer networks. Smart cities, which seek to enhance their infrastructure and provide more advanced, efficient, and environmentally friendly solutions, have emerged as a consequence of the Internet of Things. However, according to a study by ABI Research, by 2024, only 44% of the total cybersecurity costs for critical systems will be allocated to industries like healthcare, security, water, transportation, and other related fields. This means that there will be a severe lack of funding for safeguarding infrastructure from cybersecurity threats [33]. Therefore, there is a chance that there will be a number of issues involving cyberattacks on important urban infrastructure, which could have major consequences. For example, encrypting malware to disable computer systems and taking over infrastructure communication could have a major effect on a city's financial security and cause significant losses to its residents' assets and finances. Similar to this, the social structure may be destroyed and a condition of anxiety can break out if communication networks, electricity grids, water conservation measures, and other infrastructure are disrupted or destroyed. Additionally, manipulating sensor data to cause havoc, like in disaster detection systems, and stealing important data, including persons, consumers, healthcare, and private information.

The importance of artificial intelligence in identifying and stopping cyberattacks [38], fighting terrorism [39], improving security in key areas [36], and fostering resilience in vulnerable sovereign locations [34] has been the subject of many earlier studies. In his paper, Soni [35] claimed that data gathered from a wide range of scientific and technical experts indicates that the United States' ability to balance the benefits and drawbacks of AI, particularly in cybersecurity, will determine how far AI can go. AI is widely regarded as one of the most amazing technological advancements of the digital age, and cybersecurity is without a doubt the field that stands to gain the most from it. In global security markets, optimisation algorithms, tactics, tools, and businesses offering AI-based solutions are all changing

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp589-598
Vol. 21, Issue 2, 2025

[40]. It is underlined that privacy and public safety are important issues in smart cities that need more administrative, technical, and legal focus. In order to make this technology as beneficial and believable as feasible for community adoption, cybercrime must be prevented in smart cities. It will be necessary for all parties involved to keep up their support and efforts, especially lawmakers, governments, courts, power providers, communication companies, automakers, cloud hosting, research institutions, and industries [15].

Disadvantages

• Data complexity: In order to identify cybersecurity, the majority of machine learning models now in use need to be able to properly analyse massive and complicated datasets.

• Data availability: In order to provide precise predictions, the majority of machine learning models need a lot of data. The accuracy of the model may degrade if data is not accessible in large enough amounts.

• Inaccurate labelling: The accuracy of the machine learning models that are now in use depends on how well the input dataset was used for training. Inaccurate labelling of the data prevents the model from producing reliable predictions.

5. PROPOSED SYSTEM

Investigating the connection between cybersecurity and artificial intelligence is the main goal of the suggested system, which uses e-Government as a mediator and stakeholder participation as a moderator. The hypothesis developed from this study is investigated and the results are determined using a longitudinal research approach. It includes a survey on how people see the value of AI in smart city cybersecurity. 478 respondents completed a survey questionnaire that was disseminated via email and online across many social media platforms, providing the study's core data.

In order to reduce concerns about possible bias, respondents were urged to complete the questionnaire honestly and were given sufficient explanations for their responses. Finally, respondents may withdraw from the poll at any time.

Advantages

- Applications of artificial intelligence in smart cities have a favourable impact on e-Government.
- The use of e-government in smart cities has a good impact on cybersecurity.
- E-government acts as a beneficial mediator between cybersecurity and artificial intelligence.

6. IMPLEMENTATION

Modules

Service Provider

The Service Provider must use a working user name and password to log in to this module. He can do a number of tasks after successfully logging in, including browsing and training and testing data sets. See the Accuracy of Trained and Tested Datasets in

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp589-598

Vol. 21, Issue 2, 2025

a Bar Chart View Cyber Attack Type Prediction, View Cyber Attack Type Ratio Prediction, Download Predicted Data Sets, and View Accuracy Results of Trained and Tested Datasets View the Results of the Cyber Attack Type Ratio See Every Remote User.

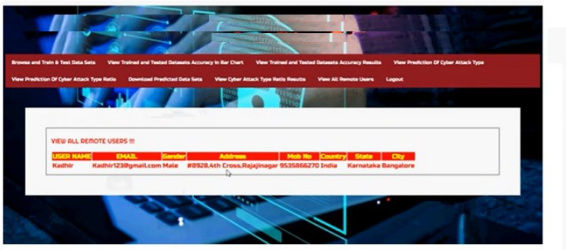
View and Authorize Users

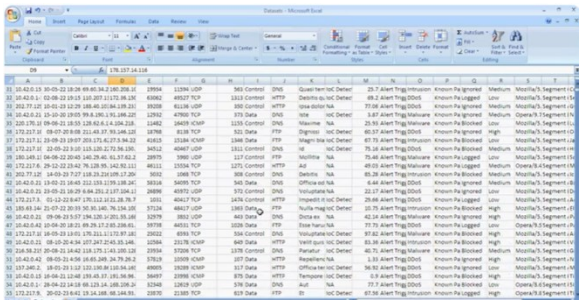
The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

Remote User

A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and authorised user name to log in. Following a successful login, the user may do tasks including registering and logging in, predicting the kind of cyberattack, and seeing their profile.

7. SCREENSHOTS



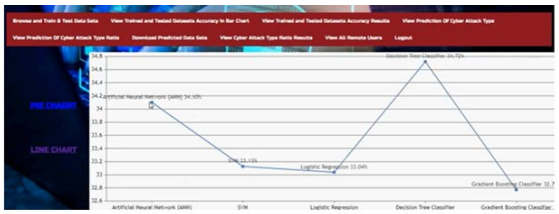


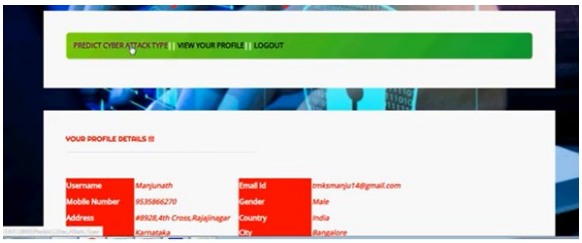
International Journal of Engineering Research and Science & Technology

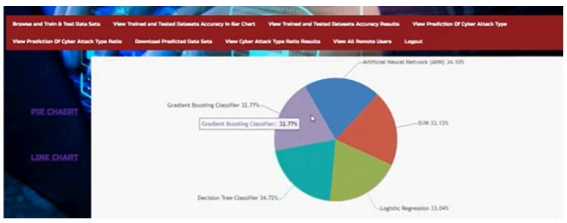
ISSN 2319-5991 www.ijerst.com

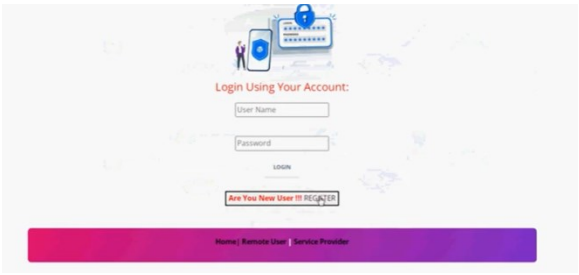
https://doi.org/10.62643/ijerst.2025.v21.i2.pp589-598

Vol. 21, Issue 2, 2025









8. CONCLUSION

Applications of artificial intelligence to address cyber security issues were investigated in the present research. According to the study results, artificial intelligence is gradually evolving into a technology that is essential for improving information security performance. Since humans can no longer carry out completely secure project-level cyberattacks, artificial intelligence provides the analytics and threat intelligence that security professionals need to reduce the possibility of an intrusion and fortify an organization's security framework. Because of the increased computational power in cyber security, danger may be assessed and eliminated more quickly. The capacity of cybercriminals to carry out very sophisticated technology and cyberattacks worries a lot of people. Additionally, artificial intelligence may help with danger categorisation and identification, incident management planning, and anticipating cyberattacks ahead of time. Therefore, in spite of any drawbacks, artificial intelligence

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp589-598
Vol. 21, Issue 2, 2025

would advance cyber security and assist businesses in developing a more robust security plan.

In addition to examining artificial intelligence and its further advancement in providing e-government services, this research aimed to emphasise the need of including cyber security measures for implementing cutting-edge social and technological procedures in government that benefit the public. The ultimate goal of smart city governments is to build and maintain connections with the majority of stakeholders since their participation increases the effectiveness of e-government, which in turn boosts cyber security. Innovative AI technologies and e-governance should be used to manage public services in comfortable ways to remove obstacles between local governments and stakeholders. State authorities may continue to promote the model for improved assistance. The public, those in positions of power, and those who support mechatronics are falling behind as e-government advances. This leads to differences in cyber security requirements for virtual environments, which might make performance much more challenging with several areas to keep an eye on. Benefits related to the virtual environment may be made possible by increased stakeholder participation and understanding of e-governance and cyber security as a result of the activities mentioned in this study.

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

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp589-598
Vol. 21, Issue 2, 2025

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.