STAKEHOLDER PERSPECTIVES ON THE INFLUENCE OF ARTIFICIAL INTELLIGENCE IN E-GOVERNANCE AND CYBERSECURITY FOR SMART CITIES

[1]*N ARAVIND KUMAR,* [2]*KADARLA NIHARIKA*
[1]*Assistant Professor,*[2]*Student*
Department of CSE
Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT

One of the most important technologies of the Fourth Industrial Revolution (Industry 4.0) is artificial intelligence (AI), which guards computer network systems against damage, phishing, malware, cyberattacks, and unauthorised access. Through e-Government, artificial intelligence (AI) has the potential to improve the cyber capabilities and security of states, local governments, and non-state enterprises. Research currently available shows a mixed link between cybersecurity, e-Government, and AI; however, it is thought that this relationship depends on the situation. Different stakeholders with varying levels of knowledge and experience in their respective fields have an impact on and influence AI, e-Governance, and cybersecurity. This research explores the direct link between cybersecurity, e-Government, and AI in order to close this context-specific gap. This research also looks at the moderating influence of stakeholder participation on the link between AI, e-Governance, and cybersecurity, as well as the mediating function that e-Governance plays in this relationship. PLS-SEM route modelling research findings showed that e-Government has a somewhat mediating effect between cybersecurity and AI. Similarly, the link between e-Governance and cybersecurity as well as AI and e-Governance was shown to be moderated by the engagement of stakeholders. Because all stakeholders have an interest in a thriving, transparent, and safe cyberspace while utilising e-services, it is implied that stakeholder participation in AI and e-Governance is crucial. This report offers smart city governments useful recommendations for bolstering their cybersecurity defences.

1. INTRODUCTION

In today's contemporary world, cyber security has emerged as a crucial issue that calls for safeguarding the computer network from possible attacks [1], [2]. An intentional assault against computer networks, pertinent data, programs, and electronic information is known as a cyber-attack. As a consequence, subnational organisations may incite violence against opponents who are not combatants. Cyber risks are evolving together with technology, which calls for the creation of fresh preventative measures [3], [4]. Cyberattacks are said to have increased in frequency in the industrial sector, causing major financial loss as well as major damage to infrastructure. Organisations are increasingly relying on internet technology

to store personal and financial data, which has led to an increase in cyberattacks [5].

Consequently, since it causes financial loss and exposes private information, it is seen as maybe the most important issue in the current environment. Cyberattacks may cause damage to any member of society and include ransomware infections, malware, phishing, and denial of service attacks [6]. Cyberattacks can significantly affect people's psychological well-being, causing stress, anxiety, and dissatisfaction [7].

Applications of artificial intelligence (AI) have the potential to enhance the cyber capabilities and national security of non-state organisations, regional governments, and sovereign nations [8], [9]. AI is a dependable method for reducing the impact of cyberattacks [10]. Artificial intelligence (AI) is machine intelligence that performs intelligence-related tasks [11]. Expertise from human professionals is incorporated for strategic planning and decision-making [12], including diagnosing medical conditions and drawing conclusions with the help of experts. Zarina et al. [10] have shown that artificial intelligence (AI) may have both positive and negative impacts on cyber security. The negative consequence of AI is that it can facilitate the instigation phase of cyber assaults, leading to faster and more severe attacks. In the future, artificial intelligence (AI) has the potential to significantly enhance cyber security by boosting security measures and encouraging security in cyberspace. Moreover, AI has improved machine learning applications for malware categorisation and networked intrusion detection and helps security professionals identify indicators of cyber hazards [13]. Finally, the current AI phenomena has enhanced city exterior assaults and modified creative remedies against significant security dangers [14].

A smart city offers several creative answers to the various problems that the management of the city encounters. But now, e-Government cannot function without information and communication technology (ICT). There are risks and challenges when integrating ICT into a city's infrastructure [15]. Individuals are vulnerable to cybercrimes such as denial-of-service attacks, cracking, and hacking when they regularly use unsecured Wi-Fi networks to check their email, e-banking, and other digital services. One of the key differentiators that may be used to classify safe cities worldwide is cyber security, which uses technology to safeguard e-Government services [16]. The "inclusive smart city" framework, which emphasises the value of social and interpersonal capital in urban initiatives that centre on stakeholders' inclusion in the digital realm and involving residents in service improvement to implement appropriate government services that match citizens' needs, has sparked a lot of interest somewhere in this trend [17], [18]. Because it is anticipated that smart cities would create robust social ecologies that heavily rely on web technology, recent research on e-services and technologies have also emphasised the need of establishing a citizens-centered approach for smart cities.

As such, stakeholder relationships may be greatly impacted by online technology and services [19].

The impact of artificial intelligence (AI) on smart mobility [20], energy management [21], public services [22], climate change [23], and smart security [24] in smart cities has been shown in earlier research; however, cyber security has received little attention, particularly when it comes to stakeholders who use online government services. The following research question was developed for this study in order to close this contextual gap:

• How can AI-powered smart city applications directly impact cyber security?

• How do AI-powered smart city apps affect e-Government, and how does e-Government directly affect cyber security?

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

Based on the idea that interactions vary depending on the situation, these primary research issues are sought to be experimentally addressed in this study. The suggested framework for classifying cyber security level in a smart city is shown in Figure 1. In order to thoroughly investigate the moderating impact of stakeholder participation, Smart PLS 4.0 used structural equation modelling, or SEM. Because PLS-SEM route modelling has been widely used to analyse research frameworks in previous studies and is recognised as a suitable analytical tool for complicated research models, it was chosen as the analytical method. Section II begins with a review of the relevant literature about the connections between e-Government, cyber security, stakeholder engagement, and artificial intelligence. Section III contains descriptions of the data sampling, research framework, methodology, and analysis. Section IV contains the statistical results. In Section V, the talks are summed up, conclusions are made, and potential directions for further study are suggested.

2. LITERATURE SURVEY

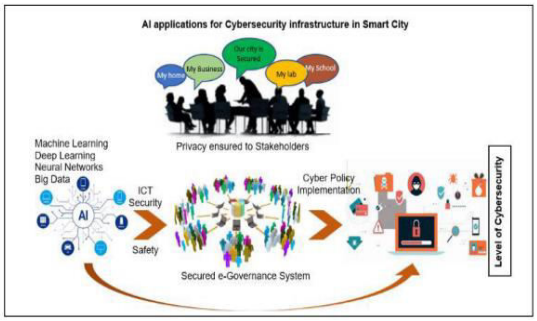
‘‘Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry,’’

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

The aim of the researcher was to determine the effectiveness of artificial intelligence techniques against cyber security risks particularly in case of Iraq, Researcher has opted for quantitative method of research design along with primary data. The researcher collected the data from employees working in this IT industry. The sample size for this study was 468 and confirmatory factor analysis, discriminant validity, basic analysis of model and lastly, hypothesis assessment was carried out. The P-values of all variables were obtained as significant apart from expert system which had no significant relation with artificial intelligence and cyber security. Geographical area, sample size, less variables and accessibility was the main issue.

''High performance adaptive system for cyber attacks detection,''
M. Komar, V. Kochan, L. Dubchak, A. Sachenko, V. Golovko, S. Bezobrazov, and I. Romanets,
To increase the security of intrusion detection system, generalized structure of highly performance adaptive system for cyber attacks detection was developed. To improve its robustness, methods of artificial intelligence were proposed. Neural immune detectors were used as the main tool for identifying cyber attacks. These detectors for cyber attacks identification and classification and other vulnerable subsystems were implemented in programmable logic arrays. To provide high performance, the Mamdani fuzzy inference rules were used and relevant subsystem structures were developed.

3. SYSTEM ARCHITECTURE



4. EXISTING SYSTEM

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 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.

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].

Disadvantages

• The complexity of data: Most of the existing machine learning models must be able to accurately interpret large and complex datasets to detect Cybersecurity.
• Data availability: Most machine learning models require large amounts of data to create accurate predictions. If data is unavailable in sufficient quantities, then model accuracy may suffer.
• Incorrect labeling: The existing machine learning models are only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

5. PROPOSED SYSTEM

The primary objective of the proposed system 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. Lastly, participants might opt out of the survey at any moment.

Advantages

- Artificial intelligence applications in smartcities contribute to e-Governance positively.
- E-Governance execution in smart cities affect cybersecurity positively.
- E-Governance mediates between artificial intelligence and cybersecurity positively.

6. IMPLEMENTATION

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Browse and

Train & Test Data Sets, View Trained and Tested Datasets Accuracy in Bar Chart, View Trained and Tested Datasets Accuracy Results, View Prediction Of Cyber Attack Type, View Prediction Of Cyber Attack Type Ratio, Download Predicted Data Sets, View Cyber Attack Type Ratio Results, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT CYBER ATTACK TYPE, VIEW YOUR PROFILE.

7. CONCLUSION

The present research looked at uses of artificial intelligence to address cyber security issues. The study's conclusions show that artificial intelligence is gradually becoming into a necessary tool for improving information security performance. People are no longer able to carry out project-level cyberattacks that are completely safe, and artificial intelligence provides the analytics and threat information that security professionals need to reduce the possibility of a breach and fortify an organization's security framework. Since greater processing power is available for cyber security, danger may be assessed and eliminated more quickly. Many people are worried about the capacity of cybercriminals to carry out very sophisticated technologies and cyberattacks. Artificial intelligence may also help in the identification and categorisation of risks, the organisation of incident response, and the preemptive detection of cyberattacks. Therefore, in spite of any possible drawbacks, artificial intelligence will advance cyber security and help businesses implement a more robust security plan.

This research aimed to explore artificial intelligence and its continuous advancement in providing e-government services. It also emphasised the need of incorporating cyber security techniques to enable the adoption of novel social and technological processes in government that benefit the community. Building and maintaining connections with the majority of stakeholders is the ultimate goal of smart city governments, since their participation enhances the effectiveness of e-government and bolsters cyber security. In order to remove obstacles between stakeholders and local governments, public services should be managed using new artificial intelligence technology and accessible e-governance modes. State authorities may continue to promote this model for even greater outcomes. E-government is advancing, but those who support mechatronics or are in positions of responsibility are not keeping up. This leads to differences in cyber

security requirements for anything in the virtual world, which might make performing more harder and need many tracks to keep an eye on. The advantages of the virtual environment may become possible if the efforts found in this study are elevated and stakeholders' engagement and understanding of e-governance and cyber security increase.

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.