ARTIFICIAL INTELLIGENCE'S ROLE IN SHAPING E-GOVERNANCE AND CYBERSECURITY IN SMART CITIES: INSIGHTS FROM STAKEHOLDERS

[1]S.Vijay Kumar,[2]Md.Ujumafathimabegum
[1]Assistant Professor, [2]MCA Student
Department Of MCA Student
Sree Chaitanya College of Engineering, Karimnagar

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 study examines the close connection between cybersecurity, e-Government, and AI in order to close this context-specific gap. Additionally, this study 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 utilising 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

Cyber security 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 noncombatant 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 ransom ware 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].

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 cyber security, 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 cyber security 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. Cyber security 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, cyber security 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 cyber security directly?

• How AI applications used in smart cities influence e-Governance and e-Governance impacts cyber security directly?

• Does e-Governance play a mediating role between the
relationship of AI applications and cyber security?

• 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 cyber security.

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 cyber security level in a smart city. The moderating significance of stakeholder involvement was systematically examined by using structural equational modeling (SEM) in Smart PLS 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, cyber security, 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.

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,

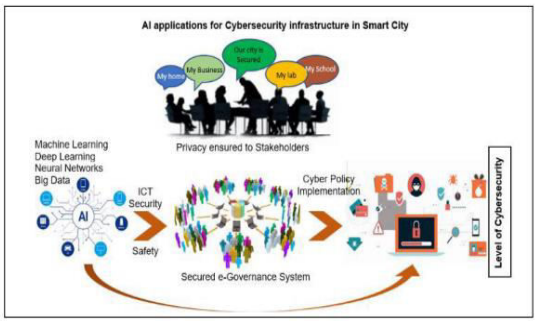
The aim of the researcher was to determine the effectiveness of artificial intelligence techniques against cyber security risks particularly in case of Iraq, Researcher has opted for quantitative method of research design along with primary data. The researcher collected the data from employees working 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.

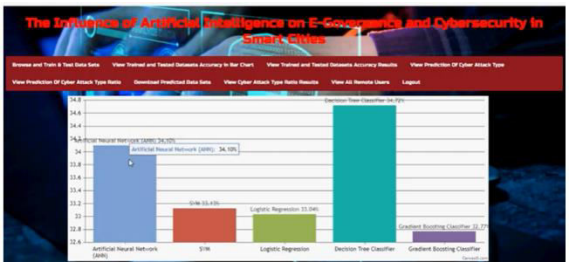
View and Authorize Users

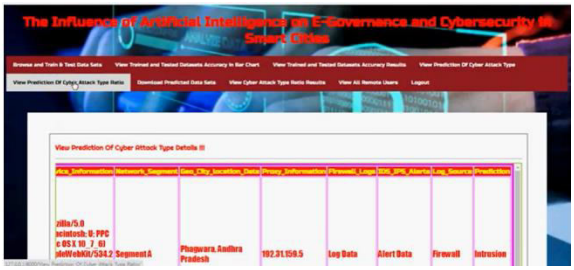
In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

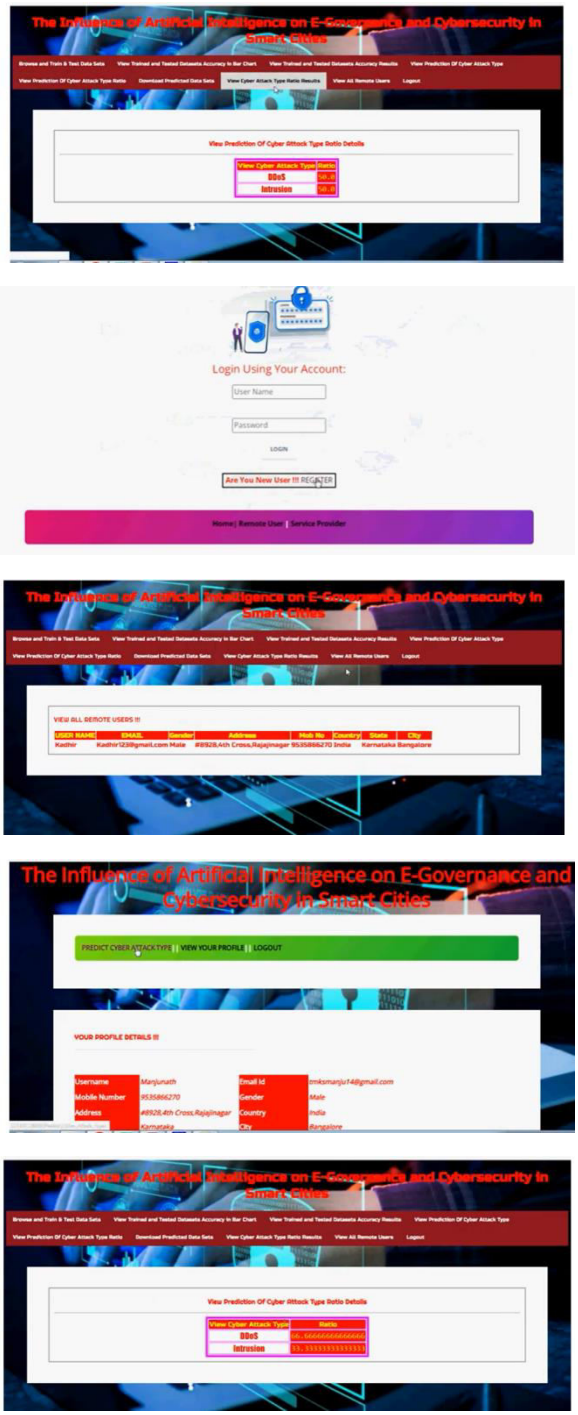
Remote User

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. RESULTS







8. CONCLUSION

Applications of artificial intelligence to address cyber security issues were investigated in the current study. According to the research findings, 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 extremely 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 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 study aimed to emphasise the necessity 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 officials can 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 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.