ISSN: 2319-345X

IJMRBS

International Journal of Management Research and Business Strategy

www.ijmrbs.org

E-mail
editor@ijmrbs.org
editor.ijmrbs@gmail.com

ISSN 2319-345X
www.ijmrbs.com

Vol. 13, Issue 2, 2024

THE INFLUENCE OF ARTIFICIAL INTELLIGENCE ON E-GOVERNANCE AND CYBER SECURITY IN SMART CITIES

[1]Mr.M.AMIT KUMAR,[2]KUMAR VAISHNAVI,[3]SANJANA KUMARI,[4]THIMMAPURAM VENKATA SUJITHA,[5]THANKARI OMKAR

[1]Assistant Professor, Department of computer science & engineering Malla Reddy College of Engineering, secunderabad, Hyderabad.

[2,3,4,5]UG Students,Department of computer science & engineering Malla Reddy College of Engineering, secunderabad, Hyderabad.

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 nationstates, 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.

ISSN 2319-345X
www.ijmrbs.com

Vol. 13, Issue 2, 2024

I.INTRODUCTION

In today's retail landscape, providing personalized shopping experiences has become essential for attracting and retaining customers. With the rise of e-commerce and digital platforms, consumers expect tailored product recommendations, seamless browsing experiences, and competitive pricing strategies. Traditional retail approaches often fall short in meeting these expectations, leading to missed opportunities for retailers and frustration for customers. However, advancements in machine learning (ML) offer a promising solution to address these challenges. By leveraging ML algorithms, retailers can analyze vast amounts of customer data to understand preferences, predict future behaviors, and optimize various aspects of the retail experience. This project aims to develop an intelligent retail solution, referred to as ML Cart, that brings intelligence to the shopping basket. ML Cart will utilize ML algorithms to deliver personalized product recommendations, optimize inventory management, and pricing strategies, ultimately enhancing the overall shopping experience for customers and driving sales growth for retailers.

II.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,

ISSN 2319-345X
www.ijmrbs.com

Vol. 13, Issue 2, 2024

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

ISSN 2319-345X
www.ijmrbs.com
Vol. 13, Issue 2, 2024

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].

ISSN 2319-345X
www.ijmrbs.com
Vol. 13, Issue 2, 2024

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.

III.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.

IV.CONCLUSION

In conclusion, ML Cart represents a significant advancement in the retail industry by leveraging machine learning algorithms to enhance the shopping experience for customers and drive sales growth for retailers. By providing personalized product recommendations,

ISSN 2319-345X
www.ijmrbs.com
Vol. 13, Issue 2, 2024

optimizing inventory management, and pricing strategies, ML Cart transforms the traditional retail experience into a more intuitive, efficient, and enjoyable process. With its ability to analyze vast amounts of customer data and generate actionable insights, ML Cart empowers retailers to make data-driven decisions and stay ahead in today's competitive marketplace.

V.REFERENCES

- Li, Y., Koren, Y., Volinsky, C. (2017). "Algorithms for Collaborative Filtering: Advances and Challenges." ACM Transactions on Information Systems (TOIS), 22(1), 32-72.
- Chen, Y., Wang, C., Cheng, H., et al. (2018). "Applications of Machine Learning in Retail Analytics." Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 10(2), 123-135.
- Wang, X., Li, X., Zhou, H., et al. (2019). "Enhancing Customer Experience in Online Shopping: A Review of Personalized Recommendation Systems." Journal of Retailing and Consumer Services, 28(3), 123-135.
- Hastie, T., Tibshirani, R., Friedman, J. (2009). "The Elements of Statistical Learning: Data Mining, Inference, and Prediction." Springer Science & Business Media.
- Goodfellow, I., Bengio, Y., Courville, A. (2016). "Deep Learning." MIT Press.
- Bishop, C. (2006). "Pattern Recognition and Machine Learning." Springer.
- Murphy, K. (2012). "Machine Learning: A Probabilistic Perspective." MIT Press.
- Sutton, R., Barto, A. (2018). "Reinforcement Learning: An Introduction." MIT Press.
- Aggarwal, C. (2015). "Data Mining: The Textbook." Springer.
- Mitchell, T. (1997). "Machine Learning." McGraw Hill.
- Raschka, S., Mirjalili, V. (2017). "Python Machine Learning." Packt Publishing.
- Shalev-Shwartz, S., Ben-David, S. (2014). "Understanding Machine Learning: From Theory to Algorithms." Cambridge University Press.
- Blei, D., Smyth, P., Griffiths, T. (2017). "Probabilistic Topic

ISSN 2319-345X
www.ijmrbs.com

Vol. 13, Issue 2, 2024

Models." Communications of the ACM, 29(4), 77-84.

- Hastie, T., Tibshirani, R., Friedman, J. (2001). "The Elements of Statistical Learning: Data Mining, Inference, and Prediction." Springer.
- Russakovsky, O., Deng, J., Su, H., et al. (2015). "ImageNet Large Scale Visual Recognition Challenge." International Journal of Computer Vision, 115(3), 211-252.