www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON E-GOVERNANCE AND CYBERSECURITY IN SMART CITIES

Mr.Konda Janardhan[1]., Badugu Lidiya[2]
1 Assistant Professor, Department of CSE, Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India
2, B.Tech CSE (21RG1A05L1),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

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 cyber security measures.

Keywords: Artificial intelligence (AI), cyber-attacks, PLS-SEM, cybersecurity.

I. INTRODUCTION

Cyber security has become a critical and vital topic that requires protecting the computer network from potential threats in today's modern world. A cyber-attack is a deliberate attack targeting computer networks, relevant data, programs, and electronic information, resulting in sub-national entities

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

inciting violence towards noncombatant opponents. As technology develops, so do cyber threats, necessitating the development of new prevention strategies. 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 .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 . Cyber- attacks also have a significant psychological impact on humans, producing unhappiness, tension, and stress among people . Artificial intelligence (AI) applications can positively influence the cyber capabilities and national security of the sovereign nation, regional government entities, and non-state organizations . AI is a reliable technique for mitigating cyber-attack effects. AI is machine intelligence that executes activities connected with intelligence.

II.RELATED WORK

Cybersecurity challenges in smart cities

Description: Smart city is a captivating concept characterized by its intel- ligent features. Its scope extends beyond improving the level of urban economic efficiency and the reduction of costs and resource consumption. Rather, it encompasses the integrationof 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. It is well-established that various infrastructure systems, including energies, grid system, healthcare, traffic, trans- portation, 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 sophis- ticated, effective, and eco- friendly solutions.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

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

Artificial intelligence and cybersecurity

Description: 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.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 pro- gram's applications with the support of augmenting defense installations, and it has proved effective in counter terrorism. 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 . The security challenges seem critical, drivingthe 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. 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.

Mediating role of e-governance

Description: 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 maxi- mum e-Government services and security for the public and other stakeholders, numerous governments have attempted to implement e-Governance . Nonetheless, most citizens are anxious about their privacy and security while utilizing e-Government facilities, as per a 2014 UN e-Government survey.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Concerning security, the primary obstacles thate-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 e Government Systems,’’ outlined 11 policies and procedures for security .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.

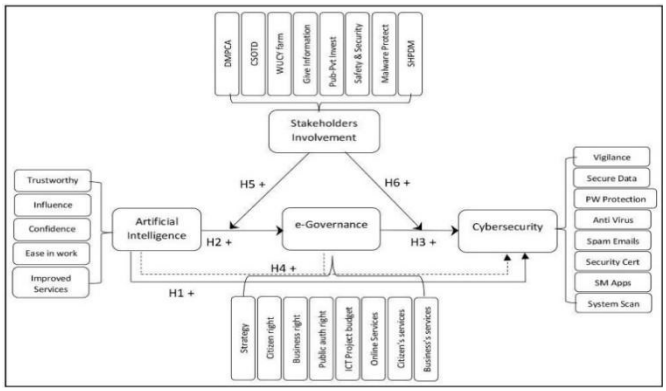

Figure:2 AI application in cybersecurity conceptual framework.

Moderating role of stakeholders involvement

Description: The concentration on involving stakeholders in the formation of technologies and workplace conditions was pioneered under participatory innovation in the Scandinavian research methodological approach . The participative conceptual model arose through 1970s socio-technical research designed to strengthen organizational democracy , 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 . The humanitarian perspective toward stakeholder involvement articulated by academics Mumford 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. The technological method of stakeholder involvement can be observed in mainstream IS design research, where the emphasis is on developing information technology infrastructure. Stakeholder involvement is

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

considered a method of assuring the knowledge and expertise requiring higher IT architecture in the research . It is often recognized as a means of growing consumer adoption of innovative technologies.

III.SYSTEM ANALYSIS

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. 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.

The primary objective of the proposed system is to investigate the relationship between artificial intelligen1ce 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.

IV.ALGORITHUMS

1.Decision tree classifiers:

Decision tree classifiers are used successfully in many diverse areas. Their most important feature is the capability of capturing descriptive decision making knowledge from the supplied data. Decision tree can be generated from training sets. The procedure for such generation based on the set of objects (S), each belonging to one of the classes C1, C2, …, Ck is as follows:

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Step 1. If all the objects in S belong to the same class, for example Ci, the decision tree for S consists of a leaf labeled with this class

Step 2. Otherwise, let T be some test with possible outcomes O1, O2,…, On. Each object in S has one outcome for T so the test partitions S into subsets S1, S2,… Sn where each object in Si has outcome Oi for T. T becomes the root of the decision tree and for each outcome Oi we build a subsidiary decision tree by invoking the same procedure recursively on the set Si.

2.Gradient boosting :

Gradient boosting is a machine learning technique used in regression and classification tasks, among others. It gives a prediction model in the form of an ensemble of weak prediction models, which are typically decision trees.[1][2] When a decision tree is the weak learner, the resulting algorithm is called gradient-boosted trees; it usually outperforms random forest.A gradient-boosted trees model is built in a stage-wise fashion as in other boosting methods, but it generalizes the other methods by allowing optimization of an arbitrary differentiable loss function.

3.K-Nearest Neighbors (KNN) :

- ❖ Simple, but a very powerful classification algorithm
- ❖ Classifies based on a similarity measure
- ❖ Non-parametric
- ❖ Lazy learning
- ❖ Does not “learn” until the test example is given
- ❖ Whenever we have a new data to classify, we find its K-nearest neighbors from the training data

4.Logistic regression Classifiers :

Logistic regression analysis studies the association between a categorical dependent variable and a set of independent (explanatory) variables. The name logistic regression is used when the dependent variable has only two values, such as 0 and 1 or Yes and No. The name multinomial logistic regression is usually reserved for the case when the dependent variable has three or more unique values, such as Married, Single, Divorced, or Widowed. Although the type of data used for the dependent variable is different from that of multiple regression, the practical use of the procedure is similar. Logistic regression competes with discriminant analysis as a method for analyzing categorical-response variables. Many statisticians feel that logistic regression is more versatile and better suited for modeling most situations than is discriminant analysis. This is because logistic regression does not assume that the independent variables are normally distributed, as discriminant analysis does.

5.Naïve Bayes :

The naive bayes approach is a supervised learning method which is based on a simplistic hypothesis: it assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature .

Yet, despite this, it appears robust and efficient. Its performance is comparable to other supervised learning techniques. Various reasons have been advanced in the literature. In this tutorial, we highlight an explanation based on the representation bias. The naive bayes classifier is a linear classifier, as well as linear discriminant analysis, logistic regression or linear SVM (support vector machine). The difference lies on the method of estimating the parameters of the classifier (the learning bias).

While the Naive Bayes classifier is widely used in the research world, it is not widespread among practitioners which want to obtain usable results. On the one hand, the researchers found especially it is very easy to program and implement it, its parameters are easy to estimate, learning is very fast even on very large databases, its accuracy is reasonably good in comparison to the other approaches. On the other hand, the final users do not obtain a model easy to interpret and deploy, they does not understand the interest of such a technique.

6.Random Forest :

Random forests or random decision forests are an ensemble learning method for classification, regression and other tasks that operates by constructing a multitude of decision trees at training time. For classification tasks, the output of the random forest is the class selected by most trees. For regression tasks, the mean or average prediction of the individual trees is returned. Random decision forests correct for decision trees' habit of overfitting to their training set. Random forests generally outperform decision trees, but their accuracy is lower than gradient boosted trees. However, data characteristics can affect their performance.

7.SVM :

SVM is a discriminant technique, and, because it solves the convex optimization problem analytically, it always returns the same optimal hyperplane parameter—in contrast to genetic algorithms (GAs) or perceptrons, both of which are widely used for classification in machine learning. For perceptrons, solutions are highly dependent on the initialization and termination criteria. For a specific kernel that transforms the data from the input space to the feature space, training returns uniquely defined SVM model parameters for a given training set, whereas the perceptron and GA classifier models are different each time training is initialized. The

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

aim of GAs and perceptrons is only to minimize error during training, which will translate into several hyperplanes' meeting this requirement.

V.RESULTS AND DISCUSSION

Fig:1 , Home Page

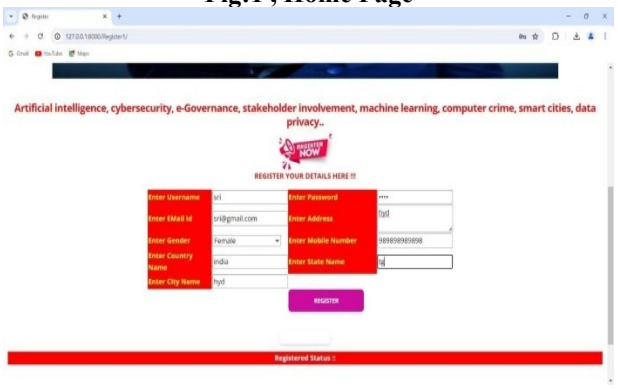

Fig:2 , Register Page

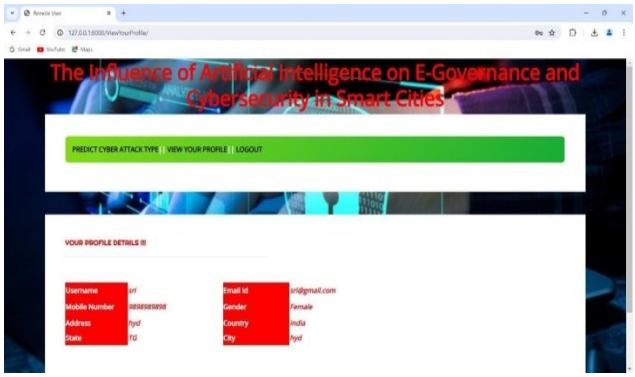

Fig:3 , Profile Details

Fig:4 , Checking

cyber attack type

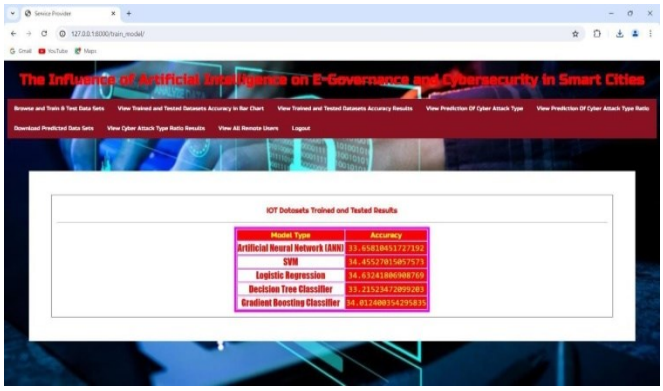

Fig:5, Browse and test datasets

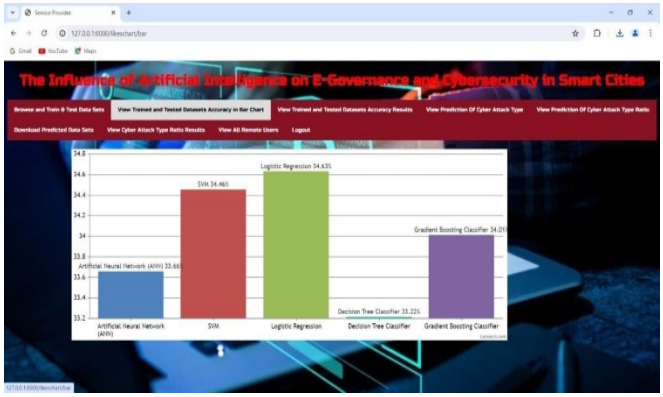

Fig:6, View tested datasets accuracy in bar chat

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Fig:7, View trained and test datasets accuracy results

Fig:8,View prediction of cyber attack type

Fig:9, View prediction of cyber attack type ratio

CONCLUSION

The current study examined artificial intelligence applications to overcome cyber security 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 cyber attacks, 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 computing in cyber security 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 cyber attacks before their occurrence. Consequently, despite potential negatives, artificial intelligence would contribute to the evolution of cyber security and support enterprises in establishing an enhanced security strategy.

FUTURE ENHANCEMENTS:

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 cybers

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 citiesin the new urban world: A comparative cluster dynamics analysis through machine learning,’’ Sustain. Cities Soc., vol. 66, Mar. 2021,Art. no. 102665.