

THE INFLUENCE OF ARTIFICIAL INTELLIGENCE ONE- GOVERNANCE AND CYBER SECURITY IN SMART CITIES A STAKEHOLDER'S PERSPECTIVE

K.BALAJI¹, SHAIK MAHABOOB SUBHANULLA², Dr.K.VIJAY³

¹PG Student, Dept of CSE, GCET, Kadapa.

²Assistant Professor, Dept of CSE, GCET, Kadapa.

³Professor, Dept of CSE, GCET, Kadapa.

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 nation states, local governments, and non-state entities through e-Governance. The project provides a mixed association between AI, e-Governance, and cyber security. This study investigates the direct relationship between AI, e-Governance, and cyber security. Furthermore, this study examines the mediating role of e-Governance between AI and cyber security and moderating effect of stakeholder's involvement on the relationship between AI, e-Governance, and Cyber security. The results of PLS-SEM path modeling analysis revealed a partial mediating impact of e-Governance between AI and cyber security. Likewise, moderating influence of stakeholder's involvement was discovered on the relationship between AI and e-Governance, as well as between e-Governance and cyber security. It implies that stakeholder's involvement has vital significance in AI and e-Governance because all stakeholders have interest in vibrant, transparent, and secured cyberspace while using e-services. The project provides practical implications for governmental bodies of smart cities for strengthening cyber security measure.

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 inciting violence towards noncombatant opponents. As technology develops, so do cyber threats, necessitating the development of new prevention strategies. 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. Human professionals' expertise is integrated for strategic planning and decision-making, including making medical diagnoses and getting insights from expertise in concluding. In terms of cyber security, Zarina et al., 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.

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. 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.

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.

Disadvantages of Existing System:

- i) The complexity of data:** Most of the existing machine learning models must be able to accurately interpret large and complex datasets to detect Cyber security.
- ii) Data availability:** Most machine learning models require large amounts of data to create accurate predictions. If data is unavailable insufficient quantities, then model accuracy may suffer.
- iii) 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 cyber security, 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 in to perceptions of the importance of AI in cyber security in smart cities. Proposed System framework for classifying cyber security level in smart city:

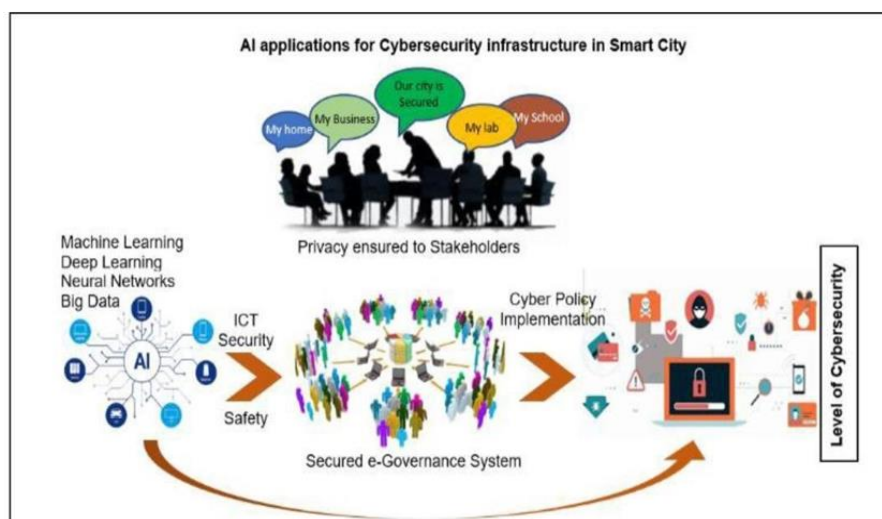


FIGURE 1. Channel of the proposed framework for classifying cybersecurity level in smart city.

Advantages of Proposed System:

- i) Artificial intelligence applications in smart cities contribute to e-Governance positively.
- ii) E-Governance execution in smart cities affects cyber security positively.
- iii) E-Governance mediates between artificial intelligence and cyber security positively.

IV. OUTPUTS

Step1: Homepage for the Influence of Artificial Intelligence on E-Governance and Cyber security in Smart Cities.



Step2: Registration Form

Artificial intelligence, cybersecurity, e-Governance, stakeholder involvement, machine learning, computer crime, smart cities, data privacy..

REGISTER NOW

REGISTER YOUR DETAILS HERE !!!

Enter Username	sam	Enter Password	*****
Enter Email Id	sam123@gmail.com	Enter Address	rayachoty
Enter Gender	Female	Enter Mobile Number	1234567899
Enter Country Name	India	Enter State Name	Andhra Pradesh
Enter City Name	Kadapa		

REGISTER

Registered Status :: Registered Successfully

Home | Remote User | Service Provider

Step3: View Single Profile Details

The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities

PREDICT CYBER ATTACK TYPE | VIEW YOUR PROFILE | LOGOUT

YOUR PROFILE DETAILS !!!

Username	Riya	Email Id	riya@123
Mobile Number	9876543210	Gender	Female
Address	Gandhi street, Bangalore	Country	India
State	Karnataka	City	Bangalore

Step4: Log into Service Provider

The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities

Admin

Login

User Login

Step5: View All Remote Users Details

The screenshot shows a web application interface with a navigation bar and a main content area. The main content area displays a table titled 'VIEW ALL REMOTE USERS !!!' with the following data:

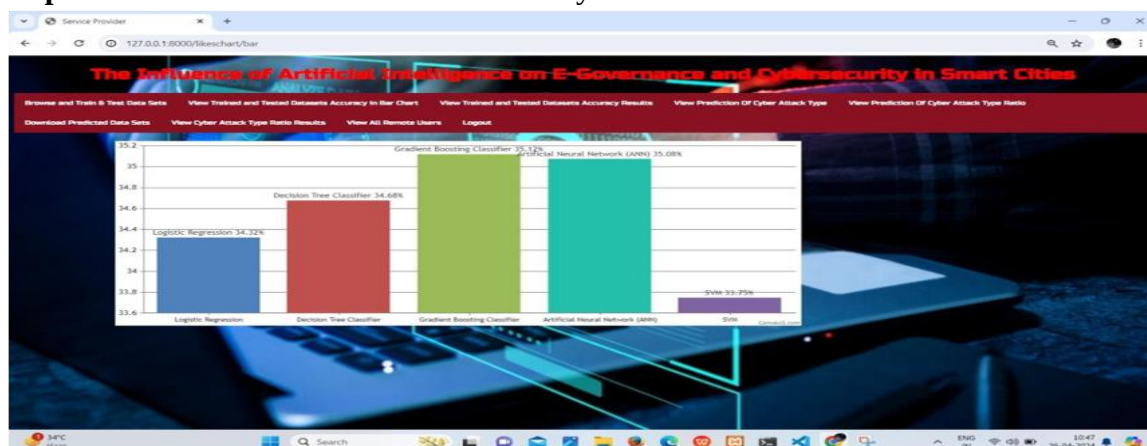
USER NAME	EMAIL	Gender	Address	Mobile No	Country	State	City
Kadhir	Kadhir123@gmail.com	Male	#8928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
Manjunath	mrksmanju14@gmail.com	Male	#8928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
naidu	naidu1@gmail.com	Male	rayachoty	9912462030	India	Andhra pradesh	Kadapa
syedda	syedda@gmail.com	Female	rayachoty	9876543210	India	Andhra pradesh	Kadapa
thamjam	tham123@gmail.com	Female	mesapet,rayachoty	1234567890	India	Andhra pradesh	Kadapa
sam	sam123@gmail.com	Female	rayachoty	1234567899	India	Andhra pradesh	Kadapa
Sofy	sofy123@gmail.com	Female	shivaji nagar, 2nd road, Shiva	3456782103	India	Karnataka	Banglore
sufiya	sufiya123@gmail.com	Female	kadapa	123456789	India	Andhra pradesh	Kadapa
sana	sana123@gmail.com	Female	kadapa	9801234567	India	Andhra pradesh	Kadapa
Shameem	shameem123@gmail.com	Female	rayachoty	3245678901	India	Andhra pradesh	Rayachoty
Riya	riya@123	Female	Gandhi street, Bangalore	9876543210	India	Karnataka	Banglore

Step6: Trained and Tested Results

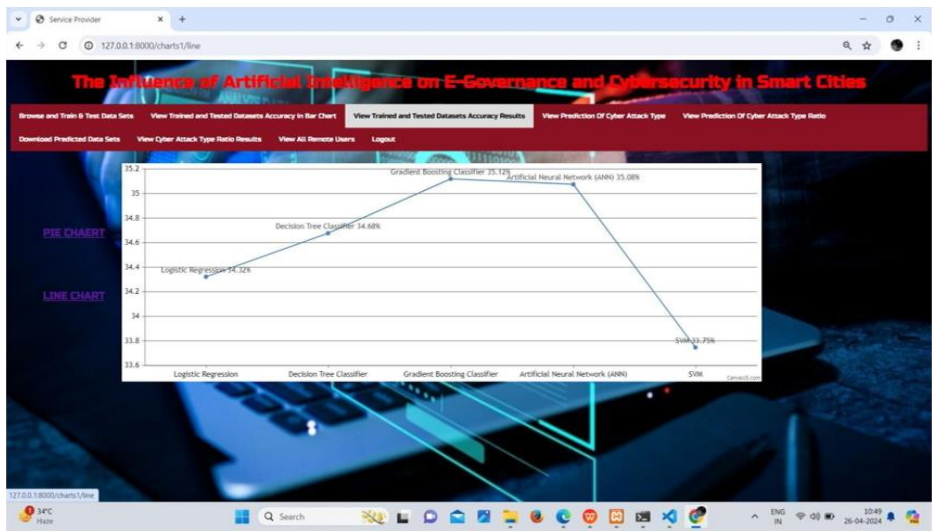
The screenshot shows a web application interface displaying 'IOT Datasets Trained and Tested Results'. The results are summarized in the following table:

Model Type	Accuracy
Logistic Regression	34.9867139861116
Decision Tree Classifier	33.65818451727192
Gradient Boosting Classifier	36.22674933569531
Artificial Neural Network (ANN)	35.875287865367585
SVM	33.746678478527984
Logistic Regression	33.65818451727192
Decision Tree Classifier	35.69518558815943
Gradient Boosting Classifier	34.012488354295431

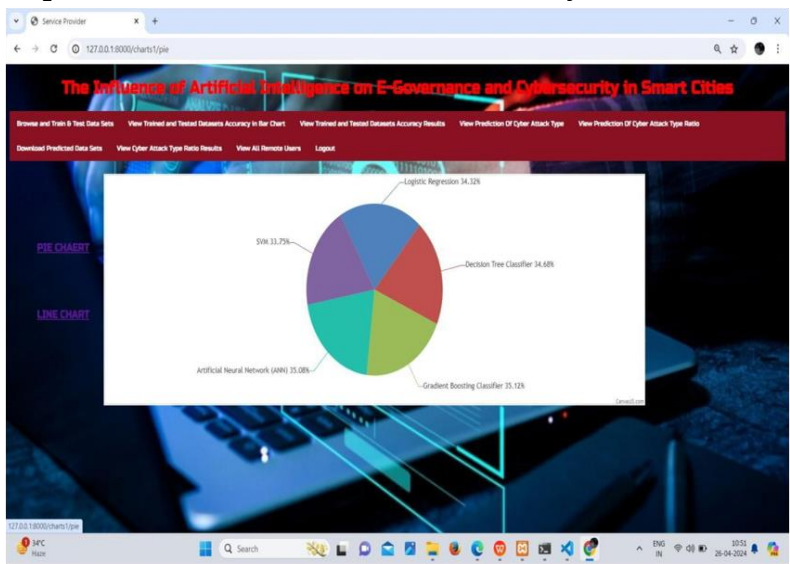
Step7: Trained and Tested Datasets Accuracy in Bar-Chart



Step8: Trained and Tested datasets Accuracy Results in Line-Chart



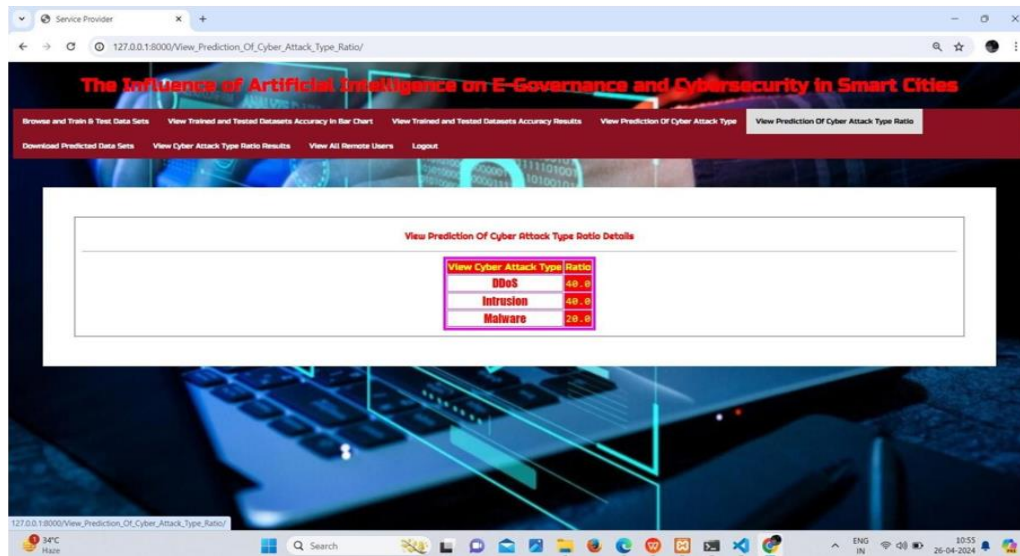
Step9: Trained and Tested datasets Accuracy Results in Pie-Chart



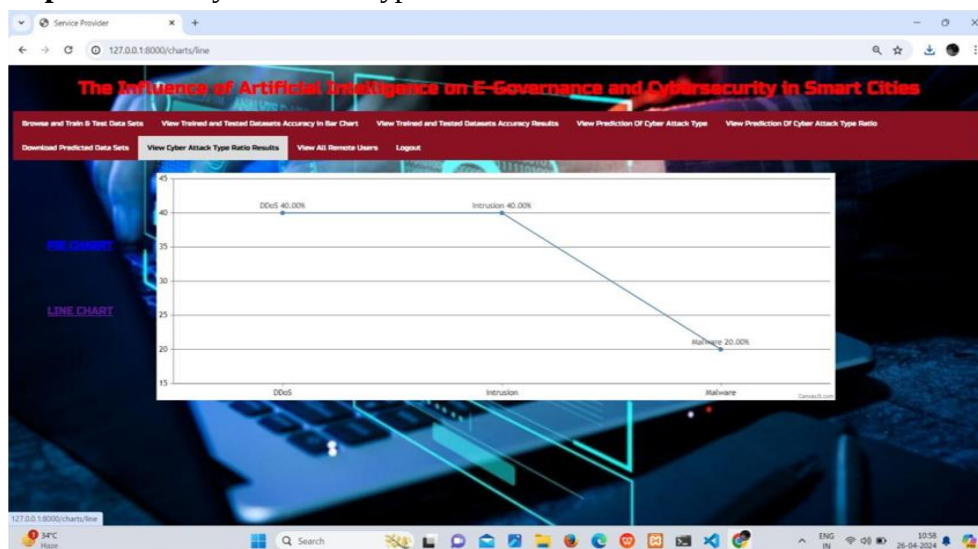
Step10: Prediction of Cyber Attack Type details

PkId	Timestamp	Source_IP_Address	Destination_IP_Address	Source_Port	Destination_Port	Protocol	Packet_Length	Pack
172.217.9.238-10.42.0.151-443-55643-6	12-02-23 7:13	1148.99.245	178.157.14.116	34489	20396	ICMP	1022	Data

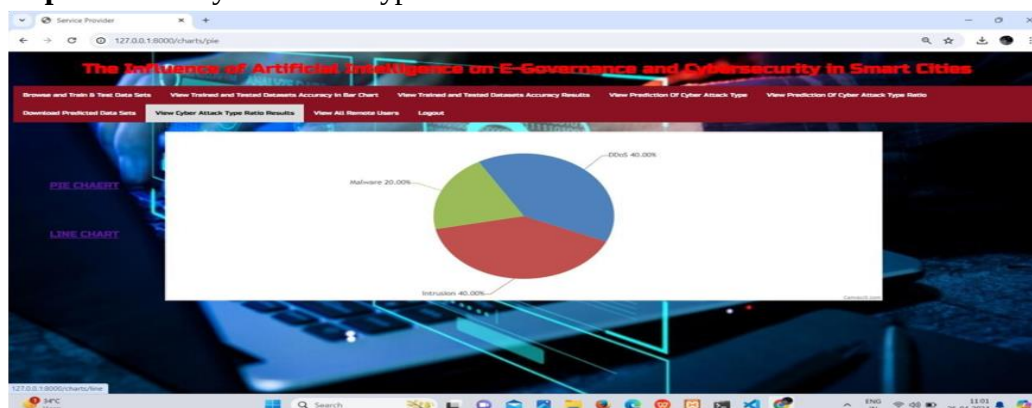
Step11: Prediction of Cyber Attacks type Ratio



Step12: View Cyber Attack type Ratio Results in Line Chart



Step13: View Cyber Attack type Ratio Results in Pie-Chart



CONCLUSION

The integration of machine learning algorithms, including ANN, SVM, Logistic Regression, Decision Tree Classifier, and Gradient Boosting, presents a powerful approach to address the complexities of e-governance and cyber security in smart cities. Through their diverse capabilities, these algorithms offer valuable insights, predictive modeling, and decision support mechanisms to various stakeholders involved in urban governance and security. **ANN** offers exceptional flexibility and adaptability in processing large volumes of data, enabling accurate predictions and pattern recognition in e-governance and cyber security applications.

SVM excels in classification tasks, particularly in scenarios with high-dimensional data and nonlinear decision boundaries.

Logistic Regression provides a simple yet effective method for binary classification tasks, making it suitable for applications such as user authentication, access control, and fraud detection in smart city systems.

Decision Tree Classifier offers transparency and interpretability in decision-making processes, making it valuable for policy formulation, regulatory compliance, and risk assessment in e-governance and cyber security.

Gradient Boosting techniques, such as Gradient Boosted Trees, combine the strengths of decision trees with ensemble learning to improve predictive accuracy and generalization performance.

In conclusion, leveraging a diverse range of machine learning algorithms empowers stakeholders in smart cities to harness the potential of artificial intelligence for e-governance and cyber security. By integrating these algorithms into decision-making processes, policymakers, government agencies, and cyber security professionals can enhance the efficiency, transparency, and resilience of urban systems, ultimately contributing to the development of safer, more responsive, and sustainable smart cities.

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.
- 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 Informations technik*, vol. 132, no. 2, pp. 106–112, Mar.2015.
- 5) A.Corallo, M.Lazoi, M.Lezzi, and A.Luperto, "Cyber security 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.VanMoer, "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 cyber attacks,” 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.