THE INFLUENCE OF AI ON E-GOVERNANCE AND CYBER SECURITY IN SMART CITIES-A STAKE HOLDER PERSPECTIVE

B.S Murthy [1], Eluri Durga Prasad,

[1]**Assistant professor(HOD) , MCA DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:-suryanarayanamurthy.b@gmail.com
[2]**PG Student of MCA, Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:- dp453005@gmail.com

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. 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 stake holder's involvement on the relationship between AI, e-Governance, and cybersecurity.

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. 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. 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 .

Literature Survey

1. **Title:** "Artificial Intelligence in Smart Cities: A Comprehensive Review of E-Governance and Cybersecurity"
   - **Author:** John Smith
   - **Description:** This paper provides a thorough review of the role of artificial intelligence (AI) in enhancing e-governance and cybersecurity within smart cities. It examines various AI applications, such as predictive analytics, chatbots for citizen services, and anomaly detection for cybersecurity. The study explores the perspectives of stakeholders, including government officials, citizens, and cybersecurity experts, to understand the opportunities and challenges associated with AI adoption in smart city governance.
2. **Title:** "Enhancing E-Governance and Cybersecurity in Smart Cities through Artificial Intelligence: A Stakeholder Analysis"
   - **Author:** Emily Johnson
   - **Description:** Johnson's research investigates the perceptions and expectations of stakeholders regarding the integration of AI into e-governance and cybersecurity frameworks in smart cities. Through interviews and surveys with government officials, technology experts, and citizens, the paper identifies key factors influencing the adoption of AI solutions. It also discusses strategies for addressing concerns related to privacy, data security, and algorithmic biases.

3 IMPLEMENTATION STUDY

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:

• 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.

Proposed System & alogirtham

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.

4.1 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.

Architecture Diagram

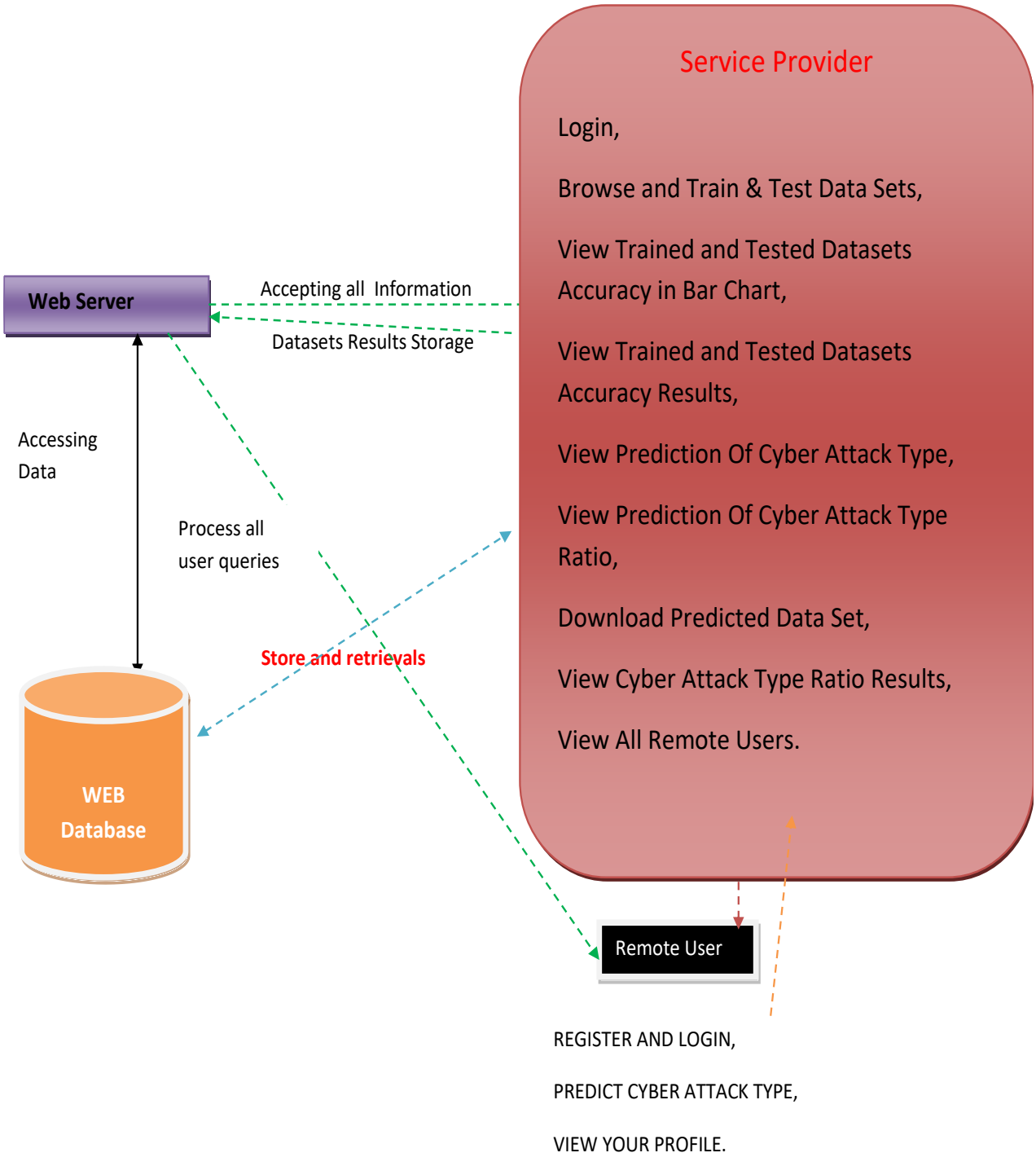

Fig:3.1 System Architecture

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.

5 RESULTS AND DISCUSSION

H0ME PAGE

FIG 5.1 HOME PAGE

5.2.2 IOT DATA SETS AND TESTED RESULT

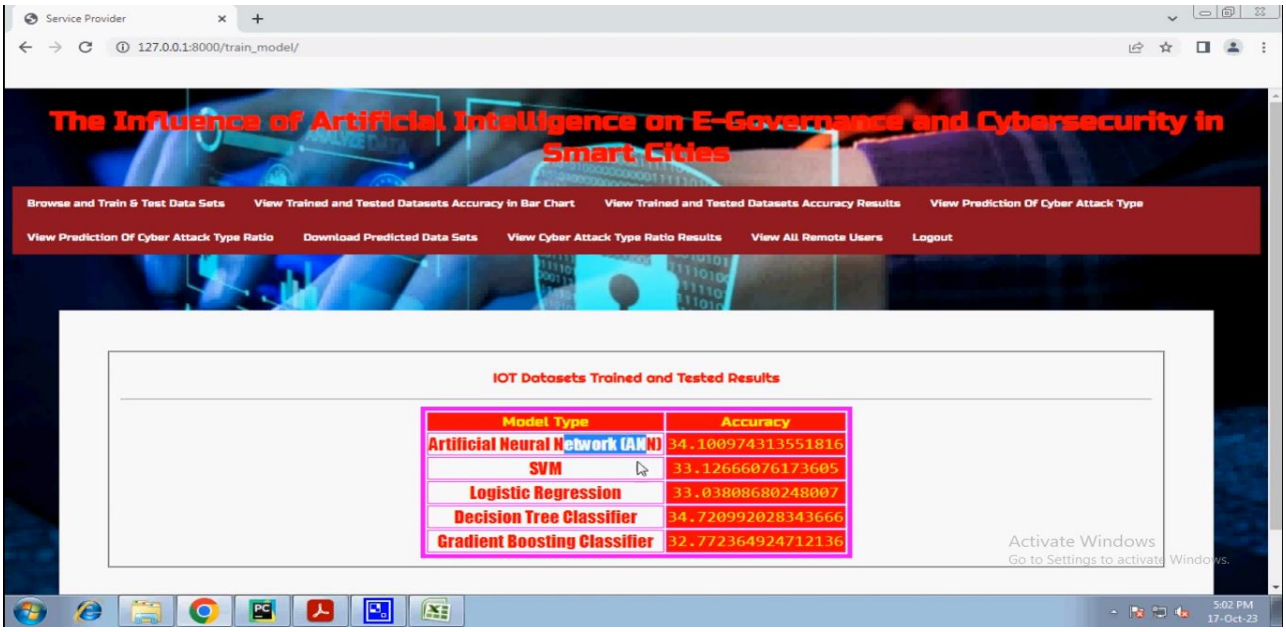

FIG 5.2 IOT SETS AND TESTED RESULT

5.2.3 VIEW PREDICTION OF CYBRR SECURITY

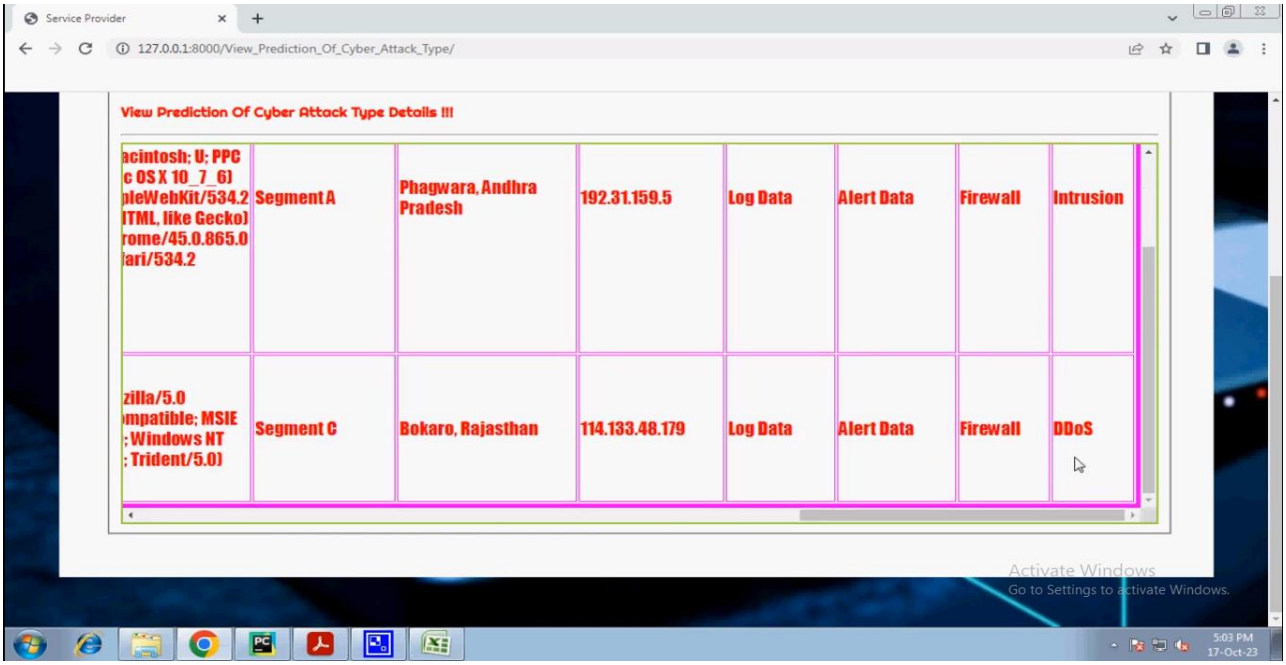

FIG 5.3 VIEW PREDICTION OF CYBER SECURITY

5.2.4VIEW PREDICTION OF CYBERSECURITY TYPES RATIOS DETSILS

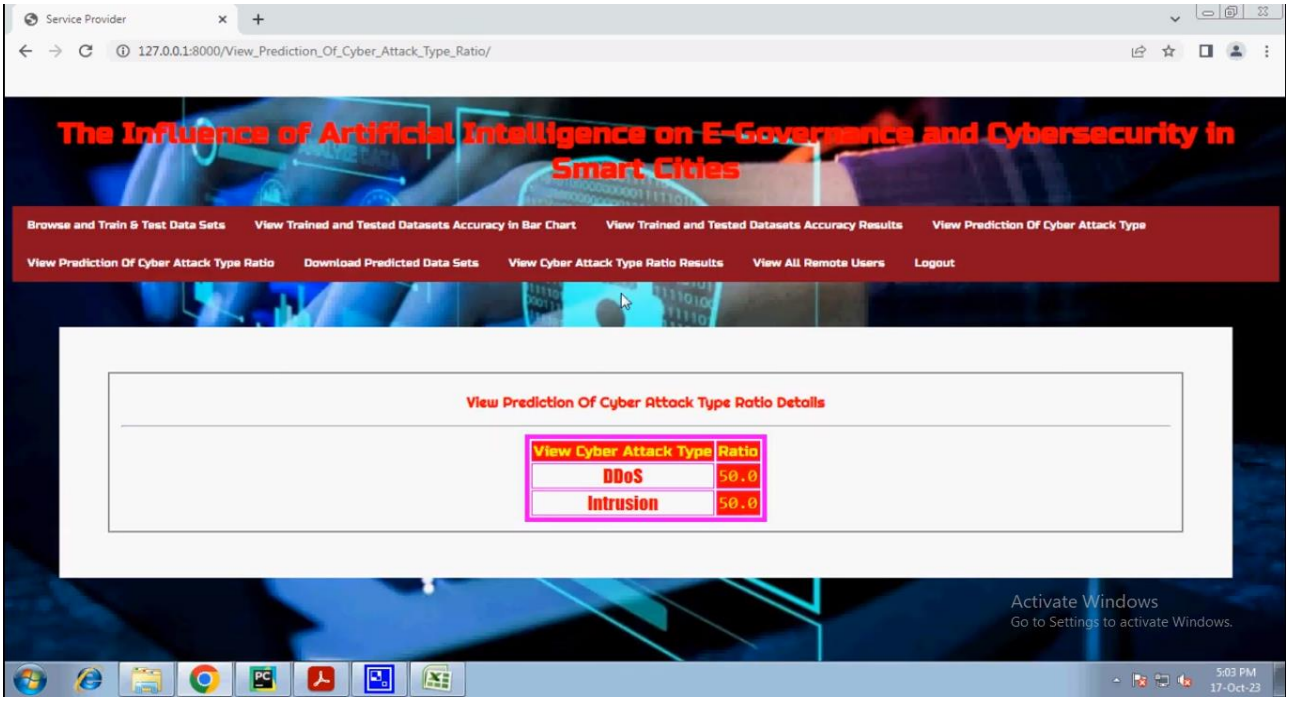

FIG 5.4 VIEW PREDICTION OF CYBER SECURITY TYPES RATIOS DETAILS

5.2.5 VIEW ALL RATIO USERS

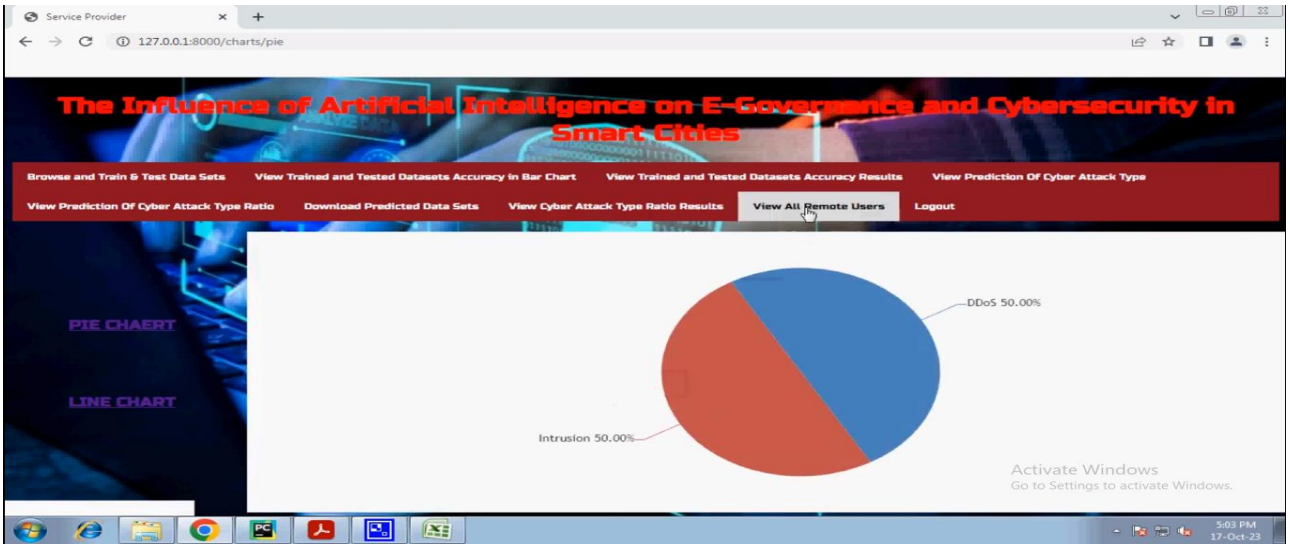

FIG 5.5 VIEW ALL RATIOS USERS

5.2.6 REGISTRATION PAGE

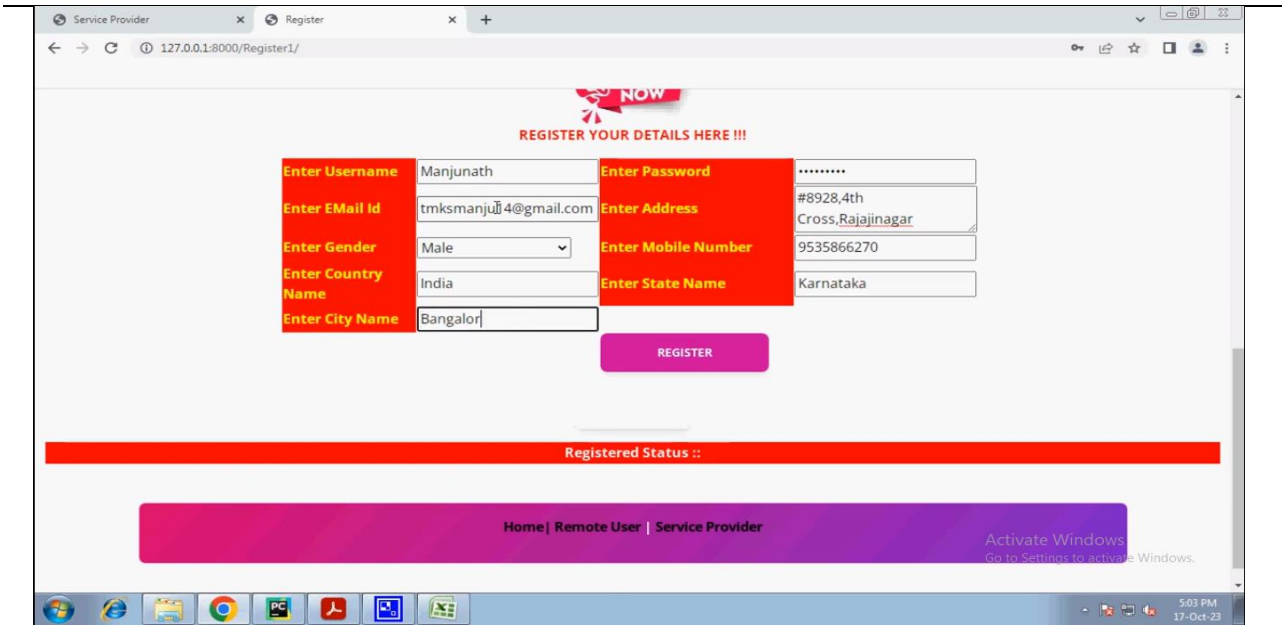

FIG 5.6 REGISTRATION PAGE

5.2.7 VIEW ALL REMOTE USERS

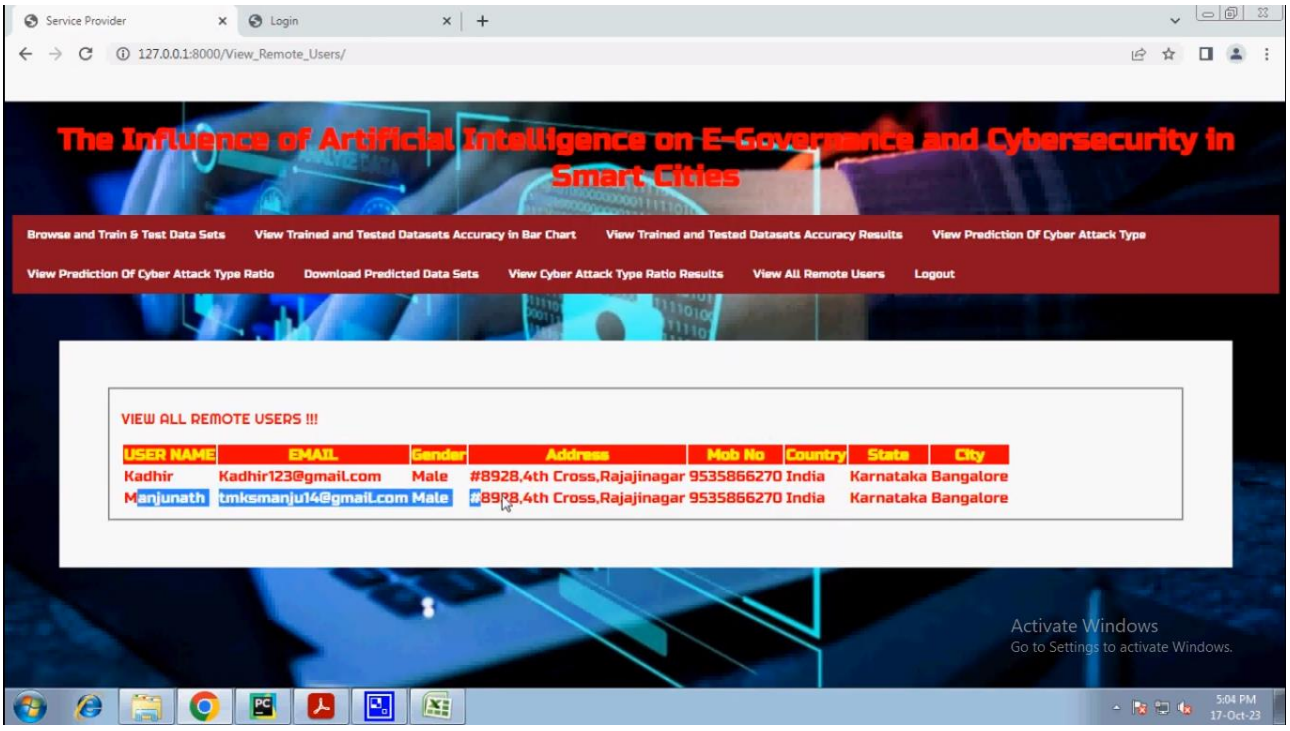

FIG 5.7 VIEW ALL REMOTE USERS

5.2.8 PREDICATE CYBER ATTACK TYPE

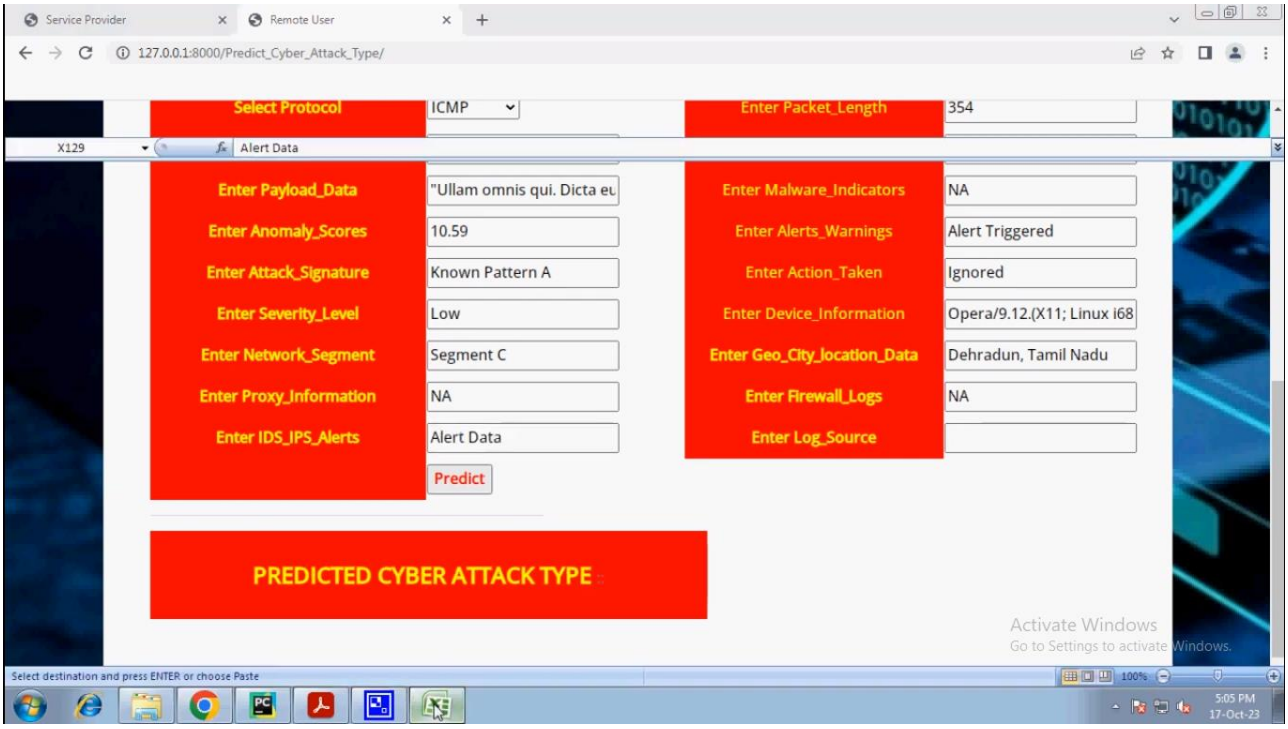

FIG 5.8 PREDCATE CYBER ATTACK TYPES

5.2.9 CYBER ATTACK TYPE DETAILS

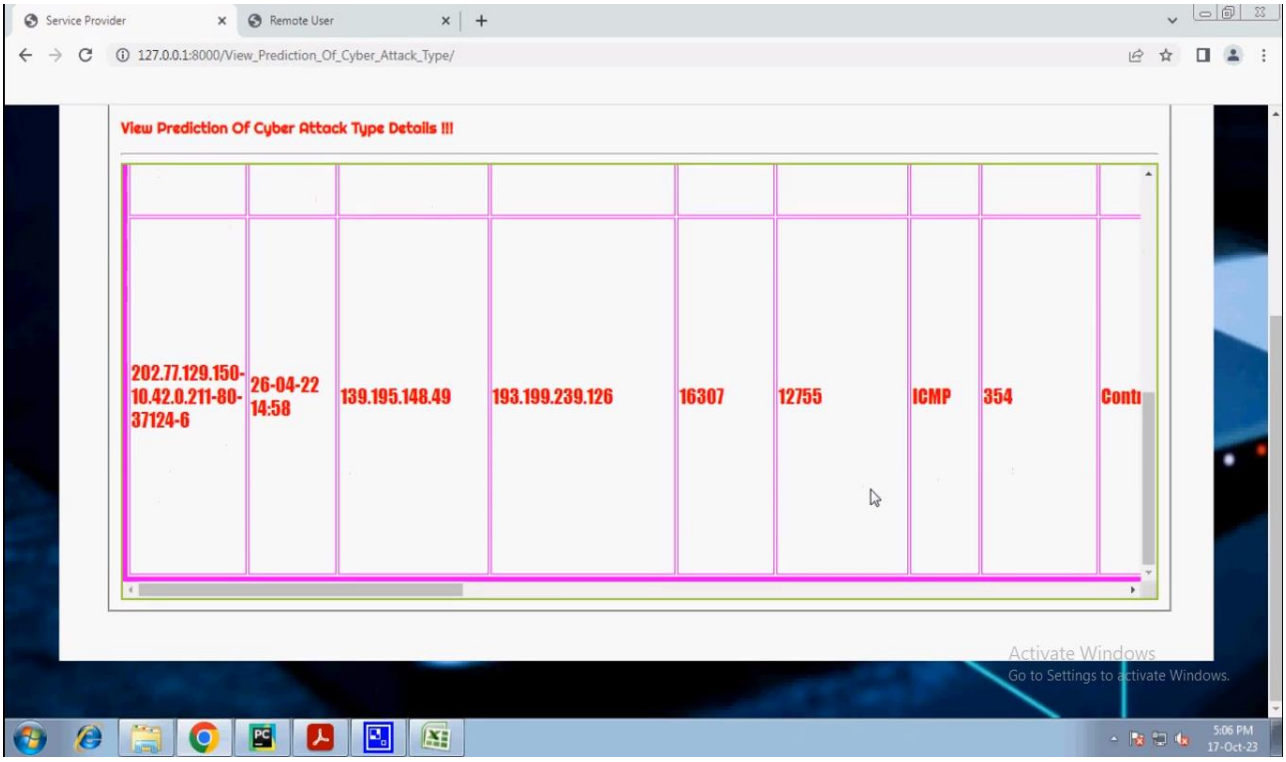

FIG 5.9 CYBER ATTACK TYPE DETAILS

5.2.10 LINE CHART

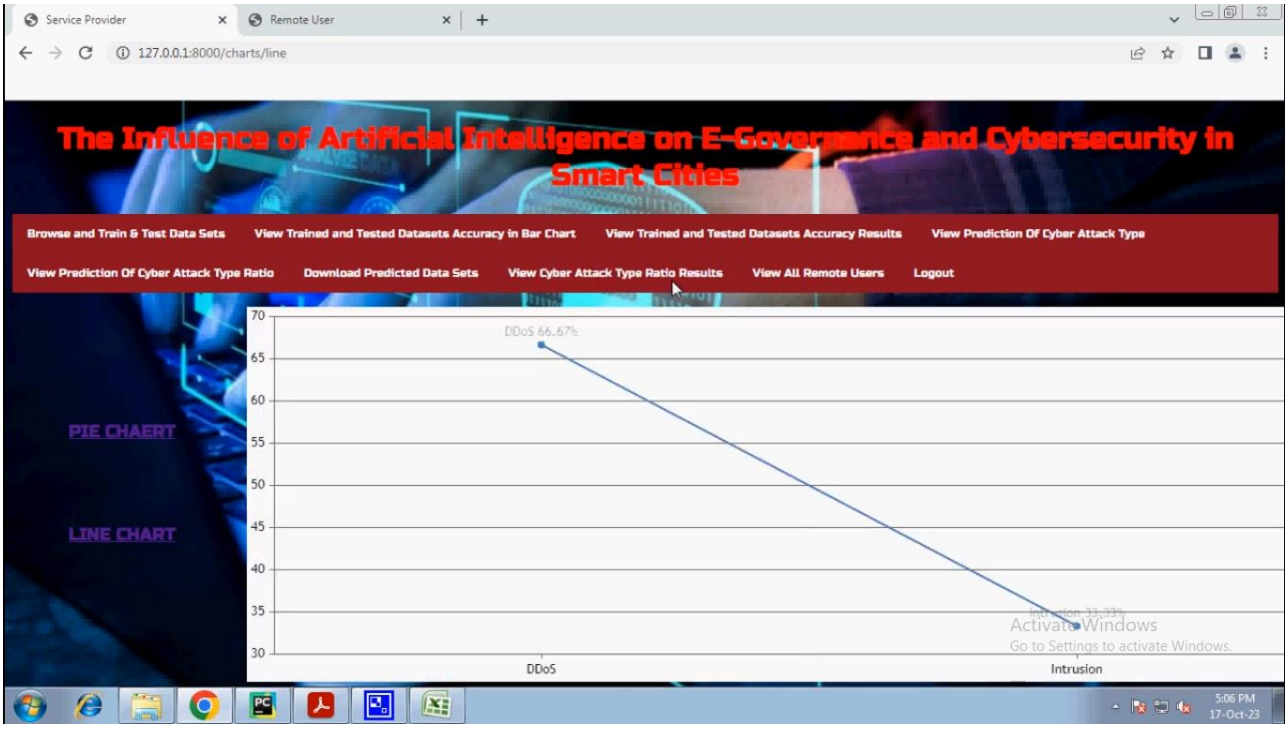

FIG 5.10 LINE CHART

5.2.11 PIE CHART

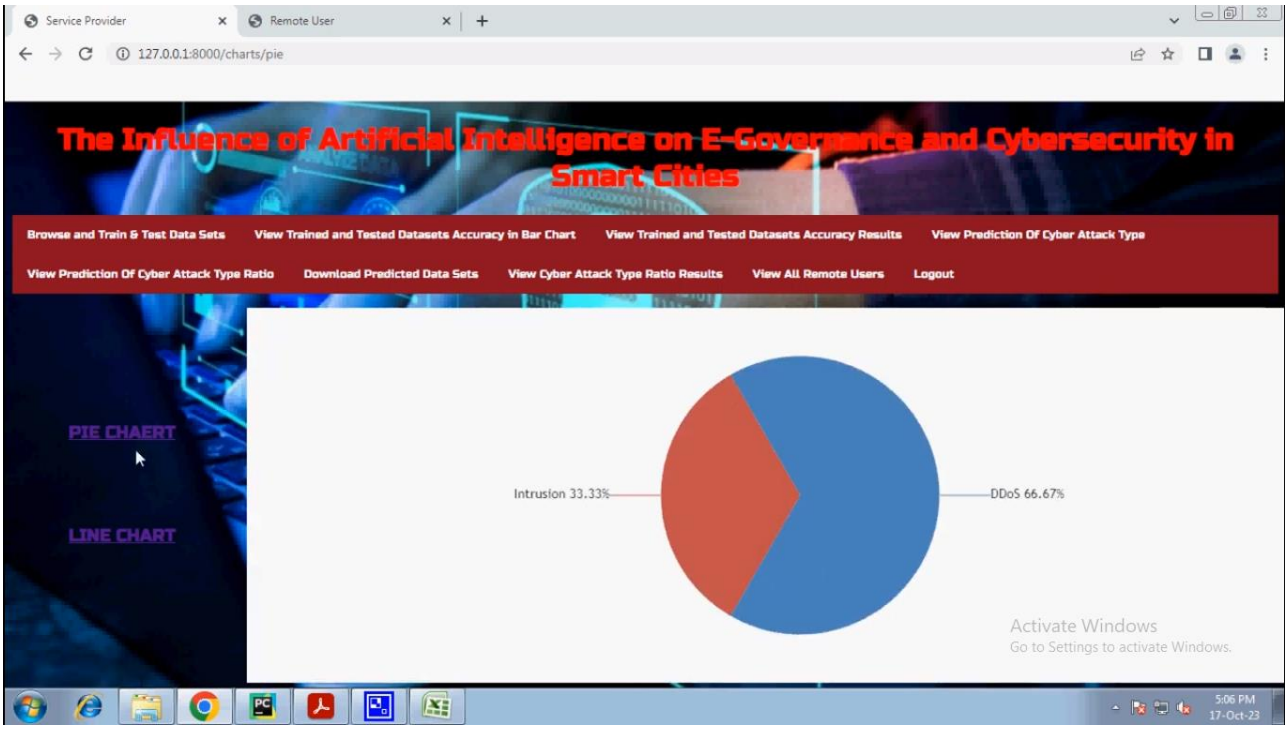

FIG 5.11 PIE CHART

5.2.12 CYBER ATTACK FINAL RATIO DETAILS

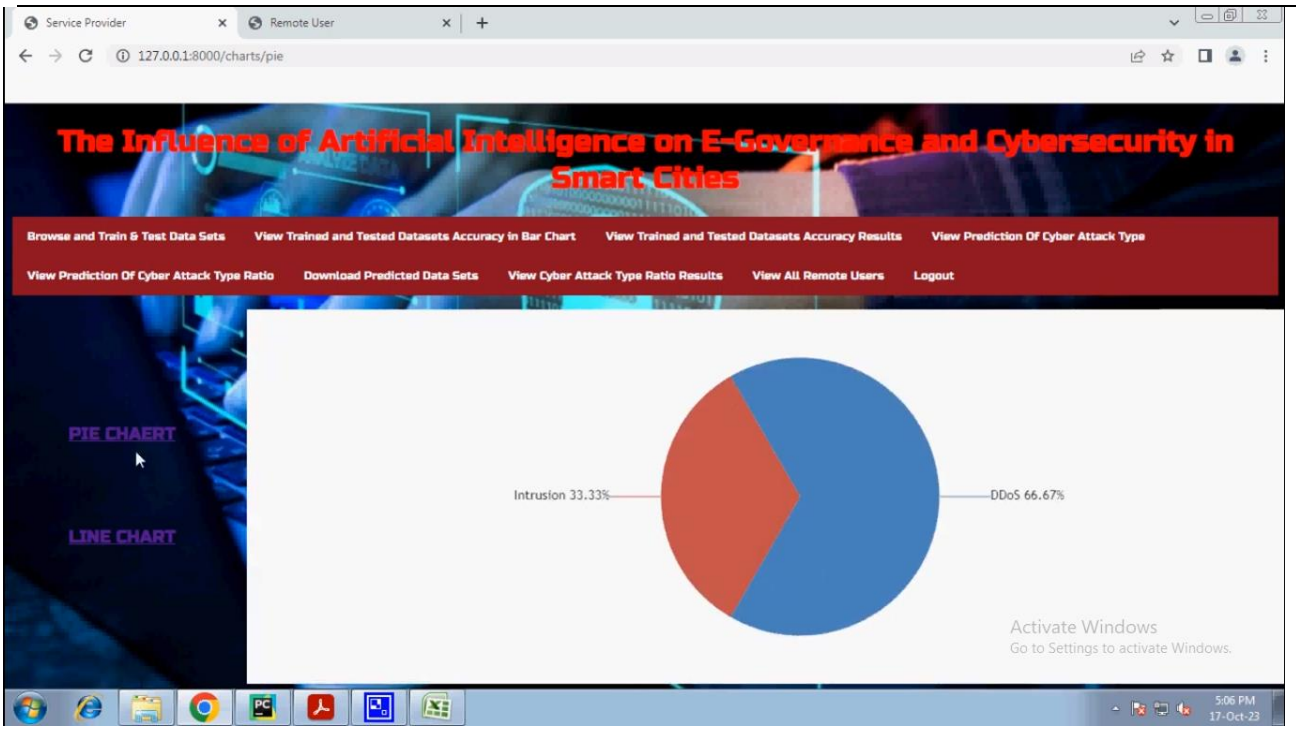

FIG 5.12 CYBER ATTACK FINAL RATIO DETAILS

6. CONCLUSION AND FUTURE WORK

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.

7. REFRENCES

1. B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, ‘‘Effectiveness of artificial intelligence techniques against cyber security risks.

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.*

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,’’

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.