ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

The Influence of AI on E-governance & Cyber security

[1]E.Sriyatha, [2]D.Sai Kumar, [3]G.Anusha, [4]E.Pavan Kumar, [5]Mrs. Palle Swetha,
[1,2,3,4] U.G.Scholor, Department of ECE, Sri Indu College Of Engineering & Technology, Ibrahimpatnam, Hyderabad.
[5]Assistant Professor, Department of ECE, Sri Indu College Of Engineering & Technology, Ibrahimpatnam, Hyderabad.

ABSTRACT

Artificial intelligence (AI) has been identified as a critical technology of FourthIndustrial Revolution (Industry 4.0) for protecting computer network systems against cyber- attacks, malware, phishing,damage, or illicitaccess. AI haspotential in strengthening thecyber 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-Governancebetween AI and cybersecurity and moderatingeffect of stakeholder'sinvolvement on the relationship between AI, e-Governance, and cybersecurity.

1INTRODUCTION

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,itisacknowledgedasperhapsthemostcriticalprobleminthemodern

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

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 .

LiteratureSurvey

1. **Title:** "ArtificialIntelligenceinSmartCities: AComprehensiveReviewofE-Governanceand 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,andanomalydetectionforcybersecurity.Thestudyexploresthe perspectives of stakeholders, including government officials, citizens, and cybersecurity experts, to understand theopportunitiesand challengesassociated with AIadoptionin smartcity governance.
2. **Title:** "EnhancingE-GovernanceandCybersecurityinSmartCitiesthroughArtificial Intelligence: A Stakeholder Analysis"
   - **Author:**EmilyJohnson
   - **Description:** Johnson's research investigates the perceptions and expectations of stakeholders regarding the integration of AI into e-governance and cybersecurity frameworksinsmartcities.Through interviewsandsurveyswithgovernmentofficials, technology experts, and citizens, the paper identifies key factors influencing the adoptionof AI solutions. It also discusses strategies for addressing concerns related to privacy, data security, and algorithmic biases.

3IMPLEMENTATIONSTUDY 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 communicationtechnology(ICT)toenhance servicedelivery.Thetransformationof conventionalurbanareasintosmartcitieshasresultedinahigherlivingstandardforcitizens.

Disadvantages:

- Thecomplexityofdata:Mostofthe existingmachinelearningmodelsmustbeableto accurately interpret large and complex datasets to detect Cybersecurity.
- Data availability: Most machine learning models require large amounts of data to create accuratepredictions.Ifdataisunavailableinsufficientquantities,thenmodelaccuracymay suffer.
- Incorrect labeling: The existing machine learning models are only as accurate as the data trainedusingtheinputdataset.Ifthedatahasbeenincorrectlylabeled,themodelcannotmake accurate predictions.

ProposedSystem& 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.

Advantages:

- Artificialintelligenceapplicationsinsmartcitiescontributetoe-Governancepositively.
- E-Governanceexecutioninsmartcitiesaffectcybersecuritypositively.
- E-Governancemediatesbetweenartificialintelligenceandcybersecuritypositively.

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

ArchitectureDiagram

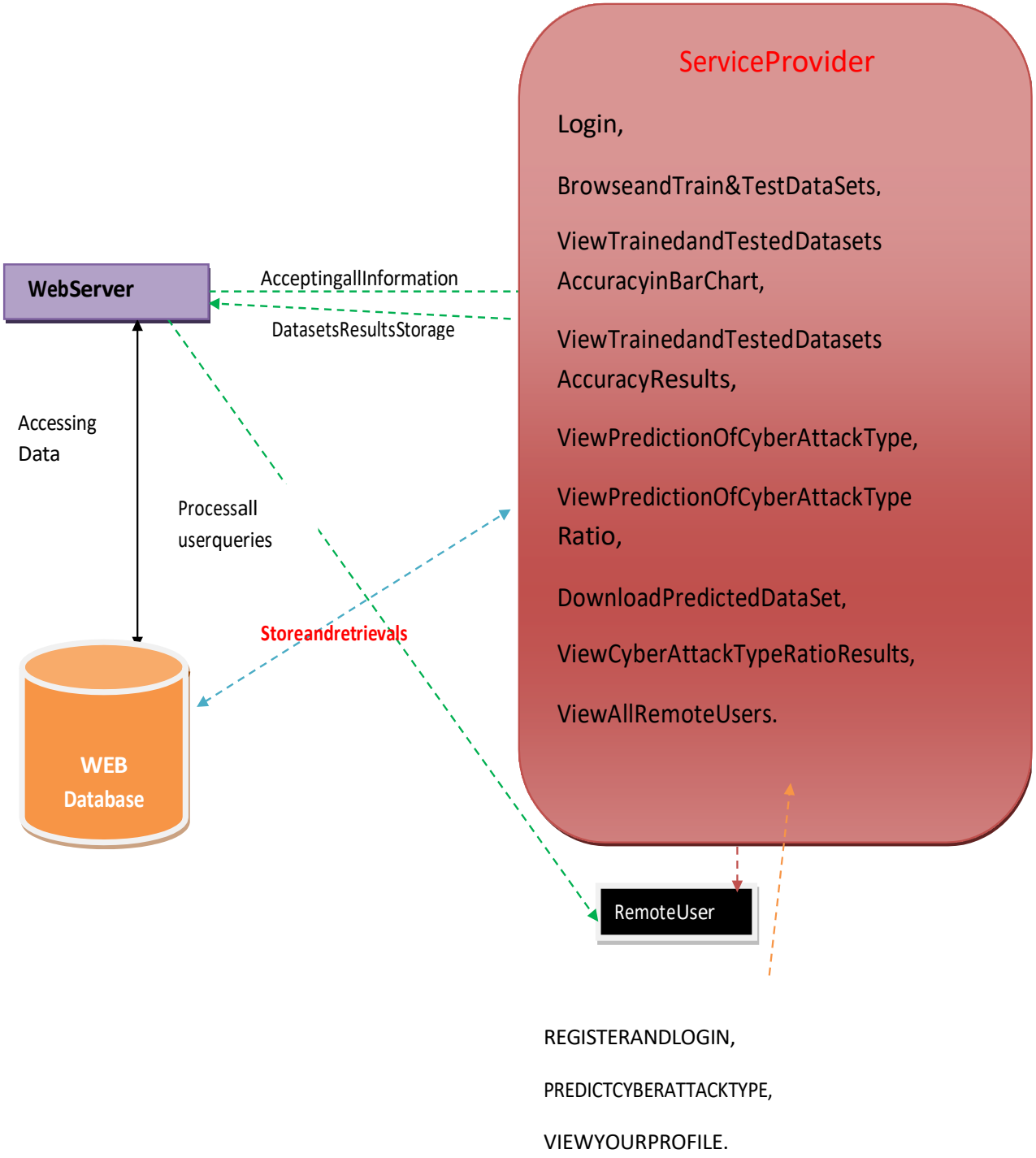


Fig:3.1SystemArchitecture

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

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

Ratio, Download Predicted Data Sets, View Cyber Attack Type Ratio Results, View All Remote Users.

ViewandAuthorizeUsers

Inthismodule,theadmincanviewthelistofuserswhoallregistered.Inthis,the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Browseand Train & Te

5RESULTSANDDISCUSSION

H0MEPAGE

FIG5.1 HOMEPAGE

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

IOT DATASETSANDTESTED RESULT

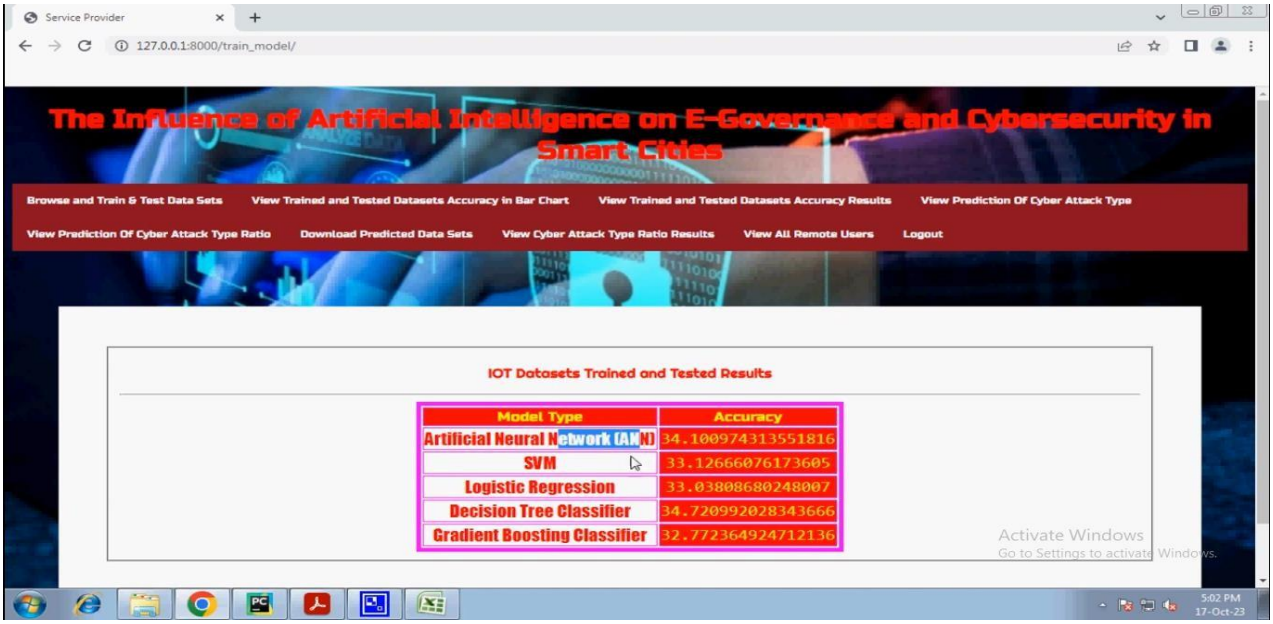


FIG5.2IOTSETSANDTESTEDRESULT

VIEWPREDICTIONOFCYBRRSECURITY

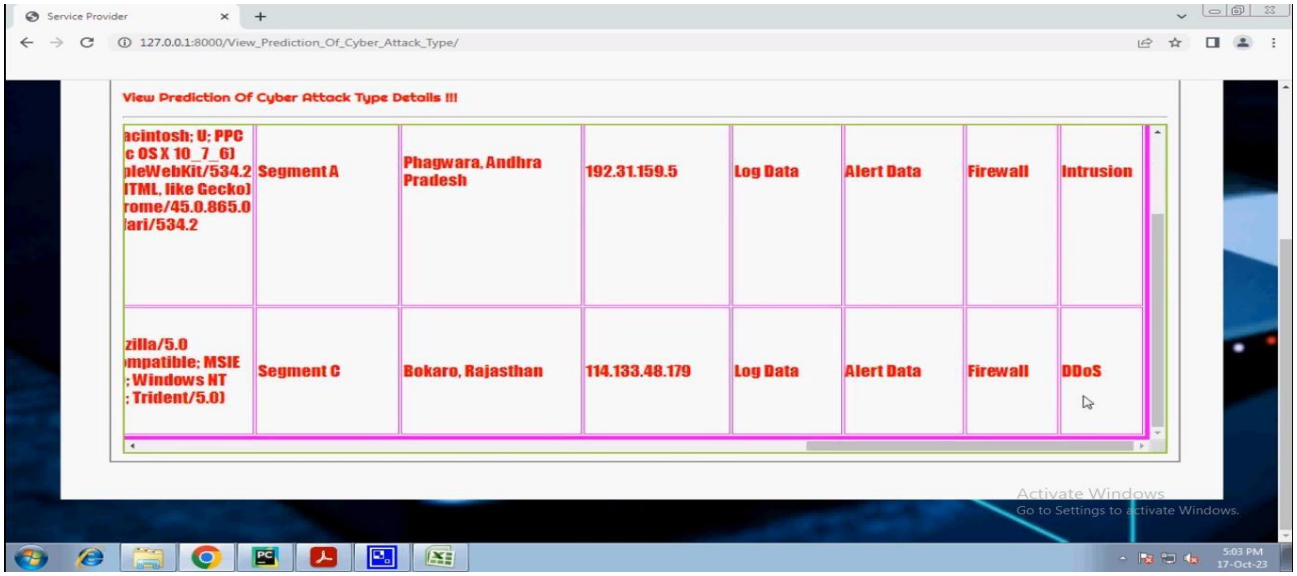


FIG5.3VIEWPREDICTIONOFCYBERSECURITY

VIEWPREDICTIONOFCYBERSECURITYTYPESRATIOS DETSILS

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

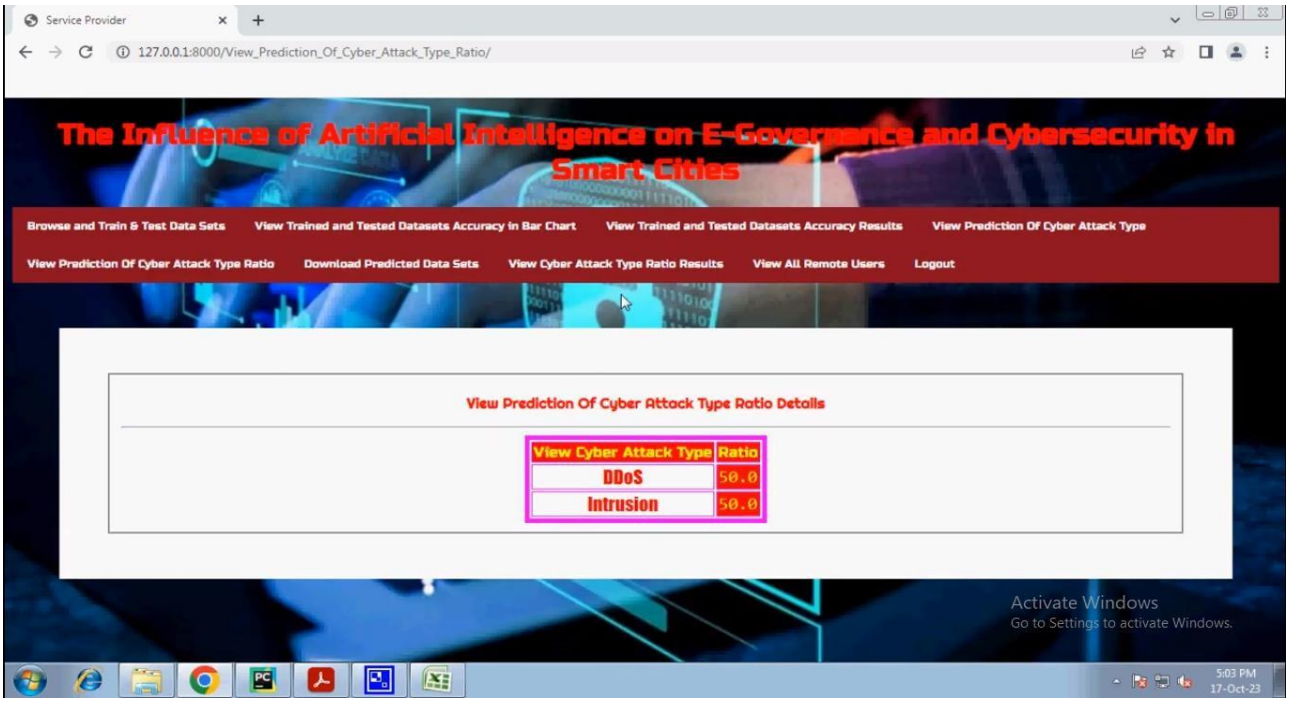


FIG5.4VIEWPREDICTIONOFCYBER SECURITYTYPESRATIOSDETAILS

VIEWALLRATIOUSERS

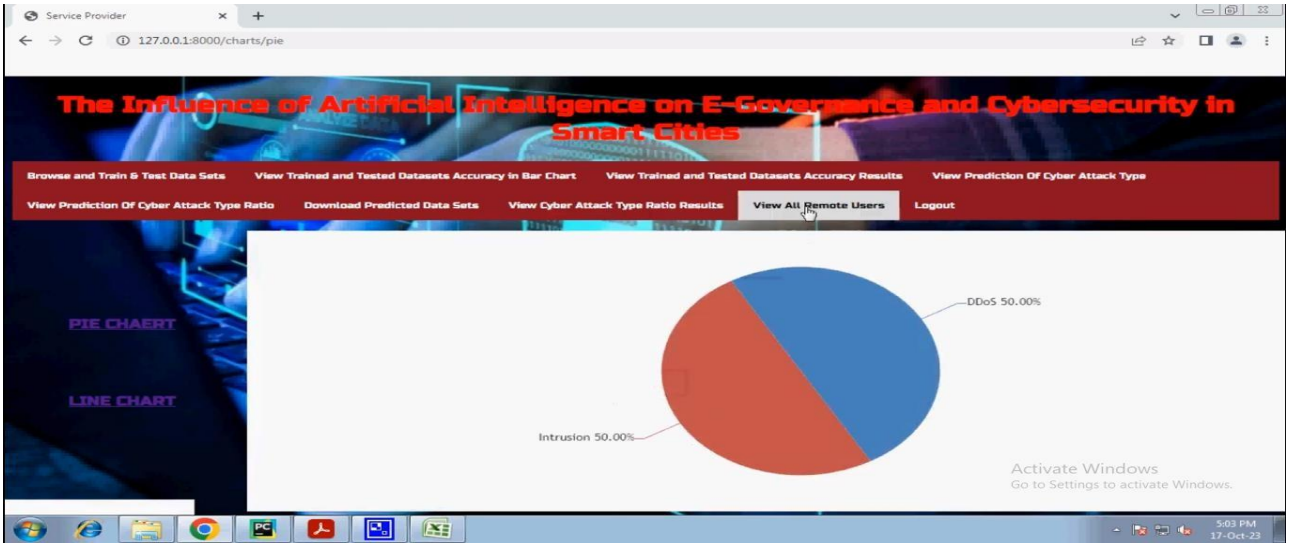


FIG5.5VIEWALLRATIOSUSERS

REGISTRATIONPAGE

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

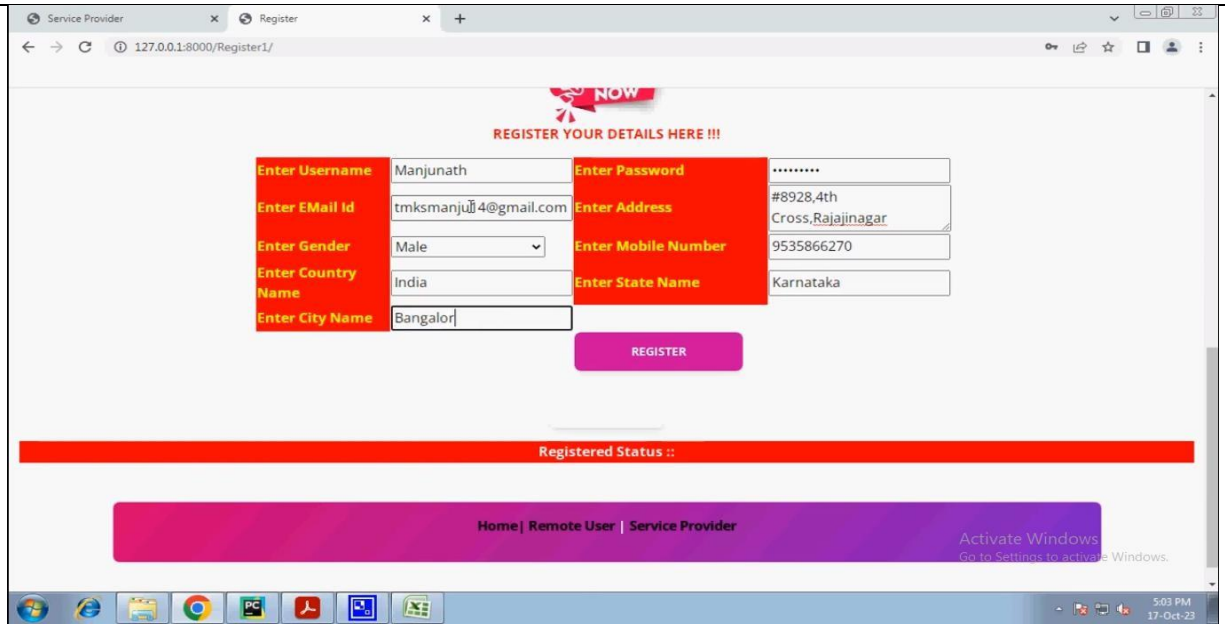
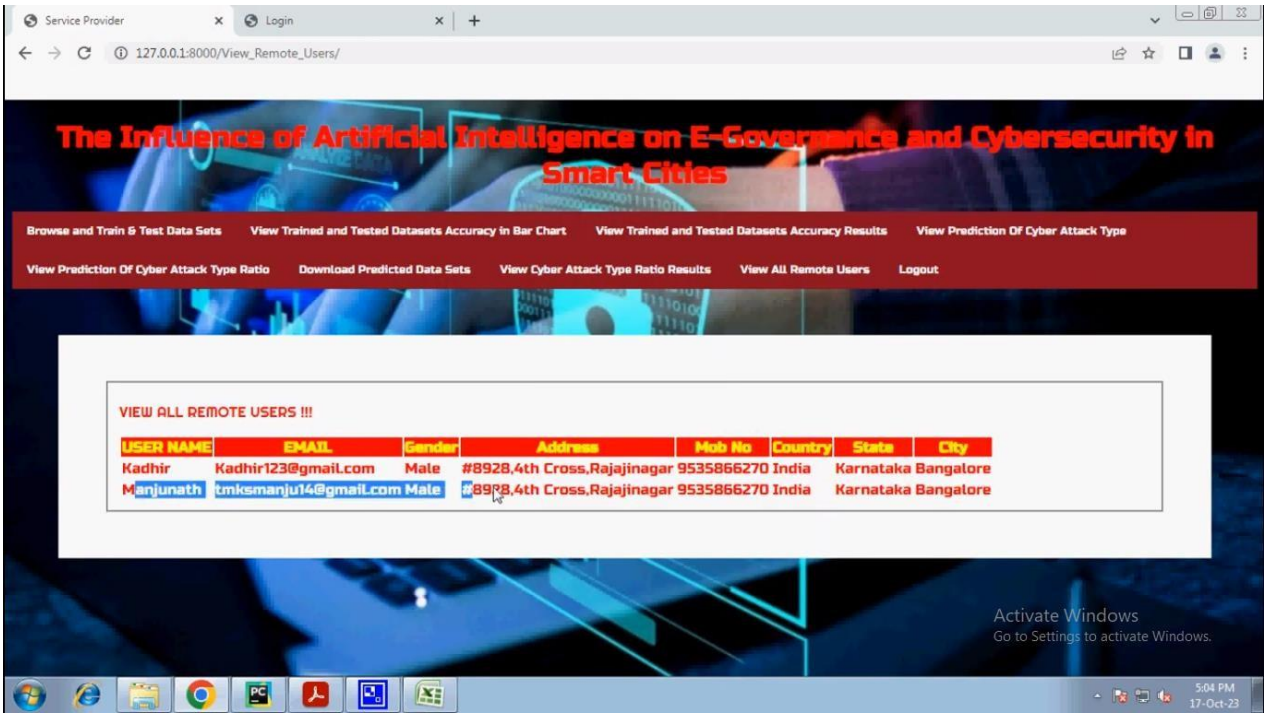


FIG5.6REGISTRATIONPAGE

VIEWALLREMOTEUSERS



ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

FIG5.7VIEWALLREMOTEUSERS

PREDICATECYBERATTACKTYPE

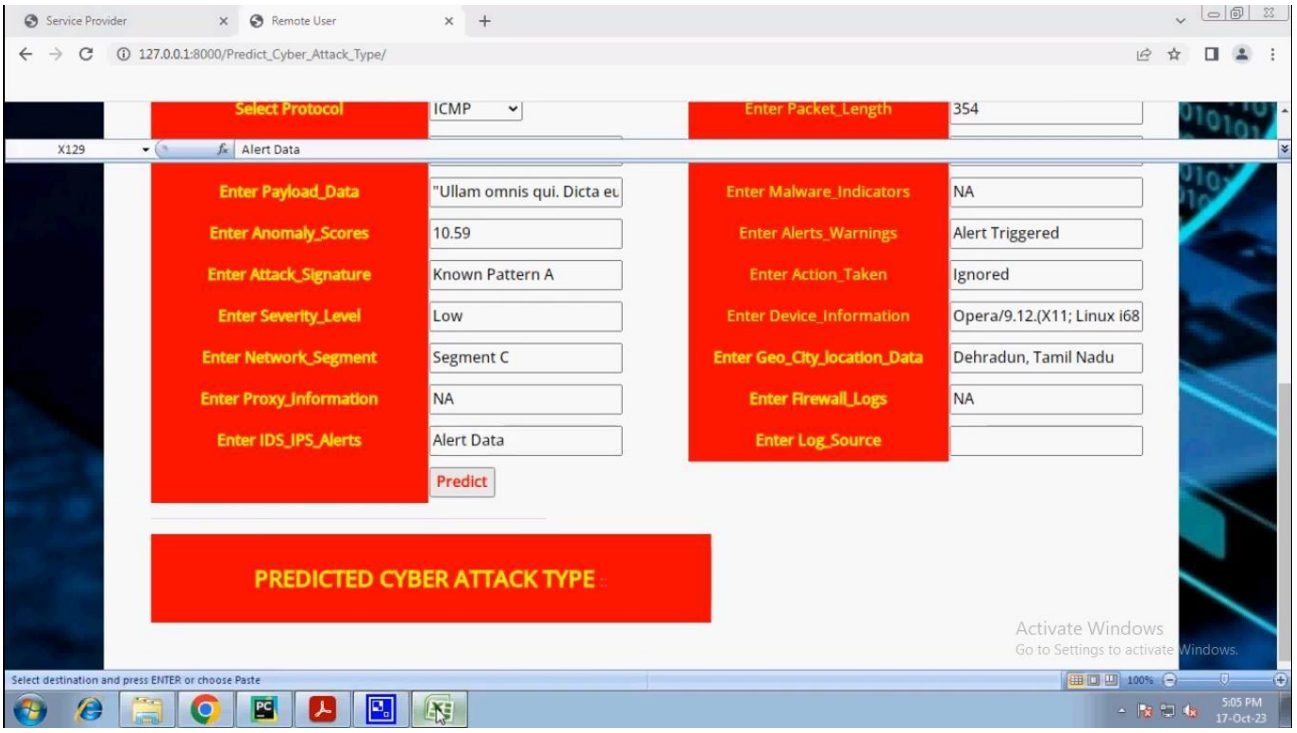
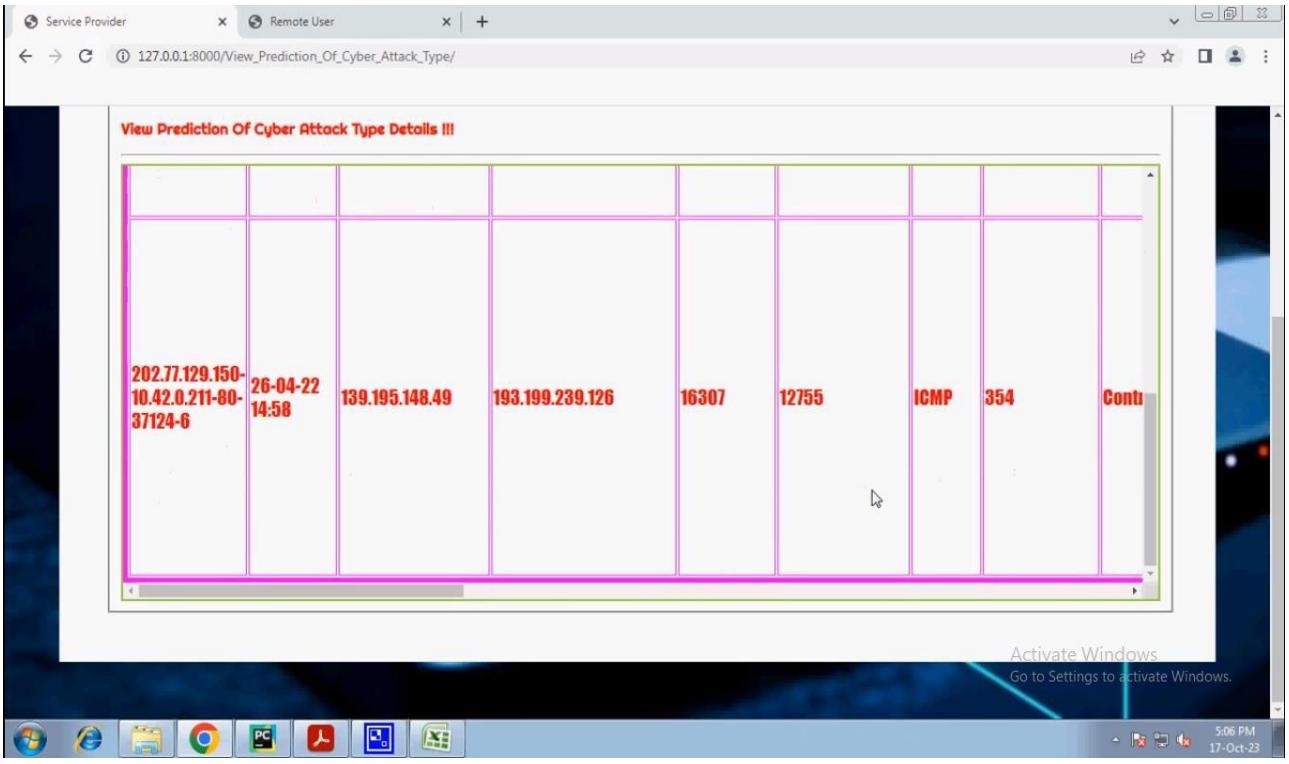


FIG5.8PREDCATECYBERATTACKTYPES

CYBERATTACKTYPE DETAILS



ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

FIG5.9 CYBERATTACKTYPEDETAILS

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

LINE CHART

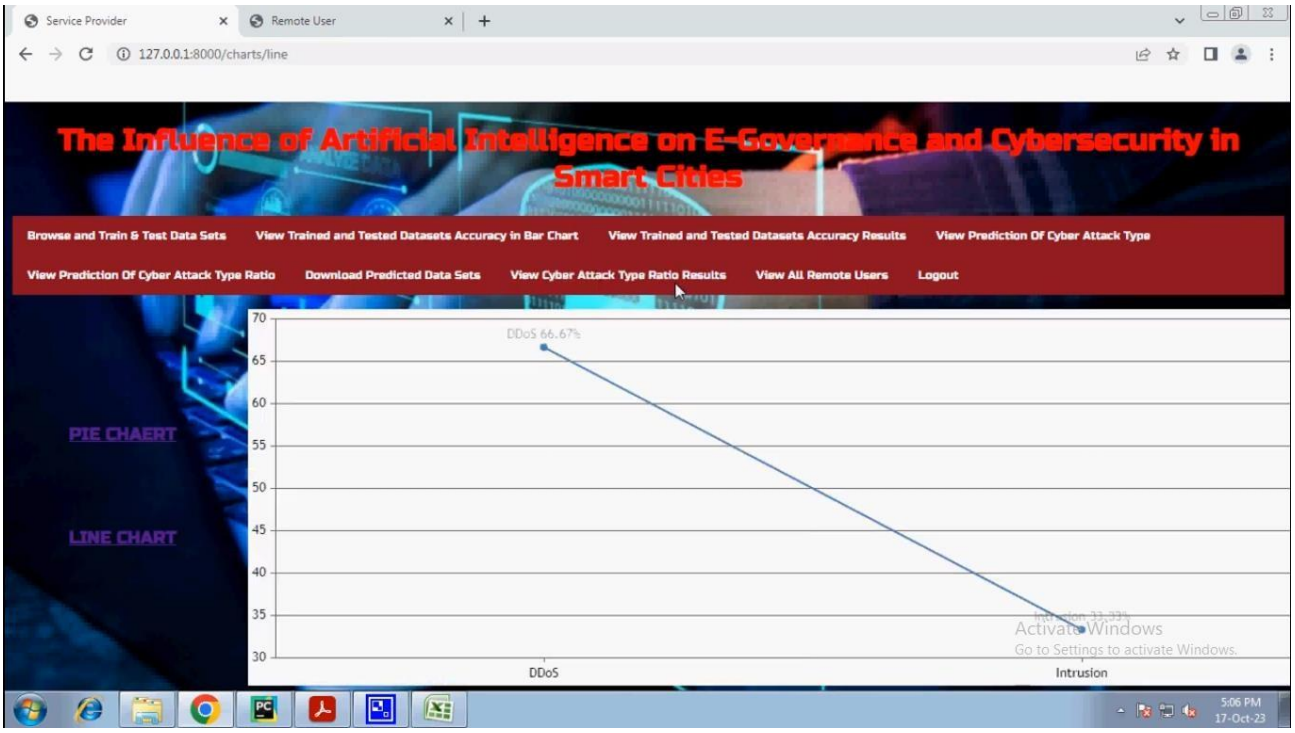


FIG5.10LINECHART

PIE CHART

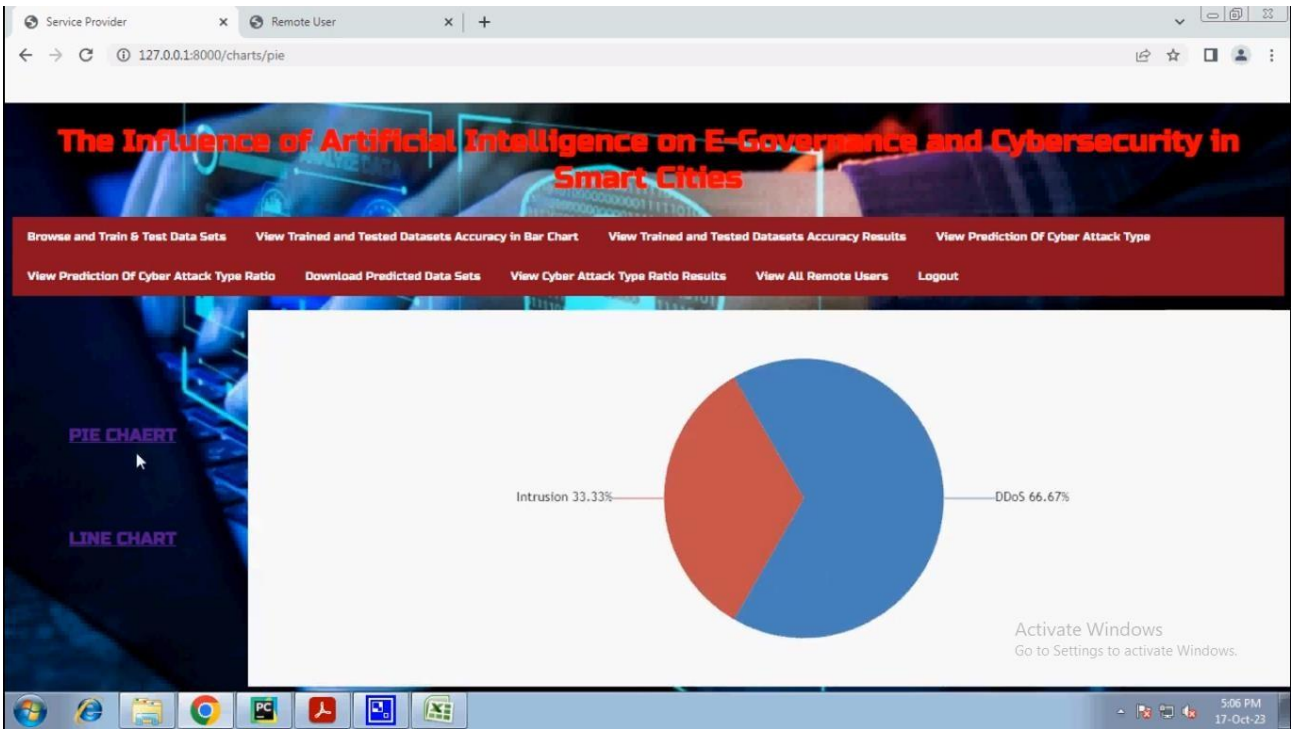


FIG5.11PIECHART

CYBERATTACKFINALRATIODETAILS

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

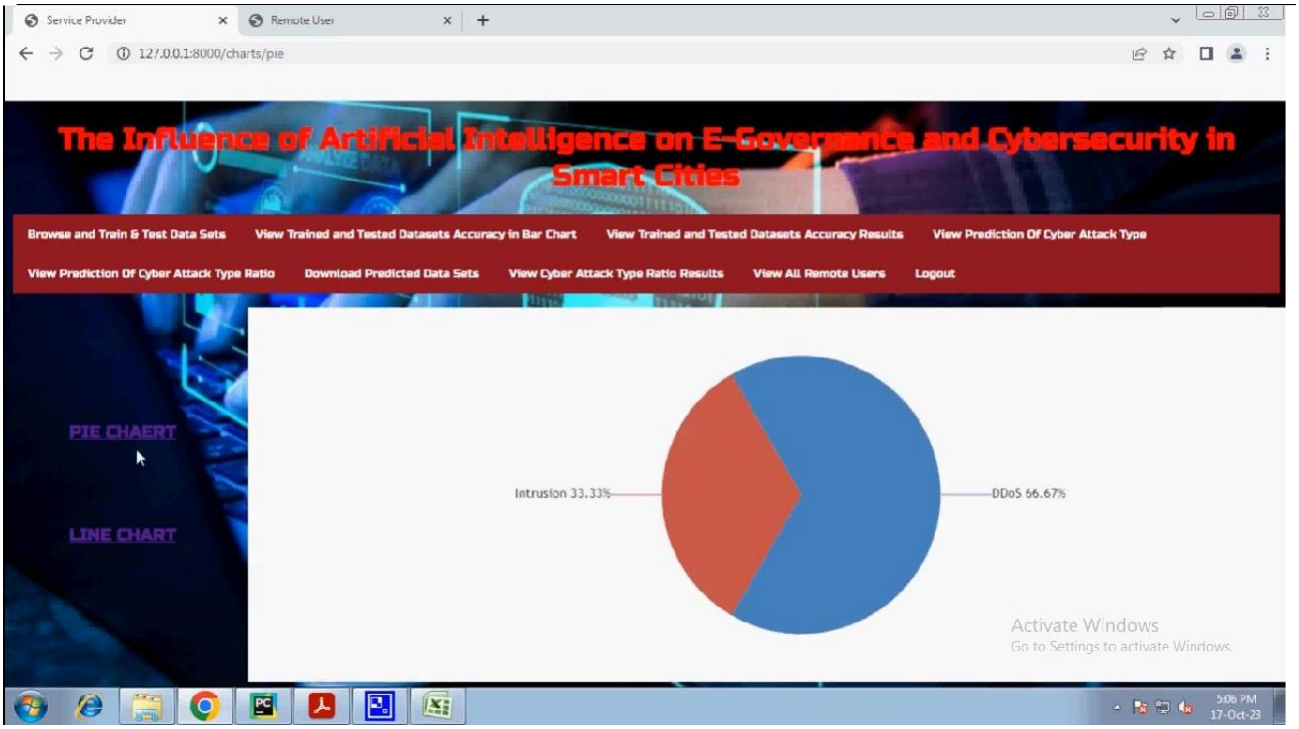


FIG5.12CYBERATTACKFINALRATIODETAILS

6. CONCLUSIONANDFUTUREWORK

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 practitionersmight 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

CONCLUSION

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,andJ.S.Ahmed,"Effectivenessofartificial intelligence techniques against cyber security risks.

2. M.Komar,V.Kochan,L.Dubchak,A.Sachenko,V.Golovko, S.Bezobrazov,andI.Romanets,"Highperformanceadaptivesystemfor cyber attacks detection," in *Proc. 9th IEEE Int.*

3. M.D.Cavelty,*Cyber-SecurityandThreatPolitics:USEfforts toSecure the Information Age*. Evanston, IL, USA: Routledge, 2007.

4. F.Fransen,A.Smulders,andR.Kerkdijk,"Cybersecurityinformation exchangeto gain insightintotheeffectsofcyber threatsand incidents,"

5. A.Corallo,M.Lazoi, M.Lezzi,andA.Lupertoo,"Cybersecurityawareness 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,andM.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.Badaand J.R.C.Nurse,"Thesocialand psychologicalimpactof cyberattacks,"in *EmergingCyberThreatsandCognitiveVulnerabilities*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 73–92.

8. G. Allen and T. Chan, *Artificial*

Intelligence and National Security. Cambridge,MA,USA :BelferCenterforScienceandInternationalAffairs, 2017.

9. Z.Zhang,H.Ning,F.Shi,F.Farha,Y.Xu,J.Xu,F. Zhang, andK.-K.R.Choo,‘‘Artificialintelligenceincybersecurity:Research advances, challenges, and opportunities,’’ *Artif. Intell. Rev.*, vol. 55, pp.1029–1053,Feb.2022.
10. Z.I.Khisamova,I.R.Begishev,andE.L.Sidorenko,‘‘Artificialintelligence and problems of ensuring cyber security,’’ *Int. J. Cyber Criminol.*, vol.13,no.2,pp.564–577,2019.