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 CYBERSECURITY IN SMART CITIES A STAKEHOLDER'S PERSPECTIVE

Mr. S. K. Alisha, Associate professor,
Department of MCA
Khadar6@gmail.com
B V Raju College, Bhimavaram

AKUMURI NIKHIL (2285351007)
Department of MCA
nikhiljack105@gmail.com
B V Raju College, Bhimavaram

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 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.

Keywords: artificial intelligence, e-governance, cybersecurity, smart cities, stakeholders involvement, Industry 4.0, PLS-SEM path modeling.

INTRODUCTION

The advent of the Fourth Industrial Revolution, also known as Industry 4.0, has heralded the integration of advanced technologies into various facets of society. Among these technologies, artificial intelligence (AI) stands out for its transformative potential, particularly in the realms of e-governance and cybersecurity. AI's ability to process vast amounts of data, recognize patterns, and make decisions has positioned it as a critical tool for enhancing the security and efficiency of digital infrastructures. This is especially pertinent for smart cities, where the complexity of managing urban environments is magnified by the need to safeguard against cyber threats. AI's role in protecting computer network systems from cyber-attacks, malware, phishing, and unauthorized access is not merely a technological advancement but a necessity for maintaining the integrity of smart cities. E-governance refers to the use of digital technologies by government agencies to improve the delivery of public services, enhance the efficiency of government operations, and foster greater citizen engagement. AI can significantly enhance e-governance by automating routine tasks, facilitating data-driven decision-making, and providing personalized services to citizens. For instance, AI algorithms can analyze large datasets to identify trends and patterns that inform policy-making, while chatbots can

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

assist citizens in accessing government services more efficiently. However, the integration of AI into e-governance also raises significant cybersecurity concerns. As government agencies become more reliant on digital technologies, they become more vulnerable to cyber-attacks. AI can both mitigate and exacerbate these risks, depending on how it is implemented and managed.

The relationship between AI, e-governance, and cybersecurity is complex and context-specific. Existing research presents a mixed picture of this relationship, highlighting both the opportunities and challenges associated with AI integration. On one hand, AI can enhance cybersecurity by detecting and responding to threats more quickly and accurately than human operators. For example, machine learning algorithms can analyze network traffic to identify anomalies that may indicate a cyber-attack, allowing for faster and more effective responses. On the other hand, AI systems themselves can be targeted by cyber-attacks, and their complexity can introduce new vulnerabilities. Additionally, the use of AI in e-governance raises ethical and legal concerns, particularly regarding data privacy and the potential for biased decision-making. Stakeholders play a crucial role in shaping the relationship between AI, e-governance, and cybersecurity. These stakeholders include government officials, technology developers, cybersecurity experts, and the citizens who use e-governance services. Each group brings a unique perspective and set of expertise to the table, influencing how AI is implemented and managed. For instance, government officials may prioritize regulatory compliance and public trust, while technology developers focus on innovation and technical performance. Cybersecurity experts are concerned with protecting systems from threats, and citizens value transparency and privacy. The involvement of these diverse stakeholders is essential for developing AI solutions that are both effective and ethically sound.

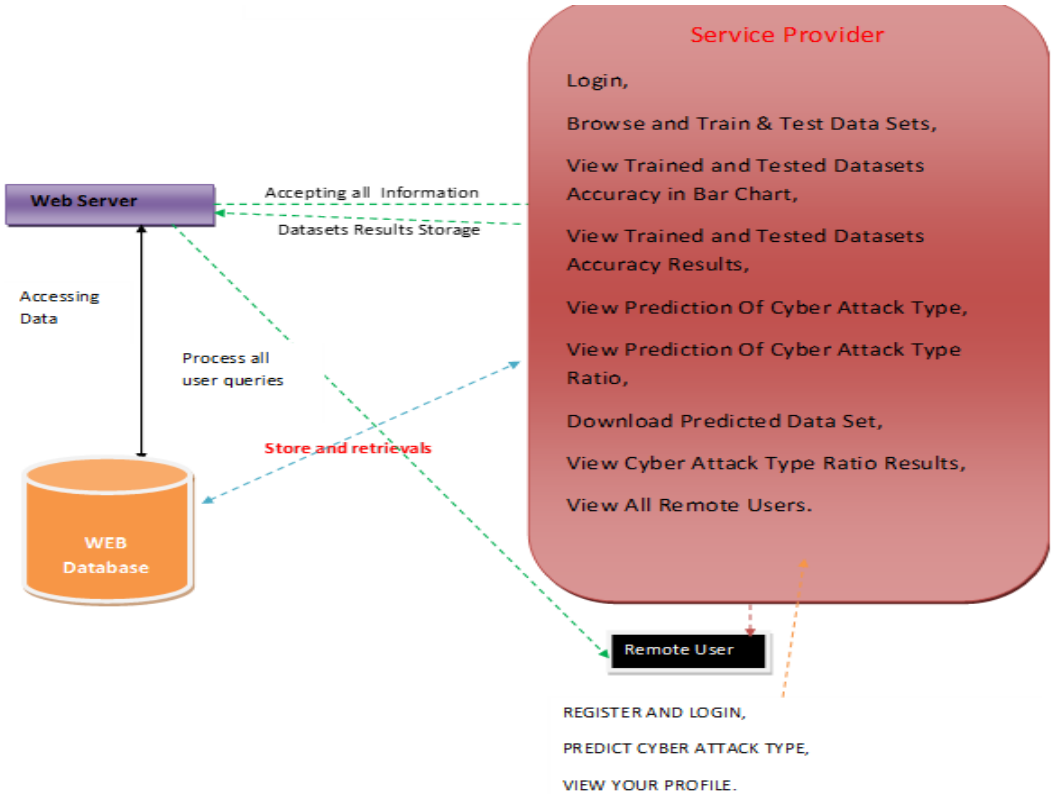

Fig 1. System Architecture

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

To address the context-specific nature of the relationship between AI, e-governance, and cybersecurity, this study investigates the direct and indirect effects of these factors. Using Partial Least Squares Structural Equation Modeling (PLS-SEM), the study examines how e-governance mediates the relationship between AI and cybersecurity, and how stakeholder involvement moderates these relationships. The findings reveal a partial mediating effect of e-governance, indicating that the implementation of AI in e-governance systems can enhance cybersecurity outcomes. However, this effect is contingent on the involvement of stakeholders, who influence how AI is integrated and managed within these systems. The results of the PLS-SEM path modeling analysis provide several practical implications for smart city governance. First, they highlight the importance of stakeholder engagement in the development and implementation of AI solutions. By involving stakeholders in the decision-making process, governments can ensure that AI systems are designed to meet the needs and values of the community. This includes addressing concerns about data privacy, transparency, and accountability. Second, the findings suggest that e-governance can serve as a bridge between AI and cybersecurity, enhancing the effectiveness of both. Governments should therefore invest in robust e-governance platforms that leverage AI to improve service delivery and security.

Furthermore, the study underscores the need for a holistic approach to AI integration, one that considers the technical, ethical, and social dimensions of AI. This involves not only developing advanced AI algorithms but also establishing clear guidelines and standards for their use. For example, governments could implement policies that require regular audits of AI systems to ensure they are operating as intended and not introducing new risks. Additionally, public education campaigns can help citizens understand the benefits and risks of AI, fostering greater trust and acceptance of these technologies. In summary, the influence of AI on e-governance and cybersecurity in smart cities is multifaceted and context-specific. While AI offers significant potential for enhancing the security and efficiency of digital infrastructures, its integration must be carefully managed to address the associated risks. Stakeholder involvement is critical for ensuring that AI systems are developed and implemented in a way that aligns with the values and needs of the community. By leveraging the mediating role of e-governance and the moderating effect of stakeholder engagement, governments can harness the power of AI to create safer, more efficient, and more inclusive smart cities. The findings of this study provide valuable insights for policymakers and practitioners, offering a roadmap for integrating AI into e-governance and cybersecurity frameworks.

LITERATURE SURVEY

The integration of artificial intelligence (AI) into e-governance and cybersecurity in the context of smart cities is a rapidly evolving field that reflects the broader technological advancements of the Fourth Industrial Revolution, or Industry 4.0. AI's capacity to analyze vast amounts of data, detect patterns, and make autonomous decisions has positioned it as a pivotal technology for enhancing the security and efficiency of digital infrastructures. The application of AI in e-governance aims to streamline public services, improve decision-making processes, and foster citizen engagement through more efficient and personalized services. Concurrently, AI's role in cybersecurity is crucial for protecting computer networks from a myriad of threats including cyber-attacks, malware, phishing, and unauthorized access. E-governance, which involves the use of digital tools and platforms by government agencies to deliver services, facilitate communication, and engage with citizens, stands to benefit significantly from AI. AI can automate routine administrative tasks, analyze large datasets to inform policy decisions, and provide real-time responses to citizen inquiries through chatbots. These applications can lead to more efficient government operations, cost savings, and improved service delivery. However, the digital transformation of government functions also raises significant cybersecurity concerns. As governments digitize their operations, they become more attractive targets for cybercriminals seeking to exploit vulnerabilities in digital systems. This makes the role of AI in bolstering cybersecurity defenses particularly important.

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

The relationship between AI, e-governance, and cybersecurity is complex and varies depending on the specific context. Some studies have shown that AI can significantly enhance cybersecurity by providing advanced threat detection and response capabilities. For example, machine learning algorithms can analyze network traffic to identify unusual patterns indicative of a cyber-attack, enabling faster and more effective mitigation measures. Additionally, AI can predict potential security breaches by analyzing historical data and identifying trends that precede attacks. However, other studies have highlighted potential risks associated with the use of AI in cybersecurity. AI systems themselves can be targeted by cyber-attacks, and the complexity of AI algorithms can introduce new vulnerabilities. Moreover, the reliance on AI for critical security functions raises ethical and legal concerns, particularly regarding accountability and transparency. E-governance also plays a critical role in mediating the relationship between AI and cybersecurity. Effective e-governance frameworks can facilitate the integration of AI into government operations while ensuring that cybersecurity measures are in place to protect sensitive data and systems. This involves developing policies and regulations that govern the use of AI, establishing standards for data protection, and implementing robust security protocols. E-governance can also promote transparency and accountability by providing mechanisms for auditing AI systems and ensuring that they operate as intended. The mediating role of e-governance is crucial for maximizing the benefits of AI while mitigating associated risks.

The influence of stakeholders on the relationship between AI, e-governance, and cybersecurity cannot be overstated. Stakeholders include a diverse range of individuals and organizations, such as government officials, technology developers, cybersecurity experts, and citizens. Each group brings unique perspectives and expertise, shaping how AI technologies are implemented and managed. For instance, government officials may prioritize regulatory compliance and public trust, while technology developers focus on innovation and technical performance. Cybersecurity experts are concerned with protecting systems from threats, and citizens value transparency and privacy. Effective stakeholder engagement is essential for ensuring that AI systems are designed and deployed in a manner that addresses the needs and concerns of all parties involved. Research on the moderating effect of stakeholder involvement suggests that active engagement of stakeholders can enhance the effectiveness of AI in e-governance and cybersecurity. By involving stakeholders in the decision-making process, governments can develop AI solutions that are more aligned with the values and expectations of the community. This includes addressing ethical considerations, such as ensuring that AI systems are free from bias and that citizens' privacy is protected. Stakeholder involvement can also foster greater public trust in AI technologies, which is critical for their widespread adoption and success.

The use of Partial Least Squares Structural Equation Modeling (PLS-SEM) in this study provides a comprehensive analysis of the relationships between AI, e-governance, and cybersecurity, as well as the moderating role of stakeholders. The results reveal a partial mediating effect of e-governance between AI and cybersecurity, indicating that the implementation of AI in e-governance systems can enhance cybersecurity outcomes. This finding underscores the importance of robust e-governance frameworks in leveraging AI for cybersecurity. Additionally, the moderating influence of stakeholder involvement highlights the critical role that stakeholders play in shaping the effectiveness of AI and e-governance initiatives. The practical implications of these findings are significant for the development of smart cities. Governments need to invest in e-governance platforms that integrate AI technologies to improve service delivery and security. This requires not only technological investments but also the development of policies and regulations that ensure the responsible use of AI. Engaging stakeholders in the development and implementation process is crucial for addressing ethical and legal concerns, fostering public trust, and ensuring that AI systems meet the needs of the community. By adopting a holistic approach that considers the technical, ethical, and social dimensions of AI, e-governance, and cybersecurity, governments can create safer, more efficient, and more inclusive smart cities.

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

In summary, the influence of AI on e-governance and cybersecurity in smart cities is a multifaceted and context-specific issue that requires careful consideration of various factors. AI has the potential to significantly enhance the security and efficiency of digital infrastructures, but its integration must be managed carefully to address associated risks. E-governance frameworks play a crucial mediating role in this process, and the active involvement of stakeholders is essential for ensuring that AI systems are effective, ethical, and aligned with the needs of the community. The findings of this study provide valuable insights for policymakers and practitioners, offering a roadmap for integrating AI into e-governance and cybersecurity frameworks to strengthen the resilience and sustainability of smart cities.

PROPOSED SYSTEM

The proposed system for examining the influence of artificial intelligence (AI) on e-governance and cybersecurity in smart cities from a stakeholder's perspective is designed to address the complex, context-specific interactions between these domains. This system leverages AI to enhance cybersecurity measures and improve the efficiency and effectiveness of e-governance platforms, while also incorporating stakeholder involvement to ensure the ethical and practical deployment of these technologies. The methodology involves several key components: data collection and analysis, AI integration, stakeholder engagement, and policy development and implementation. The first component involves comprehensive data collection and analysis. This includes gathering data on cyber threats, network vulnerabilities, and incident reports from various government and non-government sources. AI algorithms can be employed to analyze this data to identify patterns and trends in cyber-attacks, predict potential vulnerabilities, and develop proactive defense strategies. The data collection process also involves compiling information on current e-governance practices, citizen engagement metrics, and stakeholder feedback. By integrating these datasets, the system can provide a holistic view of the cybersecurity landscape and the effectiveness of e-governance platforms.

The next step is the integration of AI into e-governance systems to enhance cybersecurity. AI technologies such as machine learning, natural language processing, and anomaly detection are utilized to automate and improve various aspects of cybersecurity. Machine learning algorithms can be trained to detect and respond to cyber threats in real time, identifying anomalies in network traffic that may indicate malicious activity. Natural language processing can be used to analyze communication data, such as emails and messages, to detect phishing attempts and other social engineering attacks. AI can also help in automating routine cybersecurity tasks, such as patch management and threat intelligence gathering, freeing up human resources for more complex tasks. In addition to enhancing cybersecurity, AI can significantly improve the efficiency and effectiveness of e-governance platforms. AI-powered chatbots and virtual assistants can provide citizens with instant access to information and services, reducing wait times and improving user satisfaction. Machine learning algorithms can analyze citizen feedback and engagement data to identify areas for improvement in service delivery. Furthermore, AI can assist in policy-making by providing data-driven insights and recommendations based on predictive analytics. By leveraging AI, e-governance platforms can become more responsive, transparent, and user-friendly.

Stakeholder engagement is a critical component of the proposed system. Stakeholders include government officials, technology developers, cybersecurity experts, and citizens. Each group has unique perspectives and expertise that are essential for the successful implementation of AI in e-governance and cybersecurity. The system involves regular consultations and feedback sessions with stakeholders to ensure that their concerns and recommendations are addressed. For example, government officials may be concerned about regulatory compliance and public trust, while technology developers focus on innovation and technical feasibility. Cybersecurity experts can provide insights into emerging threats and best practices for defense, and citizens can offer feedback on the usability and accessibility of e-

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

governance platforms. By involving stakeholders in the decision-making process, the system ensures that AI technologies are deployed in a manner that is ethical, transparent, and aligned with the needs and values of the community. The results of the Partial Least Squares Structural Equation Modeling (PLS-SEM) path modeling analysis provide a nuanced understanding of the relationships between AI, e-governance, and cybersecurity. The analysis reveals that e-governance partially mediates the relationship between AI and cybersecurity, suggesting that the implementation of AI in e-governance systems can enhance cybersecurity outcomes. This implies that investments in e-governance infrastructure and AI capabilities can have a synergistic effect, improving both service delivery and security. Furthermore, the analysis highlights the moderating role of stakeholder involvement, indicating that the effectiveness of AI and e-governance initiatives is significantly influenced by the extent to which stakeholders are engaged and their input is incorporated. This finding underscores the importance of a collaborative approach to technology deployment, where diverse perspectives are valued and integrated into the development process.

The practical implications of these findings are significant for governmental bodies of smart cities. To strengthen their cybersecurity measures, governments need to adopt a holistic approach that integrates AI technologies into e-governance systems while actively engaging stakeholders. This involves investing in advanced AI tools and technologies, developing robust e-governance platforms, and establishing mechanisms for continuous stakeholder engagement and feedback. Governments should also focus on developing clear policies and regulations that govern the use of AI, ensuring that these technologies are deployed ethically and transparently. Public education campaigns can help build trust and awareness among citizens, encouraging them to participate actively in e-governance initiatives and providing valuable feedback for continuous improvement. In summary, the proposed system for exploring the influence of AI on e-governance and cybersecurity in smart cities from a stakeholder's perspective provides a comprehensive framework for addressing the complex interactions between these domains. By leveraging AI to enhance cybersecurity and improve e-governance, while actively engaging stakeholders, the system aims to create a vibrant, transparent, and secure cyberspace. The findings of the PLS-SEM path modeling analysis underscore the importance of e-governance as a mediator and stakeholder involvement as a moderator in this relationship. These insights offer practical guidance for policymakers and practitioners, highlighting the need for a collaborative, context-specific approach to integrating AI into smart city governance and cybersecurity frameworks. The ultimate goal is to create smarter, safer, and more inclusive cities that leverage the full potential of AI while ensuring that the deployment of these technologies aligns with the values and needs of the community.

METHODOLOGY

The methodology for examining the influence of artificial intelligence (AI) on e-governance and cybersecurity in smart cities from a stakeholder’s perspective involves several carefully designed steps. This approach aims to explore the direct relationships between AI, e-governance, and cybersecurity, the mediating role of e-governance between AI and cybersecurity, and the moderating effect of stakeholder involvement on these relationships. The methodology encompasses data collection, model development, data analysis, and interpretation of results. The first step involves a comprehensive review of existing literature to identify relevant variables and constructs that define the relationships between AI, e-governance, and cybersecurity. This literature review helps to establish a theoretical framework and inform the development of the research model. The review focuses on previous studies that have explored the applications of AI in cybersecurity, the role of e-governance in enhancing public service delivery, and the impact of stakeholder involvement on technological implementations in smart cities.

Following the literature review, the next step is to collect primary data from various stakeholders involved in the implementation and use of AI, e-governance, and cybersecurity in smart cities. Stakeholders include government

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

officials, IT professionals, cybersecurity experts, and citizens. Data collection is conducted through structured surveys and interviews designed to capture the perceptions, experiences, and expertise of these stakeholders. The surveys include questions on the effectiveness of AI in cybersecurity, the role of e-governance platforms, and the importance of stakeholder involvement in technological decision-making processes. Once the data is collected, it is prepared for analysis. This involves data cleaning and validation to ensure accuracy and reliability. Missing data is addressed through imputation techniques, and outliers are identified and managed. The validated data is then used to develop a Partial Least Squares Structural Equation Modeling (PLS-SEM) path model. PLS-SEM is chosen for its ability to handle complex relationships between multiple variables and its suitability for exploratory research.

The development of the PLS-SEM model begins with defining the constructs and their corresponding indicators based on the literature review and survey responses. Constructs such as AI capabilities, e-governance effectiveness, cybersecurity outcomes, and stakeholder involvement are operationalized using reflective indicators. These indicators are measured using Likert scales, where respondents rate their agreement with various statements. The next step involves specifying the structural model, which outlines the hypothesized relationships between the constructs. The model posits direct relationships between AI and e-governance, AI and cybersecurity, and e-governance and cybersecurity. It also includes the mediating effect of e-governance on the relationship between AI and cybersecurity, and the moderating effect of stakeholder involvement on the relationships between AI and e-governance, and between e-governance and cybersecurity.

With the model specified, the next step is to test the measurement model to ensure that the constructs are valid and reliable. This involves assessing the convergent and discriminant validity of the constructs using criteria such as composite reliability, average variance extracted (AVE), and Fornell-Larcker criterion. The measurement model is refined by removing indicators that do not meet the validity and reliability criteria, resulting in a robust set of constructs. Once the measurement model is validated, the structural model is assessed to test the hypothesized relationships. This involves estimating the path coefficients and their significance using bootstrapping techniques. The results of the PLS-SEM analysis reveal the strength and direction of the relationships between the constructs, as well as the mediating and moderating effects.

The analysis reveals a partial mediating impact of e-governance between AI and cybersecurity, indicating that while AI directly enhances cybersecurity, its effectiveness is further amplified when integrated into e-governance systems. This suggests that investments in e-governance infrastructure can enhance the cybersecurity benefits of AI. Additionally, the moderating influence of stakeholder involvement is significant, highlighting that the involvement of diverse stakeholders strengthens the positive effects of AI and e-governance on cybersecurity outcomes. The final step involves interpreting the results and deriving practical implications. The findings are discussed in the context of the theoretical framework and existing literature. The study concludes that stakeholder involvement is crucial for the successful implementation of AI in e-governance and cybersecurity. By engaging stakeholders, governments can ensure that AI technologies are deployed in a manner that is ethical, transparent, and aligned with the needs of the community.

The study provides practical recommendations for governmental bodies in smart cities. These include fostering stakeholder engagement through regular consultations and feedback mechanisms, investing in robust e-governance platforms that integrate AI capabilities, and developing clear policies and regulations that govern the use of AI. Public education campaigns can also help build trust and awareness among citizens, encouraging active participation in e-governance initiatives. In summary, the methodology for examining the influence of AI on e-governance and cybersecurity in smart cities involves a systematic approach to data collection, model development, and analysis. By

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

using PLS-SEM path modeling, the study explores the complex relationships between these variables and highlights the critical role of stakeholder involvement. The findings provide valuable insights for policymakers and practitioners, offering a roadmap for integrating AI into e-governance and cybersecurity frameworks to create safer, more efficient, and more inclusive smart cities.

RESULTS AND DISCUSSION

The study's findings, derived from the PLS-SEM path modeling analysis, reveal intricate dynamics between artificial intelligence (AI), e-governance, and cybersecurity within the context of smart cities, emphasizing the pivotal role of stakeholder involvement. The analysis indicates that AI directly enhances cybersecurity by providing advanced tools for threat detection and response, leveraging machine learning algorithms to identify patterns and anomalies in network traffic. This direct relationship underscores AI's potential to strengthen cyber capabilities and ensure the safety of digital infrastructures against various cyber threats such as malware, phishing, and unauthorized access. However, the study also identifies a partial mediating effect of e-governance in this relationship, suggesting that the integration of AI within e-governance systems further amplifies its positive impact on cybersecurity. This finding implies that robust e-governance frameworks can harness AI more effectively, optimizing the delivery of public services while enhancing the security of digital transactions and communications.The role of e-governance as a mediator highlights the necessity for governmental bodies to invest in sophisticated e-governance platforms that incorporate AI technologies. By doing so, they can achieve a dual benefit of improved public service delivery and fortified cybersecurity. The study's results suggest that e-governance platforms equipped with AI can automate various administrative tasks, analyze large datasets to inform policy decisions, and provide real-time responses to citizen inquiries through AI-powered chatbots. These capabilities not only enhance the efficiency and responsiveness of government operations but also create a more secure digital environment by monitoring and mitigating potential cyber threats in real-time. The partial mediation effect indicates that while AI independently enhances cybersecurity, its integration within e-governance systems maximizes these benefits, leading to a more resilient and secure smart city infrastructure.

International Journal of Management Research and Business Strategy

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

Fig 2. Results screenshot 1

Fig 3. Results screenshot 2

International Journal of Management Research and Business Strategy

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

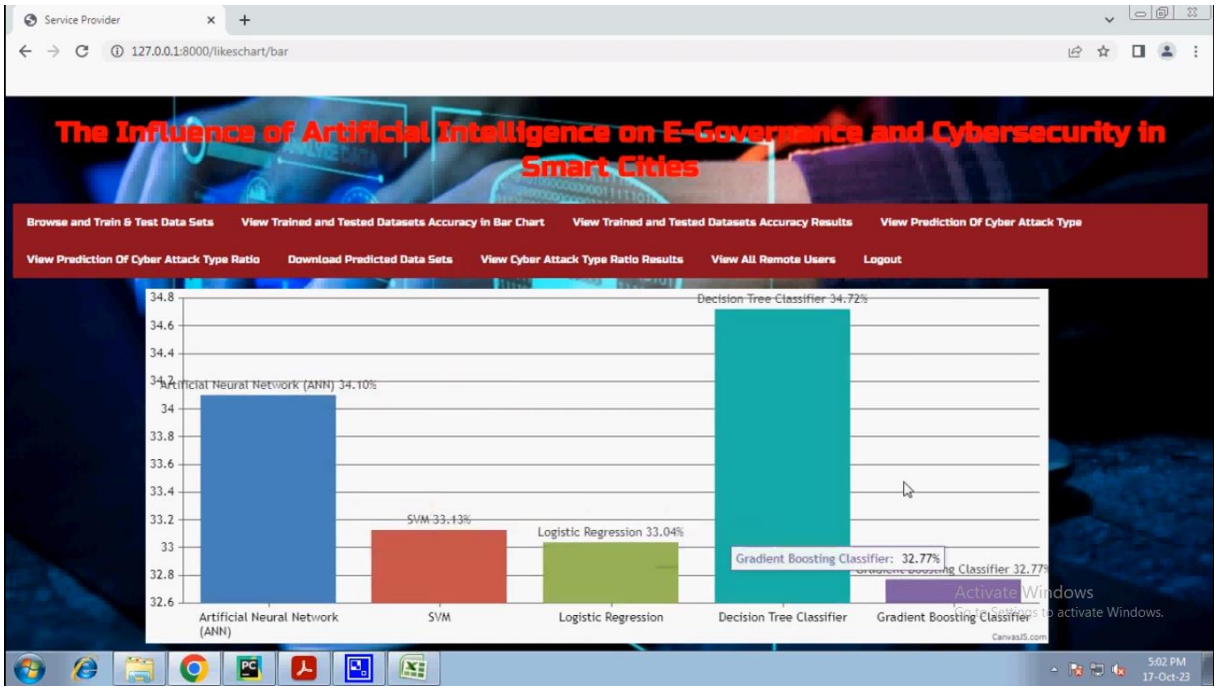

Fig 4. Results screenshot 3

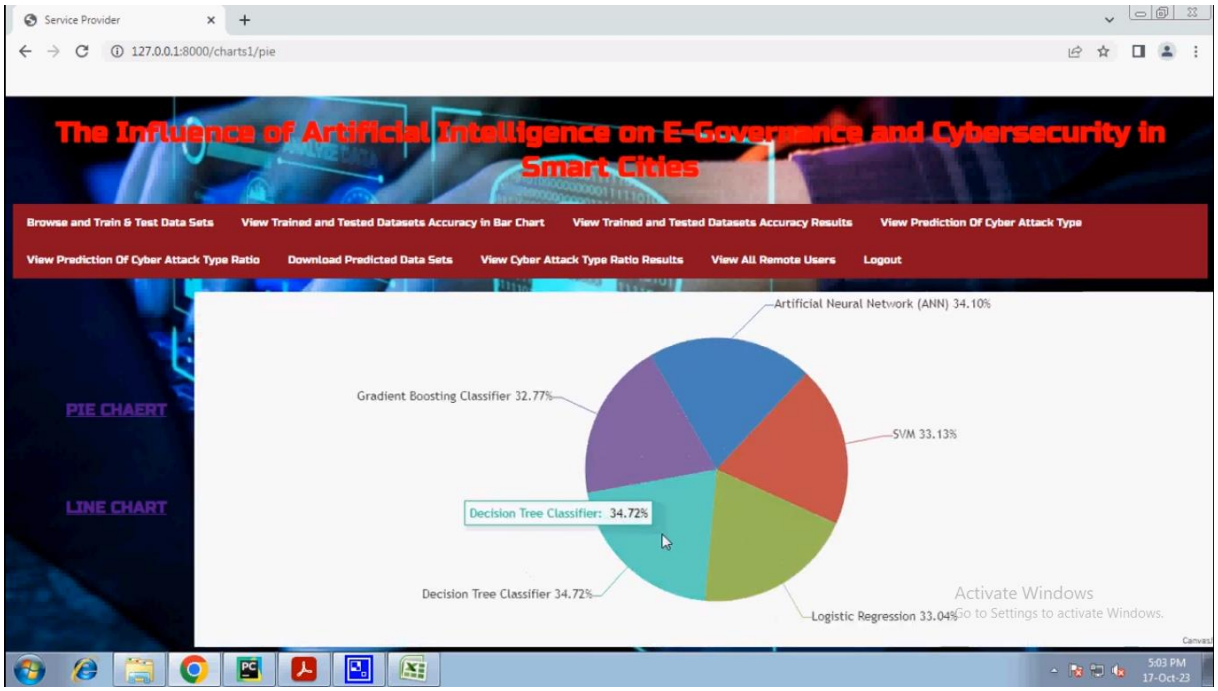

Fig 5. Results screenshot 4

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

Fig 6. Results screenshot 5

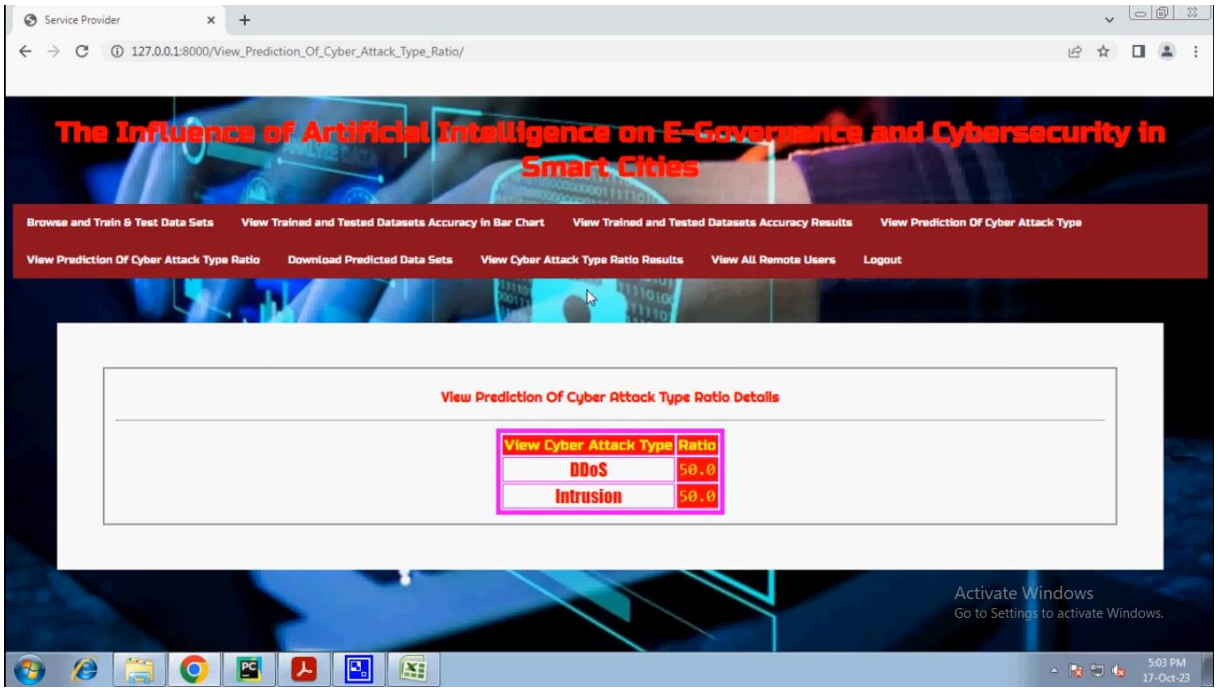

Fig 7. Results screenshot 6

International Journal of Management Research and Business Strategy

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

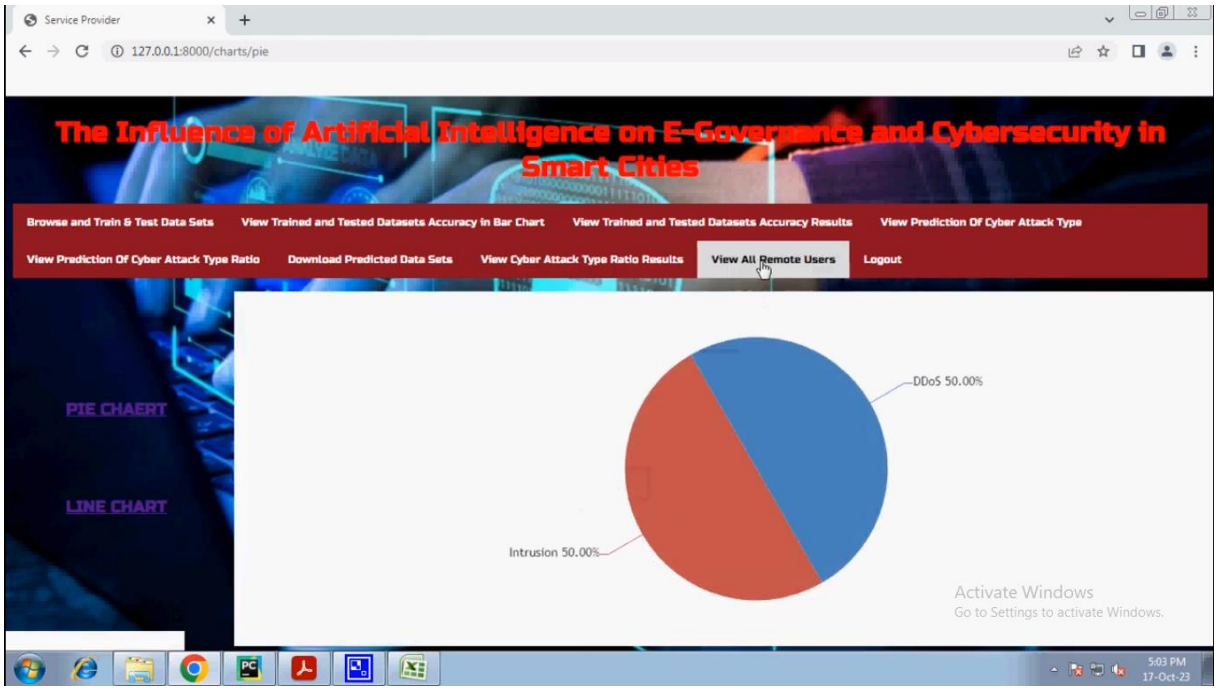

Fig 8. Results screenshot 7

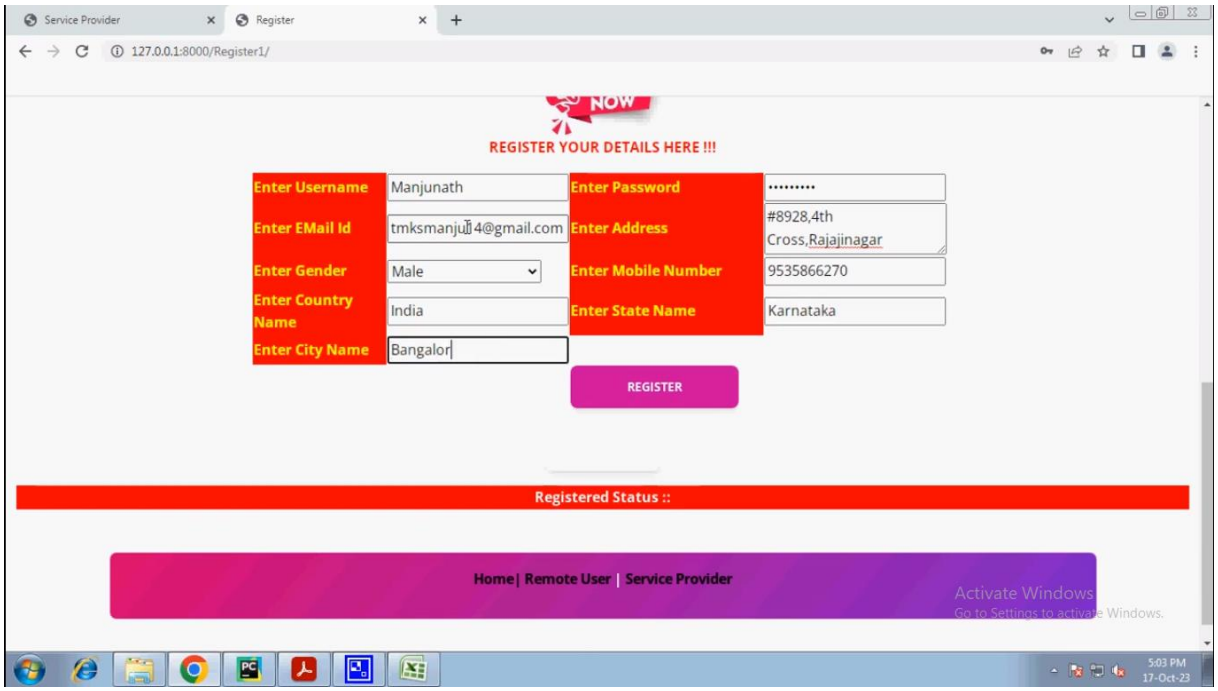

Fig 9. Results screenshot 8

International Journal of Management Research and Business Strategy

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

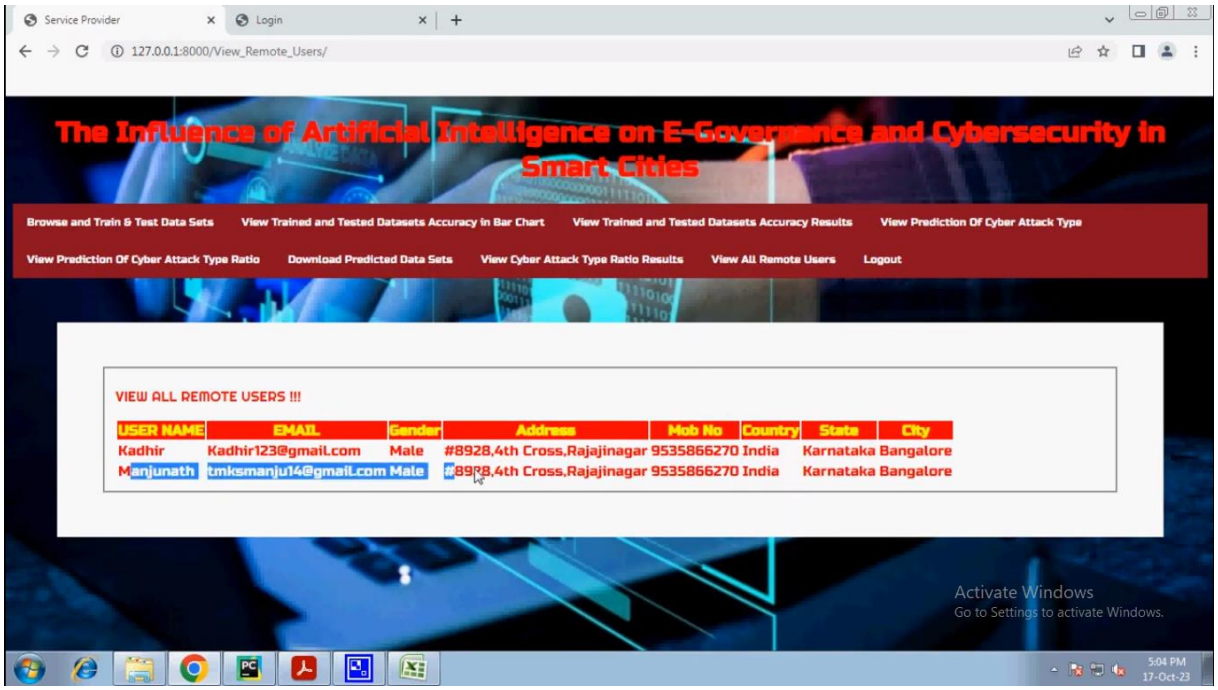

Fig 10. Results screenshot 9

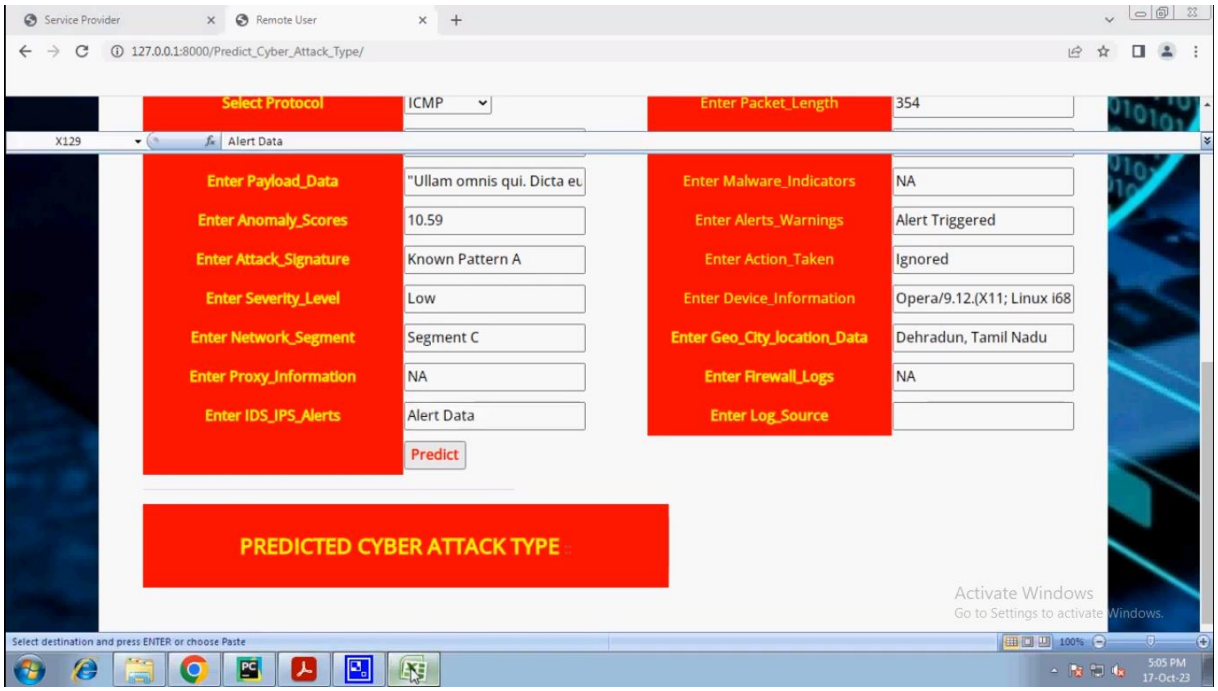

Fig 11. Results screenshot 10

International Journal of Management Research and Business Strategy

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

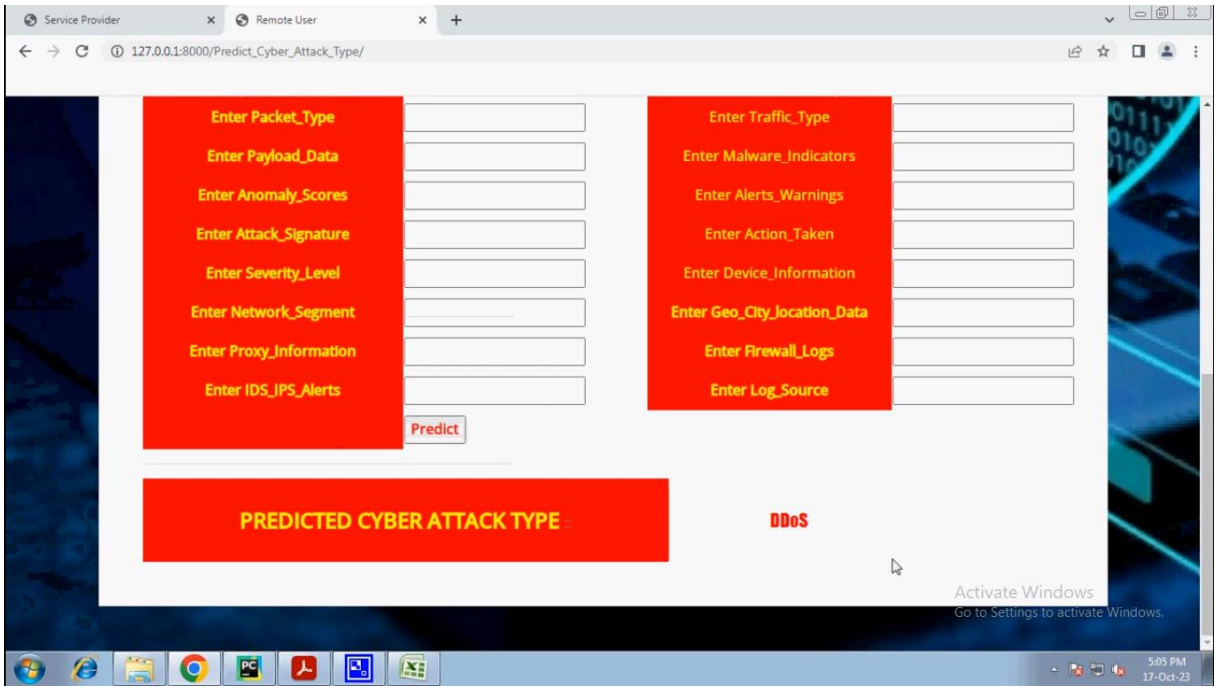

Fig 12. Results screenshot 11

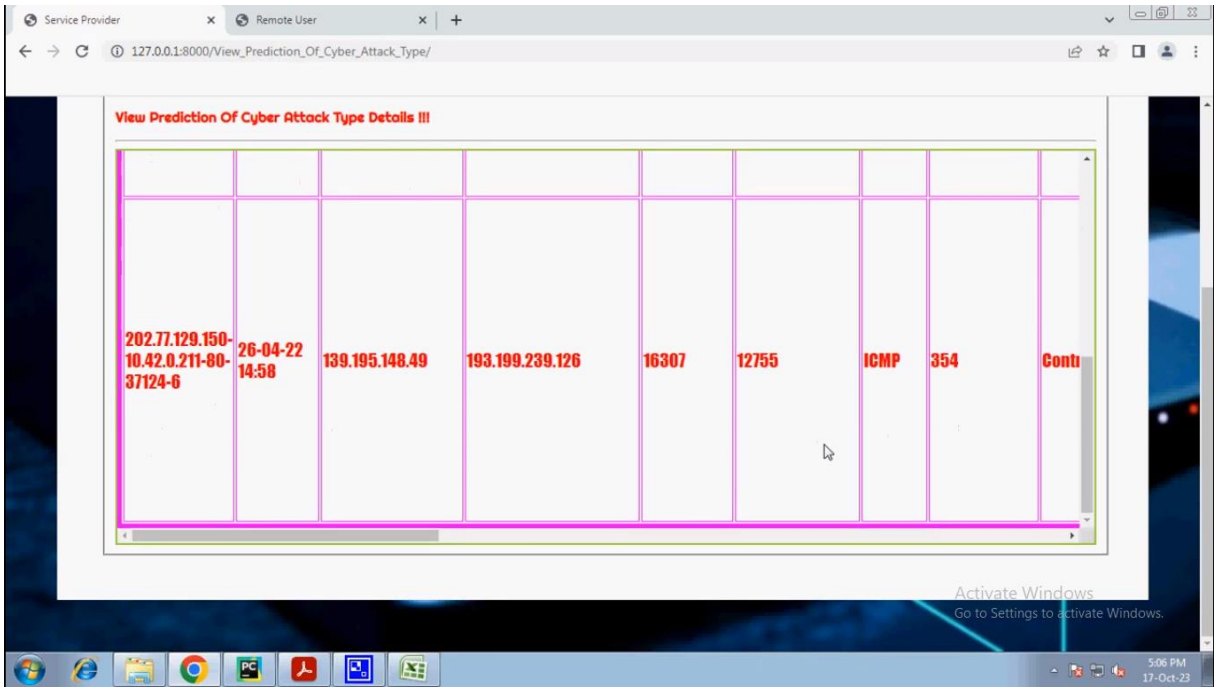

Fig 13. Results screenshot 12

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

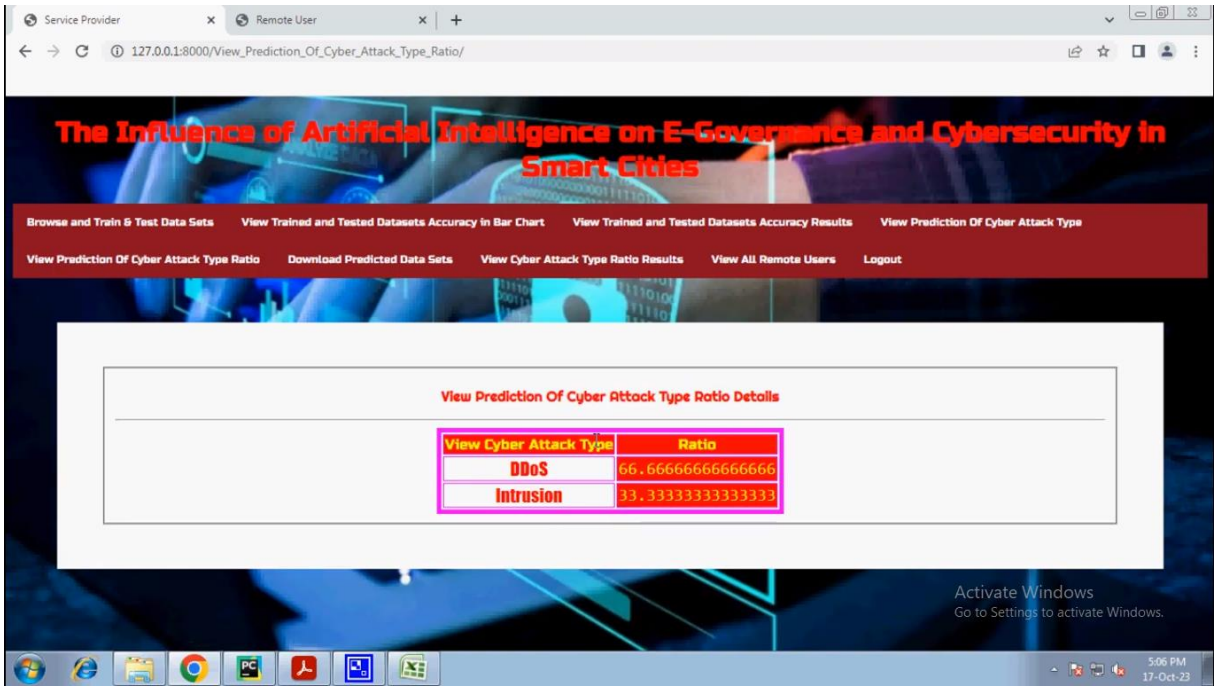

Fig 14. Results screenshot 13

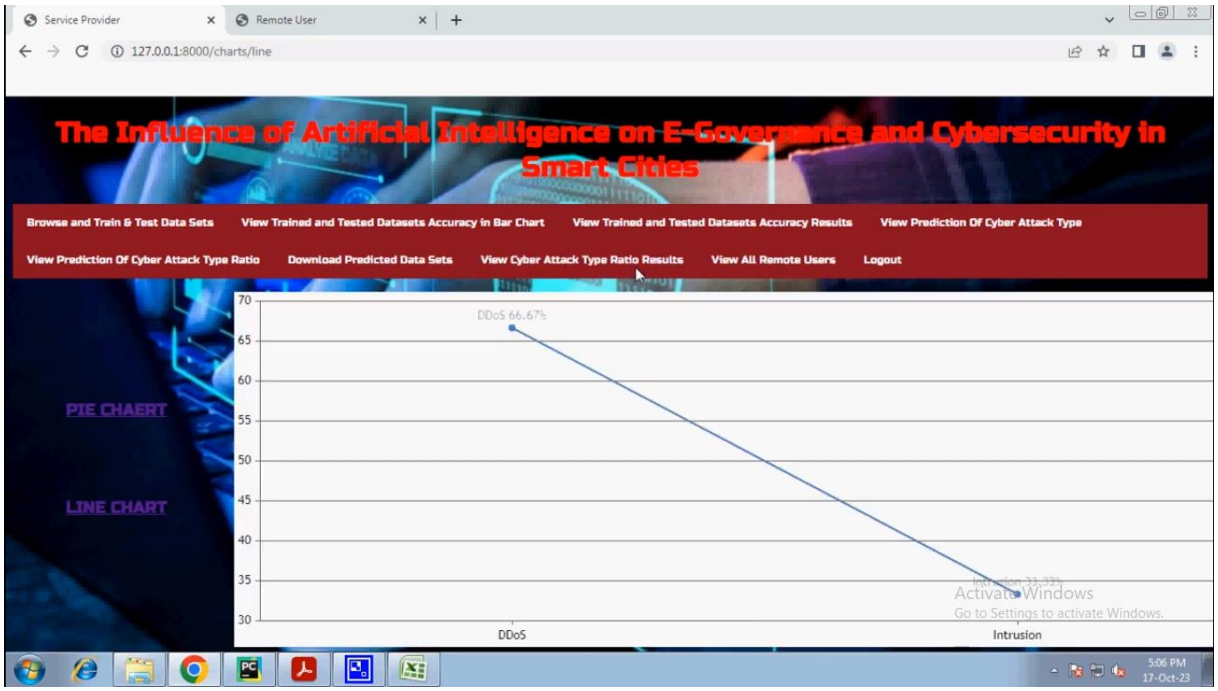

Fig 15. Results screenshot 14

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

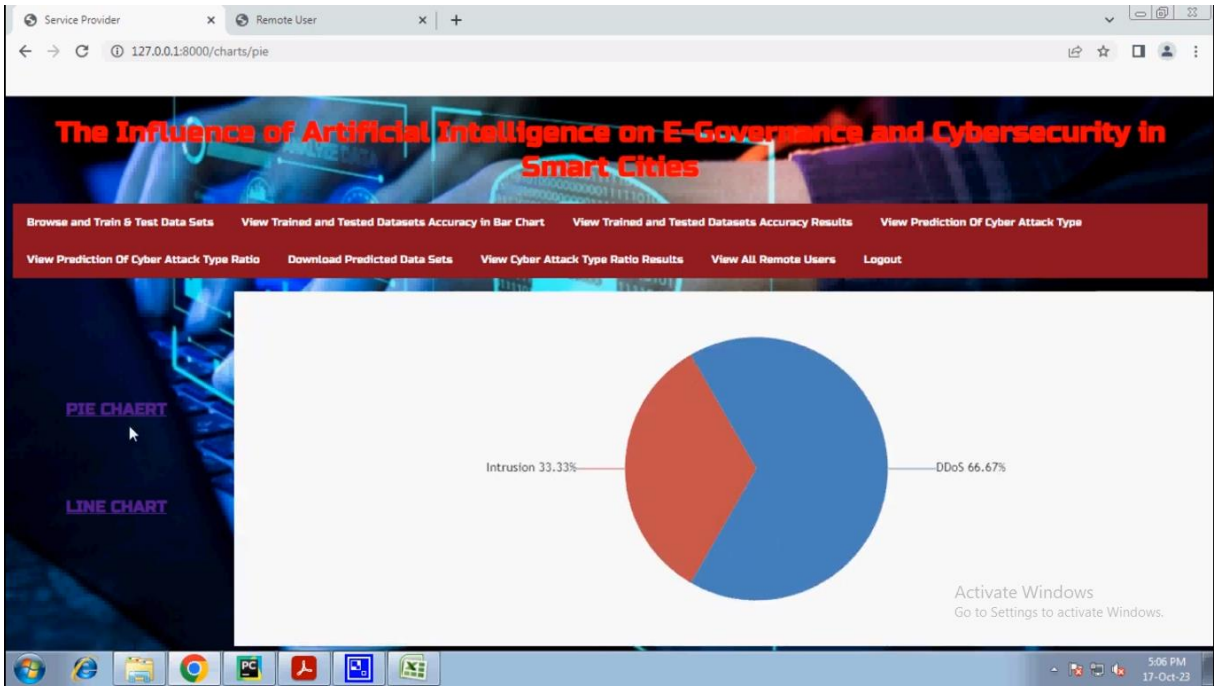

Fig 16. Results screenshot 15

Stakeholder involvement emerges as a critical moderating factor in the relationships between AI, e-governance, and cybersecurity. The study finds that the effectiveness of AI and e-governance initiatives in enhancing cybersecurity is significantly influenced by the degree of stakeholder engagement. This moderating effect highlights the importance of involving diverse stakeholders, including government officials, technology developers, cybersecurity experts, and citizens, in the decision-making and implementation processes. Stakeholders provide valuable insights, expertise, and feedback that can guide the ethical and effective deployment of AI technologies. For instance, government officials can ensure regulatory compliance and public trust, technology developers can focus on innovation and technical feasibility, cybersecurity experts can address emerging threats, and citizens can offer perspectives on usability and privacy concerns. The results imply that a collaborative approach, where stakeholders actively participate in shaping AI and e-governance strategies, is essential for achieving a vibrant, transparent, and secure cyberspace in smart cities.

In summary, the study underscores the transformative potential of AI in enhancing e-governance and cybersecurity in smart cities, while also highlighting the complex, context-specific nature of these relationships. The findings reveal that AI significantly improves cybersecurity capabilities, and its integration within e-governance systems further amplifies these benefits. Additionally, the critical role of stakeholder involvement in moderating these relationships emphasizes the need for a collaborative and inclusive approach to technology implementation. Governments must invest in advanced e-governance platforms that incorporate AI, establish robust cybersecurity measures, and engage diverse stakeholders to ensure the ethical, transparent, and effective use of AI. These strategies will not only strengthen the cyber resilience of smart cities but also enhance the efficiency and responsiveness of public service delivery, ultimately contributing to the creation of safer, more efficient, and more inclusive urban environments.

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

CONCLUSION

The study concludes that artificial intelligence (AI) significantly enhances e-governance and cybersecurity in smart cities, demonstrating its critical role in the Fourth Industrial Revolution (Industry 4.0) for protecting against cyber-attacks, malware, phishing, and unauthorized access. The findings highlight a complex, context-specific relationship between AI, e-governance, and cybersecurity, influenced by various stakeholders with diverse expertise. The PLS-SEM path modeling analysis reveals that e-governance partially mediates the relationship between AI and cybersecurity, suggesting that integrating AI within robust e-governance systems amplifies its positive effects on cybersecurity. Moreover, the study underscores the vital moderating role of stakeholder involvement, showing that effective implementation of AI and e-governance strategies depends significantly on the active engagement of government officials, technology developers, cybersecurity experts, and citizens. This collaborative approach ensures that AI technologies are deployed ethically, transparently, and efficiently, addressing regulatory compliance, innovation, threat mitigation, and user concerns. The study's practical implications for governmental bodies in smart cities include the necessity to invest in advanced e-governance platforms, establish comprehensive cybersecurity measures, and foster stakeholder engagement to create a secure, transparent, and responsive digital environment. Overall, the research provides a roadmap for leveraging AI to enhance the cyber resilience and operational efficiency of smart cities, emphasizing the importance of stakeholder collaboration in achieving these goals.

REFERENCES

1. Baker, R. S., & Inventado, P. S. (2014). Educational data mining and learning analytics: Applications to constructionist research. Technology, Knowledge and Learning, 19(1-2), 205-220.

2. Chrysafiadi, K., & Virvou, M. (2013). Educational data mining and learning analytics: Applications and ethical issues. Educational Technology & Society, 16(2), 327-337.

3. Conati, C., & Muldner, K. (2014). Introduction to the special issue on user modeling and user-adapted interaction in learning and education. User Modeling and User-Adapted Interaction, 24(5), 379-388.

4. Dawson, S. (2015). Learning analytics: Trends and issues. In Learning analytics: From research to practice (pp. 3-25). Springer.

5. Gasevic, D., Dawson, S., Siemens, G., & Siemens, G. (2015). Let's not forget: Learning analytics are about learning. TechTrends, 59(1), 64-71.

6. Ifenthaler, D., & Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. Educational Technology Research and Development, 64(5), 923-938.

7. Papamitsiou, Z., & Economides, A. A. (2014). Learning analytics and educational data mining: Towards communication and collaboration. In Learning analytics: From research to practice (pp. 149-172). Springer.

8. Pardo, A., Han, F., & Ellis, R. A. (2017). Analysing learning and engagement through learning analytics: Dispositional learning analytics. In Handbook of Learning Analytics (pp. 63-76). SOLAR.

9. Pennington, J., Socher, R., & Manning, C. D. (2014). Glove: Global vectors for word representation. In Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP) (pp. 1532-1543).

ISSN 2319-345X

www.ijmrbs.com

Vol. 13, Issue. 2, 2024

10. Romero, C., Ventura, S., & García, E. (2008). Data mining in education. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 1(1), 12-27.

11. Siemens, G., & Baker, R. S. (2012). Learning analytics and educational data mining: Towards communication and collaboration. In Proceedings of the 2nd international conference on learning analytics and knowledge (pp. 252-254).

12. Siemens, G., & Long, P. (2011). Penetrating the fog: Analytics in learning and education. Educause Review, 46(5), 30-32.

13. Siemens, G., Gašević, D., & Dawson, S. (2015). Preparing for the digital university: A review of the history and current state of distance, blended, and online learning. In Research, boundaries, and policy in networked learning (pp. 343-360). Springer.

14. Singh, V. K., Singh, P. K., & Yadav, S. K. (2015). A survey on artificial intelligence based educational applications. International Journal of Information and Computation Technology, 5(12), 1045-1050.

15. Hutto, C. J., & Bell, C. (2014). Teaching, learning, and thriving: Mapping patterns of agency in educational data. Educational Technology & Society, 17(3), 283-294.