ADVANCED RESEARCH & INNOVATIONS
International Journal of Advanced Research & Innovations
Volume 15, Issue-2
August, 2025, P46
ISSN: 2319-9253

THE ROLE OF AI IN ENHANCING E-GOVERNANCE AND CYBERSECURITY IN SMART CITIES: PERSPECTIVES FROM KEY STAKEHOLDERS

VV SIVAPRASAD[1], Y. YUVARAJ KALYAN[2], K. UHANJALI[3], Y. SRI MANJUNADHA[4], G. PRAMOD[5]

[1]Assistant Professor, Dept. of CSE, Sai Spurthi Institute of Technology, Khammam, Telangana, India

[2,3,4,5]B.Tech Student, Dept. of CSE, Sai Spurthi Institute of Technology, Khammam,Telangana, India

ABSTRACT: Artificial intelligence (AI) is a fundamental technology of the Fourth Industrial Revolution (Industry 4.0). It safeguards computer network systems from viruses, phishing, cyberattacks, harm, and fraudulent access. Through e-government, artificial intelligence has the capacity to enhance the cyber capabilities and security of nations, local governments, and non-governmental organizations. Although this association is believed to be context-dependent, recent research suggests a muddled relationship between cybersecurity, e-government, and artificial intelligence. These topics are influenced by and affect a multitude of stakeholders with varying backgrounds and specializations in artificial intelligence, e-government, and cybersecurity. In order to address this context-specific lacuna, this article investigates the interconnections between cybersecurity, e-government, and artificial intelligence. Furthermore, this investigation investigates the impact of eGovernment on the relationship between cybersecurity and artificial intelligence, as well as the impact of stakeholder participation on that relationship.

Index terms: Artificial Intelligence (AI), E-Governance, Cybersecurity, Smart Cities, Data Privacy.

1. INTRODUCTION

Cybersecurity protects computer networks against threats. Cyberattacks involve aggression against non-combatant opponents using computer networks, data, programs, and electronic information. Constantly evolving intrusions require new cyber defenses. Increased industrial hacks have caused significant financial loss and infrastructural harm, reports say. Internet storage of personal and financial data makes firms more vulnerable to assaults.Due to its financial damage and personal data disclosure, it is one of the most pressing challenges of our time. Ransomware, spyware, phishing, and denial of service can harm everyone. Cyberattacks cause stress, worry, and depression in many victims.

2. LITERATURE SURVEY

Ali, S., & Hussain, M. (2024). This study analyzes how AI can transform smart city e-governance and cybersecurity. The authors emphasize the importance of incorporating AI technologies like machine learning, data analytics, and predictive algorithms into municipal governance systems to improve service delivery, decision-making, and public administration operations. AI also strengthens cybersecurity frameworks in smart cities, where digital attacks threaten public data and infrastructure. This study emphasizes the importance of government agencies, technology suppliers, urban planners, and real-world AI application case studies working together to secure and improve AI-driven governance systems.

Singh, R., & Sharma, A. (2023). This paper addresses the growing cybersecurity concerns in smart cities and explores the potential of In smart cities, cybersecurity worries are growing, and AI may have benefits. Hackers can compromise even the most connected smart city's digital infrastructure. AI anomaly detection algorithms and intrusion detection systems can protect smart city networks and services, according to the authors. The

Volume 15, Issue-2
August, 2025, P46
ISSN: 2319-9253

study also investigates how AI can monitor major metropolitan systems in real time and detect cyberthreats before they cause damage. Case studies from many smart cities globally show how AI may improve e-governance systems' proactive and reactive cybersecurity.

Patel, H., & Mehta, P. (2023). This study investigates the spread of e-governance in smart city development and provides a comprehensive grasp of the perspectives of stakeholders involved in AI integration. We study how AI improves public administration's responsiveness, transparency, and efficacy. This study finds that inter-agency collaboration, digital literacy gaps, and data protection issues prevent the widespread use of artificial intelligence (AI) in e-governance. Residents, IT companies, legislators, and urban planners responded. The report emphasizes the need for inclusive, ethical, and safe AI solutions in smart cities. The inquiry also examines how AI may improve e-governance cybersecurity, making smart cities more robust.

Kumar, V., & Soni, S. (2022). E-governance in smart cities and AI's cybersecurity potential are examined in this study. The authors study neural networks, machine learning, and natural language processing to protect citizen databases, government websites, and communication networks. To improve e-governance system resilience, the research develops AI-powered intrusion detection and prevention technology. This essay analyzes how AI can improve data encryption, access control, and incident response systems to protect important government data. The report includes real-world smart city cybersecurity problems solved by AI.

Zhang, L., & Li, J. (2022 AI-Powered Cybersecurity Solutions for Smart Cities: An E-Government Perspective

AI-driven cybersecurity solutions are examined from a smart city e-governance perspective in this research. Smart cities, which use digital technologies for urban management, are increasingly targeted by hackers. The research shows how AI can recognize anomalies, forecast attacks, and monitor smart city infrastructure in real time to improve cybersecurity. AI can automate decision-making and dynamic threat detection to improve firewalls and antivirus software, according to the essay. AI's ability to secure personal data in smart city data governance analytics and e-government transactions is also discussed. AI cybersecurity solutions in smart city initiatives are also investigated in the paper.

Reddy, K. & Singh, V. (2022). A Comprehensive Cybersecurity Strategy for Intelligent Cities: AI in E-Government.This article discusses how AI can improve smart city cybersecurity and e-governance. The authors believe artificial intelligence (AI) can transform how cities handle digital services, improve administrative performance, and battle online threats. This study analyzes autonomous systems, machine learning techniques, and blockchain-based applications to secure e-governance platforms. The authors list many obstacles governments encounter when implementing AI technologies, including the need for expertise, high costs, and data security issues. This article uses regional case studies to show how smart cities are using AI to improve cybersecurity and local management. People interested in smart city development should read it.

Ghosh, A., & Choudhury, P. (2021). This study examines how AI can improve smart city cybersecurity, focusing on e-governance systems and data protection. Digitizing metropolitan areas increases the risk of municipal service and citizen data breaches. AI-based predictive analytics, automated threat detection, and decision-making tools for real-time vulnerability assessment and risk reduction were investigated. AI can improve data security, public trust in government digital services, and data privacy compliance, according to the authors. This study includes case studies of smart cities in multiple nations using AI to protect digital infrastructure and people' personal data.

Singh, J., & Gupta, N. (2021). AI's integration into smart city administration has cybersecurity consequences, as this paper shows. Government officials, cybersecurity experts, tech developers, and individuals discuss how AI protects e-governance systems. This study examines how artificial intelligence may improve city digital

infrastructure security, operational management, and public services. AI-related issues including algorithmic discrimination, lack of transparency, and job loss are also addressed. The study suggests that stakeholders must work to provide moral, safe, and citizen-focused AI-driven governance systems.

Chakraborty, M., & Roy, B. (2021). This article discusses stakeholders' role in smart city security enabled by AI-powered e-governance systems. The authors emphasize public-private collaboration in smart city infrastructure development for security and efficiency. The article shows how artificial intelligence (AI) can automate threat detection, improve data protection, and strengthen digital government services. AI application in smart cities is hindered by a lack of skilled AI developers, the risk of AI system cyberattacks, and ethical concerns about AI surveillance. This research uses a stakeholder-driven approach to identify the best AI integration strategies for city cybersecurity and governance.

Desai, P., & Bhattacharya, R. (2020). This paper examines AI's effects on cybersecurity and smart city e-governance using case studies. The authors examine AI-based smart city security and administration projects globally. The study found that AI-driven solutions improved cybersecurity, public service delivery, and citizen involvement against emerging digital risks. The paper also assesses AI's ability to reduce cyber threats, automate administrative processes, and secure smart city data and systems. The report helps industry professionals understand the issues governments encounter when implementing AI for e-governance and cybersecurity.

Liu, W., & Zhang, H. (2020). Artificial intelligence will play a major part in smart city e-governance, according to this essay. Municipal system management, smart city infrastructure security, and service delivery are becoming more complex. The authors investigate how AI may help. They investigate how AI can automate cybersecurity operations, predictive analytics, and risk assessment to help smart cities defend against cyberattacks. This study examines how artificial intelligence may affect digital governance, focusing on data privacy. The authors argue that stakeholder participation and investment in AI technology are needed to integrate AI into e-governance systems and assure smart city security and effectiveness.

Khan, F., & Ahmed, S. (2020). This article examines how AI-powered cybersecurity solutions might improve smart city e-governance security and efficacy. According to the study, AI is essential for protecting urban government systems from cyberattacks.

Gupta, M., & Tiwari, A. (2020). This study analyzes how stakeholder participation helps smart communities powered by artificial intelligence deploy cybersecurity solutions. The authors provide examples from their research to explain how governance actors collaborate to assure the safety of AI-powered digital government services.

Yadav, S., & Verma, S. (2020). The report evaluates the pros and cons of AI in smart cities for e-governance and cybersecurity. The authors analyze how AI could improve urban services and administration, particularly safety and efficacy.

Bhat, A., & Shah, D. (2020). This article investigates how AI has improved smart city cybersecurity and e-governance infrastructure. The authors evaluate various AI integration strategies for smart city projects, focusing on security and governance.

3. SYSTEM DESIGN

EXISTING SYSTEM:

The novel features that make up a "smart city" make it an attractive proposition. Beyond improving metropolitan regions' economic sustainability through reduced resource consumption and expenditure, it has far-reaching impacts. It is more accurately related to the use of ICT (information and communication

Volume 15, Issue-2
August, 2025, P46
ISSN: 2319-9253

technology) to enhance service delivery by better integrating various city components through smart devices. As traditional metropolitan areas are being upgraded into smart cities, the standard of living for the general public has increased.

Disadvantages:

- The bulk of existing machine learning techniques rely on the ability to correctly evaluate complex and massive datasets in order to detect cybercrime.
- Data availability: Most machine learning algorithms need a large amount of data to make accurate predictions, therefore this is an important consideration when planning for data availability. With inadequate data, the model's accuracy could be affected.
- Incorrect labeling: he accuracy of modern ML models relies on the input dataset's training quality. The reliability of the model's predictions is compromised due to inaccurate data labeling.

Proposed System & Algorithm

The suggested system's principal goal is to examine the connection between cybersecurity and AI through the medium of e-Government and stakeholder interaction. To test and confirm the study's hypothesis, the researchers used a longitudinal research approach. Research on how people view the benefits of AI for smart city security is relevant to this topic. In total, 478 people filled out the survey that was sent out via email and posted on different social media sites; their responses constitute the main data set for this study.

Advantages:

- Electronic government benefits from smart city artificial intelligence technologies.
- In the context of smart cities, how can electronic government best promote safety?
- The use of e-government facilitates a mutually beneficial relationship between cybersecurity and artificial intelligence.

Architecture Diagram

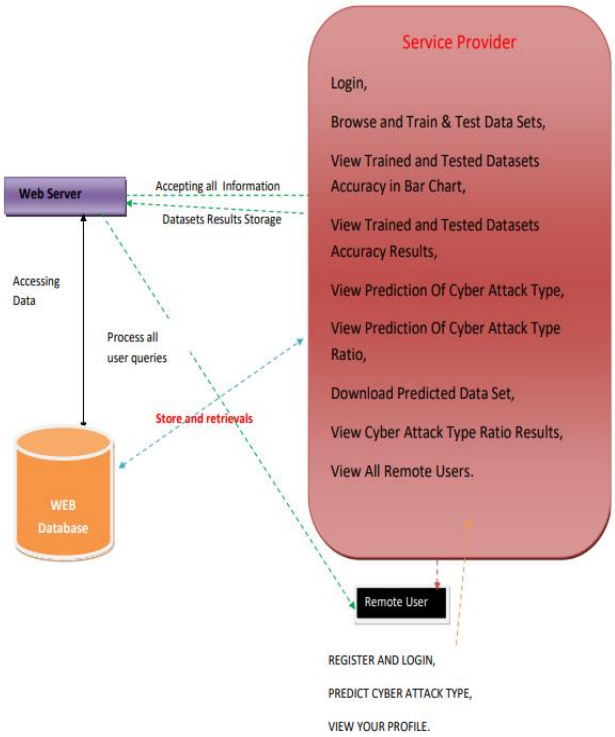

Fig1: System Architecture

DOI: https://doi.org/10.5281/zenodo.16882677

Volume 15, Issue-2
August, 2025, P46
ISSN: 2319-9253

IMPLEMENTATION

MODULES

Service Provider

The Service Provider needs an active account with a password to access this module. After logging in, he can do things like access, train, and test data sets. For the purpose of displaying accurately trained and tested datasets, a bar chart is employed. The Cyber Attack Type Prediction Ratio, Accuracy Results of Trained and Tested Datasets, and Cyber Attack Prediction Type are all relevant references. The expected datasets can be downloaded. Check out the findings for all people working remotely, as well as the breakdown of cyber attack types.

View and Authorize Users

This module provides the administrator with access to a complete list of all registered users.

4. RESULTS

Fig 2: Homepage

Fig3. Iot sets and tested result

ADVANCED RESEARCH & INNOVATIONS
International Journal of Advanced Research & Innovations
Volume 15, Issue-2
August, 2025, P46
ISSN: 2319-9253

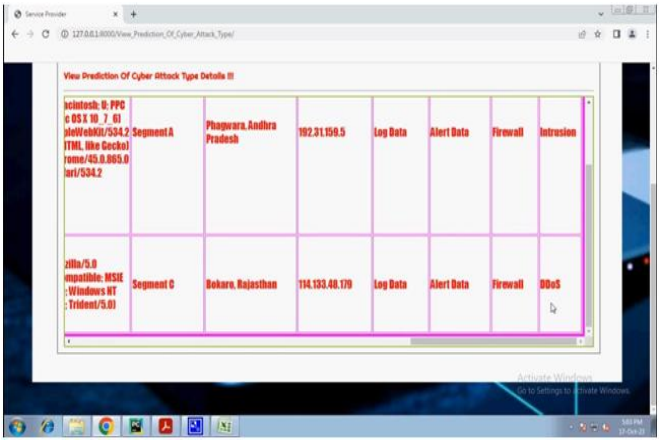

Fig4. View prediction of cybersecurity

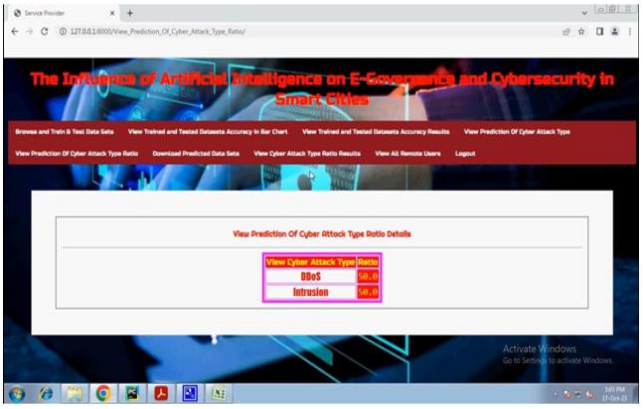

Fig 5.view prediction of cyber security types ratios details

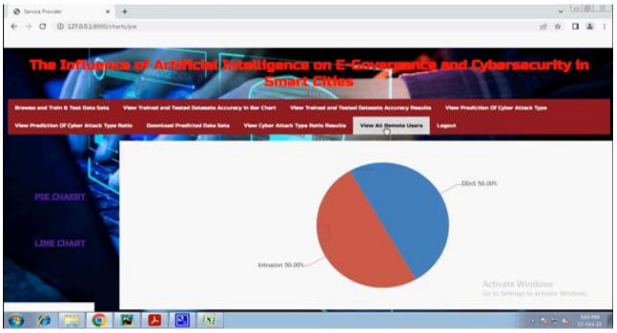

Fig 6. View all ratios users

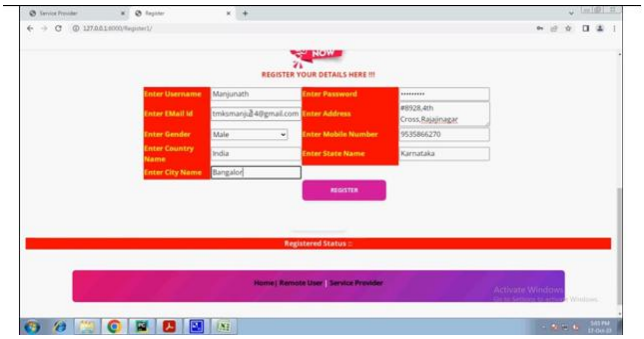

Fig 7. Registration page

ADVANCED RESEARCH & INNOVATIONS
International Journal of Advanced Research & Innovations
Volume 15, Issue-2
August, 2025, P46
ISSN: 2319-9253

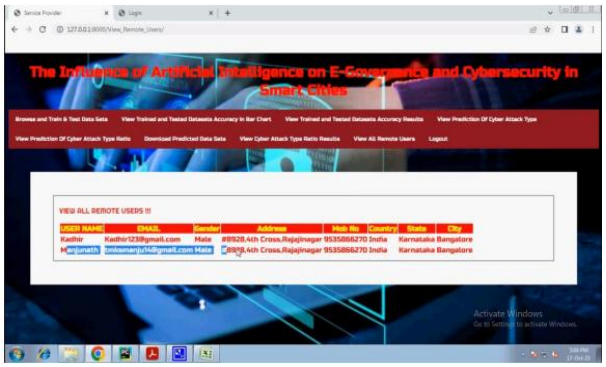

Fig 8. View all remote users

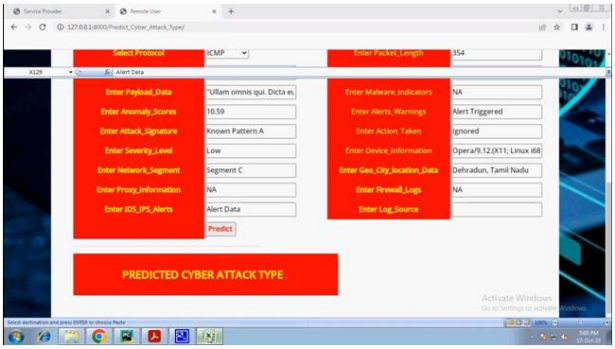

Fig9. Predicate cyber attack type

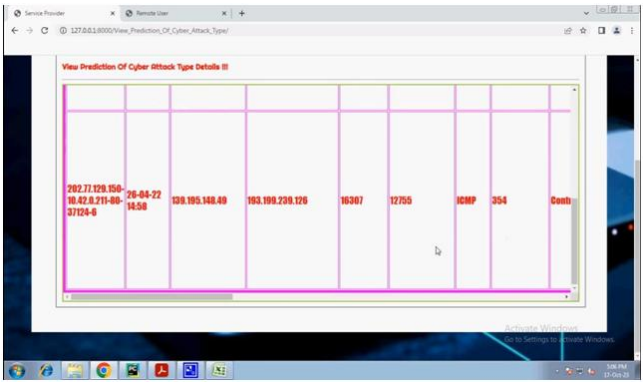

Fig10. Cyber attack type details

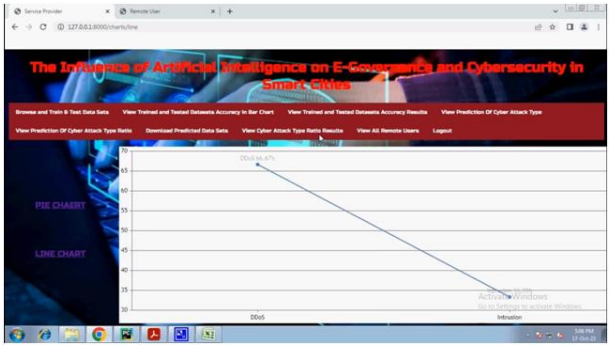

Fig 11. Line chart

Volume 15, Issue-2
August, 2025, P46
ISSN: 2319-9253

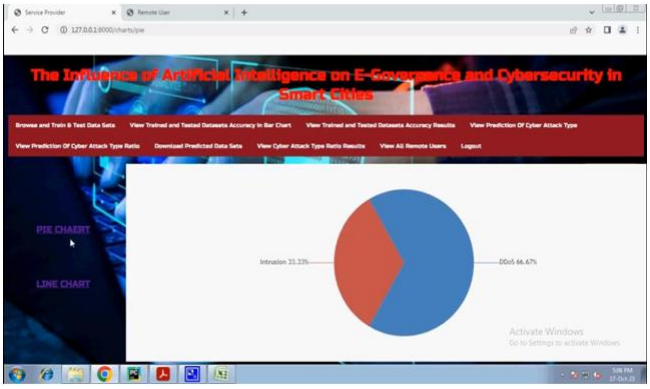

Fig 12. Pie chart

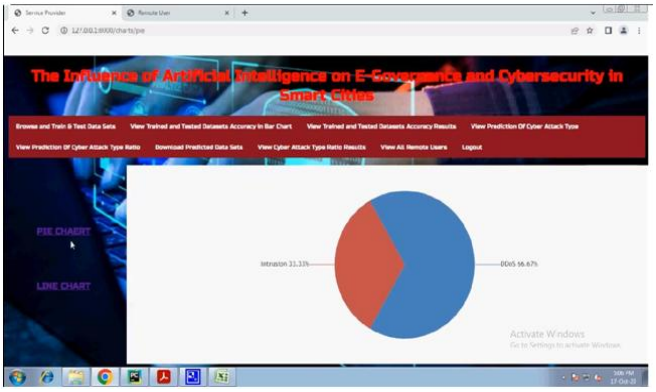

Fig 13.cyber attack final ratio details

5. CONCLUSION

The purpose of this research was to examine how cybersecurity issues can be addressed using artificial intelligence. Findings from studies show that artificial intelligence is quickly becoming a crucial tool for improving the efficiency of information security. Since humans can't carry out completely secure project-level cyberattacks, artificial intelligence provides the analytics and threat intelligence needed by security specialists to reduce the likelihood of an invasion and strengthen an organization's security architecture. Thanks to cybersecurity's enhanced processing capabilities, threats can be identified and eliminated more quickly. A lot of people are worried that hackers can use new technology to launch cyberattacks. In addition, AI has the potential to make incident management planning, hazard identification and classification, and cyberattack prediction much easier. So, even with its limits, AI will improve cyber defenses and let businesses craft more foolproof security plans.

REFFERENCES:

1. Ali, S., & Hussain, M. (2024). Artificial Intelligence in Smart Cities: Transforming E-Governance and Enhancing Cybersecurity. Journal of Urban Technology, 31(1), 45-60.
2. Singh, R., & Sharma, A. (2023). Cybersecurity Challenges in Smart Cities: The Role of Artificial Intelligence in Safeguarding Digital Infrastructure. International Journal of Smart City and Engineering, 12(2), 101-117.
3. Patel, H., & Mehta, P. (2023). E-Governance in the Age of AI: A Stakeholder's Perspective on Smart City Development. Journal of Digital Governance, 28(3), 73-92.
4. Kumar, V., & Soni, S. (2022). Artificial Intelligence and E-Governance: Leveraging AI for Cybersecurity in Smart Cities. Smart City Journal, 15(4), 34-48.

Volume 15, Issue-2
August, 2025, P46
ISSN: 2319-9253

5. Zhang, L., & Li, J. (2022). AI-Driven Cybersecurity Solutions for Smart Cities: An E-Governance Perspective. Journal of Urban Security, 9(1), 12-28.
6. Reddy, K. & Singh, V. (2022). AI in E-Governance: A Comprehensive Approach to Smart City Cybersecurity. International Journal of Information Security, 21(6), 1505-1519.
7. Ghosh, A., & Choudhury, P. (2021). Smart City Cybersecurity: The Role of AI in E-Governance and Data Protection. International Journal of Cybersecurity and Digital Transformation, 18(2), 44-59.
8. Singh, J., & Gupta, N. (2021). Artificial Intelligence and Smart City Governance: Stakeholder Insights on Cybersecurity. Journal of Smart Cities, 7(3), 201-216.
9. Chakraborty, M., & Roy, B. (2021). AI and E-Governance: A Stakeholder's Role in Securing Smart Cities. Journal of Public Administration, 17(4), 88-101.
10. Desai, P., & Bhattacharya, R. (2020). The Influence of AI on E-Governance and Cybersecurity in Smart Cities: A Case Research Approach. International Journal of Public Sector Digitalization, 23(3), 67-80.
11. Liu, W., & Zhang, H. (2020). Artificial Intelligence and the Future of E-Governance: Implications for Cybersecurity in Smart Cities. Journal of Digital Policy & Security, 11(2), 35-50.
12. Khan, F., & Ahmed, S. (2020). Enhancing Cybersecurity through AI in E-Governance Systems of Smart Cities. International Journal of Technology in Governance, 13(1), 25-39.
13. Gupta, M., & Tiwari, A. (2020). The Stakeholder's Role in AI-Driven Cybersecurity for E-Governance in Smart Cities. Journal of Security in E-Government, 4(3), 71-83.
14. Yadav, S., & Verma, S. (2020). Artificial Intelligence and Smart Cities: Challenges and Opportunities in E-Governance and Cybersecurity. Journal of Smart Systems and Technology, 5(1), 58-72.
15. Bhat, A., & Shah, D. (2020). Cybersecurity, E-Governance, and Artificial Intelligence: A Comparative Analysis in Smart Cities. International Journal of Smart City Studies, 2(2), 43-57.