ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

THE INFLUENCE OF ARTIFICIAL INTELLIGENCE ON E-GOVERNANCE AND CYBERSECURITY IN SMART CITIES A STAKEHOLDER'S PERSPECTIVE

S. Devaraju[1] M. Anjaneyulu[2]

[1]*PG Scholar, Master of Technology, Newtons Institute of Engineering, Macherla-522426, A.P., India*

[2]*Assistant Professor, Newtons Institute of Engineering, Macherla-522426, A.P., India*

Abstract:

Artificial Intelligence (AI) is transforming e-governance and cybersecurity in smart cities by enabling intelligent decision-making, automated public services, stakeholder analysis, and proactive threat detection. This study presents an AI-based framework that integrates e-governance services, cybersecurity analytics, and stakeholder perspectives involving government authorities, citizens, businesses, administrators, and cybersecurity analysts. Governance, cybersecurity, and stakeholder data are collected and processed through cleaning, normalization, feature selection, transformation, and encoding. Four supervised machine learning algorithms—Decision Tree, Random Forest, Support Vector Machine (SVM), and Logistic Regression—are applied to classify cybersecurity risks, analyze stakeholder satisfaction, predict governance outcomes, and identify anomalous activities. Model performance is evaluated using accuracy, precision, recall, F1-score, ROC curves, and confusion matrices. The proposed framework also incorporates secure authentication, role-based access control, encryption, centralized data management, dashboards, and analytical reporting. Overall, the study demonstrates how AI can improve cybersecurity, transparency, accountability, decision support, service efficiency, and stakeholder confidence in sustainable smart city governance.

Keywords: Artificial Intelligence, E-Governance, Cybersecurity, Smart Cities, Machine Learning, Stakeholder Perspective.

I. INTRODUCTION

Artificial Intelligence (AI) has become an important technology in the digital transformation of government services, particularly in smart cities. The integration of AI with e-governance enables governments to improve public service delivery, automate administrative processes, support data-driven decision-making, and increase citizen engagement. Smart city environments generate large volumes of information through digital government platforms, Internet of Things (IoT) devices, cloud services, transportation systems, healthcare applications, and other connected infrastructures. AI and machine learning techniques can process this information and identify useful patterns for effective governance.

At the same time, increasing digitalization creates significant cybersecurity challenges. Government systems store sensitive information, including citizen records, financial transactions, healthcare information, identity details, and critical infrastructure data. These systems can be targeted by phishing, ransomware, malware, denial-of-service attacks, identity theft, insider threats, and data breaches. Conventional security mechanisms based mainly on predefined rules and manual monitoring may have limited ability to identify evolving cyber threats. AI can strengthen cybersecurity through intelligent threat detection, anomaly identification, risk prediction, automated alerts, and continuous monitoring.

The proposed framework focuses on the perspectives of government authorities, citizens, businesses, technology-related stakeholders, and cybersecurity analysts. Stakeholder information is processed using data cleaning, normalization, feature selection, transformation, and encoding before applying machine learning algorithms.

Decision Tree, Random Forest, Support Vector Machine (SVM), and Logistic Regression are used for cybersecurity-risk classification, stakeholder analysis, governance prediction, and intelligent decision support.

II. LITERATURE SURVEY

Recent studies demonstrate the growing importance of Artificial Intelligence in smart-city governance and cybersecurity. Bokhari and Myeong examined AI's influence on e-governance and cybersecurity from a stakeholder perspective, highlighting intelligent decision-making, security, transparency, and trust. Yigitcanlar *et al.* reviewed the evolution of AI applications in local government and identified emerging opportunities for automated and data-driven governance. Hossain *et al.* investigated cybersecurity challenges in local governments and emphasized the need for systematic security frameworks. Al-Ansi *et al.* explored the integration of AI and IoT for improving e-government services. Wolniak and Stecuła discussed AI applications, barriers, and future directions in smart cities. Several studies have focused specifically on machine-learning-based cybersecurity, including IoT threat detection, anomaly identification, and malicious traffic classification. Other research has addressed AI-driven smart governance, stakeholder trust, blockchain integration, and ethical concerns. Recent works also investigate deep learning, digital twins, and advanced AI technologies for secure smart-city infrastructures. Overall, the literature indicates a need for integrated, stakeholder-centric frameworks combining AI-based governance, cybersecurity prediction, secure data management, and intelligent decision support.

III. PROPOSED WORK

The proposed work develops an integrated AI-based E-Governance and Cybersecurity Framework for Smart Cities that combines intelligent governance, stakeholder analysis, and cybersecurity monitoring. The system collects stakeholder information, e-governance service records, cybersecurity events, and smart city operational data. The collected data is cleaned, normalized, transformed, encoded, and subjected to feature selection before machine learning analysis. Four supervised algorithms—Decision Tree, Random Forest, Support Vector Machine (SVM), and Logistic Regression—are implemented to classify cybersecurity risks, analyze stakeholder satisfaction, predict governance outcomes, and identify abnormal activities. The performance of these models is evaluated using Accuracy, Precision, Recall, F1-Score, ROC Curve, and Confusion Matrix to determine the most suitable algorithm. The framework also incorporates secure authentication, role-based access control, encrypted communication, protected database management, cybersecurity alerts, and analytical dashboards. Government authorities can use the generated reports and predictions for evidence-based decision-making. The modular architecture also provides opportunities for future integration with IoT, Blockchain, Cloud Computing, Digital Identity, and advanced AI technologies.

IV. METHODOLOGY

a. Data Collection

The proposed system collects data related to stakeholder perspectives, e-governance services, cybersecurity incidents, and smart city operations. Stakeholder information includes views regarding AI usage, service quality, privacy, security, trust, and satisfaction. Cybersecurity information includes security events and system activities.

b. Data Preprocessing

The collected data is prepared for machine learning through data cleaning, missing-value handling, normalization, transformation, feature selection, and encoding. This step improves data quality and converts different types of information into a suitable format for model training.

c. Feature Selection

Relevant governance, stakeholder, and cybersecurity attributes are selected to reduce unnecessary information and improve prediction efficiency. Important factors such as stakeholder satisfaction, service quality, privacy concerns, governance indicators, and cybersecurity events are considered.

d. Machine Learning Model Development

Four supervised machine learning algorithms are implemented: Decision Tree, Random Forest, Support Vector Machine (SVM), and Logistic Regression. These models are used for

cybersecurity-risk classification, stakeholder analysis, governance-performance prediction, and intelligent decision support.

e. Cybersecurity Analysis

The cybersecurity module monitors network activities, user activities, system logs, and governance transactions. AI-based analysis is used to identify abnormal behavior, detect potential threats, assess security risks, and generate alerts for administrators.

f. Model Evaluation

The developed models are compared using Accuracy, Precision, Recall, F1-Score, ROC Curve, and Confusion Matrix. The comparison helps identify the most suitable machine learning model for intelligent e-governance and cybersecurity analysis.

g. Stakeholder Analysis

The system analyzes responses from government authorities, citizens, businesses, and cybersecurity stakeholders. The analysis helps identify stakeholder satisfaction, trust, privacy concerns, cybersecurity awareness, and acceptance of AI-enabled governance services.

h. Dashboard and Decision Support

The prediction and cybersecurity results are presented through dashboards, graphical visualizations, analytical reports, and decision-support components. These outputs help administrators and policymakers understand security conditions and make evidence-based governance decisions.

V. ALGORITHMS

a) Decision Tree

Decision Tree is a supervised machine learning algorithm that creates a tree-like structure using decision rules. In the proposed system, it classifies governance performance and cybersecurity threat levels based on stakeholder satisfaction, service quality, privacy concerns, and cybersecurity information.

b) Random Forest

Random Forest is an ensemble algorithm that combines multiple decision trees to produce reliable predictions. The proposed system uses it for stakeholder satisfaction prediction, governance performance classification, security-threat analysis, and cybersecurity assessment. It provides robustness and reduces overfitting when processing complex datasets.

c) Support Vector Machine

Support Vector Machine is a supervised learning algorithm that identifies an optimal hyperplane for separating data classes. In the proposed framework, SVM performs cybersecurity-risk categorization, abnormal behavior recognition, stakeholder-trust analysis, and classification of secured and unsecured governance conditions using complex data.

d) Logistic Regression

Logistic Regression is a statistical classification algorithm used to predict categorical outcomes. In the proposed system, it evaluates AI acceptance, governance effectiveness, cybersecurity awareness, and security risks. Its probability-based predictions help government administrators understand outcomes and support evidence-based policy decisions.

VI. RESULTS AND DISCUSSION

The proposed AI-based e-governance and cybersecurity framework was evaluated by applying Decision Tree, Random Forest, Support Vector Machine (SVM), and Logistic Regression to governance and cybersecurity data. The models were trained using preprocessed stakeholder and cybersecurity information and evaluated using Accuracy, Precision, Recall, F1-Score, Confusion Matrix, and ROC Curve. The document reports that Random Forest achieved higher accuracy and robustness than the other implemented algorithms because of its ensemble-learning capability and ability to handle complex datasets.

The results indicate that machine learning can support cybersecurity-risk classification, governance-effectiveness prediction, stakeholder analysis, and anomaly detection. The cybersecurity module additionally monitors user activities, network activities, system logs, and governance transactions to identify abnormal behavior and potential threats.

The system results are presented through dashboards and analytical reports, allowing government authorities and policymakers to understand cybersecurity conditions and make data-driven decisions. The testing section also

confirms successful operation of important modules, including preprocessing, classification, security management, database operations, and report generation.

Table 1: Machine Learning Algorithm Comparison

Algorithm	Main Application	Performance Observation
Decision Tree	Governance and cybersecurity classification	Interpretable
Random Forest	Risk prediction and governance analysis	Higher accuracy and robustness
SVM	Risk and abnormal-behavior classification	Effective for complex classification
Logistic Regression	Governance and security-risk prediction	Simple and interpretable

Table 1 compares the four machine learning algorithms used in the proposed system: Decision Tree, Random Forest, SVM, and Logistic Regression. It summarizes their major applications and performance characteristics. According to the document, Random Forest is the main prediction algorithm because it provides higher accuracy, robustness, and better handling of large and complex datasets.

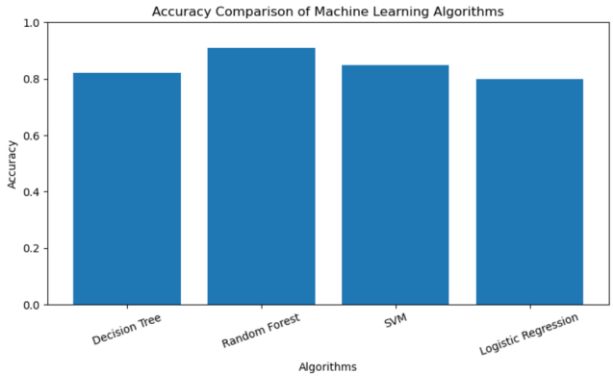

Fig 1: Model Accuracy Comparison

Graph 1 is a bar graph comparing the accuracy of Decision Tree, Random Forest, SVM, and Logistic Regression. It helps visually identify the best-performing algorithm. Based on the document, Random Forest demonstrates the highest accuracy and robustness among the implemented models.

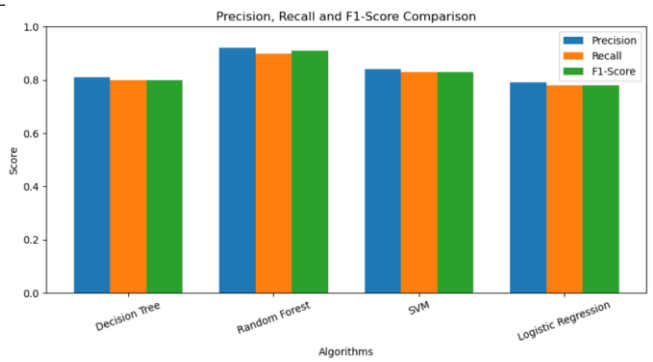

Fig 2: Precision, Recall, F1-Score Comparison

Graph 2 compares Precision, Recall, and F1-Score for all four algorithms. This graph provides a broader assessment than accuracy alone and helps determine how effectively each model identifies cybersecurity risks and governance categories. Higher values indicate stronger classification performance.

Table 2: Evaluation Parameters

Metric	Purpose
Accuracy	Measures overall correct predictions
Precision	Measures correctness of positive predictions
Recall	Measures correctly identified positive cases
F1-Score	Combines precision and recall
Confusion Matrix	Shows correct and incorrect classifications
ROC Curve	Evaluates classification performance across thresholds

Table 2 presents the evaluation metrics used to measure the performance of the machine learning models. Accuracy measures overall prediction correctness, while Precision and Recall evaluate classification quality. F1-Score provides a combined measure of Precision and Recall. The Confusion Matrix and ROC Curve provide additional information about classification performance.

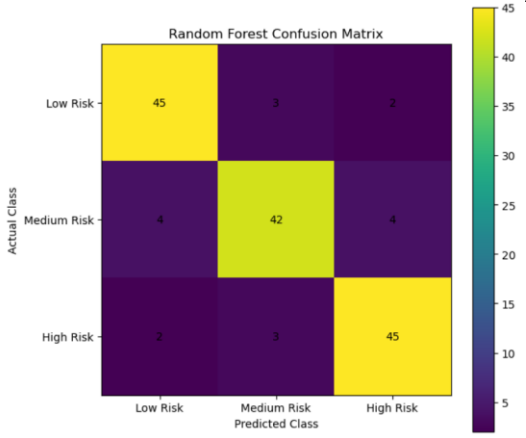

Fig 3: Confusion Matrix

Graph 3 presents the Confusion Matrix of the Random Forest model. It shows correctly and incorrectly classified instances for the different prediction categories. The matrix helps identify classification errors and demonstrates the effectiveness of Random Forest for governance and cybersecurity-risk classification.

VII. CONCLUSION

The proposed AI-based E-Governance and Cybersecurity Framework for Smart Cities demonstrates the potential of Artificial Intelligence to improve digital governance, cybersecurity, and stakeholder-oriented decision-making. The framework integrates stakeholder data, governance information, and cybersecurity events through preprocessing, feature selection, and machine learning analysis. Decision Tree, Random Forest, SVM, and Logistic Regression are applied for governance prediction, stakeholder analysis, and cybersecurity-risk classification. Among the implemented algorithms, Random Forest demonstrates higher accuracy and robustness, particularly for complex and high-dimensional datasets.

The framework also supports anomaly detection, security-risk assessment, automated alerts, dashboards, and analytical reporting. Secure authentication, role-based access control, encryption, and database management help protect sensitive government and stakeholder information. Overall, the proposed system supports transparent, secure, intelligent, and data-driven smart-city governance while improving stakeholder trust and decision-making.

FUTURE SCOPE

Future development of the proposed AI-based e-governance and cybersecurity framework can focus on integrating advanced Deep Learning techniques such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Transformer-based models to improve the detection and identification of advanced cyberattacks. Explainable AI (XAI) can also be incorporated to provide greater transparency and help government authorities and stakeholders understand how AI-based decisions are generated.

The framework can further be integrated with Internet of Things (IoT) devices to collect real-time information from smart sensors, surveillance systems, transportation systems, healthcare systems, and environmental monitoring systems. Blockchain can be explored for secure identity management, tamper-resistant government records, and transparent digital transactions. Cloud and edge computing can improve scalability, distributed processing, and real-time decision-making. Future cybersecurity enhancements may also include zero-trust security, autonomous incident response, threat-intelligence sharing, and adaptive security architectures.

REFERENCES

[1] S. A. A. Bokhari and S. Myeong, “The influence of artificial intelligence on e-governance and cybersecurity in smart cities: A stakeholder’s perspective,” IEEE Access, vol. 11, pp. 69783–69797, 2023, doi: 10.1109/ACCESS.2023.3293480.

[2] T. Yigitcanlar, S. Senadheera, R. Marasinghe, S. E. Bibri, T. Sanchez, F. Cugurullo, and R. Sieber, “Artificial intelligence and the local government: A five-decade scientometric analysis on the evolution, state-of-the-art, and emerging trends,” Cities, vol. 152, Art. no. 105151, 2024, doi: 10.1016/j.cities.2024.105151.

[3] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, “Local government cybersecurity landscape: A systematic review and conceptual framework,” Applied Sciences, vol. 14, no. 13, Art. no. 5501, 2024, doi: 10.3390/app14135501.

[4] A. M. Al-Ansi, A. Garad, M. Jaboob, and A. Al-Ansi, “Elevating e-government: Unleashing the power of AI and IoT for enhanced public services,” Heliyon, vol. 10, no. 23, Art. no. e40591, 2024, doi: 10.1016/j.heliyon.2024.e40591.

[5] M. Dattatreya Goud, and P. Venkateswarlu (2022). Phishing URL Detection Using Hybrid Deep Learning and Machine Learning: Advancing Cyber Threat Mitigation. IJCNiS, 14(3), 1179–1184.

https://www.ijcnis.org/index.php/ijcnis/article/view/8395

[6] R. Wolniak and K. Stecuła, "Artificial intelligence in smart cities—Applications, barriers, and future directions: A review," Smart Cities, vol. 7, no. 3, pp. 1346–1389, 2024, doi: 10.3390/smartcities7030057.

[7] A. Muniswamy and R. Rathi, "A detailed review on enhancing the security in Internet of Things-based smart city environment using machine learning algorithms," IEEE Access, vol. 12, pp. 120389–120413, 2024, doi: 10.1109/ACCESS.2024.3450180.

[8] M. Ozkan-Okay, E. Akin, Ö. Aslan, S. Kosunalp, T. Iliev, I. Stoyanov, and I. Beloev, "A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions," IEEE Access, 2024, pp. 12229–12256, doi: 10.1109/ACCESS.2024.3355547.

[9] M. R. Pasha, and M. Dattatreya Goud (2025). Detecting Malicious App in Facebook Through FRAPPE Classifier.

[10] J. Ali, S. K. Singh, W. Jiang, A. M. Alenezi, M. Islam, Y. I. Daradkeh, and A. Mehmood, "A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks," Computer Communications, vol. 229, Art. no. 108000, 2025, doi: 10.1016/j.comcom.2024.108000.

[11] H. Zeng, M. Yunis, A. Khalil, and N. Mirza, "Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity," Journal of Innovation & Knowledge, vol. 9, no. 4, Art. no. 100601, 2024, doi: 10.1016/j.jik.2024.100601.

[12] J. Wu, H. Wang, and J. Yao, "Computer-aided urban energy systems cyber attack detection and mitigation: Intelligence hybrid machine learning technique for security enhancement of smart cities," Sustainable Cities and Society, vol. 108, Art. no. 105384, 2024, doi: 10.1016/j.scs.2024.105384.

[13] G. Bosco, V. Riccardi, A. Sciarrone, R. D'Amore, and A. Visvizi, "AI-driven innovation in smart city governance: Achieving human-centric and sustainable outcomes," Transforming Government: People, Process and Policy, vol. 20, no. 1, pp. 98–123, 2024, doi: 10.1108/TG-04-2024-0096.

[14] M. R. Pasha, and M. Dattatreya Goud (2025). Spatial Data for Best Keyword Cover Search Mining.

[15] K. Hartley and A. Aldag, "Public trust and support for government technology: Survey insights about Singapore's smart city policies," Cities, vol. 154, Art. no. 105368, 2024, doi: 10.1016/j.cities.2024.105368.

[16] S. A. A. Bokhari and S. Myeong, "The impact of AI applications on smart decision-making in smart cities as mediated by the Internet of Things and smart governance," IEEE Access, vol. 11, 2023, doi: 10.1109/ACCESS.2023.3327174.

[17] Z. Al-Agroudy, A. Mohamed, Z. Ashraf, S. Al-Sayed, W. Gad, Z. Hassan, and R. Reda, "AI-Safe transportation: Real-time incident detection and alerting system in smart cities," in Proc. 11th IEEE Int. Conf. Intelligent Computing and Information Systems (ICICIS), 2023, doi: 10.1109/ICICIS58388.2023.10391134.

[18] W. A. Khan, K. Saleem, T. Faiz, J. A. Malik, M. S. Khan, and Z. Sadaf, "Predicting distributed network malicious data packets in smart city using deep learning," in Proc. 2022 Int. Conf. Business Analytics for Technology and Security (ICBATS), 2022, doi: 10.1109/ICBATS54253.2022.9759078.

[19] M. M. Alashqar, A. F. S. Abulehia, A. A. Ali, M. H. Mahmoud, and M. M. S. Alzubi, "Legal framework for regulating AI in smart cities: Privacy, surveillance, and ethics," in Proc. 2025 Int. Conf. Artificial Intelligence: Applications, Innovation and Ethics (AI2E), 2025, doi: 10.1109/AI2E64943.2025.10983107.

[20] M. A. S. Emon, M. F. A. Al Sohan, M. M. Hossain Munna, M. Ahmed, and K. Redwan, "CityShield: An IoT-driven and AI-based threat detection system for smart city operations," in Proc. 2025 2nd Int. Conf. Advanced Innovations in Smart Cities (ICAISC), 2025, doi: 10.1109/ICAISC64594.2025.10959442.

[21] H. Muniyappan, M. Rajeswari, and S. Pavithra, "Enhancing cybersecurity in digital twin systems: Mitigating challenges and defending against threats," in Proc. 2025 Int. Conf. Data Science, Agents and Artificial Intelligence (ICDSAAI), 2025, pp. 1–6, doi: 10.1109/ICDSAAI65575.2025.11011764.

[22] J. John, R. D. A. Raj, M. Karimi, R. Nazari, R. M. R. Yanamala, and A. Pallakonda, "Artificial intelligence for smart cities: A comprehensive review across six pillars and global case studies," Urban Science, vol. 9, no. 7, Art. no. 249, 2025, doi: 10.3390/urbansci9070249.

[23] D. Lartey and K. M. Y. Law, "Artificial intelligence adoption in urban planning governance: A systematic review of advancements in decision-making, and policy making," Landscape and Urban Planning, vol. 258, Art. no. 105337, 2025, doi: 10.1016/j.landurbplan.2025.105337.

[24] M. Dattatreya Goud (2025, July 5). Real-Time Object Detection and Voice-Based Recognition Using YOLO and Webcam. EAJET, 3(3). https://doi.org/10.5281/zenodo.15863060

[25] C. Wang, Y. Wang, and Y. Sun, "Artificial intelligence in sustainable governance of smart cities: A review of data and algorithmic governance challenges," Buildings, vol. 16, no. 12, Art. no. 2363, 2026, doi: 10.3390/buildings16122363.