Stackholder Perspectives on The Role of Artificial Intelligence In E-Governance And Cybersecurity For Smart Cities

[1] A.Yashwanth, [2] A.Murali, [3] A Satish, [4] P. Swetha
[1,2,3]UG Scholar, Department of Computer Science and Engineering, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
[4]Assistant Professor, Department of Computer Science and Engineering, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
pswethacse@gmail.com

Abstract:

Challenges abound in capturing and processing images under low light conditions, resulting in diminished image quality characterized by reduced visibility and heightened noise levels. Conventional methods for enhancing low light images typically involve manual image processing techniques like histogram equalization, contrast stretching, and noise reduction filters. While these approaches may offer some enhancement, they often fall short in achieving visually pleasing and authentic results. Their lack of adaptability and limited capacity to discern intricate patterns from data renders them less effective in handling diverse low light scenarios. The imperative for an advanced low light image enhancement technique stems from the extensive utilization of imaging devices in low light environments across various sectors such as surveillance, automotive, and photography. These industries heavily rely on cameras to capture images in challenging lighting conditions. By enhancing visibility and overall image quality in low light settings, the accuracy and dependability of image-based systems can be significantly bolstered. Hence, there is a pressing need for an intelligent approach capable of learning and adapting from data to overcome the shortcomings of traditional methods. In recent years, deep learning has emerged as a promising solution for numerous computer vision tasks, including image enhancement. This project endeavours to explore and propose a deep learning-based approach to mitigate the challenges associated with low light image enhancement, thereby enhancing visibility. By leveraging deep learning, this approach surmounts the constraints of conventional techniques by autonomously capturing intricate patterns and features within low light images. This adaptability empowers the model to generalize effectively across various low light scenarios, resulting in enhancements that are visually appealing and true to life.

Keywords: Low Light Image Enhancement, Deep Learning, Image Enhancement, Low Light Vision, Dark Image Processing, Low light image restoration, neural networks for low light.

1.INYRODUCTION

Cybersecurity is a critical issue in today's digital world, as cyber-attacks continue to evolve, targeting networks, data, and incation afrastructure. The increasing reliance on online technologies has made organizations and individuals more vulnerable to threats like phishing, malware, ransomware, and denial-of-service attacks, leading to financial losses and psychological distress.

Artificial Intelligence (AI) offers promising solutions to enhance cybersecurity by improving threat detection, prevention, and response mechanisms. AI-driven systems analyze data, identify risks, and support machine learning applications for malware classification andintrusion. However, AI also poses risks, as cybercriminals can exploit it to accelerate attacks. This dual nature of AI necessitates responsible deployment in cybersecurity strategies. In smart cities, where ICT is integrated into urban infrastructure, cybersecurity becomes even more crucial. Insecure networks used for e-services like online banking and email increase the risk of cybercrimes. Secure e-Government services play a key role in ensuring a resilient smart city. While AI has been applied to areas like mobility and energy management, its impact on cybersecurity in smart cities particularly concerning e-Governance—remains underexplored.

This study examines how AI applications influence cybersecurity in smart cities, considering the mediating role of e-Governance and the moderating effect of stakeholder involvement. Using PLS-SEM path modeling, the research highlights complex interactions between AI, e-Governance, and cybersecurity, offering insights for strengthening digital security and stakeholder engagement in urban environments. Smart cities leverage advanced technologies to enhance urban living, and e-Governance plays a crucial role in efficient city management. Artificial Intelligence (AI) is increasingly integrated into e-Governance to optimize decision-making, automate services, and improve cybersecurity. However, AI adoption brings challenges such as cyber threats, ethical concerns, and stakeholder engagement issues. This document explores the perspectives of various stakeholders on AI's role in e-Governance and cybersecurity for smart cities. AI-driven solutions help improve urban management, streamline administrative processes, and provide real-time monitoring of security threats. However, the integration of AI also raises concerns regarding privacy, data security, and ethical governance. This document explores the perspectives of various stakeholders on AI's role in e-Governance and cybersecurity for smart cities, highlighting its benefits, challenges, and future potential.

2. LITERATURE SURVEY

Smart city is a captivating concept characterized by its intelligent features. Its scope extends beyond improving the level of urban economic efficiency and the reduction of costs and resource consumption. Rather, it encompasses the integration of different components of the city through intelligent gadgets and the application of digital technologies or information and communication technology (ICT) to enhance service delivery. The transformation of conventional urban areas into smart cities has resulted in a higher living standard for citizens.

"Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry" - B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed.

The aim of the researcher was to determine the effectiveness of artificial intelligence techniques against cyber security risks particularly in case of Iraq, Researcher has opted for quantitative method of research design along with primary data. The researcher collected the data from employees working in this IT industry. The sample size for this study was 468 and confirmatory factor analysis, discriminant validity, basic analysis of model and lastly, hypothesis assessment was carried out. The P-values of all variables were obtained as significant apart from expert system which had no significant relation with artificial intelligence and cybersecurity. Geographical area, sample size, less variables and accessibility was the main issue.

"High performance adaptive system for cyberattacks detection" - M. Komar, V. Kochan, L. Dubchak, A. Sachenko, V. Golovko, S. Bezobrazov, and I. Romanets.

To increase the security of intrusion detection system, generalized structure of highly performance adaptive system for cyber attacks detection was developed. To improve its robustness, methods of artificial intelligence were proposed. Neural immune detectors were used as the main tool for identifying cyber attacks. These detectors for cyber attacks identification and classification and other vulnerable subsystems were implemented in programmable logic arrays. To provide high performance, the Mamdani fuzzy inference rules were used and relevant subsystem structures were developed.+

3. PROPOSED METHODOLOGY

The proposed methodology focuses on understanding the role of Artificial Intelligence (AI) in e-governance and cybersecurity for smart cities. The primary objective is to analyze stakeholder perspectives on how AI-driven solutions can enhance governance efficiency, data security, and decision-making processes in urban environments. This research applies AI-based frameworks, machine learning models, and data analytics techniques to assess the effectiveness and challenges of AI implementation in smart city governance and cybersecurity. Additionally, the methodology examines the scalability, adaptability, and ethical considerations of AI integration into public administration and security infrastructures. It explores how AI can optimize governance processes by automating routine administrative tasks, detecting fraud, and improving service delivery. The research also investigates how AI-driven predictive analytics can enhance law enforcement capabilities.

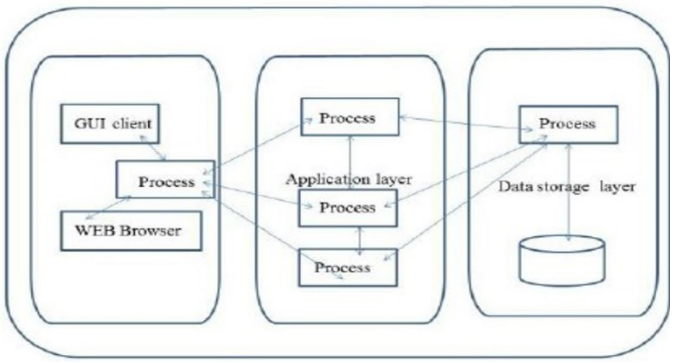

Fig 1 : AI in E-Governance Architecture

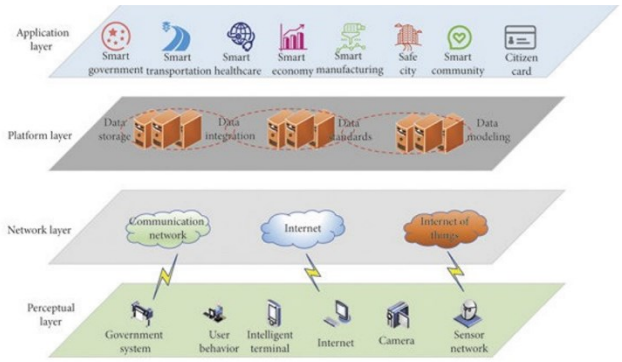

Figure 2: System architecture for AI in Smart cities

The proposed methodology typically includes the following key components:

- ***Stakeholder Analysis:*** Identification and categorization of key stakeholders, including government agencies, cybersecurity professionals, urban planners, and citizens, to understand their perspectives on AI adoption.
- ***AI-driven Data Governance:*** Implementation of AI-based algorithms to manage, analyze, and secure citizen data, ensuring compliance with privacy regulations and ethical guidelines.
- ***Cybersecurity Frameworks:*** Development of AI-enhanced cybersecurity models to detect, prevent, and respond to cyber threats in smart city infrastructures.
- ***AI-based Decision Support Systems (DSS):*** Integration of AI-driven DSS to assist policymakers in making informed decisions based on real-time data analytics and predictive modeling.*
- ***Performance*** Metrics Evaluation: Measuring the effectiveness of AI-driven e-governance and cybersecurity mechanisms using key performance indicators such as response time, threat detection accuracy, and system reliability.
- **Public Perception and Acceptance:** Conducting surveys and interviews with stakeholders to gauge public trust, acceptance, and concerns regarding AI-based governance and security solutions.

Applications:

LIME's enhanced images can be used in a wide range of applications, including:

- **Public Administration:** Enhancing transparency, efficiency, and decision-making in government services.
- **Law Enforcement and Security:** AI-powered surveillance systems for crime prevention and real-time threat detection.
- **Urban Infrastructure Management:** Predictive maintenance of smart city assets using AI-based analytics.
- **Healthcare Services:** Securing electronic health records (EHRs) and optimizing AI-driven telemedicine services.
- **Smart Transportation:** AI-driven traffic management and predictive analytics for optimizing urban mobility.
- **Environmental Monitoring:** AI-enhanced systems for real-time tracking of pollution levels, waste management, and climate resilience strategies.
- **Disaster Management:** AI-enabled early warning systems for natural disaster prediction and response planning.

Advantages:

The integration of AI in e-governance and cybersecurity for smart cities offers several benefits:

- **Enhanced Security:** AI-driven threat intelligence and automated incident response mechanisms to counter cyberattacks.
- **Improved Efficiency:** AI-powered automation streamlines administrative processes, reducing manual efforts and operational costs.
- **Data-Driven Governance:** AI analytics enable evidence-based policy formulation and resource allocation.

- **Real-time Monitoring:** AI enables continuous monitoring of urban infrastructure and cybersecurity threats, ensuring swift responses.
- **Personalized Services:** AI facilitates customized citizen services by analyzing individual needs and preferences.
- **Ethical Compliance:** AI-driven frameworks ensure compliance with data protection laws and ethical governance principles.
- **Scalability:** AI solutions can be scaled to accommodate growing urban populations and evolving governance challenges.
- **Cost Reduction:** AI automation reduces operational costs by optimizing resource allocation and administrative efficiency.
- **Fraud Detection and Prevention:** AI algorithms can detect anomalies and fraudulent activities in financial transactions, public tenders, and social welfare programs.

4. EXPERIMENTAL ANALYSIS

Figure 1: login page

Figure 1 shows a login interface for a cybersecurity application titled Optimal Ensemble Learning for Automated Android Malware Detection in Cyber Security Applications. The interface offers login options for service providers and new users to register, indicating a multi-user platform for malware detection and analysis.

Figure 2: Trained and Tested result

Figure 2 shows the trained and tested results for different machine learning models used in the Android malware detection system. The models listed include Naive Bayes, LS-SVM, Logistic Regression, Decision Tree Classifier, and K Neighbors Classifier, with their respective accuracy scores displayed. The high accuracy values indicate effective model performance in distinguishing between benign and malicious Android applications. The structured tabs at the top suggest additional features and functionalities of the application, like dataset viewing, model evaluation, and performance analysis.

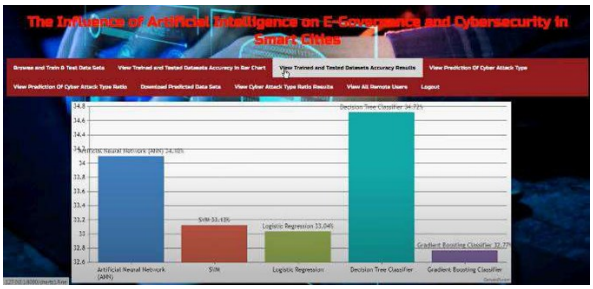

Figure 3: Accuracy Result

Figure 4: Predicted graph

Figure 5: View all remote users

5. CONCLUSION

The present research looked at uses of artificial intelligence to address cyber security issues. The study's conclusions show that artificial intelligence is gradually becoming into a necessary tool for improving information security performance. People are no longer able to carry out project-level cyberattacks that are completely safe, and artificial intelligence provides the analytics and threat information that security professionals need to reduce the possibility of a breach and fortify an organization's security framework. Since greater processing power is available for cyber security, danger may be assessed and eliminated more quickly. Many people are worried about the capacity of cybercriminals to carry out very sophisticated technologies and cyberattacks. Artificial intelligence may also help in the identification and categorisation of risks, the organisation of incident response, and the pre empitive detection of cyberattacks. Therefore, in spite of any possible drawbacks, artificial intelligence will advance cyber security and help businesses implement a more robust security plan.

This research aimed to explore artificial intelligence and its continuous advancement in providing e-government services. It also emphasised the need of incorporating cyber security techniques to enable the adoption of novel social and technological processes in government that benefit the community. Building and maintaining connections with the majority of stakeholders is the ultimate goal of smart city governments, since their participation enhances the effectiveness of e-government and bolsters cyber security. In order to remove obstacles between stakeholders and local governments, public services should be managed using new artificial intelligence technology and accessible e-governance modes. State authorities may continue to promote this model for even greater outcomes. E-government is advancing, but those who support mechatronics or are in positions of responsibility

are not keeping up. This leads to differences in cyber security requirements for anything in the virtual world, which might make performing more harder and need many tracks to keep an eye on. The advantages of the virtual environment may become possible if the efforts found in this study are elevated and stakeholders' engagement and understanding of e-governance and cyber security increase.

REFERENCES

[1] [1] B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, ‘‘Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry,’’ Mater. Today, Proc., vol. 531, pp. 1–6, 2021, doi:10.1016/j.matpr.2021.02.531.

[2] [2] M. Komar, V. Kochan, L. Dubchak, A. Sachenko, V. Golovko, S. Bezobrazov, and I. Romanets, ‘‘High performance adaptive system for cyber attacks detection,’’ in Proc. 9th IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl. (IDAACS), vol. 2, Sep. 2017, pp. 853–858.

[3] [3] M. D. Cavelty, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Evanston, IL, USA: Routledge, 2007.

[4] [4] F. Fransen, A. Smulders, and R. Kerkdijk, ‘‘Cyber security information exchange to gain insight into the effects of cyber threats and incidents,’’ Elektrotechnik Informationstechnik, vol. 132, no. 2, pp. 106–112, Mar. 2015.

[5] [5] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, ‘‘Cybersecurity awareness in the context of the industrial Internet of Things: A systematic literature review,’’ Comput. Ind., vol. 137, May 2022, Art. no. 103614.

[6] [6] G. A.Weaver, B. Feddersen, L. Marla, D.Wei, A. Rose, and M. Van Moer, ‘‘Estimating economic losses from cyber attacks on shipping ports: An optimization based approach,’’ Transp. Res. C, Emerg. Technol., vol. 137, Apr. 2022, Art. no. 103423.

[7] [7] M. Bada and J. R. C. Nurse, ‘‘The social and psychological impact of cyberattacks,’’ in Emerging Cyber Threats and Cognitive Vulnerabilities. Amsterdam, The Netherlands: Elsevier, 2020, pp. 73–92.

[8] [8] G. Allen and T. Chan, Artificial Intelligence and National Security. Cambridge, MA, USA: Belfer Center for Science and International Affairs, 2017.

[9] [9] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K.-K. R. Choo, ‘‘Artificial intelligence in cyber security: Research advances, challenges, and opportunities,’’ Artif. Intell. Rev., vol. 55, pp. 1029–1053, Feb. 2022.

[10] [10] Z. I. Khisamova, I. R. Begishev, and E. L. Sidorenko, ‘‘Artificial intelligence and problems of ensuring cyber security,’’ Int. J. Cyber Criminol., vol. 13, no. 2, pp. 564 577, 2019.

[11] [11] J.-H. Li, ‘‘Cyber security meets artificial intelligence: A survey,’’ Frontiers Inf. Technol. Electron. Eng., vol. 19, no. 12, pp. 1462–1474, 2018.

[12] [12] S. A. A. Bokhari and S. Myeong, ‘‘Use of artificial intelligence in smart cities for smart decision-making: A social innovation perspective,’’ Sustainability, vol. 14, no. 2, p. 620, Jan. 2022.

[13] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," Comput. Secur., Nov. 2019.

[14] [13] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, ‘‘Cyber threat intelligence sharing: Survey and research directions,’’ Comput. Secur., vol. 87, Nov. 2019, Art. no. 101589.

[15] [14] J. Singh, M. Sajid, S. K. Gupta, and R. A. Haidri, ‘‘Artificial intelligence and blockchain technologies for smart city,’’ in Intelligent Green Technologies for Sustainable Smart Cities. Beverly, MA, USA: Scrivener Publishing, 2022, pp. 317 330.

[16] [15] R. Khatoun and S. Zeadally, ‘‘Cybersecurity and privacy solutions in smart cities,’’ IEEE Commun. Mag., vol. 55, no. 3, pp. 51–59, Mar. 2017.

[17] [16] K. Kourtit, M. M. M. Pele, P. Nijkamp, and D. T. Pele, ‘‘Safe cities in the new urban world: A comparative cluster dynamics analysis through machine learning,’’ Sustain. Cities Soc., vol. 66, Mar. 2021, Art. no. 102665.

[18] [17] J. Engelbert, L. van Zoonen, and F. Hirzalla, ‘‘Excluding citizens from the European smart city: The discourse practices of pursuing and granting smartness,’’ Technol. Forecasting Social Change, vol. 142, pp. 347–353, May 2019.

[19] [18] C. Wang, E. Steinfeld, J. L. Maisel, and B. Kang, ‘‘Is your smart city inclusive? Evaluating proposals from the U.S. department of transporta tion’s smart city challenge,’’ Sustain. Cities Soc., vol. 74, Nov. 2021, Art. no. 103148.

[20] [19] J. Ju, L. Liu, and Y. Feng, ‘‘Citizen-centered big data analysis-driven governance intelligence framework for smart cities,’’ Telecommun. Policy, vol. 42, no. 10, pp. 881–896, 2018.

[21] [20] M. Weber, T. Weiss, F. Gechter, and R. Kriesten, ‘‘Approach for improved development of advanced driver assistance systems for future smart mobil ity concepts,’’ Auto. Intell. Syst., vol. 3, no. 1, p. 2, Feb. 2023.

[22] [21] S.U.Khan, N.Khan, F.U.M.Ullah, M.J.Kim, M.Y.Lee, and S.W.Baik, ‘‘Towards intelligent building energy management: AI-based framework for power consumption and generation forecasting,’’ Energy Buildings, vol. 279, Jan. 2023, Art. no. 112705.

[23] [22] S. Myeong, M. J. Ahn, Y. Kim, S. Chu, and W. Suh, ‘‘Government data performance: Theroles of technology, government capacity, and globaliza tion through the effects of national innovativeness,’’ Sustainability, vol. 13, no. 22, p. 12589, Nov. 2021.

[24] [23] W. L. Filho, T. Wall, S. A. R. Mucova, G. J. Nagy, A.-L. Balogun, J. M. Luetz, A. W. Ng, M. Kovaleva, F. M. S. Azam, F. Alves, Z. Guevara, N. R. Matandirotya, A. Skouloudis, A. Tzachor, K. Malakar, and O. Gandhi, ‘‘Deploying artificial intelligence for climate change adaptation,’’ Technol. Forecasting Social Change, vol. 180, Jul. 2022, Art. no. 121662.

[25] [24] M. Alamand I. R. Khan, ‘‘Application of AI in smart cities,’’ in Industrial Transformation. Boca Raton, FL, USA: CRC Press, 2022, pp. 61–86.