International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

ENHANCING E-GOVERNANCE AND CYBERSECURITY WITH AI IN SMART CITIES: A STAKEHOLDER-CENTERED PERSPECTIVE

Dr T.Srikanth
Associate Professor,Department of IT, Malla Reddy Engineering College For Women(Autonomous Institution)

ABSTRACT

AI is one of the emerging key technologies of the Fourth Industrial Revolution (Industry 4.0), particularly for safeguarding computer networks from cyber attacks, malware, phishing, and unauthorized access. It has immense potential to boost cybersecurity among governments, organizations, and non-governmental organizations in general and under the umbrella of e-Governance projects. Current research indicates mixed results in relation to AI, e-Governance, and cybersecurity; that is, the relationship depends on the context.
The dynamics of AI, e-Governance, and cybersecurity are thus influenced by many stakeholders with highly specialized knowledge and expertise. It is the reason why this paper aims to fill the gap that investigates the nature of these interactions, especially as they are more directly interdependent on each other. Further, this study delves into how e-Governance acts as a mediator of the interactions of AI and cybersecurity and how multiple stakeholders might alter these interactions.Based on findings from PLS-SEM path modeling, the research demonstrates that e-Governance partially mediates the connection between AI and cybersecurity. Furthermore, the involvement of stakeholders plays a significant moderating role in both the AI-to-e-Governance and e-Governance-to-cybersecurity relationships. This is underlined by the fact that stakeholders play an important role in AI and e-Governance, all aimed at achieving the same goal, which is the secure, transparent, and efficient digital environment in using e-services.The study can also provide hands-on insights into enhancing the strength of cybersecurity measures that government bodies might put in place. It does that by establishing engagement with other stakeholders as fundamental for developing digital governance frameworks that are secure yet effective.

Keywords : Artificial intelligence, cybersecurity, e-Governance, stakeholder involvement, machine learning, computer crime, smart cities, data privacy.

I.INTRODUCTION

Cybersecurity has become a critical issue in today's digital world, as it is essential to protect computer networks from various potential threats. A cyber-attack is a deliberate attempt to compromise computer networks, data, programs, or electronic information, often with the aim of causing harm or disruption. As technology advances, cyber threats also evolve, making it necessary to continuously develop new strategies for prevention and defense. Cyber-attacks have become increasingly common, especially in the industrial sector, where they have caused significant damage to infrastructure and led to major financial losses. The growing reliance on online technologies, which store vast amounts of personal and economic data,

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

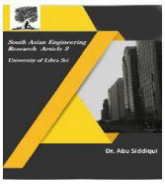
has made organizations particularly vulnerable. These attacks, which include phishing, denial-of-service, malware, and ransomware, not only result in financial and data loss but also have a profound psychological impact on individuals, causing stress and anxiety.In this context, artificial intelligence (AI) offers promising solutions to enhance cybersecurity. AI can help mitigate the effects of cyber-attacks by improving detection, prevention, and response mechanisms. AI systems, which integrate human expertise for strategic decision-making, can be used to analyze data, identify threats, and even make medical diagnoses. However, AI has a dual role: while it can be a powerful tool for enhancing cybersecurity, it can also be used maliciously to accelerate the planning and execution of cyber-attacks. This dual potential highlights the need for careful consideration of how AI is deployed in cybersecurity contexts. AI's ability to analyze patterns, detect cyber threats early, and support machine learning applications for malware classification and intrusion detection is a game-changer for protecting online systems.In smart cities, where information and communication technology (ICT) is integrated into urban infrastructure to solve various administrative challenges, cybersecurity becomes even more critical. The use of insecure Wi-Fi networks for accessing e-services like email and online banking exposes citizens to cybercrimes. Ensuring that e-Government services are secure is one of the key factors that define a safe and resilient city. The concept of an "inclusive smart city" emphasizes the importance of involving stakeholders, including citizens, in the digital ecosystem to improve services and ensure their safety and privacy.While AI has been studied in the context of smart mobility, energy management, public services, and climate change, its role in cybersecurity within smart cities, especially in relation to stakeholders' use of e-Government services, has not been fully explored. This study aims to address this gap by examining how AI applications in smart cities influence cybersecurity directly. It also explores how AI impacts e-Governance, which in turn affects cybersecurity, and whether e-Governance plays a mediating role between AI and cybersecurity. Furthermore, the study investigates the moderating effect of stakeholder involvement in the relationship between AI and e-Governance, as well as between e-Governance and cybersecurity.

The research questions aim to understand the complex interactions between AI, e-Governance, and cybersecurity in a smart city context. The study uses PLS-SEM path modeling to analyze these relationships and highlight the moderating role of stakeholders. By doing so, it seeks to provide valuable insights for smart cities and other urban entities to enhance their cybersecurity frameworks and better engage with citizens and other stakeholders in the digital age.

II.RELATED WORK

1.AI and Cybersecurity :

AI is increasingly being recognized as a game-changer in the world of cybersecurity. It has the ability to learn from large amounts of data, spot potential threats, and react to cyber-attacks almost immediately. Research by Zarina et al. (2020) highlights how AI can significantly reduce the damage caused by



cyber-attacks, from detecting malware using machine learning to building advanced systems that can identify and stop intrusions. However, AI has a downside. While it strengthens defense systems, cybercriminals can also use AI to launch faster and more sophisticated attacks. This means that AI must be used carefully in cybersecurity, ensuring its benefits are maximized while minimizing potential risks.

2. E-Governance and Cybersecurity :

E-Governance, which uses digital technologies to manage government services, offers many advantages, like improving efficiency, transparency, and citizen engagement. However, it also comes with the challenge of protecting sensitive data. With personal and confidential information being stored and processed online, these systems are vulnerable to cyber-attacks such as hacking, denial-of-service, and data breaches. Researchers suggest that integrating AI-based solutions into e-Governance systems can enhance their ability to protect against such threats. By using AI, governments can better secure online services and ensure that citizens' data remains safe.

3.Smart Cities and Cybersecurity:

In smart cities, where digital services, infrastructure, and connected devices are integrated on a large scale, cybersecurity becomes even more crucial. Smart cities rely on technologies like sensor networks, smart grids, and the Internet of Things (IoT), all of which are susceptible to cyber threats. Research by Hussain et al. (2021) shows that AI can be a key player in protecting smart cities from these dangers. For instance, AI systems can detect weaknesses in city networks before they become problems, allowing authorities to act quickly. But there's a challenge: as cities become more connected, the risk of cyber-attacks grows, and finding the right balance between innovation and security is critical.

4.Stakeholder Involvement in E-Governance :

Involving various stakeholders—such as citizens, businesses, and government officials—in the development and execution of e-Governance strategies is essential for success. Recent studies highlight the importance of an inclusive approach to governance, where all key players are part of decision-making processes. The "inclusive smart city" concept focuses on building strong social ties and collaboration between the government, private sector, and the public. This teamwork is vital for addressing urban challenges, including cybersecurity. When stakeholders are actively involved, it helps create digital services that meet the needs of the people while also ensuring privacy and security.

5. AI, E-Governance, and Stakeholder Involvement :

While there's ample research on how AI can enhance e-Governance, fewer studies have explored how AI, e-Governance, and stakeholder involvement are interconnected, especially in terms of cybersecurity. Some researchers suggest that involving stakeholders in the process can play an important role in how AI is adopted and used in government systems. Stakeholders bring valuable perspectives, skills, and knowledge that can help create better AI solutions for cybersecurity challenges. Their participation also leads to more effective policies and

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

security measures that cater to the needs of all citizens.

6. Mediating Role of E-Governance : One of the gaps in current research is understanding the role of e-Governance as a mediator between AI and cybersecurity. E-Governance could be the bridge that connects AI technologies with the wider public, making sure that AI is used effectively to enhance cybersecurity in smart cities. The literature suggests that when e-Governance systems integrate AI, they can improve cyber defenses by enabling real-time monitoring, sharing intelligence about threats, and responding quickly to incidents. This mediation is key in building a robust digital governance framework that not only secures city infrastructure but also builds trust among citizens, who are the ultimate users of these systems.

III.IMPLEMENTATION

1. Model Specification

Define Latent Variables: Identify the key variables such as AI, e-Governance, cybersecurity, and stakeholder involvement.

Create Indicators: Establish measurable indicators for each latent variable, such as survey questions or observations.

Specify Relationships: Determine the direct and indirect relationships between the variables (e.g., AI → e-Governance → Cybersecurity).

2. Data Collection

Survey Distribution: Collect data from participants (478 respondents) using a structured questionnaire.

Data Input: Input the collected data into the PLS-SEM software (e.g., SmartPLS).

3. Model Estimation

Outer Model Estimation: Calculate the relationship between observed data (indicators) and the latent variables (AI, e-Governance, etc.).

Inner Model Estimation: Estimate the relationships between latent variables themselves (e.g., AI → e-Governance → Cybersecurity).

4. Path Modeling

Direct and Indirect Effects: Run the path analysis to calculate the direct and indirect effects between variables.

Moderating and Mediating Effects: Include stakeholder involvement as a moderating variable and e-Governance as a mediating variable.

5. Model Evaluation

R-Squared (R^2) Values: Assess the explained variance for each dependent variable (e.g., cybersecurity).

Path Coefficients: Analyze the strength and direction of relationships (e.g., AI's effect on cybersecurity).

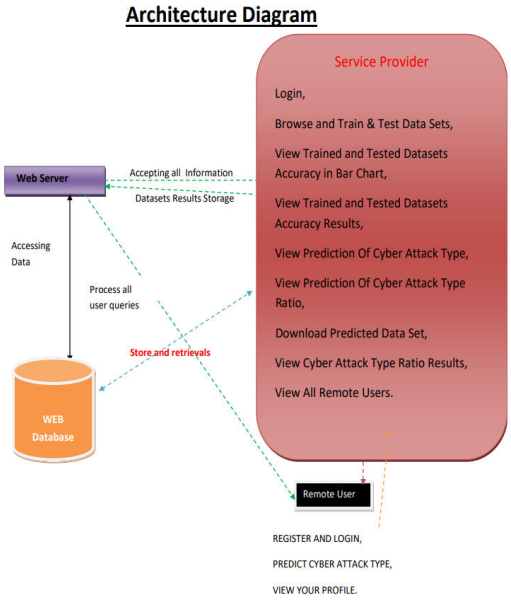
Significance Testing: Use bootstrapping to test the statistical significance of path coefficients.

6. Interpret Results

Analyze Findings: Examine the path coefficients and significance levels to draw conclusions about the relationships between AI, e-Governance, and cybersecurity.

Model Fit: Ensure that the model fits well with the data and all relationships are statistically significant.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal



IV.ALGORITHM USED

1. Overview of PLS-SEM: PLS-SEM is a powerful statistical technique used to analyze complex relationships between observed and latent variables. It is widely used in social sciences, marketing, and management studies to assess models with multiple dependent and independent variables.

The algorithm focuses on:

Path Analysis: It models direct, indirect, and total effects among variables.

Factor Analysis: It helps in examining latent variables, which are not directly measurable but are inferred from observed indicators.

PLS-SEM is suitable for research that involves:

- Complex relationships.
- Small sample sizes (compared to covariance-based SEM).
- Non-normally distributed data.

2. Steps in the PLS-SEM Algorithm:

a. Model Specification:

Measurement Model: Defines the relationships between latent variables (e.g., AI, cybersecurity, e-Governance, stakeholder involvement) and their observed indicators (survey responses).

Structural Model: Defines the relationships between the latent variables themselves, such as how AI influences cybersecurity, or how e-Governance mediates this relationship.

b. Model Estimation:

PLS-SEM uses an iterative algorithm to estimate the weights and loadings of the indicators and the structural paths between latent variables. The key steps in model estimation include:

Outer Model Estimation: This is where the relationship between the observed data (indicators) and the latent variables is established. The weight of each indicator is computed based on how much it explains the variation in the latent variable.

Inner Model Estimation: This step calculates the relationships between the latent variables themselves (e.g., the relationship between AI and e-Governance, or e-Governance and cybersecurity).

PLS-SEM uses a **consistent estimation approach**, optimizing a least-squares criterion for each relationship in the model.

c. Path Modeling:

Once the model is specified, the PLS-SEM algorithm calculates the direct and indirect paths:

Direct paths: These are the direct effects between variables, such as the effect of AI on cybersecurity.

Indirect paths: These are mediated relationships, such as the role of e-Governance as a mediator between AI and cybersecurity.

Moderating effects: The algorithm can also analyze how stakeholders' involvement

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

moderates the relationship between e-Governance and AI, or between e-Governance and cybersecurity.

These paths are calculated based on **bootstrapping techniques**, which allow for determining the statistical significance of each path.

d. Model Evaluation:

PLS-SEM provides various evaluation criteria, such as:

R-squared (R^2): Measures the explained variance of each endogenous variable. For instance, R^2 will show how much of the variation in cybersecurity is explained by AI and e-Governance.

Path Coefficients: These coefficients represent the strength and direction of relationships between variables.

Significance Testing: PLS-SEM uses **bootstrapping** to assess the significance of the path coefficients. This method helps test hypotheses about the relationships (e.g., does e-Governance significantly mediate the relationship between AI and cybersecurity?).

e. Moderation and Mediation Analysis:

Mediation: This is evaluated by testing if e-Governance acts as a mediator between AI and cybersecurity. A mediation effect is significant if the path from AI to cybersecurity is explained by e-Governance.

Moderation: Stakeholder involvement is tested as a moderator to see if it changes the strength or direction of the relationships between AI and e-Governance, or between e-Governance and cybersecurity.

PLS-SEM Path Formula: The PLS-SEM algorithm calculates the path relationships using a recursive formula like:

$$Y_i = \beta_i X_i + \epsilon_i$$

where:

- Y_i represents the dependent variables (e.g., cybersecurity),
- X_i represents the independent variables (e.g., AI, e-Governance),
- β_i represents the path coefficients, and
- ϵ_i is the error term.

V.RESULTS

Fig 1 : User Login

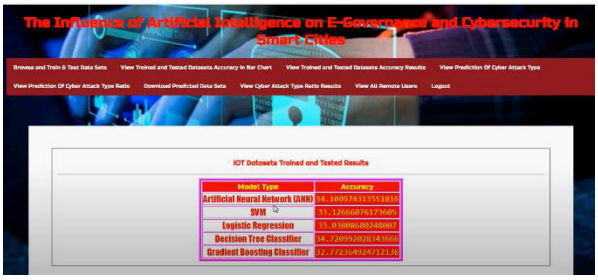


Fig 2 : Trained and Tested Results

Fig 3 : Accuracy Results

Fig 4 : Predicted Garph

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

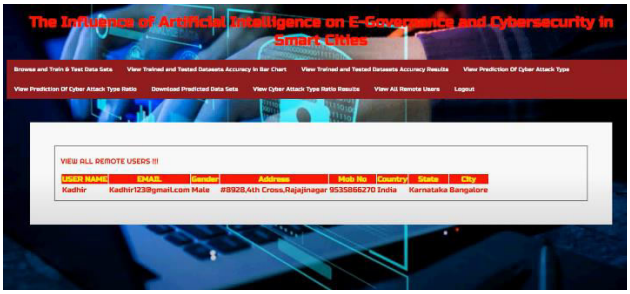


Fig 5 : View all remote users

VI.CONCLUSION

This paper investigates the relationship between Artificial Intelligence (AI), e-Governance, and cybersecurity within smart cities, focusing on how e-Governance acts as a mediator and how stakeholder involvement influences these connections.

The findings reveal that e-Governance plays a crucial role in enhancing cybersecurity by integrating AI technologies into government systems. This not only strengthens security measures but also helps in combating cyber threats more effectively. Additionally, the involvement of various stakeholders, such as citizens, businesses, and government officials, was found to significantly impact the effectiveness of AI and e-Governance strategies. Their participation ensures that these systems are more inclusive, practical, and well-rounded.The study underscores the importance of collaboration and the inclusion of all relevant parties to create a safer, more secure digital environment in smart cities. By engaging stakeholders, cities can develop more effective, adaptive, and citizen-centric cybersecurity solutions.

In conclusion, this research offers valuable insights for policymakers and urban planners, demonstrating that combining AI, e-Governance, and stakeholder involvement can significantly improve cybersecurity strategies in smart cities. Future studies can build on these findings to explore deeper insights into how these elements interact in various contexts, ultimately leading to better and more secure digital governance frameworks.

REFERENCES

[1] B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, ‘‘Effec tiveness of artificial intelligence techniques against cyber security risks apply of IT industry, 2021

[2] M. Komar, V. Kochan, L. Dubchak, A. Sachenko, V. Golovko, S. Bezobrazov, and I. Romanets, ‘‘High performance adaptive system for cyber attacks detection,’’ Sep. 2017

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

[4] F. Fransen, A. Smulders, and R. Kerkdijk, ‘‘Cyber security information exchange to gain insight into the effects of cyber threats and inci dents,’’ Mar. 2015.

[5]A.Corallo,M.Lazoi,M.Lezzi,andA.Lupert o,‘‘Cybersecurityawareness in the context of the industrial Internet of Things: A systematic literature review, May 2022,

[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,’’ Apr. 2022,

[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

[8] G.Allen and T.Chan,ArtificialIntelligence and National Security. Cambridge,MA,USA:BelferCenterforScienceandInternationalAffairs, 2017.

[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,'' Feb. 2022.

[10] Z. I. Khisamova, I. R. Begishev, and E. L. Sidorenko, ''Artificial intelli gence and problems of ensuring cyber security,'' Int. J. Cyber Criminol., 2019.

[11] J.-H. Li, ''Cyber security meets artificial intelligence: A survey,'' Frontiers Inf. Technol. 2018.

[12] S. A. A. Bokhari and S. Myeong, ''Use of artificial intelligence in smart cities for smart decision-making: A social innovation perspective,'' Sus tainability, 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] J. Singh, M. Sajid, S. K. Gupta, and R. A. Haidri, ''Artificial intelli gence and blockchain technologies for smart city,'' in Intelligent Green Technologies for Sustainable Smart Cities. Beverly, 2022,

[15]R.KhatounandS.Zeadally, ''Cybersecurity and privacy solutions in smart cities,'' Mar. 2017.

[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,'' Mar. 2021.

[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.

[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., Nov. 2021,

[19] J. Ju, L. Liu, and Y. Feng, ''Citizen-centered big data analysis-driven governance intelligence framework for smart cities,''

[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,'' Feb. 2023.

[21]S.U.Khan,N.Khan,F.U.M.Ullah,M.J.Kim,M.Y.Lee,andS.W.Baik, ''Towards intelligent building energy management: AI-based framework for power consumption and generation forecasting,'' Jan. 2023.

[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,'' Nov. 2021.

[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,'', Jul. 2022