1. 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.

2. INTRODUCTION

Cybersecurity has become a critical and vital topic that requires protecting the computer network from potential threats in today's modern world. A cyber-attack is a deliberate attack targeting computer networks, relevant data, programs, and electronic information, resulting in sub-national entities inciting violence towards non-combatant opponents. As technology develops, so do cyber threats, necessitating the development of new prevention strategies. It has been alleged that cyber-attacks have become more prevalent in the industrial sector, resulting in serious infrastructure damage and significant monetary loss. The rise of cyber-attacks among organizations is primarily due to the growing reliance on online technologies that enable the storage of personal and economic data.

Artificial intelligence (AI) applications can positively influence the cyber capabilities and national security of the sovereign nation, regional government entities, and non-state organizations. AI is a reliable technique for mitigating cyber-attack effects. AI is machine intelligence that executes activities connected with intelligence . Human professionals' expertise is integrated for strategic planning and decision-making , including making medical diagnoses and getting insights from expertise in concluding. In terms of cybersecurity, Zarina et al., have illustrated that AI has both beneficial and harmful effects, with the harmful effect of facilitating the instigation phase of cyberattacks, resulting in quicker and more devastating attacks. Looking forward, AI has the potential to greatly improve cybersecurity by increasing security precautions and promoting security in cyberspace. Furthermore, AI assists security experts in detecting cyber hazard symptoms and has enhanced the machine learning applications for malware classification and networked intrusion detection . Lastly, the modern phenomenon in AI has transformed innovative solutions and improved city external attacks against serious security threats.

A smart city provides multiple innovative solutions to several challenges that city administration faces. However, information and communication technology (ICT) has become a vital component of e-Government. Implementing ICT into a city's infrastructure introduces hazards and obstructions People frequently use insecure Wi-Fi networks to check their email messages, e-banking, and other digital services, uncovering themselves to cybercrimes including hacking, denials of service, and cracking. Cybersecurity applying technologies to protect e-Government services is among the most important distinctive features that can be utilized to categorize safe cities globally. Somewhere in this tendency, the 'inclusive smart

city' framework has triggered strong interest because it emphasizes the importance of interpersonal and social capital in urban initiatives that focus on stakeholders' inclusion in the Digital Realm and involving inhabitants in service improvement to implement appropriate government services that match citizens' necessities. Recent studies on e-services and technologies also have emphasized the importance of implementing a citizens-centered strategy for smart cities because it is expected to develop strong social ecologies that depend strongly on web technology. Consequently, web technologies and services can significantly impact stakeholder interactions .

Although previous literature demonstrated influence of AI in smart mobility , energy management, public services, climate change, and smart security in smart cities, cybersecurity has widely been neglected, especially in the context of stakeholders who use online government services. To fill this contextual gap, this study formulated the following research question:

- How AI applications used in smart cities influence cybersecurity directly?
- How AI applications used in smart cities influence e-Governance and e-Governance impacts cybersecurity directly?
- Does e-Governance play a mediating role between the relationship of AI applications and cybersecurity?

These main research questions are attempted to address empirically in this study, based on the premise that the interactions are context-dependent.

3. MOTIVATIONAND LITERATURE SURVEY

3.1 Motivation:

The motivation behind presenting this technical seminar report lies in the imperative need to address the pressing challenges of cybersecurity and e-governance in the context of rapidly evolving smart cities. The dawn of the digital era has given rise to a transformative wave of smart city development, where information technology and data-driven solutions are shaping urban landscapes. In this paradigm, e-governance stands as a pivotal element in redefining the interaction between citizens and their governing bodies. It promises efficient public service delivery, increased citizen engagement, and streamlined administrative processes. However, the transformative potential of e-governance is intricately linked with the security of digital systems, as the proliferation of digital platforms and the collection of vast amounts of data inherently elevate the risks of cyber threats. Cybersecurity breaches can disrupt critical city functions, compromise citizen privacy, and undermine the very principles of transparency and trust that e-governance aims to foster.

As smart cities continue to grow in number and scale, the fusion of e-governance and cybersecurity becomes both an opportunity and a necessity. The urgency of this topic cannot be overstated, given the exponential increase in cyberattacks targeting city infrastructure and services. Thus, the motivation for this technical seminar report is driven by the need to understand and address the intricate relationship between artificial intelligence, e-governance, and cybersecurity in the unique context of smart cities. By delving into these topics, we aim to equip individuals, administrators, and technology stakeholders with insights and knowledge necessary to build secure, efficient, and citizen-centric smart cities. In essence, this report serves as a call to action to harness the potential of AI in e-governance and to construct robust defenses that protect the future of smart cities and the well-being of their inhabitants.

3.2 Literature Survey:

The literature survey provides a comprehensive understanding of the intricate relationships between artificial intelligence (AI), e-governance, and cybersecurity in the dynamic landscape of smart cities. While smart cities hold great promise in terms of improved urban living, increased efficiency, and citizen engagement, they are also exposed to significant challenges in ensuring the security and privacy of digital systems and data. To navigate these complexities, a deep exploration of the existing knowledge base is essential.

E-governance, as one of the four pillars of e-government, refers to the use of information and communication technology (ICT) to enhance government operations, provide public services, and engage citizens in the decision-making process. The evolution of e-governance has been driven by its potential to improve administrative processes, increase transparency, and foster citizen participation. However, as noted in the research paper, e-governance's effectiveness is intrinsically linked to cybersecurity, making it a critical focus area.

The integration of AI in e-governance marks a transformative shift. AI-driven solutions are powering chatbots for citizen interactions, predictive analytics for resource allocation, and data-driven decision-making. The paper highlights the significance of AI in enhancing e-governance by analyzing its direct impact on cybersecurity, emphasizing its role in securing the vast amounts of data generated in e-governance processes.

The rise of smart cities has brought about new opportunities and vulnerabilities. The interconnected nature of smart city infrastructure, such as IoT devices, introduces a plethora of entry points for potential cyberattacks. The paper underlines the urgency of securing smart city environments, underscoring the importance of considering cybersecurity as an integral component of the smart city ecosystem.

The research paper presented a systematic analysis using Partial Least Squares Structural Equation Modeling (PLS-SEM) to assess the relationships between AI, e-governance, stakeholder involvement, and cybersecurity. The paper findings confirmed that AI plays a pivotal role in enhancing cybersecurity and e-governance. The mediating effect of e-governance and the moderating role of stakeholders were also identified, indicating that the relationships between these components are complex and interdependent.

4. OBJECTIVE

1.The primary objective is to develop a thorough understanding of the role of Artificial Intelligence (AI) in the realm of e-governance, focusing on how AI technologies are transforming public administration, citizen services, and governance structures in smart cities.

2.Investigate the significance of cybersecurity in the context of smart cities, recognizing the unique challenges and vulnerabilities that arise due to the digitalization and interconnected nature of urban environments.

3.Delve into the intricate relationships between AI, e-governance, and cybersecurity, as highlighted in the research paper, to discern the interdependencies, direct effects, mediating roles, and moderating influences among these components.

4.Recognize the importance of stakeholders' involvement and perspectives in shaping effective e-governance and cybersecurity strategies, considering their roles in ensuring the security and privacy of smart city systems.

5.Synthesize the knowledge gained from the literature survey and research findings to provide a holistic view of how AI, e-governance, and cybersecurity collectively contribute to the development and protection of smart cities.

6. Assess the future scope of this interdisciplinary field and the potential for further research and innovations in AI-driven e-governance and cybersecurity practices within smart cities.

5.TOPIC DESCRIPTION

5.1 E-Governance in Smart Cities

Definition and Significance:

E-Governance, or electronic governance, is the utilization of digital technology, primarily the internet and information and communication technologies (ICTs), in public administration and government operations. It involves transforming traditional governance processes into digital, data-driven, and citizen-centric approaches.

In smart cities, e-governance is pivotal for enhancing the delivery of public services, ensuring efficient urban management, and engaging citizens through digital platforms. Smart cities leverage technology to connect and streamline various municipal services, such as transportation, healthcare, education, and security.

Pillars of E-Governance:

The four pillars of e-governance are resources, processes, people, and technology (the 4Ts).

Resources: This pillar refers to the financial and human resources allocated for e-governance initiatives, ensuring the availability of funds, skilled personnel, and infrastructure.

Processes: It emphasizes reengineering existing administrative processes to align with digital systems, reducing paperwork, and enhancing efficiency.

People: Citizens and public officials are integral to the success of e-governance. It involves creating digital interfaces for citizen engagement and fostering digital literacy.

Technology: Advanced technology infrastructure, including data centers, connectivity, and software systems, forms the foundation of e-governance.

Challenges and Opportunities:

Challenges in implementing e-governance in smart cities include data security and privacy concerns, the digital divide, and resistance to change.

Opportunities encompass data-driven decision-making, improved citizen services, enhanced administrative efficiency, and sustainability through smart city initiatives.

5.2 Artificial Intelligence in Governance

Role of AI in E-Governance:

AI plays a transformative role in e-governance by automating routine tasks, enhancing data analysis, and enabling predictive decision-making. For instance, chatbots can provide instant responses to citizen inquiries, and machine learning can help predict and address urban challenges like traffic congestion.

It facilitates the creation of intelligent systems capable of understanding and responding to citizen needs.

AI Techniques and Applications:

AI encompasses various techniques, including machine learning, natural language processing (NLP), computer vision, and deep learning.

Applications range from virtual assistants for citizen services to data analytics for predicting trends and optimizing resource allocation.

Benefits and Concerns:

Benefits include increased efficiency, cost reduction, better services, and data-driven governance. AI enables predictive maintenance, real-time monitoring of urban services, and personalized services for residents.

Concerns revolve around data privacy, transparency, and ethical use. Collecting and processing vast amounts of data may pose privacy risks, and the 'black-box' nature of AI algorithms can raise concerns about fairness and accountability.

5.3 Cybersecurity in Smart Cities

Smart City Cybersecurity:

Cybersecurity in smart cities encompasses safeguarding digital infrastructure, data, and connected services against cyber threats. Smart cities are characterized by extensive data exchanges and interconnectivity, making them attractive targets for cyberattacks.

Cybersecurity Challenges:

Securing IoT Devices: The proliferation of Internet of Things (IoT) devices in smart cities introduces vulnerabilities that cybercriminals can exploit. Ensuring the security of these devices is a significant challenge.

Data Protection: Smart cities generate and process vast amounts of sensitive data. Protecting this data from breaches and ensuring privacy is a top priority.

Reliability of Digital Services: Smart cities rely on digital services for various functions, including transportation, healthcare, and energy management. Ensuring the uninterrupted availability and reliability of these services is a critical concern.

Evolving Threat Landscape: Cyber threats are continually evolving. Smart cities need to adapt to new attack vectors and tactics used by cybercriminals.

Strategies for Cyber Resilience:

Threat Detection and Prevention: Implementing robust threat detection systems and proactive prevention measures are essential to safeguard against cyberattacks.

Security Awareness Training: Promoting cybersecurity awareness among city officials, employees, and residents can help prevent security breaches.

Incident Response Plans: Smart cities should have well-defined incident response plans to mitigate the impact of cyber incidents promptly.

5.4 Interplay of AI, E-Governance, and Cybersecurity

Direct Effects:

Enhancing Administrative Efficiency: AI can automate repetitive administrative tasks in e-governance, reducing human error and enhancing efficiency in public service delivery.

Predictive Decision-Making: AI enables predictive analytics, which helps government agencies anticipate issues and allocate resources more effectively.

Mediating Role of E-Governance:

Governance Framework: E-governance plays a pivotal role in shaping how AI technologies are incorporated into public administration. It influences decision-making, data management, and service delivery.

Moderating Effect of Stakeholders:

Public Sector Stakeholders: Government officials and agencies influence policies, regulations, and the deployment of AI for e-governance and cybersecurity.

Private Sector Stakeholders: Industry representatives, technology providers, and businesses have a stake in ensuring that smart city initiatives align with security and governance standards.

Citizen Engagement: Citizens' involvement and feedback influence the direction of smart city projects, including those related to AI, governance, and cybersecurity.

Implications of the Interplay:

Data-Driven Governance: The combination of AI, e-governance, and cybersecurity leads to data-driven governance practices. Decision-makers have access to real-time data and predictive insights for informed decision-making.

Enhanced Security: AI and e-governance together bolster cybersecurity by automating security processes, identifying threats early, and enhancing incident response capabilities.

6. CONCLUSION

The current study examined artificial intelligence applications to overcome cybersecurity challenges. The research findings indicate that artificial intelligence is progressively converting into an indispensable technology to enhance information security performance. Individuals are not capable anymore of fully secure project-level cyberattacks, and artificial intelligence offers the desired analytics and threat intelligence that security practitioners might use to minimize the likelihood of an infringement and strengthen the security structure of an enterprise. Since more technologies are introduced into the usual human lifestyle, the impact of artificial intelligence on daily human life may intensify. Several scholars assert that AI will have a catastrophic influence on technological development, whereas others have a contradictory assumption of AI applications' positive effect on everyday human life. One of the major features of cloud computing in cybersecurity is the capacity to evaluate and eliminate risk faster. Several individuals are concerned about cybercriminals' capability to perform incredibly advanced cyber and technological attacks. Moreover, artificial intelligence can contribute to the detection and classification of hazards, the structuring of incident management, and the detection of cyberattacks before their occurrence. Consequently, despite potential negatives, artificial intelligence would contribute to the evolution of cybersecurity and support enterprises in establishing an enhanced security strategy.

7. Questions Asked by Experts

1. How does the integration of AI and e-governance benefit smart cities in terms of public service delivery?

   Ans: The integration of AI and e-governance enhances smart cities' public service delivery by automating processes, increasing efficiency, and personalizing services, ultimately improving the citizen experience.

2. What are the key cybersecurity challenges specific to smart cities, and how can AI assist in addressing these challenges?

   Ans: Smart cities face unique cybersecurity challenges due to their interconnected nature. AI helps by detecting and mitigating threats, ensuring data security, and enhancing overall resilience.

8. REFERENCES

[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.

[2] M. Komar, V. Kochan, L. Dubchak, A. Sachenko, V. Golovko, S. Bezobrazov, et al., "High performance adaptive system for cyber attacks detection", *Proc. 9th IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst. Technol. Appl. (IDAACS)*, vol. 2, pp. 853-858, Sep. 2017.

[3] 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.

[4] 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.

[5] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, et al., "Artificial intelligence in cyber security: Research advances challenges and opportunities", *Artif. Intell. Rev.*, vol. 55, pp. 1029-1053, Feb. 2022

[6] 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, pp. 620, Jan. 2022.

[7] 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, pp. 317-330, 2022