SMARTER BANKING CHATFIN

[1]MR. T.SRINIVASULU, [2]VANKE AMRUTHA LAKSHMI, [3]REBBAVARAPU KAVYA, [4]PASUPULETI PRAVEEN, [5]M VIJAY

[1](ASSISTANT PROFESSOR), [2345]B.TECH STUDENTS
DEPARTMENT OF CSE, RISE KRISHNA SAI PRAKASAM GROUP OF INSTITUTIONS

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 nationstates,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 becontext-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. Theresults 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 stakeho

1.INTRODUCTION

Cybersecurity has become a critical and vital topic that requires protecting the computer network from potential threats in today's modern world [1], [2]. A cyber-attackis 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 [3], [4]. 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 [5]. Consequently, it is acknowledged as perhaps the mostcritical problem in the modern context because it create seconomic loss and discloses confidential information. Cyber attacks include phishing, denial of service, malware, and ransom ware infestations, which can harm anybody in society[6]. Cyber-attacks also have a significant psychological impact on humans, producing unhappiness, tension, and stress among people [7]. Artificial intelligence (AI) applications can positively influence the cyber capabilities and national security of the sovereign nation, regional government entities, and non-state organizations [8], [9]. AI is a reliable technique for mitigating cyber-attack effects [10]. AI is machine intelligence thatexecutes activities connected with intelligence [11]. Human professionals' expertise is integrated for strategic planning and decision-making [12], including making medical diagnoses and getting insights from expertise in concluding. In terms of cybersecurity, Zarina et al., [10] have illustrated that AI has both beneficial and harmful effects, with the harmful effect of facilitating the instigation phase of cyber attacks, 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 [13]. Lastly, the modern phenomenon in AI has transformed innovative solutions and improved city external attacks against serious security threats [14].

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 [15]. People frequently use insecure Wi-Fi networks to check their email messages, e-banking, and other digital services, uncovering themselves to cyber crimes including hacking, denials of service, and cracking. Cyber security applying

technologies to protect e-Government services is among the most important distinctive features that can be utilized to categorize safe cities globally [16].Somewhere in this tendency, the 'inclusive smart city' frame work 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 [17], [18]. Recent studies on e-servicesand 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 stake holder interactions [19] Although previous literature demonstrated influence of AI in smart mobility [20], energy management [21], public services [22], climate change [23], and smart security [24]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 influencee-Governance and e-Governance impacts cybersecurity directly?

• Does e-Governance play a mediating role between the
relationship of AI applications and cybersecurity?

• Additionally, this study examines the moderating role of stakeholders' involvement in the relationship between AI and e-Governance and on the relationship betweene-Governance and cybersecurity.

These main research questions are attempted to address empirically in this study, based on the premise that the interaction sare context-dependent. Figure 1 explains the channel of the study's proposed framework to classify cyber security level in a smart city. The moderating significance of stakeholder involvement was systematically examined byusing structural equational modeling (SEM) in SmartPLS 4.0.PLS-SEM path modeling was selected as the analytical toolbecause of its widespread utilization in examining researchframeworks in prior studies and its acknowledged

appropriateness for analyzing complex research models.

MODULES

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Browse and Train & Test Data Sets, View Trained and Tested Datasets Accuracy in Bar Chart, View Trained and Tested Datasets Accuracy Results, View Prediction Of Cyber Attack Type, View Prediction Of Cyber Attack Type Ratio, Download Predicted Data Sets, View Cyber Attack Type Ratio Results, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN,PREDICT CYBER ATTACK TYPE, VIEW YOUR PROFILE

2.LITERATURE SURVEY

A. Cybersecurity Challenges in Smart Cities

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 [25]. An illustration of a smart city can be outlined by using several fundamental elements, as exemplified

Smart government comprises various aspects such as smart office, smart supervision, smart services, and smart decision-making to enhance the performance of city governance and optimize the life

standard of citizens by establishing a bilateral collaboration between the government and citizens [26]. Smart public services offer various electronic information and online services to enhance the standard of living and satisfaction of the public, thereby developing the perception of a service-oriented government. The evolution of a smart economy can facilitate the smooth development of resource driven cities, enhance the efficiency of urban economies, and generate sustainable employment opportunities [27]. Smart healthcare systems that utilize e-health records to forecast the individual's health, like remote tracking of individuals with cardiac disease, has the potential to assess the state of vulnerability and furnish essential information for optimal treatment [28]. Smart education is a concept that involves using data-centric intelligent education in different contexts in smart cities to deliver individuals a smooth educational experience with customized individual assistance [29]. Smart buildings that effectively apply different information. The building is capable of satisfying the necessities of its users and residents, as well as identifying any defects in its operation. Buildings with features such as security, flexibility, ease of use, and efficiency are extremely attractive [30]. Smart transport systems are multifaceted and digitally managed to help with urban development and decision-making, thereby organizing smart transportation. Strategic travel scheduling can be achieved by the use of route projection and real-time roadway state monitoring [31]. Smart Security offers an assortment of benefits including detection, alarm, emergency assistance, and other functions pertaining to personal protection of individuals and safeguarding cybersecurity [32].

It is well-established that various infrastructure systems, including energies, grid system, healthcare, traffic, transportation, water distribution, and wastewater disposal, are furnished with computer networks. The use of Internet of Things has resulted in the emergence of smart cities, which aim at improving their facilities and developing more sophisticated, effective, and eco-friendly solutions. Nonetheless, a study ABI Research has projected that by 2024, barely 44% of the overall cybersecurity expenses for critical systems will be assigned to sectors such as healthcare, security, water, transport, and other related areas, leading to a significant lacking funding for protecting infrastructure against cybersecurity risks [33].

Consequently, there is a likelihood of various challenges involving cyber-attacks on crucial urban infrastructure, resulting in serious repercussions including the act of hijacking infrastructure communication and encrypting malware to disable computer systems has the potential to significantly impact the financial security of a city, resulting in substantial losses to both the finances and assets of inhabitants. Similarly, the disruption or destruction of communication systems, power grids, water conservation mechanisms, and other facilities can destroy the social system and cause an outbreak of a state of anxiety. Moreover, interfering with sensor data for creating a situation of chaos, such as in disaster detection technologies, and stealing of crucial information such as people, healthcare, customers, and private information.

B. Artificial Intelligence and Cybersecurity

Every nation on the planet necessitates security for economic progress and political stability. The advanced economies invest heavily in intelligence to safeguard their strategic interests and legitimacy in the face of terror threats. They confront high vulnerabilities, and new technologies may enhance security inside the state's sensitive zones [34], [35]. AI contributes to eliminating physical interaction, increasing the probability of operations detecting extremist threats at multiple stages. Different aspects of computation require security improvements from AI devices to monitor the specific regions' security, including technological infrastructure and data security. The US emphasizes the intelligence program's applications with the support of augmenting defense installations, and it has proved effective in counterterrorism. It is suggested that the usage of artificial intelligence is a significant point in enhancing security mechanisms in strategic industries, including public treasury centers and airport terminals [36]. The security challenges seem critical, driving the US to formulate a strategy toward future AI technologies that will support the elimination of all complications associated, including the curtailing of terrorist organizations' routine activities [37].

Several prior research has explored the significance of artificial intelligence in detecting and preventing cyberattacks [38], combating terrorism [39], enhancing security in strategic sectors [36], and

building resilience in vulnerable sovereign places [34]. Soni [35] stated in his study that Information obtained from a broad selection of scientific and engineering specialists suggests that AI development depends on the United States capabilities to reconcile the advantages and disadvantages of AI, specifically in cybersecurity. AI is universally perceived among the most impressive technologies of the digital world, and cybersecurity is undoubtedly the domain that might benefit greatly from it. Optimization algorithms, strategies, devices, and companies providing AI-based solutions are evolving in international security markets [40]. It is emphasized that privacy and public security constitute critical concerns in smart cities which require additional legislative, technological, and administrative attention. Combating cybercrime in smart cities is essential for making this technology as advantageous and credible as possible for community acceptance. All stakeholders, particularly legislators, administrations, judicial systems, power companies, telecom firms, automobile manufacturers, cloud hosting, research institutes, and industries, will have to continue their assistance and endeavors [15]. Following previous literature, we propose our hypothesis:

Hypothesis 1: Artificial intelligence applications in smart cities affect cybersecurity positively

C. Mediating Role of E-Governance

E-governance is a revolutionary system implemented by a city government that applies AI and ICT to interconnect public bodies and corporate enterprises. To ensure maximum e-Government services and security for the public and other stakeholders, numerous governments have attempted to implement e-Governance [15]. Nonetheless, most citizens are anxious about their privacy and security while utilizing e-Government facilities, as per a 2014 UN e-Government survey [41]. Concerning security, the primary obstacles that e-Government should address are secrecy, integrity, and accessibility. Indeed, e-Governance security comprises standard security apparatus (verification, privacy, reliability, and accessibility), with a stronger reliance on information security and economic growth planning. The official statement of the European initiative, “Security of eGovernment Systems,” outlined 11 policies and procedures for security [20]. This initiative focused on security in e-Governance by developing a “Privacy by Design” technical expertise,

encouraging professional and procedural measures to ensure privacy, and providing security effect evaluations of e-Government technology obligatory and accessible.

Artificial intelligence (AI) has revolutionized the way corporations work; several municipalities have begun to incorporate AI into everyday operations, yet there seem to be a substantial number of nations that would not get an advantage using Artificial intelligence and machine learning. E-voting, e-decision making, and e-participation are prominent phenomena. However, the level of adoption of e-services varies substantially across countries. Despite such advancements, governments may not benefit from e-decision making, yet the United Nations recognizes it as a critical concern [42]. AI adoption by government agencies is rising, with the United States of America and China gaining ground. Countries gain from AI in various domains, including healthcare, mobility, education, security, telecommunications, and defense services [43]. E-governance is categorized into four major brackets: governments, population, commerce, and workforce, all of which are interconnected. Every component can use one of several frameworks to incorporate e-Governance. Cybersecurity includes safeguarding network servers, storage systems, and software applications and employing appropriate technology [44]. The emergence of the e-Governance approach necessitates a complex and resilient cybersecurity strategy based on examining previous literature. Cybersecurity is therefore identified as one of the most critical domestic, regional, and national challenges. It restricts data breaches and promotes numerous users' security and privacy [15], [38], [45]. Hence, we propose our hypotheses based on previous literature as follows:

Hypothesis 2: Artificial intelligence applications in smart cities contribute to e-Governance positively

Hypothesis 3: E-Governance execution in smart cities affect cybersecurity positively

Hypothesis 4: E-Governance mediates between artificial intelligence and cybersecurity positively

3. EXISTING SYSTEM

Smart city is a captivating concept characterized by its intelligent features. Its scope extends beyond improving the levelof urban economic efficiency and the reduction

of costs and resource consumption. Rather, it encompasses the integration of different components of the city through intelligent gad gets 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 forcitizens [25]. An illustration of a smart city can be outlined by using several fundamental elements, as exemplified in Figure 2.Smart government comprises various aspects such assmart office, smart supervision, smart services, and smart decision-making to enhance the performance of city governance and optimize the life standard of citizens by establishing a bilateral collaboration between the government and citizens [26]. Smart public services offer various electronic information and online services to enhance the standard of living and satisfaction of the public, thereby developing the perception of a service-oriented government. The evolution of a smart economy can facilitate the smooth development of resource driven cities, enhance the efficiency of urban economies, and generate sustainable employment opportunities[27]. Smart healthcare systems that utilize e-health records to forecast the individual's health, like remote trackingof individuals with cardiac disease, has the potential to assess the state of vulnerability and furnish essential information for optimal treatment [28]. Smart education is a concept that involves using data-centric intelligent education in different contexts in smart cities to deliver individuals asmooth educational experience with customized individual assistance [29]. Smart buildings that effectively apply different in formation. The building is capable of satisfying the necessities of its users and residents, as well as identifying any defects in its operation. Buildings with features such assecurity, flexibility, ease of use, and efficiency are extremely attractive [30]. Smart transport systems are multifacetedand digitally managed to help with urban development and decision-making, thereby organizing smart transportation. Strategic travel scheduling can be achieved by the use of route projection and real-time roadway state monitoring [31].Smart Security offers an assortment of benefits including detection, alarm, emergency assistance, and other functions pertaining to personal protection of individuals and safeguarding cybersecurity [32]. It is well-established that various infrastructure systems, including energies, grid system, healthcare, traffic,

transportation, water distribution, and wastewater disposal, are furnished with computer networks. The use of Internet of Things has resulted in the emergence of smart cities, which aim at improving their facilities and developing more sophisticated, effective, and eco-friendly solutions. Nonetheless,a study ABI Research has projected that by 2024, barely 44%of the overall cybersecurity expenses for critical systems will be assigned to sectors such as healthcare, security, water, transport, and other related areas, leading to a significant lacking funding for protecting infrastructure against cyber security risks [33]. Consequently, there is a likelihood of various challenges involving cyber-attacks on crucial urban infrastructure, resulting in serious repercussions including the act of hijacking infrastructure communication and encrypting malware to disable computer systems has the potential to significantly impact the financial security of a city, resultingin substantial losses to both the finances and assetsof inhabitants. Similarly, the disruption or destruction ofcommunication systems, power grids, water conservation mechanisms, and other facilities can destroy the social system and cause an outbreak of a state of anxiety. Moreover, interfering with sensor data for creating a situation of chaos, such as in disaster detection technologies, and stealing ofcrucial information such as people, healthcare, customers, and private information. Several prior research has explored the significance of artificial intelligence in detecting and preventing cyberattacks[38], combating terrorism [39], enhancing security instrategic sectors [36], and building resilience in vulnerable overeign places [34]. Soni [35] stated in his study that Information obtained from a broad selection of scientific and engineering specialists suggests that AI development depends on the United States capabilities to reconcile the advantages and disadvantages of AI, specifically in cybersecurity. AI is universally perceived among the most impressive technologies of the digital world, and cybersecurity is undoubtedly the domain that might benefit greatly from it. Optimization algorithms, strategies, devices, and companies providing AI-based solutions are evolving in international security markets[40]. It is emphasized that privacy and public security

constitute critical concerns in smart cities which require additional legislative, technological, and administrative attention. Combating cybercrime in smart cities is

essential for making this technology as advantageous and credible as possible for community acceptance. All stakeholders, particularly legislators, administrations, judicial systems, power companies, telecom firms, automobile manufacturers, cloudhosting, research institutes, and industries, will have to continue their assistance and endeavors [15].

Disadvantages

• The complexity of data: Most of the existing machine learning models must be able to accurately interpret large and complex datasets to detect Cybersecurity.

• Data availability: Most machine learning models requirelarge amounts of data to create accurate predictions. If data is unavailable in sufficient quantities, then model accuracy may suffer.

• Incorrect labeling: The existing machine learning modelsare only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

3.1 PROPOSED SYSTEM

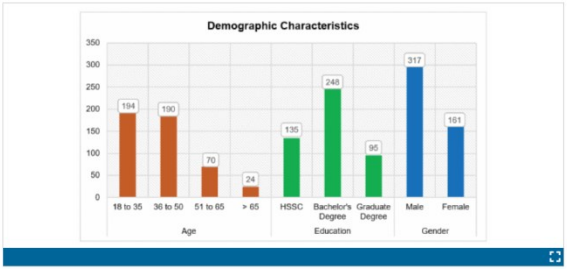
The primary objective of the proposed system is to investigate the relationship between artificial intelligence and cybersecurity, performing e-Governance as a mediator and stake holders' involvement as a moderator. A longitudinal research methodis conducted to investigate the hypothesis derived from thisstudy and ascertain the findings. It comprises a study into perceptions of the importance of AI in cybersecurity in smartcities. The primary data for this study was collected from478 respondents through a survey questionnaire distributed via emails and online through several social media networks.

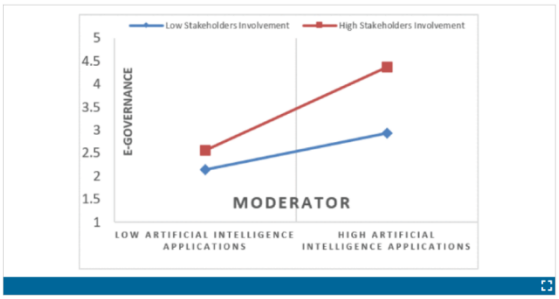
Respondents were adequately explained about answers and were encouraged to respond to the questionnaire with utmost honesty, that may minimize issues about potential bias. Lastly, participants might opt out of the survey at any moment.

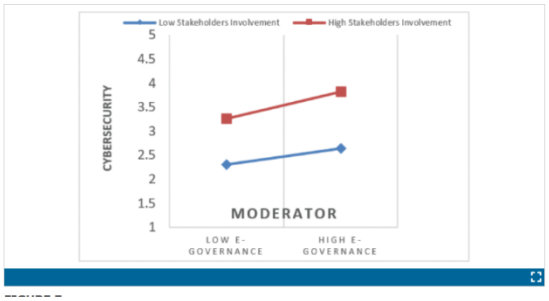
Advantages

- Artificial intelligence applications in smartcities contribute to e-Governance positively.
- E-Governance execution in smart cities affect cybersecurity positively.
- E-Governance mediates between artificial intelligence and cybersecurity positively.
-

4. OUTPUTSCREENS







5. 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 cap able anymore of fully secure project-level cyber attacks, and artificial intelligence offers the desired analytics and threat intelligence that security practitioners might use to minimize the likelihood of an infringement and strengthen thesecurity structure of an enterprise. Since more technologies 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 cyber attacks before their occurrence. Consequently, potential negatives, artificial intelligence would contribute to the evolution of cybersecurity and supportenterprises in establishing an enhanced security strategy.

This study further sought to investigate artificial intelligence and its ongoing development in offering e-government services and then highlight the need to accommodate strategies regarding cybersecurity for adopting innovative social and technical processes in government serving the community. The eventual objective of smart city governments isto establish and strengthen relationships with

most stakeholders, as their involvement strengthens e-government efficacy which fortifies cybersecurity. Public services should be administered using innovative AI technologies and e-governance in convenient modes to eliminate the barriers between stakeholders and city governments, while state official scan still sustain the model for better support. Whilee-government is progressing, the citizens and those in authority or advocating mechatronics are lagging. That creates disparities in cybersecurity standards for something in the virtual environment, potentially turning performance into a much more difficult experience with several grooves to monitor. With an elevation in the initiatives identified in this research, stakeholders' involvement and awareness ofe-governance and cybersecurity may rise, enabling benefits associated with the virtual environment.

6. REFERENCE

[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] 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] 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 incidents,'' Elektrotechnik Informationstechnik, vol. 132, no. 2, pp. 106–112, Mar. 2015.

[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] 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.