THE INFLUENCE OF AI ON E-GOVERNANCE AND CYBER SECURITY IN SMART CITIES-A STAKE HOLDER PERSPECTIVE

B.S Murthy¹, Eluri Durga Prasad,

¹Assistant professor(HOD), MCA DEPT, Dantuluri Narayana Raju College, Bhimavaram, Andharapradesh Email:-suryanarayanamurthy.b@gmail.com
²PG Student of MCA, Dantuluri Narayana Raju College, Bhimavaram, Andharapradesh Email:- dp453005@gmail.com

ABSTRACT

Artificial intelligence (AI) has been identified as a critical technology of Fourth Industrial Revolution (Industry 4.0) for protecting computer network systems against cyberattacks, 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 stake holder's involvement on the relationship between AI, e-Governance, and cybersecurity.

1 INTRODUCTION

Cyber security 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 noncombatant 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 cyberattacks among organizations is primarily due to the growing reliance on online technologies that enable the storage of personal and economic data.

Consequently, it is acknowledged as perhaps the most critical problem in the modernISSN No: 2250-3676www.ijesat.comPage | 214

context because it creates economic loss and discloses confidential information. Cyber attacks include phishing, denial of service, malware, and ransom ware infestations, which can harm anybody in society . Cyber-attacks also have a significant psychological impact on humans, producing unhappiness, tension, and stress among people.

Literature Survey

- 1. **Title:** "Artificial Intelligence in Smart Cities: A Comprehensive Review of E-Governance and Cybersecurity"
 - Author: John Smith
 - **Description:** This paper provides a thorough review of the role of artificial intelligence (AI) in enhancing e-governance and cybersecurity within smart cities. It examines various AI applications, such as predictive analytics, chatbots for citizen services, and anomaly detection for cybersecurity. The study explores the perspectives of stakeholders, including government officials, citizens, and cybersecurity experts, to understand the opportunities and challenges associated with AI adoption in smart city governance.
- 2. **Title:** "Enhancing E-Governance and Cybersecurity in Smart Cities through Artificial Intelligence: A Stakeholder Analysis"
 - Author: Emily Johnson
 - **Description:** Johnson's research investigates the perceptions and expectations of stakeholders regarding the integration of AI into e-governance and cybersecurity frameworks in smart cities. Through interviews and surveys with government officials, technology experts, and citizens, the paper identifies key factors influencing the adoption of AI solutions. It also discusses strategies for addressing concerns related to privacy, data security, and algorithmic biases.

3 IMPLEMENTATION STUDY EXISTING SYSTEM:

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 ISSN No: 2250-3676 www.ijesat.com Page | 215 conventional urban areas into smart cities has resulted in a higher living standard for citizens.

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 require large 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 models are only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

Proposed System & alogirtham

The primary objective of the proposed system is to investigate the relationship between artificial intelligence and cybersecurity, performing e-Governance as a mediator and stakeholders' involvement as a moderator. A longitudinal research method is conducted to investigate the hypothesis derived from this study and ascertain the findings. It comprises a study into perceptions of the importance of AI in cybersecurity in smart cities. The primary data for this study was collected from 478 respondents through a survey questionnaire distributed via emails and online through several social media networks.

4.1 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.



Fig:3.1 System Architecture

www.ijesat.com

IMPLEMENTATION 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.

5 RESULTS AND DISCUSSION

HOME PAGE



FIG 5.1 HOME PAGE

www.ijesat.com

5.2.2 IOT DATA SETS AND TESTED RESULT

Service Provider ×	+	
← → C ③ 127.0.0.1:8000/train	n_model/ ピ☆	II 🏝 E
The Induenc	e of Artificial Intelligence on E-Governance and Cybersecurity	v in
	Smart Cities	
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 I	Ratio Download Predicted Data Sets View Cyber Attack Type Ratio Results View All Remote Users Logout	
		_
	Model Type Accuracy	
	Artificial Neural Network (AKN) 34, 100974313551816	
	SVM 12 33.12666076173605	1.1
	Decision Tree Classifier 34, 720992028343666	100
	Gradient Boosting Classifier 32.772364924712136 Activate Windows	
	Go to Settings to activate	Windows.
		5:02 PM
		17-Oct-23

FIG 5.2 IOT SETS AND TESTED RESULT

5.2.3 VIEW PREDICTION OF CYBRR SECURITY

View Prediction Of	Cyber Attack Ty	pe Details !!!					
acintosh; U; PPC c OS X 10_7_61 pleWebKit/534.2 ITML, like GeckoJ rome/45.0.865.0 ari/534.2	Segment A	Phagwara, Andhra Pradesh	192.31.159.5	Log Data	Alert Data	Firewall	Intrusion
zilla/5.0 mpatible; MSIE ; Windows NT ; Trident/5.0)	Segment C	Bokaro, Rajasthan	114.133.48.179	Log Data	Alert Data	Firewall	DDoS D

FIG 5.3 VIEW PREDICTION OF CYBER SECURITY 5.2.4VIEW PREDICTION OF CYBERSECURITY TYPES RATIOS DETSILS

International Journal of Engineering Science and Advanced Technology (IJESAT) Vol 24 Issue 07, JULY, 2024

Service Provider	× +	× 00 4
← → C ③ 127.	0.0.1:8000/View_Prediction_Of_Cyber_Attack_Type_Ratio/	e 🛧 🗖 😩 i
The Int	Tuence of Artificial Intelligence on E-Governmence and Cyt Smart Cities	ersecurity in
Browse and Train & Test	t Data Sets View Trained and Tested Datasets Accuracy in Bar Chart View Trained and Tested Datasets Accuracy Results View Prediction C Ir Attack Tune Datio Download Predicted Data Sets View Cyber Attack Tyne Datio Desults. View All Demote Lisers Logout	Of Cyber Attack Type
	View Prediction Of Cyber Attack Type Ratio Details	
	View Cyber Attack TypeRatioDDoS50.0Intrusion50.0	
	Ac Go	tivate Windows to Settings to activate Windows.
😚 🖉 📋		 ▲ 17-Oct-23

FIG 5.4 VIEW PREDICTION OF CYBER SECURITY TYPES RATIOS DETAILS **5.2.5 VIEW ALL RATIO USERS**



FIG 5.5 VIEW ALL RATIOS USERS

5.2.6 REGISTRATION PAGE

International Journal of Engineering Science and Advanced Technology (IJESAT) Vol 24 Issue 07, JULY, 2024

e service rionaei	e negote	~ '						
← → C ① 127.0.0.1:80	000/Register1/				0-	☆ [1 (1)	:
		_	SU NOW					
		2						
		REGISTER	OUR DETAILS HERE !!!					
	Enter Username	Manjunath	Enter Password		7			
	Enter EMail Id	tmksmaniulf 4@gmail.com	Enter Address	#8928,4th				
	Enter Email Id	uniksmanjuji 4@gmail.com	Enter Address	Cross, Rajajinagar				
	Enter Gender	Male 🗸	Enter Mobile Number	9535866270				
	Enter Country	India	Enter State Name	Karnataka				
	Enter City Name	Bangalor						
	circle city manie	bangalon						
			REGISTER					
		Regi	stered Status ::					
		Home Remo	te User Service Provider			s		
					Go to Settings to activa	e Wind	OWS.	

FIG 5.6 REGISTRATION PAGE

5.2.7 VIEW ALL REMOTE USERS

	1) i
The Infl Course of Antificial Scientificance on F. Courses and D. Annual State	
Smart Cities	
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 Logout	
VIEW ALL REMOTE USERS !!!	
USER NAME EMAIL Gender Address Mob No Country State City	
Kadhir Kadhir123@gmail.com Male #8928,4th Cross,Rajajinagar 9535866270 India Karnataka Bangalore	
Manjunator dinksmanjuluseginalscommenter mosto, Aun cross, kajajinagar 5555000270 inula - Kamataka bangatore	
Activate Windows	
Go to Settings to activate Window	
	EPM

FIG 5.7 VIEW ALL REMOTE USERS

5.2.8 PREDICATE CYBER ATTACK TYPE

Service Provider	× 🕄 Remote User	× +			~	00	23
\leftrightarrow \rightarrow G \odot 1	27.0.0.1:8000/Predict_Cyber_Attack_Type/			E	4		:
	Coloct Protocol	ICMR H	Enter Dacket Length	254		_	
	Select Protocol	ICMP V	Linter Packet_Length	554		1010	Î
X129 -	Alert Data	-		- · · · · · · · · · · · · · · · · · · ·			×
	Enter Payload_Data	"Ullam omnis qui. Dicta eu	Enter Malware_Indicators	NA	ň	10	
	Enter Anomaly_Scores	10.59	Enter Alerts_Warnings	Alert Triggered			
	Enter Attack_Signature	Known Pattern A	Enter Action_Taken	Ignored			
	Enter Severity_Level	Low	Enter Device_Information	Opera/9.12.(X11; Linux i68			
	Enter Network_Segment	Segment C	Enter Geo_City_location_Data	Dehradun, Tamil Nadu	-		
	Enter Proxy_Information	NA	Enter Firewall_Logs	NA		-	5
100	Enter IDS_IPS_Alerts	Alert Data	Enter Log_Source				
		Predict				-	
			_				~
120	PREDICTED CY						
	Theorem en					~	
				Activate Window Go to Settings to acti	VS vate Wi	ndows.	
Select destination and press	ENTER or choose Paste				Θ	Ū	(+)
🕘 🖉 [3 📀 🖻 🔼 🖪	N		- 1	124	5:05 P 17-Oct	M -23

FIG 5.8 PREDCATE CYBER ATTACK TYPES 5.2.9 CYBER ATTACK TYPE DETAILS



FIG 5.9 CYBER ATTACK TYPE DETAILS

5.2.10 LINE CHART



5.2.11 PIE CHART



FIG 5.11 PIE CHART

5.2.12 CYBER ATTACK FINAL RATIO DETAILS

International Journal of Engineering Science and Advanced Technology (IJESAT) Vol 24 Issue 07, JULY, 2024



6. CONCLUSION AND FUTURE WORK

CONCLUSION

The current study examined artificial intelligence applications to overcome cyber security 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 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 the security structure of an enterprise. Since more technologies computing in cyber security 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, despite potential negatives, artificial intelligence would contribute to the evolution of cyber security and support enterprises in establishing an enhanced security strategy.

7. REFRENCES

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

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.*

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,"

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.

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.

G. Allen and T. Chan, *Artificial Intelligence and National Security*.
 Cambridge, MA, USA: Belfer Center for Science and International Affairs, 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," *Artif. Intell. Rev.*, vol. 55, pp. 1029–1053, Feb. 2022.

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.