Implementing AI Techniques for Combating Cybercrimes in Political Science and Management

Gunawan Widjaja, Sridevi J, S. Rama Sree, Dr.A.Jasmine*, Dr Melanie Lourens

Universitas pancasila, widjaja_gunawan@yahoo.com

Vel Tech Rangarajan,Dr.Sagunthala R&D Institute of science and technology, phoneixsridevi1@gmail.com

Department of CSE,Aditya Engineering College,Surampalem. ramasree_s@aec.edu.in

Associate Professor of Commerce,TBAK College for Women,Kilakarai

Affiliated to Alagappa University Karaikudi. carolinejas621@gmail.com

Deputy Dean Faculty of Management Sciences,Durban University of Technology South Africa

melaniel@dut.ac.za,Orcid: 0000-0002-4288-8277

Abstract:

In today's environment, artificial intelligence plays major role in every field .Political science and management are only two of the many professions that have seen opportunities and challenges resulting from the quick development of digital technologies. The threat of cybercrimes has evolved into a severe issue as our reliance on digital platforms and information systems keeps growing. In order to combat cybercrimes in the fields of political science and management, this research paper will examine the application of artificial intelligence (AI) techniques in those fields. The study explores how AI might be used to identify, stop, and respond to cyber threats while simultaneously addressing the drawbacks and moral questions raised by various implementations.

Keywords:Cyber crime ,Artificial Intelligence, Cyber security ,Politics ,thread detection ,data privacy.

DOI: 10.48047/ecb/2023.12.8.716

Introduction:

Political science and management are affected by this technological change, as digital platforms are essential for facilitating organizational, decision-making, and governance processes. While these developments have opened up previously unimaginable doors for productivity and communication, they have also shown weaknesses that malevolent actors exploit, fueling the ever-increasing threat of cybercrimes. Cybercrimes, which include a broad range of illegal behaviors carried out online, have grown to be a serious threat to the security and stability of political systems and business operations. The potential impact of cyber attacks is expanding as the globe becomes more linked through the internet and digital platforms.

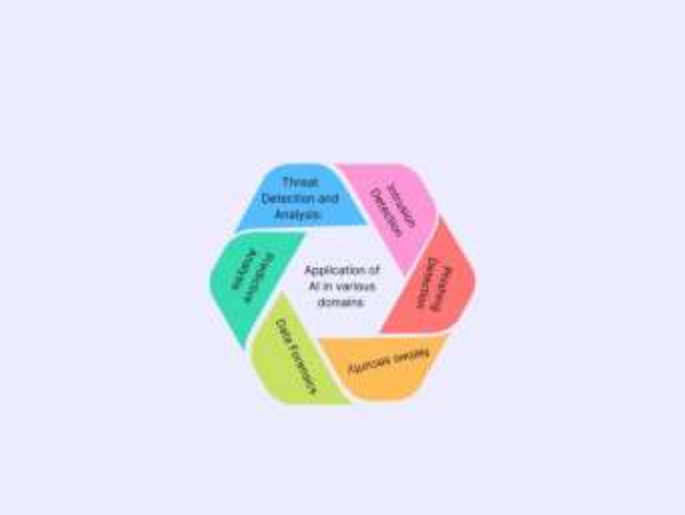

Fig1: Application of AI in various domains

Introduction:

In the digital age, where information and communication technologies are deeply interwoven in every part of our lives, the rise of cybercrimes has become a critical concern for both the management and political science professions. Thanks to the unmatched connectivity offered by the digital world, a new type of criminal behavior has evolved that transcends geographical limits and traditional investigative approaches. Utilizing the potential of artificial intelligence (AI) solutions is essential to combating these rapidly emerging dangers. To uncover weaknesses, cybercriminals continuously adapt their strategies. This research study examines how the intersection of artificial intelligence, political science, and management might alter the prevention, detection, and mitigation of cybercrimes in both political and managerial contexts.

In the context of political science and management, the application of AI tools, such as machine learning, data analytics, and pattern recognition, holds enormous promise for preventing cybercrimes. AI-driven solutions give users the capacity to instantly evaluate massive amounts of data, quickly spotting anomalies and potential hazards that could have escaped notice using more traditional techniques. AI systems can proactively predict and repel cyber threats by continuously adapting to changing techniques and learning from prior attack patterns. This shifts cyber security from a reactive to a proactive discipline. Additionally, applying AI techniques to risk management and policy implementation could improve decision-making processes and better allocate resources for preventing and mitigating cybercrimes.

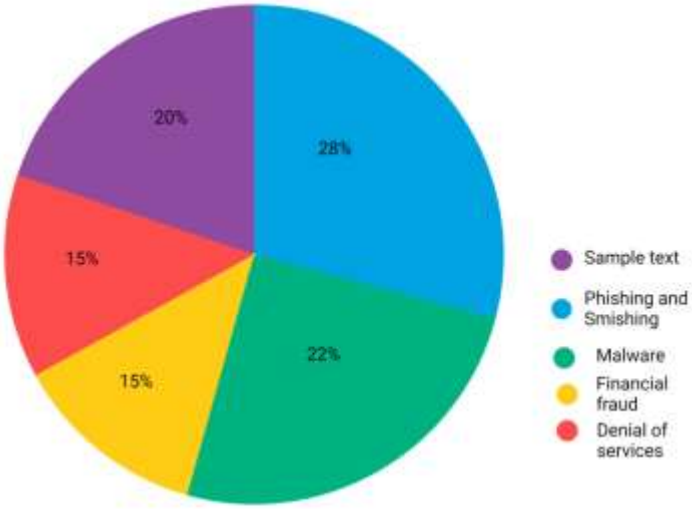

Fig :types of cyber crime happens in 2022

However, using AI to fight cybercrime is not without its difficulties. A balanced strategy is required to fully realize the potential of artificial intelligence because of ethical issues with data privacy, algorithmic bias, and unforeseen repercussions. Additionally, there is a lack of qualified experts who can create, implement, and manage AI-driven cyber security systems, which emphasizes how urgent it is for academia, business, and government organizations to work together. This research study aims to shed light on the prospects, challenges, and implications of this revolutionary journey towards a safer digital landscape by investigating the various aspects of applying AI approaches for combating cybercrimes in political science and management.

Literature review:

Ramanpreet Kaur , Du san Gabrijel ci c , Toma z Klobu ca (2023),et.al " Artificial intelligence for cyber security: Literature review and future research direction" The application of artificial intelligence (AI) for cybersecurity is examined in this research paper through a survey of the relevant literature. The author carefully reviewed 2029 articles, reduced that number to 638 based on title and abstract analysis, then further decreased that number to 236 primary studies after reviewing the entire text. The author then used the information she had gleaned from these original investigations to draw conclusions about links and interconnections. In order to address new concerns for the successful deployment of AI for cybersecurity, the research study identifies research gaps, conducts a descriptive analysis of the synthesized literature review, and suggests future research topics. The key findings and research ramifications of the systematic literature review are presented in the research paper's conclusion.

Sourabh Bhattacharya , (2023) Challenges Faced in Countering Cyber Crimes in Political Science and Management: a Critical Study .This author presents a critical analysis of the difficulties encountered in political science and management when tackling cybercrime. It talks about how common cybercrimes are in different industries and how they affect businesses. The paper highlights the necessity of a thorough and team-based strategy for cyber security that takes into account technical, human, legal, and ethical considerations. It also recommends putting in place a cybersecurity structure that can aid in preventing cyberattacks, seeing them early, and efficiently retaliating. In order to stay up with the fast changing cyber security scene, the study emphasizes the necessity of routine system evaluation and updating.

Nassereldin A. Osman , Mohammad M. Alshammari , and Tarek I. Mohamed1(2023) ,et.al " AI Techniques for Combating Electronic Crimes and Enhancing Cyber security: Kuwait's Security Services as a Model" Security organizations can employ AI to fight various electronic crimes, such as virus attacks, phishing scams, fraudulent transactions, and identity theft. By examining user activity patterns, spotting anomalies or discrepancies, and raising the red flag on suspicious transactions, AI can assist in the detection and prevention of these crimes. AI may also be used to identify and stop malware assaults, such as ransom ware, which can seriously harm networks and computer systems. The employment of AI in law enforcement raises a number of ethical and legal issues that need to be properly studied and resolved.

Proposed work:

This block diagram shows the progression of events in the application of AI methods for thwarting cybercrimes in the management and political science disciplines. Data gathering and preparation come first, then threat intelligence sources are used for AI-based threat identification and prediction. The security analytics platform makes use of AI to track and examine data pertaining to security. AI-assisted incident response planning is used in the event of an incident. AI also helps with the creation and application of governance frameworks and policies to deal with online dangers. Overall, these interrelated steps demonstrate a thorough strategy for using AI to fight cybercrimes. Please note that this is a high-level depiction and that it may need to be further detailed depending on the particular technology and approaches being used.

Data Preprocessing:

It starts with data collection and preprocessing, followed by utilizing threat intelligence sources for AI-based threat detection and prediction. The security analytics platform leverages AI to monitor and analyze security-related data. In the event of an incident, AI-assisted incident response planning is employed. Additionally, AI supports the formulation and implementation of policies and governance frameworks to address cyber threats. Overall, these interconnected stages illustrate a comprehensive approach to combating cybercrimes through AI techniques. Keep in mind that this diagram is a high-level representation and can be further detailed based on the specific technologies and strategies being utilized.

Threat Intelligence Sources:

These sources include current and past details on new threats, weaknesses, and attack strategies. Data on malicious IP addresses, domains, malware samples, and hacker strategies can be found in threat intelligence feeds. This data is processed and analyzed using AI techniques to look for patterns and correlations that could point to possible dangers.

AI –based Threat detection and Prediction:

AI-based Threat Detection and Prediction: At this level, data from both internal and external sources is analyzed using machine learning algorithms and AI models. These algorithms are able to recognize patterns and outliers that may indicate recent or upcoming invasions by learning from prior attack data. Predictive analytics can be used to anticipate potential threats based on current patterns and historical data.

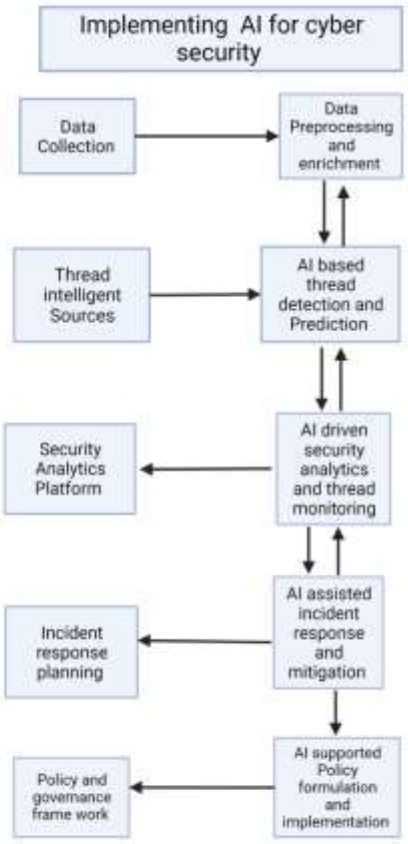
Implementing AI for cyber security
Data Collection
Data Preprocessing and enrichment
Thread intelligent Sources
AI based thread detection and Prediction
Security Analytics Platform
AI driven security analytics and thread monitoring
Incident response planning
AI assisted incident response and mitigation
Policy and governance frame work
AI supported Policy formulation and implementation

Fig 2: Implementing AI techniques for combating cybercrimes

Security Analytics Platform: The security analytics platform serves as a focal point for gathering and analyzing security-related data. Real-time AI-driven algorithms scan incoming data for any odd patterns or behaviors that might indicate a security compromise. Various security solutions, such as firewalls, intrusion detection systems, and endpoint security software, can communicate with this platform.

Incident response Planning:

Incident response planning is a methodical procedure that organizations employ to manage and lessen cyber security issues. These occurrences can include everything from malware infections and data breaches to denial-of-service assaults and insider threats. Incident response planning's main objectives are to lessen the effects of security incidents, promptly return to regular operations, and learn from the incident to avoid repeating it in the future.

AI assisted incidence and response: When a security incident is discovered, AI can help create a suitable incident response plan. This may entail making suggestions for activities to be taken, setting priorities for tasks, and offering mitigation techniques. The ability of AI to quickly evaluate large amounts of data aids in determining the effects of the incident and developing a successful response strategy.

Policy and Governance Framework: AI approaches are employed to support the creation and application of cyber security rules and governance frameworks. These guidelines for organizational behavior assure data security, legal compliance, and consistency with best practices. AI can help with policy gap analysis, update suggestions, and effectiveness evaluation of implemented actions.

AI uses in Infrastructure management :

Infrastructure management uses AI to improve system resilience and operational efficiency across a variety of disciplines. It facilitates smart grid management for effective energy distribution, enhances traffic flow through real-time data analysis, enhances water and waste management processes by monitoring usage patterns, improves building energy efficiency via occupancy-based control systems, supports supply chain management through demand prediction and inventory optimization, and ensures structural integrity.

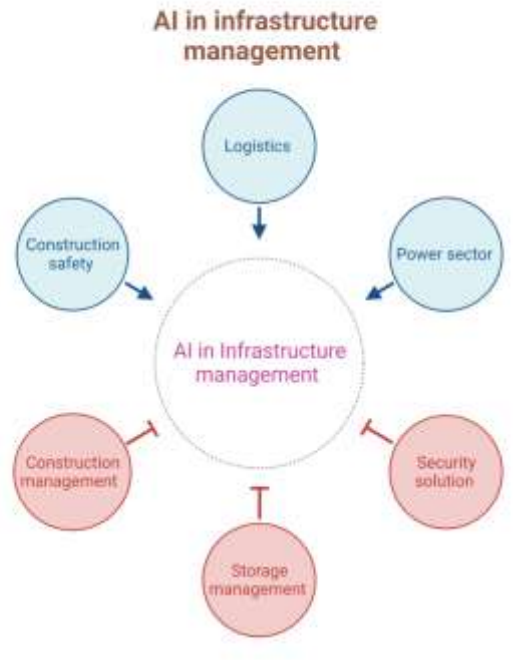

Fig 3: AI uses Infrastructure management

Challenges of Implementing AI techniques for combating cybercrimes in Politics :

Complexity of Political Threats:

Political cybercrimes sometimes entail complex and multifaceted threats, including state-sponsored assaults, disinformation campaigns, and election meddling. A thorough grasp of political dynamics and motivations is necessary to develop AI models that can efficiently detect and neutralize these complex dangers. Cyber security political risks are complicated due to the delicate interplay of advanced technology, geopolitical motives, and discourse manipulation. These complex threats include state-sponsored cyber operations that target vital infrastructure, the dissemination of false information to sway public opinion and undermine democratic processes, the planning of cyber espionage operations to gather sensitive information, and the complex interplay of transnational motives in a rapidly changing international environment. This complexity calls for the creation of cutting-edge AI-driven tools to detect, analyze, and counteract these threats while preserving the integrity of political processes and institutions. It also necessitates a nuanced understanding of political dynamics, technological intricacies, and international relations.

Attribution and Geopolitical Considerations:

It can be very difficult to pinpoint the source of cyber attacks, particularly when nation-states are involved. The sophistication of strategies used to disguise identities may make it difficult for AI models to attribute attacks effectively, perhaps resulting to misidentification or misattribution. Geopolitical factors and attribution are complex components of cyber security, especially in the context of politically driven online threats. Due to sophisticated obfuscation tactics, false flags, and common infrastructure among threat actors, attributing cyber attacks is a difficult task. Geopolitical factors make the problem even more difficult because assigning blame for assaults can have significant diplomatic, strategic, and reputational repercussions. Technical evidence must be balanced with broader international relations dynamics in order to make accurate attributions without inciting political tensions, errors, or unintentional escalation. This emphasizes the need for careful analysis and international cooperation in navigating these murky waters.

False Information and Deep Fakes:

The spread of deep fakes and misleading information in the political sphere is a developing problem. To stop the swaying of public opinion, AI-powered technologies that identify false information and deep fakes must be extremely precise. In the current digital environment, deep fakes and false information present serious problems. The quick dissemination of false information, which is frequently presented as reliable news, can undermine public confidence in authorities and cause strife among populations. Furthermore, the development of sophisticated deep fake technology raises questions regarding the veracity of audiovisual information because modified hyper-realistic media might fool viewers and obfuscate the distinction between fact and fiction. These two challenges highlight the urgent need for innovative technology solutions to recognize and mitigate the negative effects of deep fakes and false information on society.

Legal and Ethical Issues:

There are a number of legal and ethical issues that arise when using AI to tackle cybercrime. When AI systems use personal data to identify potential cyber threats, issues like privacy and data protection come up legally. It can be difficult to strike a compromise between efficient cybercrime prevention and protecting people's rights. Concerns about algorithm accountability and transparency also surface when AI systems are used to make decisions that affect specific people or groups of people. The possibility of biased results ethically poses issues with justice and discrimination. AI algorithms may unintentionally reinforce biases seen in training data, which could result in unfair targeting or incorrect identification of suspects. Furthermore, as an excessive dependence on automated choices is required when using AI to combat cybercrime, explicit restrictions on the scope of AI's authority are required. Furthermore, as an excessive dependence on automated choices could circumvent human oversight and due process, the use of AI for the prevention of cybercrime requires clear limitations on the scope of the technology's authority. To ensure that AI tools effectively tackle cybercrimes while preserving the ideals of justice, privacy, and fairness, it is imperative to address these legal and ethical issues.

Policy and Regulation: In the context of AI, policy and regulation entails developing thorough frameworks that direct the creation, implementation, and oversight of artificial intelligence systems. These frameworks cover topics like data security, algorithm openness, responsibility, bias reduction, international cooperation, and moral usage. In order to protect individual rights, prevent discrimination, advance fairness, and address the changing challenges posed by AI technologies in a variety of domains, including the prevention of cybercrime, governments and international organizations have established clear guidelines.

Human-Technology Interaction: Interaction between humans and different technological systems is referred to as human-technology interaction. It includes the ways in which people use and influence technology as well as the ways in which technology affects how people behave, think, and perceive the world. This connection takes place in a variety of settings, ranging from routine interactions with computers and cell phones to more involved interactions with cutting-edge technologies like robotics, virtual reality, and artificial intelligence. Designing user-friendly interfaces, taking into account cognitive and emotional factors, discussing ethical issues, and making sure that technology enhances human abilities while respecting individual preferences and maintaining user agency are all necessary for understanding and optimizing human-technology interaction. This multidisciplinary field looks at how technology might improve communication, productivity, and quality of life while simultaneously looking at potential drawbacks such dependency, privacy problems, and the need for safeguards. This interdisciplinary topic examines how technology can improve communication, productivity, and quality of life while simultaneously looking at potential drawbacks such reliance, privacy problems, and the requirement for continual education to deal with the ever changing technological scene.

Bias and Disinformation in AI Model:

The term "bias in AI models" refers to the existence of unfair or discriminating results brought on by skewed training data or defective algorithms, frequently magnifying societal biases and maintaining inequities. Contrarily, disinformation is the deliberate dissemination of inaccurate or misleading information, which is made worse by AI-generated content like deep fakes that can conflate legitimate and unreliable sources of information. Both bias and misinformation put AI systems' fairness and credibility in jeopardy, necessitating ongoing efforts to correct biased training, improve algorithmic fairness, and create tools for spotting and combating manipulated content. This will ensure responsible AI use and accurate information dissemination.

Table 1 shows Challenges of using AI in Political Science and Management .

Challenge	Political Science	Management
Ethical Consideration	Balancing privacy and security concerns in surveillance systems.	Ensuring unbiased decision-making in employee management based on AI evaluations.
Transparency and Accountability	Explaining AI-driven policy recommendations to citizens.	Ensuring transparency in AI-based supply chain decisions for stakeholders
Bias and Fairness	Mitigating bias in AI models that analyze public sentiment.	Addressing biases in hiring and promotion decisions made by AI-driven systems.
Data Quality and Availability	Accessing reliable and unbiased data for policy analysis.	Managing and cleaning diverse data sources for accurate demand forecasting.
Interpretability of Decisions	Understanding the rationale behind AI-generated policy suggestions	Justifying AI-generated investment recommendations to stakeholders.
Human-AI Collaboration	Integrating AI insights with policymakers' expertise for informed decisions.	Balancing AI's data-driven insights with managers' strategic intuition.
Security and privacy	Protecting sensitive political data from cyber threats and attacks.	Safeguarding confidential business information processed by AI systems.
Policy and regulation	Adapting regulations to account for AI-driven policy analysis.	Navigating legal frameworks in AI-based financial decision-making.
Public Perception and Challenge	Overcoming concerns about AI's influence on political decision-making.	Gaining stakeholder trust in AI-driven management strategies.
Resource allocation	Allocating resources for AI research and implementation in governance.	Budgeting for AI adoption and training in management practices.

Table 1 : Challenges of using AI in political and Managements

Conclusion:

In conclusion, the application of AI approaches to the fight against cybercrime has enormous promise for the study of management and political science. The complexity of cyberthreats and the changing character of criminal activity in the digital sphere have been underlined in this study paper. Political institutions can strengthen cyber security measures, protecting sensitive data and important infrastructures, by utilizing

AI's capabilities. Additionally, AI can offer real-time threat analysis, early identification, and proactive mitigation measures in the management domain, assuring business continuity and safeguarding priceless assets. However, prioritizing ethical issues, openness, and the requirement for cooperation among technical experts, politicians, and practitioners is necessary. This paper emphasizes the value of creating public-private collaborations, raising cyber security awareness, and regularly revising rules to keep up with technological changes. In order to maximize the beneficial effects of AI in combating cybercrimes in the fields of Political Science and Management, this paper emphasizes the significance of continuously updating regulations to keep up with technological advancements, encouraging public-private partnerships, and promoting cyber security awareness. The ethical adoption of AI technology is essential to preserving digital environments and enhancing social wellbeing as both sectors traverse an increasingly digital future.

Future work:

Future investigations resulting from this work on the application of AI methods for thwarting cybercrimes in Political Science and Management may focus on improving AI models through continuous learning and adaptation to changing cyber threats particular to these fields. The creation of hybrid strategies that mix AI and human skills for more precise threat assessment and decision-making may be the subject of future research. Additionally, addressing potential resource limits while investigating the scalability of AI solutions across various scales of political and administrative contexts remains a key direction. Examining methods for fostering cross-disciplinary collaboration and knowledge sharing as well as the long-term socio-political and economic repercussions of widespread AI adoption in cybercrime prevention and management could improve the practical application and efficacy of AI strategies in these crucial fields.

References:

1. Dan Jerker B. Svantesson (2017) “Cybercrime and the Adoption of Artificial Intelligence Systems for Judicial Decision-Making in Criminal Justice Systems”
2. Nassereldin A. Osman , Mohammad M. Alshammari , and Tarek I. Mohamed1 (2023),” AI Techniques for Combating Electronic Crimes and Enhancing Cybersecurity: Kuwait's Security Services as a Model”
3. Artificial intelligence, data analytics and cyber security – laws & practice
4. Alkaabi, Ali & Mohay, George & Mccullagh, Adrian & Chantler, Nicholas. (2010). Dealing with the Problem of Cybercrime. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST.
5. Dilek, Selma & Çakır, Hüseyin & Aydın, Mustafa. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications. 6. 10.5121/ijaia.2015.6102.
6. Selma Dilek , Hüseyin Çakır and Mustafa Aydın (2015),” Applications of artificial intelligence techniques to combating cyber crimes: a review”
7. Mohsin, Kamshad, Regulation of AI and AI Crimes (March 10, 2020).
8. Ganesan and P. Mayilvahanan (2017), Vels University, Chennai Cyber Crime Analysis in Social Media Using Data Mining Technique
9. Taddeo, Mariarosaria. (2019). Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity. Minds and Machines.

10. Choraś, M., Woźniak, M. The double-edged sword of AI: Ethical Adversarial Attacks to counter artificial intelligence for crime
11. Harikumar Pallathadka, Edwin Hernan Ramirez-Asis, Telmo Pablo Loli-Poma, Karthikeyan Kaliyaperumal, Randy Joy Magno Ventayen, Mohd Naved(2023) “Applications of artificial intelligence in business management, e-commerce and finance”
12. Selma Dilek1 , Hüseyin Çakır2 and Mustafa Aydın3(2015) “Applications of artificial intelligence techniques to combating cyber crimes: a review”.
13. Mahesh Chandra (2019),”Reduction of Cyber Crimes by Effective Use of Artificial Intelligence Techniques”
14. Alansari, Mariam & Aljazzaf, Zainab & Sarfraz, Muhammad. (2019). On Cyber Crimes and Cyber Security. 10.4018/978-1-5225-8304-2.ch001.
15. Nidhi Kataria Chawla “Review of Cyber Crime in India: An Overview”
16. Usanov, Artur. (2015). Assessing Cyber Security: A Meta-analysis of Threats, Trends, and Responses to Cyber Attacks.
17. Johri, S., Rajagopal, B. R., Ahamad, S., Kannadasan, B., Dixit, C. K., & Singh, P. (2023). Cloud computing based renewable energy demand management system. PROCEEDING OF INTERNATIONAL CONFERENCE ON ENERGY, MANUFACTURE, ADVANCED MATERIAL AND MECHATRONICS 2021. https://doi.org/10.1063/5.0126132
18. RajBalaji, S., Raman, R., Pant, B., Rathour, N., Rajagopa, B. R., & Prasad, C. R. (2023, January 27). Design of deep learning models for the identifications of harmful attack activities in IIOT. 2023 International Conference on Artificial Intelligence and Smart Communication (AISC). https://doi.org/10.1109/aisc56616.2023.10085088
19. Malathi, M., Muniappan, A., Misra, P. K., Rajagopal, B. R., & Borah, P. (2023). A smart healthcare monitoring system for patients using IoT and cloud computing. PROCEEDING OF INTERNATIONAL CONFERENCE ON ENERGY, MANUFACTURE, ADVANCED MATERIAL AND MECHATRONICS 2021. https://doi.org/10.1063/5.0126275
20. Ahdal, A. A., Rakhra, M., Rajendran, R. R., Arslan, F., Khder, M. A., Patel, B., Rajagopal, B. R., & Jain, R. (2023, February 8). Monitoring Cardiovascular Problems in Heart Patients Using Machine Learning. Journal of Healthcare Engineering; Hindawi Publishing Corporation. https://doi.org/10.1155/2023/9738123
21. Banu, S. R., Rajagopal, B. R., Venkatesan, K., & Rawat, P. (2023, May 10). Smart Financial Management System Based on Integrated Artificial Intelligence and Big Data analytics. ResearchGate. https://www.researchgate.net/publication/370652400_Smart_Financial_Management_System_Based_on_Integrated_Artificial_Intelligence_and_Big_Data_analytics
22. Rajagopal, B. R., Anjanadevi, B., Tahreem, M., Kumar, S., Debnath, M., &Tongkachok, K. (2022). Comparative Analysis of Blockchain Technology and Artificial Intelligence and its impact on Open Issues of Automation in Workplace. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 288-292. https://doi.org/10.1109/ICACITE53722.2022.9823792
23. Rajagopal, B. R.,Kannapiran, E., Gupta, A. D., Momin, M. & Chakravarthy, D. S. K. (2022).The future prospects and challenges of implementing big data in healthcare management using Structural equation model analysis. Bull. Env. Pharmacol. Life Sci., (Spl Issue [1] 2022), 1111-1119

24. Krishnam, N. P., Ashraf, M. S., Rajagopal, B. R., Vats, P., Chakravarthy, D. S. K., & Rafi, S. M. (2022). ANALYSIS OF CURRENT TRENDS, ADVANCES AND CHALLENGES OF MACHINE LEARNING (ML) AND KNOWLEDGE EXTRACTION: FROM ML TO EXPLAINABLE AI. Industry Qualifications The Institute of Administrative Management UK, 58(Special Issue May 2022), 54-62.
25. Gupta, A. D., Rafi, S. M., Rajagopal, B. R., Milton, T., &Hymlin, S. G. (2022). Comparative analysis of internet of things (IoT) in supporting the health care professionals towards smart health research using correlation analysis. Bull.Env.Pharmacol. Life Sci., (Spl Issue [1] 2022), 701-708.
26. Bhanushali, M. M., Sharma, A., Sharma, S., Gehlot, A., Rawal, P., & Kapila, D. (2023, May). A detailed and significant analysis of The Effects of Big-Data over The Revolution of Internet Marketing. In 2023 3rd International Conference on Advance Computing and Innovative Technologiesin Engineering (ICACITE) (pp. 1026-1031). IEEE, doi: 10.1109/ICACITE57410.2023.10182372.
27. Bhanushali, M. M., & Sharma, A. (2020). A Bibliometric Study on Purchase and Technology Transfer with Reference to Industrial Equipments. Journal of Computational and Theoretical Nanoscience, 17(9-10), 4698-4702, DOI: https://doi.org/10.1166/jctn.2020.9303
28. Sharma, S. Poojitha, A. Saxena, M. M. Bhanushali and P. Rawal, "A Conceptual Analysis of Machine Learning Towards Digital Marketing Transformation," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 313-316, doi: 10.1109/IC3I56241.2022.10073416.
29. M. Thaseen, G. L, P. Tripathi, Y. Z. Elena, M. M. Bhanushali and J. Alanya-Beltran, "An Review on Internet of Things (IOT) in Creating Better World Through Reduction in Emission of Greenhouse Gases – Multiple Regression Analysis," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 312-316, doi: 10.1109/ICACITE53722.2022.9823835.
30. Sidana, T. Jindal, U. K. Pandey, J. Singh, S. T. Vasantham and M. M. Bhanushali, "Investigation of Block chain Technology Based on Digital Management System with Data Mining Technology for Green Marketing," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 1309-1313, doi: 10.1109/ICACITE53722.2022.9823696.
31. Veerasamy, K., Sanyal, S., Almahirah, M.S., Saxena, M., Manohar Bhanushali, M. (2022). An Investigative Analysis for IoT Based Supply Chain Coordination and Control Through Machine Learning. In: Balas, V.E., Sinha, G.R., Agarwal, B., Sharma, T.K., Dadheech, P., Mahrishi, M. (eds) Emerging Technologies in Computer Engineering: Cognitive Computing and Intelligent IoT. ICETCE 2022. Communications in Computer and Information Science, vol 1591. Springer, Cham. https://doi.org/10.1007/978-3-031-07012-9_13
32. S. K, A. Sabarirajan, K. S. U, P. Narang, M. M. Bhanushali and A. K. Turai, "Human Resource Management based Economic analysis using Data Mining," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 872-876, doi: 10.1109/ICIEM54221.2022.9853202.
33. Sindhura, K., Sabarirajan, A., Narang, P., Bhanushali, M. M., & Turai, A. K. (2022, April). Human Resource Management based Economic analysis using Data Mining. In 2022 3rd

International Conference on Intelligent Engineering and Management (ICIEM) (pp. 872-876). IEEE.

34. Bhanushali, M. M., Bhattacharyya, R., Agarkar, S. C., & Moghe, S. COVID-19.
35. Bhanushali, M., &Periwal, D. Designing the Distributor Evaluation Criteria with reference to the Indian Consumer Durable Industry. Srujan, 33.
36. Bhanushali, M. M., & George, S. P. (2017). MARKET RESEARCH ON CONSUMER BUYING BEHAVIOUR FOR MICROWAVE OVENS IN THANE DISTRICT.
37. Gedamkar, R., & Bhanushali, M. M. A MULTI-PERSPECTIVE ANALYSIS OF INTERNATIONALIZATION STRATEGIES.
38. Durga, S., Perugu, P., Nidhi Sree, D., Podile, V., Bhanushali, M. M., & Revathi, R. Human Resource Data Analysis & prediction using Decision Tree Algorithm and Random Forest.
39. Sindhura, K., Sabarirajan, A., Narang, P., Bhanushali, M. M., & Turai, A. K. (2022, April). Human Resource Management based Economic analysis using Data Mining. In 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM) (pp. 872-876). IEEE.