WIEDZA OBRONNA
2024, Vol. 286 No. 1
ISSN: 2658-0829 (Online) 0209-0031 (Print)
Journal homepage: http://wiedzaobronna.edu.pl
DOI: https://doi.org/10.34752/2024-f286

MACIEJ GRUNT, PhD*
Uniwersytet Pomorski w Słupsku, Słupsk, Polska
PIOTR POTEJKO, PhD**
Uniwersytet Warszawski, Warszawa, Polska

IMPLEMENTING MACHINE LEARNING FOR ENHANCED CRITICAL INFRASTRUCTURE PROTECTION: A FRAMEWORK-CENTRIC APPROACH FOR LEGACY SYSTEMS

WDROŻENIE UCZENIA MASZYNOWEGO W CELU WZMOCNIONEJ OCHRONY INFRASTRUKTURY KRYTYCZNEJ: PODEJŚCIE OPARTE NA FRAMEWORKACH STARSZYCH SYSTEMÓW

ABSTRACT: This article introduces a comprehensive framework for integrating Artificial Intelligence (AI) into critical infrastructure security systems, with a focus on overcoming integration challenges with legacy systems. It details the necessity of a structured approach to AI deployment, addressing technical, regulatory, and operational hurdles to enhance security and maintenance. Through the lens of a pilot study, the paper discusses the encountered integration challenges, underscoring the framework's role in facilitating a smoother transition to AI-enhanced infrastructure. This work lays a foundation for future advancements in critical infrastructure protection through AI.

KEYWORDS: legacy systems, machine learning, AI integration, critical infrastructure

ABSTRAKT: W artykule przedstawiono kompleksowe ramy integracji sztucznej inteligencji (AI) z systemami bezpieczeństwa infrastruktury krytycznej, ze szczególnym uwzględnieniem pokonywania wyzwań związanych z integracją ze starszymi systemami. Szczegółowo opisano konieczność ustrukturyzowanego podejścia do

* dr Maciej Grunt, Pomeranian University in Słupsk, Poland
https://orcid.org/0000-0001-6327-3557, maciej.grunt@upsl.edu.pl

** dr Piotr Potejko, Universty of Warsaw, Poland
https://orcid.org/0000-0002-5342-905X, p.potejko@uw.edu.pl

wdrażania sztucznej inteligencji, uwzględniającego przeszkody techniczne, regulacyjne i operacyjne w celu zwiększenia bezpieczeństwa i konserwacji. W artykule przez pryzmat badania pilotażowego omówiono napotkane wyzwania związane z integracją, podkreślając rolę frameworku w ułatwianiu płynniejszego przejścia na infrastrukturę wzmocnioną sztuczną inteligencją. Praca ta kładzie podwaliny pod przyszłe postępy w ochronie infrastruktury krytycznej za pomocą sztucznej inteligencji.

SŁOWA KLUCZOWE: systemy klasy legacy, uczenie maszynowe, infrastruktura krytyczna, integracja AI.

INTRODUCTION

In an era where the security of critical infrastructure systems is paramount, the sophistication of potential threats necessitates an equally advanced line of defense. Critical infrastructure—encompassing sectors as diverse as energy, water supply, communications, and transportation—forms the backbone of modern societies, making its protection a top priority[1]. Traditional security measures, while essential, are increasingly complemented by innovative technologies capable of predictive and automated responses to emerging threats. Among these, Artificial Intelligence (AI) and Machine Learning (ML) stand out for their ability to revolutionize the way critical infrastructure is monitored, maintained, and protected.

This paper delves into the strategic integration of ML algorithms within critical infrastructure security systems, guided by a comprehensive framework designed to navigate the complexities of AI adoption. The framework, developed from extensive analysis and practical insights, outlines a phased approach encompassing needs assessment, technology evaluation, regulatory compliance, and stakeholder engagement, culminating in the implementation of AI solutions tailored to enhance operational efficiency and resilience.

By contextualizing the deployment of ML technologies within a structured framework, this article aims to bridge the gap between theoretical potential and practical application, ensuring that AI's integration into critical infrastructure security is both effective and sustainable. Through this lens, we explore the multifaceted benefits of ML—from predictive maintenance and anomaly detection to real-time threat intelligence—while addressing the challenges inherent in modernizing legacy systems and navigating the regulatory landscape. Discussion underscores the importance of a strategic, framework-centric approach to harnessing

[1] J. D. Moteff, C. Copeland, J. W. Fischer, Critical infrastructures: What makes an infrastructure critical? *Congressional Research Service*, Library of Congress, Washington 2003, pp. 145-159.

AI in safeguarding critical infrastructure, offering valuable insights for policymakers, industry stakeholders, and the academic community engaged in the pursuit of enhanced security and resilience in an increasingly interconnected world.

The transition towards integrating ML into infrastructure management is not devoid of challenges, particularly when addressing the vulnerabilities of critical infrastructure and the complexities associated with legacy systems[2]. Critical infrastructure—encompassing utilities, transportation, and communications networks—forms the backbone of national security and economic vitality. These systems are increasingly targeted by sophisticated cyber and physical threats, posing significant risks to societal well-being and national security[brown]. The integration of ML offers a proactive stance against such threats, employing anomaly detection and predictive threat modeling to safeguard these essential services[3].

Concurrently, the incorporation of ML technologies into legacy systems presents a unique set of challenges. Legacy systems, characterized by their outdated architectures and software, are often integral to the operations of critical infrastructure[4][5].Their transformation requires meticulous planning, ensuring compatibility, and the seamless integration of modern AI capabilities without compromising system integrity or operational continuity[6].

EXAMINATION OF THE PROSPECTS FOR PREDICTIVE MAINTENANCE IN ENHANCING SECURITY SYSTEMS WITHIN CRITICAL INFRASTRUCTURE

Predictive maintenance represents a transformative approach in the management of critical infrastructure, employing machine learning (ML) to preemptively identify and rectify potential system failures before they escalate into disruptive outages[7]. This proactive strategy is essential for the seamless operation and reliability of infrastructure systems that are pivotal to societal well-being and economic stability, including but not limited to electrical grids, water treatment facilities, transportation networks, and communication systems. The traditional

---

[2] C. Alcaraz, S. Zeadally, C*ritical infrastructure protection: Requirements and challenges for the 21st century*, "International journal of critical infrastructure protection", 2015 Vol. 8, pp. 53-66.

[3] K. Dick, L. Russell, Y. Souley Dosso, F. Kwamena, J. R. Green, *Deep learning for critical infrastructure resilience*, "Journal of Infrastructure Systems", 2019 Vol. 25 Issue 2, pp. 050190031- 050190039.

[4] S. Jha, M. Jha, L. O'Brien, M. Wells, *Integrating legacy system into big data solutions: Time to make the change*, Asia-Pacific World Congress on Computer Science and Engineering 2014, Publisher: IEEE, pp. 1-10.

[5] E. Brynjolfsson, T. Mitchell, *What can machine learning do? Workforce implications*, "Science", 2017 Vol. 358 Issue 6370, pp. 1530-1534.

[6] R. Cao, M. Iansiti, *Digital transformation, data architecture, and legacy systems*, "Journal of Digital Economy", 2022 Vol. 1 Issue 1, pp. 1-19.

[7] J. D. Moteff, C. Copeland, J. W. Fischer,*op. cit.*, pp. 201-205.

maintenance methodologies, which primarily operate on a reactive or scheduled basis, often result in inefficiencies, such as unnecessary downtime, excessive operational costs, and reduced asset lifespan[8]. Predictive maintenance, through the analytical prowess of ML algorithms, leverages both historical and real-time data to uncover patterns, anomalies, and trends that signal impending failures[9].

This predictive insight enables maintenance teams to act swiftly and precisely, scheduling interventions at opportune moments to mitigate risks without disrupting the normal operations of critical services. The advantages of such an approach are multifold: it significantly reduces maintenance costs by avoiding the expenses associated with emergency repairs and unplanned downtime; it extends the life expectancy of infrastructure components by preventing excessive wear and tear; and it upholds a high standard of service delivery to the public and businesses alike.

Moreover, the integration of ML in predictive maintenance initiatives facilitates a deeper understanding of infrastructure behavior, leading to improved operational decisions and strategic planning. By continuously analyzing data, ML models become increasingly accurate in their predictions, adapting to new patterns and evolving conditions within the infrastructure ecosystem[10]. This dynamic capability underscores the importance of predictive maintenance in building resilient, efficient, and sustainable critical infrastructure systems.

The implementation of predictive maintenance powered by ML also necessitates a robust framework for data collection, processing, and analysis. This involves the deployment of sensors and IoT devices to capture real-time operational data, sophisticated data management systems to handle the volume and velocity of the data generated, and skilled personnel to interpret the findings and implement actionable maintenance strategies[11].

As delved deeper into the applications and implications of ML in predictive maintenance for critical infrastructure, it becomes clear that this technology-driven approach is not merely an operational upgrade but a strategic necessity. It empowers infrastructure managers to transition from conventional, often inefficient maintenance practices to a more intelligent,

---

[8] K. Hemme, C*ritical infrastructure protection: Maintenance is national security*, "Journal of Strategic Security", 2015 Vol. 8 Issue 3, pp. 25-39.

[9] A. Gorenstein, M. Kalech, *Predictive maintenance for critical infrastructure*, "Expert Systems with Applications", 2022 Vol. 210, pp.118413-118422.

[10] K. Dick, L. Russell, Y. Souley Dosso, F. Kwamena, J. R. Green, *op. cit.*, pp. 050190031- 050190039.

[11] S. Selcuk, *Predictive maintenance, its implementation and latest trends*, *Proceedings of the Institution of Mechanical Engineers*, Part B: "Journal of Engineering Manufacture", 2017 Vol. 231 Issue 9, pp. 1670-1679.

data-driven model that promises enhanced reliability, performance, and sustainability of essential services.

In the domain of predictive maintenance for critical infrastructure, the application of advanced machine learning (ML) algorithms plays a pivotal role.

The integration of machine learning algorithms into predictive maintenance strategies enables infrastructure managers to leverage vast amounts of data for informed decision-making. By analyzing historical performance and real-time operational data, ML models can predict when and where maintenance should be performed, optimizing the allocation of resources and minimizing the risk of unexpected failures.

Furthermore, the evolution of ML algorithms, driven by advancements in computational power and data analytics techniques, continues to expand the potential of predictive maintenance. Techniques such as reinforcement learning and anomaly detection algorithms are gaining traction, offering new ways to enhance the resilience and efficiency of critical infrastructure systems[12].

This exploration into the application of advanced ML algorithms underscores their significance in the predictive maintenance of critical infrastructure. By harnessing the power of data analytics, these algorithms enable a proactive approach to maintenance, ensuring the continuous and reliable operation of essential services.

STRATEGIC DATA MANAGEMENT FOR PREDICTIVE MODELING BASED ON LEGACY SYSTEMS IN CRITICAL INFRASTRUCTURE

The success of predictive maintenance in critical infrastructure is fundamentally rooted in strategic data management. This detailed process involves several intricate steps: meticulous data collection, advanced processing techniques, sophisticated feature engineering, rigorous model training and validation, followed by continuous learning and adaptation to ensure the predictive models remain accurate over time. Each step is vital for transforming raw data into actionable insights that can preemptively identify potential failures within critical systems.

The data collection phase is the cornerstone of predictive modeling, requiring the deployment of a vast network of sensors and data-gathering devices across critical

[12] Z. M. Çınar, A. Abdussalam Nuhu, Q. Zeeshan, O. Korhan, M. Asmael, B. Safaei, *Machine learning in predictive maintenance towards sustainable smart manufacturing in industry 4.0*, "Sustainability", 2020 Vol. 12 Issue 19, p. 8211.

infrastructure components[13]. This stage is characterized by the careful selection of sensors and instruments capable of capturing a wide range of operational parameters, from temperature fluctuations to vibration patterns, electrical currents, and even acoustic emissions. The goal is to amass a comprehensive dataset that reflects the operational realities of the infrastructure under scrutiny.

Once collected, the raw data undergoes a rigorous processing regimen designed to cleanse, normalize, and structure it for analysis. This involves sophisticated algorithms to filter out noise, correct anomalies, and handle missing or incomplete data points. The objective is to refine the dataset into a clean, coherent format that accurately represents the system's operational state, free from distortions that could mislead the predictive models.

At the heart of strategic data management lies feature engineering, a critical step where raw data is transformed into informative features that significantly enhance the predictive model's performance. This process requires deep domain expertise to identify which data attributes are most indicative of system health and impending failures. Engineers and data scientists work collaboratively to craft features that capture the complex relationships and patterns within the data, often employing techniques such as principal component analysis (PCA) to reduce dimensionality and enhance model efficiency[14].

With a refined dataset in hand, the next step involves training the ML models using historical data where the outcomes of system performance and failures are known. This phase is critical for teaching the model to recognize patterns and predict future states accurately. Validation plays a crucial role here, employing separate datasets to test the model's predictions, ensuring its reliability and accuracy before full-scale deployment[15].

Given the dynamic nature of critical infrastructure environments, predictive models must evolve to reflect changing conditions and emerging failure modes. This necessitates a framework for continuous learning, where new data is regularly fed into the model to refine

---

[13] C. Krupitzer, T. Wagenhals, M. Züfle, V. Lesch, D. Schäfer, A. Mozaffarin, et al., *A survey on predictive maintenance for industry 4.0*, arXiv preprint arXiv:2002.08224 2020.

[14] T. Zonta, C. A. Da Costa, R. da Rosa Righi, M. J. de Lima, E. S. da Trindade, G. P. Li, *Predictive maintenance in the Industry 4.0: A systematic literature review*, "Computers & Industrial Engineering", 2020 Vol. 150, pp. 106889-106896.

[15] T. P. Carvalho, F. A. Soares, R. Vita, R. d. P. Francisco, J. P. Basto, S. G. Alcalá, *A systematic literature review of machine learning methods applied to predictive maintenance*, " Computers & Industrial Engineering", 2019 Vol. 137, pp. 106024-106030.

its predictions[16]. This adaptive approach ensures that the model remains effective over time, capable of anticipating failures even as the system it monitors undergoes changes in operation, maintenance practices, or external influences.

This comprehensive approach to strategic data management underscores its importance in leveraging ML for predictive maintenance. By systematically collecting, processing, and analyzing data, and by continuously refining the models based on new insights, predictive maintenance can significantly improve the reliability, efficiency, and longevity of critical infrastructure systems. This not only minimizes downtime and maintenance costs but also ensures that these essential services can meet the demands of modern societies with greater resilience and sustainability.

OVERCOMING INTEGRATION CHALLENGES WITH LEGACY AND MODERN SYSTEMS

Legacy systems pose significant limitations in the protection of critical infrastructure due to their outdated architectures, software, and inability to seamlessly integrate with advanced AI technologies[17]. These systems, often deeply embedded in the operations of critical services, are not originally designed with the flexibility to adapt to the dynamic nature of cyber and physical threats faced today. The challenges include technical disparities, data integration issues, and the substantial effort required for modernization without disrupting operational continuity. Addressing these limitations necessitates meticulous planning, development of custom solutions for technology compatibility, and a strategic approach to incorporate AI capabilities, ensuring the resilience and security of critical infrastructure in an increasingly interconnected and digital world.

The foundational challenge lies in the technical disparities between older, legacy systems and the latest ML technologies. Legacy systems often operate on outdated hardware and software platforms, lacking the necessary interfaces for direct integration with advanced ML algorithms. This discrepancy can lead to significant data integration issues, where extracting and processing data from these systems becomes a labor-intensive process. Addressing this challenge requires a detailed analysis of legacy system architectures, followed by the

[16] W. Zhang, D. Yang, H. Wang, *Data-driven methods for predictive maintenance of industrial equipment: A survey*, "IEEE Systems Journal", 2019 Vol. 13 Issue 3, pp. 2213-2227.

[17] W. Hurst, N. Shone, *Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation*, n: *Management and Engineering of Critical Infrastructures*, Publisher: Elsevier 2024, pp. 265-286.

development of custom adapters or middleware solutions that can bridge the gap, facilitating data flow and communication between old and new technologies[18].

Beyond technical hurdles, the integration process must also contend with organizational and cultural barriers. Legacy systems are frequently embedded within established operational processes and supported by staff familiar with their quirks and capabilities. Introducing ML-based predictive maintenance can disrupt these established practices, encountering resistance from personnel hesitant to adopt new technologies[19]. Overcoming these barriers necessitates comprehensive training programs, stakeholder engagement initiatives, and clear demonstrations of the value and benefits that ML integration brings to maintenance practices.

Another significant challenge arises from the quality and consistency of data generated by legacy systems. These systems may not have been designed with data capture for predictive analytics in mind, resulting in incomplete, inconsistent, or unstructured data outputs. Addressing this issue involves implementing data cleansing and transformation processes that standardize data formats and fill in missing information, thereby making legacy system data compatible with ML models.

As predictive maintenance systems evolve, they must remain flexible and scalable to accommodate new data sources, updated ML models, and changes in infrastructure components. This requires the adoption of modular system architectures and cloud-based solutions that can dynamically adjust to changing needs, ensuring that the integration of ML technologies remains a sustainable and adaptable component of critical infrastructure maintenance strategies[20].

Integrating ML into critical infrastructure also raises significant security and privacy concerns, especially when dealing with sensitive operational data. Ensuring the secure transmission and processing of data between legacy and modern systems is paramount. This involves implementing robust cybersecurity measures, including encryption, access controls,

[18] R. C. Seacord, D. Plakosh, G. A. Lewis, *Modernizing legacy systems: software technologies, engineering processes, and business practices*, Publisher: Addison-Wesley Professional 2003, pp. 25-38.
[19] B. Engelmann, A.-M. Schmitt, L. Theilacker, J. Schmitt, *Implications from Legacy Device Environments on the Conceptional Design of Machine Learning Models in Manufacturing*, "Journal of Manufacturing and Materials Processing", 2024 Vol. 8 Issue 1, pp. 15.
[20] F. Hussain, R. Hussain, S. A. Hassan, E. Hossain, *Machine learning in IoT security: Current solutions and future challenges*, "IEEE Communications Surveys & Tutorials", 2020 Vol. 22 Issue 3, pp. 1686-1721.

and secure data storage practices, to protect against potential data breaches and ensure compliance with regulatory requirements[21].

By addressing these challenges through meticulous planning, strategic investment, and the fostering of a culture that embraces innovation and continuous improvement, infrastructure managers can successfully integrate ML technologies into their maintenance regimes. This not only enhances the predictive maintenance capabilities of critical infrastructure systems but also ensures their resilience and reliability in the face of evolving operational demands and technological advancements.

ETHICAL AND SOCIO-ECONOMIC CONSIDERATIONS IN PREDICTIVE MAINTENANCE USAGE IN CRITICAL INFRASTRUCTURE SECURITY SYSTEMS

The integration of machine learning (ML) in predictive maintenance introduces ethical challenges, notably concerning data privacy, algorithmic bias, and transparency. Ensuring data privacy involves not just adhering to legal standards like GDPR but also fostering trust by transparently communicating data use to stakeholders. Algorithmic bias, if unchecked, can exacerbate inequalities, making certain infrastructure components less likely to receive timely maintenance based on flawed data interpretations[22]. Therefore, implementing fairness and accountability measures in algorithm development is crucial. Transparency is not merely about open algorithms but about creating channels for feedback and scrutiny, ensuring that predictive maintenance systems are accountable and understandable by non-experts.

The socio-economic implications of applying ML to predictive maintenance are profound and dual-sided. While these technologies promise operational efficiencies and potential economic growth by preventing critical infrastructure failures, they also pose risks of job displacement[23]. The automation of maintenance tasks could reduce the demand for certain skill sets, pushing the workforce towards obsolescence unless retraining and upskilling initiatives are put in place. Furthermore, the transition to ML-driven maintenance requires

---

[21] M. Xue, C. Yuan, H. Wu, Y. Zhang, W. Liu, *Machine learning security: Threats, countermeasures, and evaluations*, "IEEE Access", 2020 Vol. 8, pp. 74720-74742.

[22] M. Al-Rubaie, J. M. Chang, *Privacy-preserving machine learning: Threats and solutions*, "IEEE Security & Privacy", 2019 Vol. 17 Issue 2, pp. 49-58.

[23] S. Athey, *The impact of machine learning on economics, The economics of artificial intelligence: An agenda*, University of Chicago Press 2018, pp. 149-175.

significant investment, which could exacerbate existing digital divides between communities with varying levels of access to resources and technology.

Balancing Technological Advancements with Social Responsibility: Navigating the balance between technological progress and social responsibility requires a multi-stakeholder approach. This balance seeks not only to harness the operational benefits of ML for predictive maintenance but also to ensure these benefits do not come at the expense of social equity and workforce well-being. Engaging with diverse groups—from technology developers to the end-users of critical infrastructure, policy-makers, and the labor force—is essential for identifying and addressing the broader impacts of these technologies on society.

Regulatory and Policy Frameworks: Developing and implementing comprehensive regulatory and policy frameworks is critical to address the ethical and socio-economic challenges posed by ML in predictive maintenance. These frameworks should be dynamic, capable of evolving with technological advancements, and inclusive, considering the diverse impacts of these technologies across different segments of society. Effective frameworks will provide guidelines for ethical data use, ensure algorithmic fairness, protect against cybersecurity threats, and facilitate equitable access to the benefits of technology.

The ultimate aim is to ensure that the advancement of ML in predictive maintenance for crtitcal infrastructures appliances contributes to an inclusive future where the benefits are shared broadly, mitigating risks of inequality and fostering societal resilience. This involves proactive investments in the workforce through education and skills development, supportive policies for those affected by technological transitions, and a commitment to sustainable and resilient infrastructure that serves the needs of all communities. By addressing these considerations thoughtfully, the path towards integrating ML into predictive maintenance can be aligned with broader societal goals, ensuring technology serves the public good.

CHARTING THE FUTURE: EMERGING TRENDS AND RESEARCH FRONTIERS

As approaching to the brink of a new era in predictive maintenance for critical infrastructure, the convergence of machine learning (ML), artificial intelligence (AI), and emerging technologies heralds transformative prospects. This expanded discussion delves into the nuances of these advancements, revealing the depth and breadth of potential impacts across the predictive maintenance landscape.

The horizon of AI and ML is expanding with algorithms becoming increasingly adept at handling complex, multidimensional data. Research is now pivoting towards deep learning techniques that mimic human cognitive processes, offering nuanced insights into predictive maintenance[24]. These advancements promise not only to refine failure predictions but also to revolutionize decision-making processes in infrastructure management, making them more adaptive and foresighted.

The integration of the Internet of Things (IoT) with edge computing is set to redefine data collection and analysis. By processing data at the edge of the network, closer to where it's generated, predictive maintenance systems can leverage real-time insights to initiate preventive actions swiftly[25]. This shift not only reduces latency but also minimizes bandwidth usage, enhancing the efficiency of predictive maintenance operations, especially in remote and complex infrastructure settings.

Digital twins are emerging as a cornerstone technology for predictive maintenance, providing a dynamic, virtual model of physical systems. These digital replicas offer a sandbox for simulating potential failures, testing maintenance strategies, and predicting the outcomes of interventions in a risk-free environment[26]. The fidelity and precision of digital twins continue to improve, driven by advancements in simulation algorithms and data analytics, paving the way for more predictive and prescriptive maintenance practices.

As critical infrastructure systems become increasingly interconnected and reliant on digital technologies, cybersecurity emerges as a paramount concern. Future research is focusing on developing secure ML algorithms and robust encryption methods to protect predictive maintenance data from cyber threats. The goal is to ensure that these systems are not only effective but also secure against evolving cyber risks, preserving the integrity and reliability of critical infrastructure.

The environmental implications of predictive maintenance are gaining attention, with a focus on how ML can contribute to more sustainable infrastructure practices. By optimizing resource use and reducing waste, predictive maintenance can significantly lower the

---

[24] K. Sharifani, M. Amini, *Machine Learning and Deep Learning: A Review of Methods and Applications*, "World Information Technology and Engineering Journal", 2023 Vol. 10 Issue 07, pp. 3897-3904.

[25] E. Adi, A. Anwar, Z. Baig, S. Zeadally, *Machine learning and data analytics for the IoT*, "Neural computing and applications", 2020 Vol. 32, pp. 16205-16233.

[26] D. M. Botín-Sanabria, A.-S. Mihaita, R. E. Peimbert-García, M. A. Ramírez-Moreno, R. A. Ramírez-Mendoza, J. d. J. Lozoya-Santos, *Digital twin technology challenges and applications: A comprehensive review*, "Remote Sensing", 2022 Vol. 14 Issue 6, pp. 1335-1345.

environmental footprint of infrastructure operations. Future developments are likely to emphasize green algorithms and eco-friendly practices, aligning predictive maintenance with broader environmental sustainability goals[27].

The ethical dimensions of AI in predictive maintenance encompass concerns around data privacy, algorithmic fairness, and the digital divide. As these technologies advance, there's a growing imperative to address their social implications, ensuring equitable access and benefits across different communities. The development of ethical guidelines and governance frameworks for AI in predictive maintenance is critical to fostering trust and ensuring that these innovations benefit society as a whole.

STRATEGIC FRAMEWORK FOR AI INTEGRATION IN CRITICAL INFRASTRUCTURE SECURITY LEGACY SYSTEMS

In conducted case study, which will be the centre of gravity of future spin-off paper, machine learning algorithms were employed to enhance the reliability and effectiveness of a critical infrastructure's legacy security system. The approach involved collecting and analyzing historical data on security incidents and system performance anomalies. By applying sophisticated pattern recognition and anomaly detection techniques, the ML model was able to identify potential vulnerabilities and predict future failures in the security apparatus.

The predictive model facilitated a shift from reactive to proactive security management, enabling the deployment of preventative measures before the occurrence of actual system breaches or malfunctions. This approach not only improved the overall security posture but also reduced the operational costs associated with emergency responses to security failures.

During the development process, significant integration challenges were encountered, particularly in merging advanced AI technologies with existing legacy systems within critical infrastructure. These challenges underscored the necessity for a structured approach to successful integration, leading to the formulation of a comprehensive framework. Aimed at navigating the complexities of AI deployment, this framework addresses technical,

[27] B. B. Gupta, A. Gaurav, P. K. Panigrahi, V. Arya, *Analysis of artificial intelligence-based technologies and approaches on sustainable entrepreneurship*, "Technological Forecasting and Social Change", 2023 Vol. 186, pp. 122152-122161.

regulatory, and operational hurdles, thus facilitating a smoother transition towards enhanced security and maintenance capabilities within critical infrastructure environments.

The development of the proposed framework is the culmination of a pilot implementation of AI technologies within a critical infrastructure system characterized by legacy components. This preliminary deployment aimed to evaluate the feasibility, benefits, and challenges of integrating modern AI solutions into existing, often outdated, infrastructural frameworks. By navigating the complexities of merging cutting-edge artificial intelligence with traditional systems, the pilot provided invaluable insights into the strategic, technical, and operational considerations essential for successful AI adoption. A comprehensive account of this implementation, detailing the methodology, outcomes, and lessons learned, will be the focus of a subsequent publication, offering a roadmap for organizations looking to enhance their critical infrastructure security and efficiency through AI.

The framework proposed in this study serves as a comprehensive guide for integrating Artificial Intelligence (AI) into the domain of critical infrastructure security, especially focusing on systems burdened by legacy technologies. It systematically addresses the multifaceted aspects of AI deployment, from initial need assessment and technological readiness to ensuring regulatory compliance and engaging stakeholders. This structured approach is designed to navigate the complexities inherent in melding AI with established systems, aiming to facilitate a seamless transition towards more intelligent, adaptive, and resilient critical infrastructure operations.

1. Comprehensive Operational Analysis: Initiate with an exhaustive evaluation of operational challenges within security and critical infrastructure systems. This phase entails pinpointing specific domains where AI might augment capabilities, focusing on threat detection, operational efficiency, and predictive maintenance. Inclusion of stakeholder perspectives is vital to align AI integration with organizational needs and priorities.

2. Data Infrastructure Appraisal: Conduct a critical examination of the current data infrastructure's capacity to support AI endeavors. This involves assessing data quality, volume, and diversity, alongside the mechanisms for data acquisition and preservation. Ensuring data governance and adherence to privacy standards is imperative for regulatory compliance.

3. Assessment of Technological Preparedness: Scrutinize the existing technological ecosystem, noting any deficiencies or constraints that could impede AI adoption. This step

necessitates contemplating technological enhancements or investments required to facilitate AI functionalities.

4. Regulatory and Legal Compliance: Acquire a deep understanding of the legal and regulatory landscape governing AI applications within the realms of security and critical infrastructure. This encompasses data protection statutes and ethical guidelines, necessitating the formulation of a comprehensive compliance strategy.

5. Financial Implications Analysis: Execute a meticulous financial evaluation contrasting the expenditure involved in AI implementation against anticipated advantages. This analysis should encompass initial capital outlays, operational costs, and potential economic gains derived from enhanced efficiency or downtime reduction, informing strategic AI project prioritization.

6. Stakeholder Engagement Strategy: Develop an inclusive plan to engage all pertinent stakeholders throughout the AI deployment process. This strategy should encapsulate technical personnel, administrative bodies, end-users, and external collaborators, ensuring the AI interventions align with comprehensive stakeholder expectations.

7. Pilot Project Implementation: Design and implement pilot projects on a manageable scale to assess the viability and impact of AI solutions. These pilot initiatives are instrumental in refining AI models and resolving any emergent technical or operational issues ahead of widespread deployment.

8. Proactive Risk Management: Identify and evaluate potential risks associated with AI deployment, including cybersecurity vulnerabilities, operational disturbances, and ethical dilemmas. Crafting a risk management framework incorporating mitigation tactics, emergency protocols, and periodic risk evaluations is essential for proactive risk handling.

9. AI Competency Development: Institute a training and development agenda aimed at fostering AI expertise within the organization. This agenda should cover technical instruction for IT personnel and awareness sessions for the broader employee base, enhancing organizational understanding of AI's benefits and challenges.

10. Ongoing AI Application Evaluation: Establish definitive metrics for gauging AI application success and implement a continuous monitoring framework. This iterative feedback mechanism is crucial for the sustained enhancement of AI models and their integration within security and critical infrastructure domains.

SUMMARY

The article introduced a strategic framework for integrating AI into critical infrastructure security, especially focusing on legacy systems. It highlights the initial pilot implementation's insights, demonstrating the feasibility and benefits of AI in enhancing infrastructure resilience. The framework addresses various aspects such as need assessment, technological readiness, regulatory compliance, and stakeholder engagement, offering a systematic approach to AI deployment. A detailed implementation account, aimed at guiding organizations through AI integration challenges, is promised in a forthcoming publication, marking a significant step towards modernizing critical infrastructure with AI technologies.

REFERENCES LIST

LITERATURE

Adi E., Anwar A., Baig Z., Zeadally S., *Machine learning and data analytics for the IoT*, "Neural computing and applications", 2020 Vol. 32.

Alcaraz C., Zeadally S., *Critical infrastructure protection: Requirements and challenges for the 21st century*, "International journal of critical infrastructure protection" 2015 Vol. 8.

Al-Rubaie M., Chang J. M., *Privacy-preserving machine learning: Threats and solutions*, "IEEE Security & Privacy", 2019 Vol. 17 Issue 2.

Athey S., *The impact of machine learning on economics, The economics of artificial intelligence: An agenda*, University of Chicago Press 2018, Chicago.

Botín-Sanabria D. M., Mihaita A.-S., Peimbert-García R. E., Ramírez-Moreno M. A., Ramírez-Mendoza R. A., Lozoya-Santos J. d. J., *Digital twin technology challenges and applications: A comprehensive review*, "Remote Sensing" 2022 Vol. 14 Issue 6.

Brynjolfsson E., Mitchell T., *What can machine learning do? Workforce implications*, "Science", 2017 Vol. 358 Issue 6370.

Cao R., Iansiti M., *Digital transformation, data architecture, and legacy systems*, "Journal of Digital Economy", 2022 Vol. 1 Issue 1.

Carvalho T. P., Soares F. A., Vita R., Francisco R. d. P., Basto J. P., Alcalá S. G., *A systematic literature review of machine learning methods applied to predictive maintenance*, "Computers & Industrial Engineering", 2019 Vol. 137.

Çınar Z. M., Abdussalam Nuhu A., Zeeshan Q., Korhan O., Asmael M., Safaei B., *Machine learning in predictive maintenance towards sustainable smart manufacturing in industry 4.0*, "Sustainability", 2020 Vol. 12 Issue 19.

Dick K., Russell L., Souley Dosso Y., Kwamena F., Green J. R., *Deep learning for critical infrastructure resilience*, "Journal of Infrastructure Systems", 2019 Vol. 25 Issue 2.

Engelmann B., Schmitt A.-M., Theilacker L., Schmitt J., *Implications from Legacy Device Environments on the Conceptional Design of Machine Learning Models in Manufacturing*, "Journal of Manufacturing and Materials Processing" 2024 Vol. 8 Issue 1.

Gorenstein A., Kalech M., *Predictive maintenance for critical infrastructure*, "Expert Systems with Applications", 2022 Vol. 210.

Gupta B. B., Gaurav A., Panigrahi P. K., Arya V., *Analysis of artificial intelligence-based technologies and approaches on sustainable entrepreneurship*, "Technological Forecasting and Social Change", 2023 Vol. 186.

Hemme K., *Critical infrastructure protection: Maintenance is national security*, "Journal of Strategic Security", 2015 Vol. 8 Issue 3.

Hurst W., Shone N., *Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation*, n: *Management and Engineering of Critical Infrastructures*, Elsevier 2024.

Hussain F., Hussain R., Hassan S. A., Hossain E., *Machine learning in IoT security: Current solutions and future challenges*, "IEEE Communications Surveys & Tutorials", 2020 Vol. 22 Issue 3.

Jha S., Jha M., O'Brien L., Wells M., *Integrating legacy system into big data solutions: Time to make the change*, Asia-Pacific World Congress on Computer Science and Engineering 2014, IEEE 2014.

Krupitzer C., Wagenhals T., Züfle M., Lesch V., Schäfer D., Mozaffarin A., et al., *A survey on predictive maintenance for industry 4.0*, arXiv preprint arXiv:2002.08224 2020.

Moteff J. D., Copeland C., Fischer J. W., *Congressional Research Service*, Library of Congress, Washington 2003.

Sharifani K., Amini M., *Machine Learning and Deep Learning: A Review of Methods and Applications*, "World Information Technology and Engineering Journal", 2023 Vol. 10 Issue 07.

Seacord R. C., Plakosh D., Lewis G. A., *Modernizing legacy systems: software technologies, engineering processes, and business practices*, Publisher: Addison-Wesley Professional 2003.

Selcuk S., *Predictive maintenance, its implementation and latest trends, Proceedings of the Institution of Mechanical Engineers*, Part B: "Journal of Engineering Manufacture", 2017 Vol. 231 Issue 9.

Xue M., Yuan C., Wu H., Zhang Y., Liu W., *Machine learning security: Threats, countermeasures, and evaluations*, IEEE Access, 2020 Vol. 8.

Zhang W., Yang D., Wang H., *Data-driven methods for predictive maintenance of industrial equipment: A survey*, "EEE Systems Journal", 2019 Vol. 13 Issue 3.

Zonta T., Da Costa C. A., da Rosa Righi R., de Lima M. J., da Trindade E. S., Li G. P., *Predictive maintenance in the Industry 4.0: A systematic literature review*, "Computers & Industrial Engineering", 2020 Vol. 150.