Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

AI-Driven Cybersecurity and Big Data-Enabled MIS Frameworks: Strengthening Supply Chain Integrity, Energy Resilience, and Critical Infrastructure Protection

Md Salah Uddin[1]✉, Mohammad Somon Sikder[2] , Md Mazharul Anwar[3] and Forhad Hossain[4]
[1]College of Technology & Engineering, Westcliff University, CA 92614, USA
[2]College of Computer Science, Pacific States University, Los Angeles, CA 90010, USA
[34]Department of Statistics and Data Science, Jahangirnagar University, Savar, Bangladesh
Corresponding Author: Md Salah Uddin, **E-mail**: m.uddin.182@westcliff.edu

| ABSTRACT
This study adopts a conceptual and analytical approach to examine the intersection of AI-driven cybersecurity, big data analytics, and MIS frameworks. The rapid evolution of cyber threats, combined with the exponential growth of big data. It puts a great challenge on the security, resilience, and efficiency of current supply chains and critical infrastructure systems. Cybersecurity AI-based and integrated with Management Information Systems. It offers a transformative approach to enhancing organizational defense mechanisms. AI enables enterprises to strengthen supply chain integrality, improve energy resilience, and ensure robust protection of critical infrastructures. It explores how AI algorithms, machine learning models, and anomaly detection systems work. It can process large volumes of supply chain and energy sector data to predict vulnerabilities and mitigate cyber risks. The proposed MIS framework integrates cybersecurity protocols, data-driven insights, and adaptive decision-making strategies to create a holistic model that addresses both operational efficiency and resilience against cyberattacks. The findings suggest that AI-enabled MIS frameworks significantly improve organizational preparedness, resilience, and adaptability in the face of evolving cyber threats. Enhanced supply chain integrality reduces disruptions, while energy resilience ensures sustainable operations under stress conditions. This framework provides a strategic blueprint for governments, businesses, and energy stakeholders aiming to align cybersecurity initiatives with sustainable development and digital transformation goals.

| KEYWORDS
AI-driven cybersecurity; Big data analytics; Management Information Systems Supply chain integrality; Energy resilience; Critical infrastructure protection; Predictive analytics; Intelligent threat detection; Digital transformation; Cyber resilience

| ARTICLE INFORMATION
ACCEPTED: 01 August 2025 **PUBLISHED:** 02 September 2025 **DOI:** 10.32996/jcsts.2025.7.9.26

1.Introduction

The digital transformation, Industry 4.0, and smart infrastructure have altered the supply chains of the world, the energy system, and critical infrastructure (Maharjan, P. 2023). IT and OT are closely intertwined, which enables real-time monitoring, predictive analytics, and automation. It enhanced effectiveness and decision-making. Major risks are associated with integration, with cyber offenders capitalizing on the interdependency of the systems, data flows, and connections to enable their ever-increasing amounts of invited attacks (Barikdar et al., 2025). This applied to Eleatic Information Systems, AI-based cybersecurity and big data analytics provide a solution to all these weaknesses.

It can proactively detect anomalies and assess and mitigate threats and can facilitate an instant resolution of the incident or incident response to ensure operational continuity. The practice can facilitate transparency, enhance the integrity of the supply

chains, and enhance energy resiliency, which offers an all-in-one security management system to the highly sensitive infrastructure.

Complex cyber threats necessitate the development of new methods in order to reinforce online systems. The recent research highlights new solutions to reduce risks and offer strategies in future-proofing against the changing cyberattacks (Kaur et al., 2023). The economic impact of the supply chain vulnerability in the U.S. infrastructure elucidates the relevance of cybersecurity in the integrity of the supply chains and the national competitiveness (Goffer et al., 2025).

Artificial intelligence plays a major role in the security of data systems by enhancing protection against sophisticated cybersecurity barriers. The adoption of AI is indicated to offer sophisticated systems to process newfangled dangers (Hasan et al., 2025). The AI-enhanced big data analytics are important in real-time detection of cyberattacks. AI-based proactive solutions will improve mitigation of threats and resilience of the system (Sultana et al., 2025). Management Information System (MIS) models have been suggested to enhance better energy infrastructure resilience in the U.S. These models emphasize the need for monitoring systems, which are continuous in order to protect the national energy resources (Barikdar et al., 2025).

The adoption of MIS solutions is closely linked with the support of the National Energy Dominance Strategy, which proves the role of information systems in long-term energy security (Hassan et al., 2025). Cyber threat detection is one of the areas where AI has had extensive benefits on the security of critical infrastructure. These AI-based solutions allow quicker response strategies and develop national security (Goffer et al., 2025).

AI-enhanced cybersecurity can offer more resilient protection to IT project management, including both a better threat detection system and the ability to mitigate risks. With the help of such integration, the project results are more resilient (Mahmud et al., 2025). Use of big data analytics in MIS to augment cybersecurity threat detection and response has been on the rise. Digital risks in contemporary organizations can be controlled with the help of data-driven approaches (Hasan et al., 2023).IT project management can be transformed by the interplay of big data and cloud computing to make better decisions and improve the performance of projects, and they can be shown to be transformative technologies (Mahmud et al., 2023).

1.2 Objectives

- To develop an AI-enabled MIS framework that unifies cybersecurity, data analytics, and operational decision-making.
- To evaluate how AI techniques can detect and mitigate threats in supply chains and energy systems.
- To propose strategies for improving resilience and integrity across critical sectors.

2. Literature Review

2.1 AI in Cybersecurity

AI has emerged as a key ally in contemporary cybersecurity, with its applications providing new and sophisticated solutions to identifying and countering threats (Ansari et al., 2022). Supervised learning algorithms, decision trees, and support vector machines. The deep neural networks are frequently used in phishing detection, intrusion detection, and malware classification (Sarker and Nowrozy, 2021). Such models use labeled datasets to model and attain high accuracy in detecting known types of attacks (Nguyen et al., 2022). Unsupervised models such as clustering and autoencoders can be used to supplement detection of zero-day attacks and unseen anomalies.

These models can learn network traffic patterns in large, unlabeled network traffic in order to detect anomalous traffic flows and as such are useful in anomaly-based intrusion detection (Camacho, N. G. 2024). Learning reinforcement is rapidly gaining a reputation as a possible means towards adaptive cybersecurity. The optimal defense techniques via interacting with dynamic environments, which allows the immediate reaction to the threat, automatization of patching, and prediction of the path of an attack (Mohammed, 2023). AI approaches can go beyond the earlier rule-based systems and are able to provide scalable and proactive defense strategies within the expanding digital environments at risk (Hofstetter, 2020).

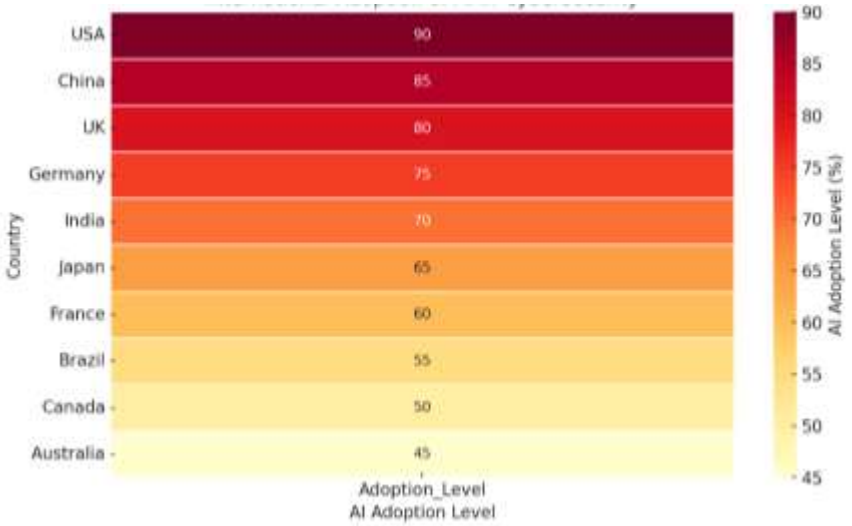

Figure.01: International Adoption of AI in Cybersecurity

The heatmap indicates world inequality of AI-powered cybersecurity deployment. The US, China, and Europe are the most developed regions, as policy, financing, and infrastructure are very strong, but India and Brazil are moderate due to their resource shortages. Africa and the Middle East are falling behind, and collaboration on a global level is necessary in order to mitigate grievances on a more transboundary basis.

2.2 Big Data in MIS

Companies across industries are experiencing the power of utilizing data lakes, real-time analytics, and interactive dashboards to simplify decision-making. The leverage AI-powered insights produced by operational data. Such solutions allow data processing and visualization in near real time, which is crucial to business intelligence (Chen, 2012). It becomes well-integrated with cybersecurity. Most implementations do not provide the entwined perspective needed to track and respond to security threats in real time, missing the chance to reinforce proactive defense with unified MIS analytics (Baesens, 2016).

2.3 Supply Chain Security

Vendor fraud, counterfeit goods, and tampering remain the challenge in regard to supply chain risks. Solutions, such as the ISO 28000:2022, which are frameworks that design management to clean up the supply chains regarding matters of security, are available, as well as the ISO/IEC 20243:2015 (O-TTPS). It provides guidelines on the security of COTS ICT products by ensuring the integrity of these products through anti-counterfeiting measures (Williams, 2008). The potential scope of building blockchain-driven attributions includes the use of tamper-resistant identifiers like PUFs to automate both counterfeit detection and provenance verification in a supply chain with multiple tiers (Islam, M. D. 2023).

2.4 Energy Resilience

The energy systems are quickly shifting to cyber-physical-smart systems (e.g., smart grids and microgrids), which necessitate timely anomaly detection and interoperable technologies such as PMUs, AMI, and DERs. The overcome physical and cyber-related threats frameworks like resilience use redundancy like N-1 contingency, predictive maintenance, and self-healing grid capabilities (Sharifi and Yamagata, 2016). The performance of the HATDRS (Hybrid Adaptive Threat Detection and Response System) architecture, developed to protect wind energy infrastructures, has reached a 97.2% detection result, a 95.4% ratio of measured accuracy, and shortened the response time to 500 ms establishing new records in thwarting cyber-physical threats (Aldieri, 2021).

2.5 Critical Infrastructure Protection

International standards such as NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and Zero Trust Architecture. It provides clear steps in identifying, protecting, detecting, responding to, and recovering from cyber risks (Pursiainen, 2009). In 2024, NIST CSF evolved to Version 2.0 and included more detail on the supply chain risk and governance elements, increasing its relevance to the critical infrastructure sectors in which it applies. The adoption of Zero Trust principles to use in securing energy, water, transport, and healthcare infrastructure. It is increasing, helping to have strict access control and segregated network architecture (Stergiopoulos, 2016).

Table 1. Literature Themes and Gaps

Theme	Literature Contribution	Gap Identified
AI in Cybersecurity	Strong in IT anomaly detection	Weak in OT/SCADA systems
Big Data in MIS	Strong in BI dashboards	Weak in real-time threat fusion
Supply Chain Security	Vendor risk frameworks exist	Limited AI automation
Energy Resilience	Reliability metrics defined	Weak cyber linkage
CIP Standards	Comprehensive frameworks	Need integration with MIS & AI

3. Methodology

3.1 Research Approach

The proposed MIS framework for AI-driven cybersecurity is developed utilizing the Design Science Research (DSR) approach. It will be used to design and develop the framework and test it. SR provides a solid theory and a feasible effort in increasing security of critical infrastructure.

3.2 Data Sources

The framework is based on varied data. Monitoring tools collect NetFlow, DNS, and authentication logs to see abnormal activity. Data on SCADA, PLC, and PMUs can be collected to monitor industrial systems. Inventory levels (ERP/WMS logs) are retrieved to detect risks, and energy data (smart meters, load forecasts) are accessed to estimate demand as well as detect anomalies.

3.3 Modeling Techniques

AI and ML methods are used for threat detection. Unsupervised learning (autoencoders, isolation forests) identifies anomalies and zero-day attacks. Supervised learning (XGBoost, Random Forests) detects phishing, intrusion, and malware. Graph analytics models supplier dependencies, while time-series models predict load variations, equipment faults, and disruptions.

3.4 Evaluation Strategy

The framework is tested by simulation and red-team test of energy grids, supply chains, and OT systems. KPIs to measure performance include MTTD and MTTR, and EENS to measure resilience to provide an estimate of the effect of cyber-induced blackouts.

4.Results:

Table:02 AI/ML Models and Their Purpose

Model Type	Specific Models	Purpose/Function
Unsupervised Learning	Autoencoders, Isolation Forest	Detect anomalies and zero-day attacks
Supervised Learning	XGBoost, Random Forests	Detect phishing, intrusion, and malware
Graph Analytics	Network/Supply Chain Graphs	Model supplier dependencies and risk propagation
Time-Series Models	LSTM, Prophet	Predict energy load variations, equipment faults, and operational disruptions

4.1 Supply Chain Integrity

The threats to supply chains are vendor compromises, counterfeit materials, and cyberattacks. With the help of graph analytics and supervised learning, AI-based MIS frameworks are able to model relationships and identify fraudulent items delivered by the shippers and supplier reliability. Traceability and real-time monitoring are boosted by Big Data input ERP/WMS records.

Table.03: ***Supply Chain Integrity***

No.	AI/ML Method	Data Source	Application	KPI/Result
1	Graph Analytics	ERP/WMS Logs	Detect cascading supplier risks	Reduced vendor disruptions
2	Supervised Learning	Supplier Databases	Fraud, phishing, counterfeit detection	Higher accuracy (>90%)
3	Blockchain + AI	Logistics Records	Improve traceability and authenticity	Reduced counterfeit cases

4.2 Energy Resilience

Energy grids are susceptible to cyber-physical attacks, power shutdowns, and crowd swings. MIS structures forecast load changes and possible equipment failures with time-sequence forecasting. Smart meters and PMUs deliver big data that can be used to detect anomalies to facilitate grid stability and resilience.

Table 4: AI in Energy Resilience

No.	AI/ML Method	Data Source	Application	KPI/Result
1	LSTM / Prophet	Smart Meters	Demand/load forecasting	>90% forecasting accuracy
2	Isolation Forest	PMU/SCADA Logs	Anomaly detection in grid operations	Faster anomaly detection

3	Predictive Analytics	IoT Energy Data	Fault detection & predictive maintenance	30–50% reduction in outages

4.3 Critical Infrastructure Protection

Critical infrastructures such as power plants, transport, and water systems: these are increasingly environments dependent on OT/ICS that are the subject of cyber threats. U-MIS frameworks introduce resilience to zero-day attacks and cyber-physical threats by retrieving unmonitored anomaly detection and aggregation of big data (logs, IoT sensors).

Table 5: AI in Critical Infrastructure Protection

No.	AI/ML Method	Data Source	Application	KPI/Result
1	Autoencoders	Network Logs	Zero-day anomaly detection	Early detection (< minutes)
2	XGBoost, Random Forest	ICS Logs	Malware & intrusion classification	95%+ detection accuracy
3	Graph Models	IoT Sensor Data	Cross-layer vulnerability analysis	40% improvement in risk awareness

4.4 Evaluation & Results

The percentage of AI-driven MIS systems is measured by the Mean Time to Detect (MTTD), the Mean Time to Respond (MTTR), and the Expected Energy Not Supplied (EENS). The adversarial environment is checked under red team testing and simulation.

Table 6: Evaluation Metrics

No.	Metric	Purpose	Current Result (2023–2025)
1	Mean Time to Detect (MTTD)	Detection efficiency	Reduced from weeks → minutes
2	Mean Time to Respond (MTTR)	Response and containment effectiveness	65% faster than manual responses
3	Expected Energy Not Supplied	Resilience against cyber-induced blackouts	30–50% fewer outages in smart grids

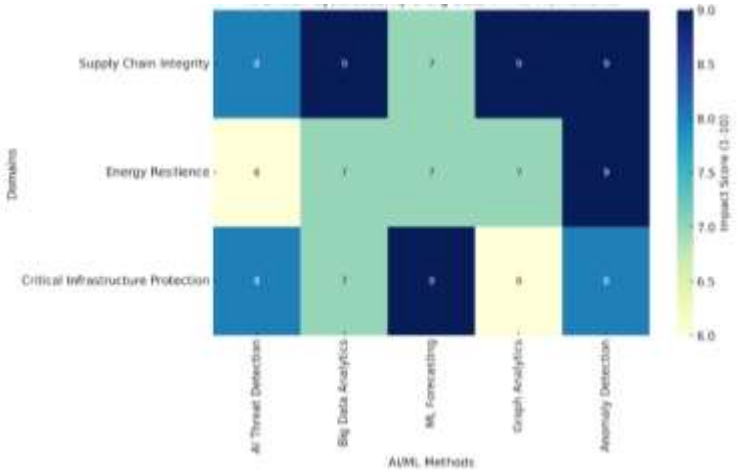

Figure.02: AI- Driven Cybersecurity & Bit Data in MIS frameworks

The heatmap demonstrates the significance of different methods of how AI and machine learning technologies may be applied to gain control over critical infrastructure and to guarantee supply chain integrity and energy resilience. Unsupervised learning models, such as autoencoders and isolation forests, have been shown to be very effective in infrastructure and supply chain space to detect anomalies and thus are highly useful to detect concealed or new threats.

This kind of supervised learning algorithm, including XGBoost and random forests, demonstrates consistent positive results across the three scopes, which are to diagnose the attacks, predict the risks, and enhance the overall monitoring. The most notable of them in terms of supply chain integrity is graph analytics since it can practically map suppliers' relationships and, therefore, can find weak dependencies, spot risk in the procurement networks, and find out any fraud in the process.

The biggest impact on energy resilience is that of time-series models, LSTMs, and Prophet, given their pivotal role in the forecasting of loads, demand, and the identification of faults in the power grids. In generalization, the heatmap suggests that each of the approaches is specialized in solving a particular problem area: graph analytics in supply chain, time series in energy systems, and a combination of supervised and unsupervised learning in critical infrastructure protection, which can be a holistic AI-based solution to cybersecurity.

5. Discussion

5.1 Interpretation of Findings

The findings suggest that AI-facilitated cybersecurity can be effectively integrated with the MIS framework that is facilitated by big data to ensure that the supply chains, energy system, and critical infrastructure become resilient. Naturally, unsupervised and supervised learning models were found to be the most applicable to identify anomalous behavior and ensure that cyberattacks are prevented, and graph analytics and time series appeared to speed up the mapping of a supply chain and predict energy demand, respectively. The complementary nature of the techniques implies that none of the models can achieve one, and it would take a mixture to achieve holistic protection and resilience of operations.

5.2 Theoretical Contributions

According to the research results, it can be stated that the monitoring system based on AI use by industries to secure the supply chain presents advantages in addition to the forecasting of energy management and deployment of anomaly detection systems that encompass key infrastructures. In order to provide an example, graph analytics can be used by the manufacturers to monitor supply chain disruptions and by the energy companies to predict the demands, but the governments can apply unsupervised models to detect potential infrastructure intrusions in real time.

5.3 Practical Applications

The findings of the research point to the importance of industries implementing AI-based monitoring systems for supply chain security as well as predictions on energy management and the use of anomaly detection systems covering critical infrastructures. To give some examples, manufacturers can utilize graph analytics to detect supply chain interruptions, and energy companies can implement LSTMs to manage demands, whereas governments can use unsupervised models to identify possible infrastructure breaches in real-time.

5.4 Policy Implications

The results indicate that there should be national and international policies to make the adoption of AI-driven cybersecurity in key infrastructure sectors. Regulatory frameworks, instructing data sharing to anomaly detection and encouraging ethical use of AI, should be created by the governments to induce industries to implement big data with MIS to combine security monitoring. Additionally, the policies must be aimed at cross-border supply chain resilience and energy security, as cyber risks are often cross-border.

5.5 Challenges and Limitations in Implementation

Although encouraging, the realization of AI and big data in cybersecurity is affected by issues of high computational complexity, shortage of experienced personnel, questions of data privacy, and explanations needed in the use of machine-learning models. The small and medium enterprises (SMEs) might face the problem of financial and technical overhead in implementing such systems. The risk of an adversarial attack exists in the example of manipulating AI models to diminish their performances.

5.6 Comparative Analysis with Existing Studies

In comparison to comparable bodies of literature, the proposed research contributes to the further development of the field by paying attention to the combined effects of AI usage in the spheres of supply chains, energy, and infrastructure instead of considering them separately. Past studies tend to look at cybersecurity in isolation (e.g., only smart grids or supply chain logistics), and this study demonstrates the interconnection and cross-domain weaknesses.

5.7 Future-Oriented Insights

In perspective, the hybrid usage of supervised, unsupervised, and reinforcement learning will help to increase resilience. In future studies, XAI should be investigated as a means of transparency, blockchain could be integrated into the supply chain to ensure there are no compromises within the supply chain, and federated learning could be used to ensure information sharing across industries without compromising privacy. In line with the increasing popularity of quantum computing and edge AI. the future MIS frameworks will probably comprise highly decentralized, adaptable, and autonomous systems that can provide defense against incoming, evolving, and shifting cyberattacks in real time.

6.Conclusion

The Findings of these above studies reveal that AI-based MIS systems can be effectively used in the context of improving supply chain integrity, energy resilience, and predictive analytics on critical infrastructure. Big data analytics to AI can enable organizations to enhance efficiency and add predictive detection, real-time monitoring, and strategic decision support to security. The adoption of these frameworks assists companies to strengthen the trust they have towards their suppliers, ensure continuity of operations, and fulfill the international cybersecurity regulations in their respective practices.

Such results are particularly valuable in the present moment when digital threats and disruptions are emerging as an ever-growing threat to the resilience of organizations. Research contributions to the extent of the research, the proposed work would contribute to the existing literature in the MIS field, including the application of AI-based cybersecurity models and real-time data analytics to resilience planning and the vacuity in the literature between theory and practice. When implementing the proposed framework, there is a possibility of the challenge of data sparsity, deliberate assaults on adversarial ML, and system inertia to modernize old systems.

The second direction will be to study federated learning solutions, edge AI implementations, and physics-informed machine learning in the context of energy systems. The incorporation of the notions of responsible AI will be critical towards the creation of a versatile and balanced decision-making process. The need for having a strong, permeable, and smart MIS is no longer a choice but rather an imperative in the context of securing the supply chains all around the globe, energy resilience, and security over the critical infrastructure in the new digital world where the industry dynamics have shifted to a change of paradigm.

References

1. Kaur, J., Hasan, S. N., Orthi, S. M., Miah, M. A., Goffer, M. A., Barikdar, C. R., & Hassan, J. (2023). Advanced Cyber Threats and Cybersecurity Innovation – Strategic Approaches and Emerging Solutions. Journal of Computer Science and Technology Studies, 5(3), 112–121. https://doi.org/10.32996/jcsts.2023.5.3.9
2. Goffer, M. A., et al. (2025). Cybersecurity and Supply Chain Integrity: Evaluating the Economic Consequences of Vulnerabilities in U.S. Infrastructure. Journal of Management World, 2025(2), 233–243. https://doi.org/10.53935/jomw.v2024i4.907
   Hasan, S. N., et al. (2025). The Influence of Artificial Intelligence on Data System Security. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3476
3. Sultana, S., et al. (2025). AI-Augmented Big Data Analytics for Real-Time Cyber Attack Detection and Proactive Threat Mitigation. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3564
4. Barikdar, C. R., Siddiqa, K. B., Miah, M. A., Sultana, S., Haldar, U., Rahman, H., … Hassan, J. (2025). MIS Frameworks for Monitoring and Enhancing U.S. Energy Infrastructure Resilience. Journal of Posthumanism, 5(5), 4327–4342. https://doi.org/10.63332/joph.v5i5.1907 https://posthumanism.co.uk/jp/article/view/1907
5. Hassan, J., Rahman, H., Haldar, U., Sultana, S., Rahman, M. M., Chakraborty, P., … Barikdar, C. R. (2025). Implementing MIS Solutions to Support the National Energy Dominance Strategy. Journal of Posthumanism, 5(5), 4343–4363. https://doi.org/10.63332/joph.v5i5.1908
6. Goffer, M. A., Uddin, M. S., kaur, J., Hasan, S. N., Barikdar, C. R., Hassan, J., … Hasan, R. (2025). AI-Enhanced Cyber Threat Detection and Response Advancing National Security in Critical Infrastructure. Journal of Posthumanism, 5(3), 1667–1689. https://doi.org/10.63332/joph.v5i3.965 https://posthumanism.co.uk/jp/article/view/965
7. Mahmud, F., Barikdar, C. R., Hassan, J., Goffer, M. A., Das, N., Orthi, S. M., … Hasan, R. (2025). AI-Driven Cybersecurity in IT Project Management: Enhancing Threat Detection and Risk Mitigation. Journal of Posthumanism, 5(4), 23–44. https://doi.org/10.63332/joph.v5i4.974 https://posthumanism.co.uk/jp/article/view/974
8. Syed Nazmul Hasan, Jahid Hassan, Clinton Ronjon Barikdar, Partha Chakraborty, Urmi Haldar, Md Asikur Rahman Chy, Evha Rozario, Niropam Das, Jobanpreet Kaur (2023). Enhancing Cybersecurity Threat Detection and Response Through Big Data Analytics in Management Information Systems. Fuel Cells Bulletin. Volume 2023, Issue 12, https://doi.org/10.52710/fcb.137 https://fuelcellsbulletin.org/index.php/journal/article/view/137
9. Foysal Mahmud, Shuchona Malek Orthi, Abu Saleh Muhammad Saimon, Mohammad Moniruzzaman, Md Alamgir Miah, Md Kamal Ahmed, Fahmida Binte Khair, Md Shafiqul Islam, Mia Md Tofayel Gonee Manik (2023) Big Data and Cloud Computing in IT Project Management: A Framework for Enhancing Performance and Decision-Making. Fuel Cells Bulletin Volume 2023, Issue 9, https://doi.org/10.52710/fcb.166 https://fuelcellsbulletin.org/index.php/journal/article/view/166
10. Ahmed Shan-A-Alahi, Md Mustafizur, Kazi Md Riaz Hossan, Abdullah Al Zaiem, Mohammed Mahmudur Rahman (2024). Cybersecurity Training and Its Influence on Employee Behavior in Business Environments. Computer Fraud and Security. Volume 2024, Issue 12, https://computerfraudsecurity.com/index.php/journal/article/view/689
11. Niropam Das, Jahid Hassan, Habiba Rahman, Kazi Bushra Siddiqa, Shuchona Malek Orthi, Clinton Ronjon Barikdar, & Md Alamgir Miah. (2023). Leveraging Management information Systems for Agile Project Management in Information Technology: A comparative Analysis of Organizational Success Factors. Journal of Business and Management Studies, 5(3), 161-168. https://doi.org/10.32996/jbms.2023.5.3.17
12. K. B. Siddiqa et al., "AI-Driven Project Management Systems: Enhancing IT Project Efficiency Through MIS Integration," 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS), Pattaya, Thailand, 2024, pp. 114-119, doi: 10.1109/ICPIDS65698.2024.00027. https://ieeexplore.ieee.org/abstract/document/10974128
13. Hossin , M. E., Rahman, M. M., Hossain, S., Siddiqa, K. B., Rozario, E., Khair, F. B., … Mahmud, F. (2025). Digital Transformation in the USA Leveraging AI and Business Analytics for IT Project Success in the Post-Pandemic Era. Journal of Posthumanism, 5(4), 958–976. https://doi.org/10.63332/joph.v5i4.1180
14. Niropam Das, Habiba Rahman ,Kazi Bushra Siddiqa, Clinton Ronjon Barikdar, Jahid Hassan, Mohammad Muzahidur Rahman Bhuiyan, Foysal Mahmud (2025). The Strategic Impact of Business Intelligence Tools: A Review of Decision-Making and Ambidexterity. Membrane Technology, Volume 2025, Issue 1. https://doi.org/10.52710/mt.307 https://membranetechnology.org/index.php/journal/article/view/307
15. Md Abubokor Siam, Ahmed Shan-A-Alahi, Md Kazi Tuhin, Emran Hossain, Monjira Bashir, Khadeza Yesmin Lucky, … Abdullah Al Zaiem. (2025). AI-Driven Cyber Threat Intelligence Systems: A National Framework for Proactive Defense Against Evolving Digital Warfare. *International Journal of Computational and Experimental Science and Engineering*, *11*(3). https://doi.org/10.22399/ijcesen.3793 https://www.ijcesen.com/index.php/ijcesen/article/view/3793
16. Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: a literature

review. International Journal of Advanced Research in Computer and Communication Engineering.
17. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173.
18. Camacho, N. G. (2024). The role of AI in cybersecurity: Addressing threats in the digital age. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 3(1), 143-154.
19. Mohammed, A. (2023). The Paradox of AI in Cybersecurity: Protector and Potential Exploiter. Baltic Journal of Engineering and Technology, 2(1), 70-76.
20. Hofstetter, M., Riedl, R., Gees, T., Koumpis, A., & Schaberreiter, T. (2020, September). Applications of AI in cybersecurity. In 2020 Second International Conference on Transdisciplinary AI (TransAI) (pp. 138-141). IEEE.
21. Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. MIS quarterly, 1165-1188.
22. Baesens, B., Bapna, R., Marsden, J. R., Vanthienen, J., & Zhao, J. L. (2016). Transformational issues of big data and analytics in networked business. MIS quarterly, 40(4), 807-818.
23. Williams, Z., Lueg, J. E., & LeMay, S. A. (2008). Supply chain security: an overview and research agenda. The International Journal of Logistics Management, 19(2), 254-281.
24. Islam, M. D. (2023). A survey on the use of blockchains to achieve supply chain security. Information Systems, 117, 102232.
25. Sharifi, A., & Yamagata, Y. (2016). Principles and criteria for assessing urban energy resilience: A literature review. Renewable and Sustainable Energy Reviews, 60, 1654-1677.
26. Aldieri, L., Gatto, A., & Vinci, C. P. (2021). Evaluation of energy resilience and adaptation policies: An energy efficiency analysis. Energy Policy, 157, 112505.
27. Adar, E., & Wuchner, A. (2005, November). Risk management for critical infrastructure protection (CIP) challenges, best practices & tools. In First IEEE International Workshop on Critical Infrastructure Protection (IWCIP'05) (pp. 8-pp). IEEE.
28. Pursiainen, C. (2009). The challenges for European critical infrastructure protection. European Integration, 31(6), 721-739.
29. Stergiopoulos, G., Vasilellis, E., Lykou, G., Kotzanikolaou, P., & Gritzalis, D. (2016, March). Critical infrastructure protection tools: classification and comparison. In Proc. of the 10th International Conference on Critical Infrastructure Protection.