JCSEI
Journal of Computational Systems & Engineering Insights

JOURNAL
OF COMPUTATIONAL SYSTEMS
& ENGINEERING INSIGHTS

Volume 4, No 1, 2026

AI-Powered Cyber Resilience Strategies for Modern Organizations

Khamzat Hamdan, Faculty of Computing, Universiti Teknologi Malaysia
khamzathamdan@utm.my

ABSTRACT-- The rapid digital transformation, cloud computing, Internet of Things (IoT), and artificial intelligence (AI) technologies have transformed the outlook of cybersecurity of the modern organizations significantly. On the one hand, digital innovation improves efficiency and connectivity in operation, and it leaves the organization more exposed to more advanced cyber threats, including ransomware, phishing, insider attacks, and supply chain breaches. The traditional cybersecurity practices that were more preventative fail in the dynamic threat landscape. This results in organizations shifting to more cyber resilience models, that emphasize preparedness, response, recovery, continuity, and flexibility.

It is a review article on AI-powered cyber resilience solutions and the ways they can be applied to improve organizational security and operational resilience. The article explores the integration of machine learning, behavioral analytics, predictive intelligence, autonomous incident response, the Zero Trust Architecture, artificial intelligence-based threat detection, cloud security resilience, and Security Information and Event Management systems into existing cybersecurity ecosystems. The research also covers the strategic benefits of AI-based resilience, including real-time threat detection, predictive analytics, and automated defense mechanisms, and adaptive security architectures.

In addition, the article identifies significant problems with AI-driven cybersecurity that include adversarial attacks, privacy, algorithmic bias, ethical governance, workforce skill shortage, and regulatory ambiguity. New technologies such as generative AI, federated learning, explainable AI, and autonomous Security Operations Centers are also discussed.

The results indicate that AI-based cyber resilience is much more effective in terms of threat detection accuracy, incident response effectiveness, and organizational adaptability. Nevertheless, effective implementation is based on effective governance systems, ethics, human-AI interactions, and ongoing workforce development. In conclusion, the article states that AI-based cyber resilience will be a strategic business capacity that ensures operational continuity and protection of digital transformation efforts in contemporary organizations.

INDEX TERMS-- *Artificial Intelligence, Cyber Resilience, Cybersecurity, Machine Learning, Threat Intelligence, Zero Trust Architecture, Predictive Analytics, Digital Transformation*

Article History

Article Received: Nov 11, 2025

Article Processed: Dec 23, 2025

Article Published: Jan 27, 2026

JCSEI
Journal of Computational Systems & Engineering Insights

JOURNAL
OF COMPUTATIONAL SYSTEMS
& ENGINEERING INSIGHTS

Volume 4, No 1, 2026

INTRODUCTION

Contemporary organizations are working in highly networked digital ecosystems in which cyber threats are becoming more frequent, sophisticated, and severe. Cloud computing, remote work systems, artificial intelligence, edge computing, mobile systems, and IoT devices are technologies that have increased the pace of digital transformation in industries. These technologies have offered flexibility of operations and innovation but also increased attack surface of cybercriminals [1].

Cyberattacks have developed beyond the solitary cases of malware to highly organized and smart campaigns with ransomware, phishing automation, insider threats, supply chain intrusions and AI-based techniques of attacks [2]. Automation and machine learning are increasingly becoming popular among cybercriminals in detecting vulnerabilities, avoiding detection systems, and performing machine-speed adaptive attacks. Consequently, organizations are coming to the realization that the conventional cybersecurity strategies that emphasized only on prevention are not adequate [3].

Cyber resilience has thus become a strategic organizational capability that focuses on preparedness, response, recovery, continuity, and adaptation . Unlike conventional cybersecurity models, cyber resilience acknowledges that cyber incidences are bound to happen and aims at mitigating the consequences of operational discontinuity but in a way that recovery is achieved in a timely manner [4]. Cyber resilience integrates cybersecurity, business continuity, disaster recovery, governance, and risk management into one system [5].

Artificial intelligence is one of the greatest technologies that has improved cyber resiliency. Using AI-driven solutions, large amounts of data can be analyzed, latent patterns of attacks can be identified, incident response can be automated, and it is much easier to predict a probable attack than with traditional security tools [6]. Machine learning, deep learning, natural language processing, and behavioral analytics are becoming the part of modern cybersecurity systems.

AI-based cybersecurity solutions have several strategic advantages. These systems enable real-time tracking, anomaly identification, predictive risk detection, malware classification, and intelligent threat detection [7]. AI can handle large volumes of network traffic, endpoint telemetry data, user behavior data, and threat intelligence feeds more quickly and detect indicators of compromise more accurately.

The advent of multi-clouds and hybrid workplaces has only increased the pressure of smart and flexible security systems. Organizations require cybersecurity systems capable of operating in distributed environments without disrupting operations [8]. Scalability and flexibilities are required to protect multifaceted digital infrastructures with AI-based cyber resilience.

In addition to these advantages, there are also serious concerns related to the introduction of AI in the sphere of cybersecurity. AI systems can be attacked by adversarial attacks, model manipulation, and data poisoning [9]. Additionally, the use of AI is still affected by algorithmic bias, explainability, privacy protection, ethical governance, and regulatory compliance [10].

This review article discusses AI-based cyber resilience measures in contemporary organisations. The paper will present the conceptual framework of cyber resilience, AI role in cybersecurity

JCSEI
Journal of Computational Systems & Engineering Insights
JOURNAL
OF COMPUTATIONAL SYSTEMS
& ENGINEERING INSIGHTS
Volume 4, No 1, 2026

transformation, major resilience plans, implementation frameworks, organizational concerns, and future trends that will remodel the intelligent cybersecurity ecosystems.

CONCEPTUAL FOUNDATIONS OF CYBER RESILIENCE

Cyber resilience is an organization's capacity to prepare, endure, react, recover, and adapt from cyber incidents, with minimal impact on mission-critical functions. Continuity, adaptability, and recovery are the pillars of cyber resilience as compared to the conventional cybersecurity strategies, which are mainly based on prevention.

As cyber threats have become more complex and organisations rely on digital technologies, the term cyber resilience was born. The previous perimeters-based security systems are no longer working, since the current infrastructures are the cloud, the IoT, remote working systems and connected supply chains.

Cyber resilience frameworks are built upon several key principles:

- Anticipation of threats through predictive analytics and threat intelligence.
- Resistance through strong security controls and adaptive architectures.
- Recovery through incident response and disaster recovery planning.
- Adaptation through continuous learning and improvement.
- Continuity through resilient business operations.

Cyber Resilience is the result of technology, organisation and human factors. It combines cybersecurity controls and governance systems, employee awareness, operating continuity planning and strategic risk management.

Companies with holistic and well-prepared cyber resilience strategies are more likely to minimize disruptions, maintain customer trust, enhance compliance, and boost long-term viability.

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

AI is an essential part of today's cybersecurity infrastructure [11]. As cybersecurity threats grow in volume, size, and complexity, intelligent systems must be able to deal with big data, detect stealthy attack patterns, and respond quickly to the incident.

One of the most widely-used AI technologies in cybersecurity is machine learning. Typically, supervised learning models are applied for spam filtering, phishing detection, malware classification and fraud detection [12]. The process of detection of anomalies and identification of insider threats is helped by unsupervised learning because of the recognition of abnormal behavioral patterns.

Neural network designs of deep learning technologies are designed to detect more sophisticated threats by analyzing complex data interactions [13]. These systems are more frequently used in malware analysis, intrusion detection and behavioral analytics.

NLP facilitates the capacity of cybersecurity systems to scan emails, threat reports, social media content, and dark web messages [14]. NLP technologies are used in phishing detection, automated threat intelligence analysis, and security reporting.

JCSEI
ournal of Computational
Systems & Engineering Insights

JOURNAL
OF COMPUTATIONAL SYSTEMS
& ENGINEERING INSIGHTS

Volume 4, No 1, 2026

One of the important applications of AI in cybersecurity is behavioral analytics [15]. AI-powered User and Entity Behavior Analytics (UEBA) platforms are designed to detect suspicious login patterns, access attempts, device usage, and network activities, which helps uncover insider threats and suspicious activities [16].

Both structured and unstructured data sources are fed into AI-driven threat intelligence platforms which then deliver predictive information about new threats. These systems can be part of an organization's proactive risk management efforts, improving situational awareness.

A. AI-DRIVEN THREAT DETECTION

An AI-based threat detection system monitors networks, endpoint, apps and cloud environments, looking for suspicious activity at any given time [17]. Malware, phishing, ransomware activities, insider threats and unauthorized access trends are difficult to be recognized by rule-based systems, but can be detected effectively by Machine Learning algorithms [18].

AI-based detection improves:

- Threat visibility
- Detection accuracy
- Response speed
- Reduction of false positives
- Continuous monitoring capabilities

B. PREDICTIVE ANALYTICS AND THREAT INTELLIGENCE

Organisations will be able to anticipate cyber threats using predictive analytics and to ward them off. Artificial intelligence models are fed with previous attack data, trends in vulnerabilities, environmental context, and external feeds of threat information.

Predictive cybersecurity supports:

- Risk forecasting
- Vulnerability prioritization
- Proactive defense planning
- Security resource optimization
- Threat anticipation

AI-powered threat intelligence systems provide real-time situational awareness and improve strategic decision-making.

C. AUTONOMOUS INCIDENT RESPONSE

The existing cyberattacks are carried out at machine speed, and responding manually is turning into an increasingly difficult task. SOAR is an AI-based automated tool that defends against threats, isolates devices, blocks malicious traffic, and remediates [19].

Autonomous response mechanisms improve:

- Incident response speed
- Operational efficiency
- Recovery coordination

JCSEI
ournal of Computational
Systems & Engineering Insights

JOURNAL
OF COMPUTATIONAL SYSTEMS
& ENGINEERING INSIGHTS

Volume 4, No 1, 2026

- Threat mitigation
- Business continuity

Human intervention required to ensure accountability and prevent undesired interferences in operations.

D. ZERO TRUST ARCHITECTURE

The principle of Zero Trust Architecture (ZTA) is 'never trust, always verify'. AI technologies can help with Zero Trust approaches by providing authentication, behavioral modeling and adaptive access controls [20].

AI-enhanced Zero Trust systems support:

- Continuous identity verification
- Dynamic access management
- Context-aware authentication
- Behavioral risk assessment
- Micro-segmentation

These functions reduce the attack surfaces and limit the lateral movement within networks

E. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

AI-based SIEM systems collect and process security information in multiple organizational sources [21]. These systems improve event correlation, anomaly detection, and threat prioritization.

Benefits of AI-enhanced SIEM include:

- Real-time visibility
- Automated alerting
- Improved incident investigation
- Faster decision-making
- Reduced analyst workload

F. EXTENDED DETECTION AND RESPONSE (XDR)

Extended Detection and Response integrates endpoint, network, cloud environments, and application telemetry data to a single detection platform [22].

AI-driven XDR solutions provide:

- Cross-domain threat visibility
- Integrated threat intelligence
- Automated investigation
- Coordinated incident response
- Advanced threat hunting

G. SELF-HEALING SECURITY SYSTEMS

Self-healing cybersecurity systems utilize AI to automatically identify vulnerabilities, isolate threats, and recover affected systems.

These systems support:

- Automated patch management
- Configuration correction

JCSEI
ournal of Computational
Systems & Engineering Insights
JOURNAL
OF COMPUTATIONAL SYSTEMS
& ENGINEERING INSIGHTS
Volume 4, No 1, 2026

- Dynamic infrastructure recovery
- System stabilization
- Operational continuity

The ability to self-heal is becoming significant in critical infrastructure protection.

ORGANIZATIONAL FRAMEWORKS FOR CYBER RESILIENCE

It is essential to have strong governance and organizational management to implement effective AI-driven cyber resilience. The concept of cyber resilience should be integrated into enterprise risk management, strategic planning, and business continuity initiatives [23].

A. GOVERNANCE AND LEADERSHIP

The executive leadership is an important contributor to setting objectives for resilience, cyber security resources and risk tolerance. As cyber resilience moves to a strategic business concern, the board level is gaining significance.

B. HUMAN-AI COLLABORATION

While AI can streamline certain cybersecurity functions, it will not replace the human element for strategic analysis, ethical implications, and interpreting cyber incidents [24]. In essence, cyber resilience is a sign of cooperation between intelligent systems and proficient cybersecurity experts.

C. WORKFORCE DEVELOPMENT

Cybersecurity awareness and AI literacy training, phishing, and incident response exercises are areas that should be invested in by the organization [25]. One of the major causes of cybersecurity incidents is human error, which is why the workforce should be prepared.

D. Regulatory Compliance

Organizations must align AI-powered resilience strategies with regulatory and industry frameworks such as:

- NIST Cybersecurity Framework
- ISO/IEC 27001
- GDPR
- HIPAA
- PCI DSS
- NIS2 Directive

AI systems can support automated compliance monitoring and reporting.

E. INCIDENT RESPONSE AND CONTINUITY PLANNING

Incident response systems powered by AI enhance resilience by automating forensic analysis, orchestrating recoveries, and ensuring constant monitoring.

Business continuity planning should incorporate:

- Automated backup systems
- AI-based recovery mechanisms
- Resilience testing exercises
- Crisis communication strategies
- Continuous operational monitoring

INDUSTRY APPLICATIONS OF AI-POWERED CYBER RESILIENCE

JCSEI
ournal of Computational
Systems & Engineering Insights

JOURNAL
OF COMPUTATIONAL SYSTEMS
& ENGINEERING INSIGHTS

Volume 4, No 1, 2026

A. HEALTHCARE SECTOR

Cyber threats continue to pose growing dangers to healthcare organizations because of the sensitive patient information and linked medical devices. AI-driven resiliency assists in ransomware detection, medical device protection, fraud prevention, and healthcare continuity.

B. FINANCIAL SERVICES

Artificial intelligence-powered resilience systems are applied by financial institutions to detect fraud, monitor transactions, anti-money laundering analytics, and behavioral authentication.

C. MANUFACTURING AND INDUSTRIAL SYSTEMS

Industrial organizations are relying more on operational technologies and Industrial IoT systems. AI is used in predictive maintenance, anomaly detection, and protecting industrial infrastructure.

D. GOVERNMENT AND PUBLIC SECTOR

AI-driven cyber resilience is used by government agencies to monitor critical infrastructure, carry out national cybersecurity activities, share threat intelligence, and defend against nation-state attacks.

E. EDUCATION SECTOR

Educational institutions implement AI-powered security mechanisms to protect research data, student information, and remote learning systems.

F. RETAIL AND E-COMMERCE

Retail organizations use AI-based fraud prevention, customer identity protection, payment security, and transaction monitoring systems.

CHALLENGES AND ETHICAL CONCERNS

A. ADVERSARIAL AI ATTACKS

AI systems can be susceptible to adversarial attacks, which include data poisoning, manipulation of the model, and generation of malicious inputs. Organizations need to safely set AI training pipelines and constantly check model performance.

B. DATA PRIVACY AND CONFIDENTIALITY

Cybersecurity systems powered by AI demand huge amounts of data, casting doubts on the protection of privacy, the threat of surveillance, and the governance of cross-border data.

C. ALGORITHMIC BIAS

Biased training data may lead to false threat prioritization and discriminating security results. Organizations are supposed to use explainable AI and mechanisms of fairness.

D. EXPLAINABILITY AND TRANSPARENCY

Most AI systems are black boxes, which restrict transparency and accountability. Regulatory compliance and human oversight require explainable AI structures.

E. WORKFORCE SKILL GAPS

Cybersecurity and AI professional shortage is also a significant issue. Organizations must invest in workforce development, interdisciplinary training and lifelong learning.

F. ETHICAL GOVERNANCE

JCSEI
Journal of Computational Systems & Engineering Insights
JOURNAL
OF COMPUTATIONAL SYSTEMS
& ENGINEERING INSIGHTS
Volume 4, No 1, 2026

AI-based cybersecurity presents ethical issues regarding surveillance, intrusion of privacy, autonomy in decision-making, and responsibility. Ethical AI governance frameworks are needed to ensure that AI is implemented responsibly.

FUTURE TRENDS IN AI-POWERED CYBER RESILIENCE

A. GENERATIVE AI IN CYBERSECURITY

Even automated threat analysis, security reporting, phishing simulations and intelligent assistants are possible with Generative AI technologies. Attacks can also be more sophisticated, with attackers using a generative AI to create more sophisticated phishing attacks and malware.

B. AUTONOMOUS SECURITY OPERATIONS CENTERS

The rest of the Future Security Operations Centers (SOCs) will be all about the day to day automation of AI-powered monitoring, investigation, incident response and threat prioritization.

C. QUANTUM COMPUTING AND CYBERSECURITY

The conventional encryption practices and more sophisticated optimization and threat analysis can be affected by quantum computing. It is essential for organizations to be ready for the coming of Post-quantum cryptography.

D. FEDERATED LEARNING

Organisations can train AI models without having to share their central data with federated learning. This will improve privacy protection and collective threat intelligence.

E. EXPLAINABLE AI

The future cybersecurity initiatives will emphasize transparency, explainability, and accountability, thereby fostering trust, compliance with regulations, and responsible management.

F. CYBER RESILIENCE AS A STRATEGIC CAPABILITY

In an era where organizations are increasingly connected to digital transformation, customer trust and business sustainability, Cyber resilience, as a competence, is becoming a key element. AI will continue to play a crucial role in the quest for resilience in the future, making it a relevant topic for the competition to stay competitive.

CONCLUSION

The Web is quickly morphing and has completely transformed the cyber security challenges faced by today's organizations. As the nature of cyber threats becomes more complex, the implementation of cloud adoption, IoT and AI-driven attack methods, the organizations need to turn to more modern approaches of cyber resilience, not prevention-based approaches of cyber security.

The advent of artificial intelligence (AI) technologies, such as machine learning, behavioral analytics, predictive intelligence and autonomous security systems, is changing the modern-day ecosystem of cybersecurity. The AI function of the cyber resiliency can enhance threat detection, incident response, operational resiliency and adaptive defence.

However, the implementation of AI is also linked to such problems as adversarial attacks, threat to privacy, ethical concerns, a lack of explainability, and workforce shortages. In order to achieve this, it is

JCSEI
Journal of Computational Systems & Engineering Insights
JOURNAL
OF COMPUTATIONAL SYSTEMS
& ENGINEERING INSIGHTS
Volume 4, No 1, 2026

important that organizations determine a balance between automation and governance, transparency and regulation compliance, and human controls.

The building blocks of future cyber resilience strategies are autonomous security systems, Zero Trust architecture, explainable AI and federated learning and human-AI collaboration. Strategically investing in AI-driven resilience solutions puts those organizations ahead of the curve in protecting critical assets, ensuring business continuity, driving digital transformation, and long-term sustainability.

Ultimately, AI-powered cyber resilience gets to be not just a technical need, but actually a strategic tool for the organization that should be considered as an asset to help them thrive amid the evolving landscape of cyber threats.

REFERENCES

[1] S. K. Sundaramurthy, N. Ravichandran, A. C. Inaganti, and R. Muppalaneni, "AI-powered operational resilience: Building secure, scalable, and intelligent enterprises," *Artif. Intell. Mach. Learn. Rev.*, vol. 3, no. 1, pp. 1–10, 2022.

[2] A. S. George, "Cyber resilience in an AI-driven world: A strategic framework," *Partners Univ. Innov. Res. Publ.*, vol. 3, no. 6, pp. 86–118, 2025.

[3] A. S. George, "Cyber resilience in an AI-driven world: A strategic framework," *Partners Univ. Innov. Res. Publ.*, vol. 3, no. 6, pp. 86–118, 2025.

[4] F. Amin and U. Imtiaz, "Mitigating advanced persistent threats: A framework for enhancing organizational cybersecurity posture," *J. Eng. Comput. Intell. Rev.*, vol. 3, no. 1, pp. 99–113, 2025.

[5] S. M. H. Shah, F. Amin, and A. Khan, "Cyber-resilient mobile edge computing: A deep neural approach for secure and efficient task offloading," *Asian Bull. Big Data Manag.*, vol. 5, no. 1, pp. 200–215, 2025.

[6] S. T. Hasan, "Mitigating algorithmic bias in AI-driven hiring systems in the United States," *J. Bus. Insight Innov.*, vol. 5, no. 1, pp. 78–90, 2026.

[7] U. Imtiaz, S. Malik, and A. Khan, "Blockchain-driven cybersecurity framework for smart homes: Integrating IoT and machine learning for secure automation," *Asian Bull. Big Data Manag.*, vol. 4, no. 4, pp. 570–583, 2024.

[8] U. Imtiaz and H. Elbedour, "Cybersecurity risk management in the digital era: The strategic value of ethical hacking," *Spectrum Eng. Sci.*, pp. 1076–1086, 2025.

[9] S. T. Hasan, "Machine learning models for forecasting employee demand in healthcare HR," *J. Eng. Comput. Intell. Rev.*, vol. 3, no. 2, pp. 159–172, 2025.

[10] F. T. Zohora and P. Paul, "Maternocare prediction for maternal and child well-being using survey data and machine learning approaches," *Excel Int. J. Technol. Eng. Manag.*, vol. 11, no. 4, pp. 170–180, 2024.

[11] M. S. R. Aronno et al., "A study of cyber bullying classification using social media and textual analysis based on machine learning approaches," in *2023 14th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2023, pp. 1–8.

[12] M. T. Islam, A. Azeem, M. Jabir, A. Paul, and S. K. Paul, "An inventory model for a three-stage supply chain with random capacities considering disruptions and supplier reliability," *Ann. Oper. Res.*, vol. 315, no. 2, pp. 1703–1728, 2022.

[13] A. A. M. Jabir, L. Salazar, and J. Li, "Investigation of process parameters to fabricate TiWMo refractory medium entropy alloy via laser powder bed fusion," *Prog. Addit. Manuf.*, pp. 1–11, 2026.
[14] J. H. Tarek and W. Rahman, "AI-driven cybersecurity, IoT networking, and resilience strategies for industrial control systems: A systematic review for US critical infrastructure protection," *Int. J. Sci. Interdiscip. Res.*, vol. 4, no. 4, pp. 144–176, 2023.
[15] S. Butt, I. Mubeen, and N. Yazdani, "Exploring the lived experiences of individuals to manage and cope with type 2 diabetes applying IPA," *Pak. Lang. Humanit. Rev.*, vol. 8, no. 2, pp. 526–539, 2024.
[16] S. Butt and N. Yazdani, "Relationship between execution of quality management practices and firm's innovation performance: A review of literature," *J. Asian Dev. Stud.*, vol. 12, no. 3, pp. 432–451, 2023.
[17] K. Saurabh, "Building resilient IT infrastructures: The role of AI and cybersecurity in program management," *J. Data Anal. Crit. Manag.*, vol. 1, no. 4, pp. 103–113, 2025.
[18] N. Rane, S. Choudhary, and J. Rane, "Artificial intelligence for enhancing resilience," *J. Appl. Artif. Intell.*, vol. 5, no. 2, pp. 1–33, 2024.
[19] M. M. Alnfiai, "AI-powered cyber resilience: A reinforcement learning approach for automated threat hunting in 5G networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2025, no. 1, Art. no. 68, 2025.
[20] S. A. Syed, "Adversarial AI and cybersecurity: Defending against AI-powered cyber threats," *Iconic Res. Eng. J.*, vol. 8, no. 9, pp. 1030–1041, 2025.
[21] A. Arif, M. I. Khan, and A. R. A. Khan, "An overview of cyber threats generated by AI," *Int. J. Multidiscip. Sci. Arts*, vol. 3, no. 4, pp. 67–76, 2024.
[22] G. Waizel, "Bridging the AI divide: The evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defenses," in *Int. Conf. Mach. Intell. Secur. Smart Cities (TRUST) Proc.*, vol. 1, Jul. 2024, pp. 141–156.
[23] R. Muppalaneni, A. C. Inaganti, and N. Ravichandran, "AI-driven threat intelligence: Enhancing cyber defense with machine learning," *J. Comput. Innov. Appl.*, vol. 2, no. 1, pp. 1–11, 2024.
[24] J. S. Ibitoye and F. E. Ayobami, "Unmasking vulnerabilities: AI-powered cybersecurity threats and their impact on national security – Exploring the dual role of AI in modern cybersecurity – A threat and a shield," *CogNexus*, vol. 1, no. 1, pp. 311–326, 2025.
[25] J. Sivakumar, N. R. Salman, F. R. Salman, H. R. Salimova, and E. Ghimire, "AI-driven cyber threat detection: Enhancing security through intelligent engineering systems," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 19, pp. 790–798, 2025.