Indonesian Journal of Electrical Engineering and Computer Science
Vol. 42, No. 3, June 2026, pp. 631~636
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v42.i3.pp631-636

Editorial

Resilient artificial intelligence, secure digital ecosystems, and intelligent computing for a connected future

Tole Sutikno
Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Article Info

Keywords:

Artificial intelligence
Blockchain
Cybersecurity
Digital transformation
Intelligent computing
Internet of things
Resilient systems

ABSTRACT

This editorial introduces the articles published in Volume 42, Number 3, June 2026 of the Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), highlighting recent advances and emerging research directions in artificial intelligence, cybersecurity, intelligent computing, and digital transformation. The published studies span a broad range of topics, including machine learning, intelligent analytics, healthcare technologies, computer vision, cryptography, privacy-preserving systems, internet of things (IoT) security, cloud computing, distributed optimization, blockchain applications, and decentralized digital platforms. Emerging trends highlighted throughout this issue include foundation and multimodal AI models, AI-enabled cybersecurity, privacy-preserving machine learning, Zero-Trust architectures, edge intelligence, decentralized computing, and digital trust ecosystems. Collectively, these contributions underscore the growing importance of resilient artificial intelligence and secure digital infrastructures in enabling adaptive, efficient, and trustworthy connected environments. The increasing integration of intelligence, security, resilience, and human-centered design principles reflects the evolving requirements of next-generation technologies that support sustainable innovation, economic development, and societal well-being. The research presented in this issue provides valuable perspectives on the opportunities and challenges associated with building secure, resilient, and intelligent digital ecosystems for an increasingly interconnected future.

The rapid advancement of digital technologies continues to reshape the landscape of electrical engineering, computer science, and information and communication technologies (ICT). Artificial intelligence (AI), intelligent computing, cloud services, cybersecurity, and interconnected digital infrastructures are increasingly driving innovation across industry, healthcare, education, transportation, and public services. At the same time, the growing dependence on data-driven decision-making, autonomous systems, and pervasive connectivity has introduced new challenges related to security, privacy, trust, scalability, and responsible technology deployment. As digital transformation accelerates worldwide, the development of intelligent, secure, and resilient systems has become a fundamental priority for researchers, practitioners, and policymakers seeking to balance technological innovation with societal needs.

Recent advances in machine learning, deep learning, computer vision, natural language processing, distributed computing, and intelligent analytics have expanded the capabilities of modern digital systems. Emerging paradigms such as foundation and multimodal AI models, privacy-preserving machine learning, AI-enabled cybersecurity, Zero-Trust architectures, edge intelligence, blockchain-enabled platforms, and decentralized computing are redefining the design and operation of next-generation technologies. These developments are fostering a transition from isolated intelligent applications toward integrated digital ecosystems capable of supporting adaptive, autonomous, and trustworthy services across increasingly complex

environments. Consequently, resilience, security, and human-centered design are becoming essential considerations alongside performance and efficiency.

The articles published in Volume 42, Number 3, June 2026 of the Indonesian Journal of Electrical Engineering and Computer Science (IJEECS) reflect these evolving trends and challenges. The contributions span a broad range of topics, including artificial intelligence, intelligent analytics, healthcare technologies, cybersecurity, cryptography, privacy-preserving systems, IoT security, computer vision, cloud computing, distributed optimization, blockchain applications, and digital trust frameworks. Although addressing diverse technical domains, the studies collectively highlight a common objective: the development of intelligent systems that are secure, resilient, efficient, and capable of operating within highly interconnected digital environments. This growing convergence of resilient intelligence, cybersecurity, and digital transformation provides an important context for understanding the research contributions presented in this issue and the emerging directions that are shaping the future of engineering and computing technologies.

The convergence of resilient intelligence, security, and digital transformation

The accelerating pace of digital transformation is reshaping the relationship between intelligence, connectivity, and security across modern technological ecosystems. Advances in artificial intelligence, intelligent computing, cloud services, edge computing, and distributed digital infrastructures are increasingly converging to support adaptive and data-driven operations across diverse sectors. Recent developments in machine learning, deep learning, foundation models, and multimodal AI architectures have significantly expanded the capabilities of intelligent systems, enabling more sophisticated decision-making, automation, and knowledge extraction. As organizations and societies become increasingly reliant on digital technologies, the integration of intelligence into critical infrastructures, communication networks, industrial systems, and public services continues to create new opportunities for innovation and efficiency.

At the same time, the growing complexity and interconnectedness of digital environments have intensified concerns regarding cybersecurity, privacy, trust, and operational resilience. The rapid expansion of cloud platforms, internet of things (IoT) ecosystems, cyber-physical systems, and autonomous applications has broadened potential attack surfaces while increasing the consequences of system failures and security breaches. Emerging approaches such as Zero-Trust architectures, privacy-preserving machine learning, secure multi-party computation, homomorphic encryption, and AI-enabled cybersecurity are redefining strategies for protecting digital assets and maintaining system integrity. These developments highlight the increasing importance of embedding security and resilience throughout the entire lifecycle of digital systems rather than treating them as isolated technical considerations.

Another significant trend involves the growing convergence of cloud intelligence, edge computing, decentralized platforms, and digital trust frameworks. Edge intelligence enables real-time processing closer to data sources, reducing latency while improving privacy and operational efficiency. Meanwhile, blockchain technologies and decentralized computing architectures are creating new opportunities for secure information exchange, transparent transactions, and distributed coordination among multiple stakeholders. Together, these advances are supporting the development of resilient digital ecosystems capable of operating across highly dynamic and interconnected environments. The studies presented in this issue collectively reflect this transformation and demonstrate how the integration of intelligence, security, resilience, and human-centered innovation is shaping the future of electrical engineering, computer science, and information and communication technologies.

Artificial intelligence, machine learning, and intelligent analytics

Artificial intelligence (AI) continues to be one of the most transformative technologies shaping modern engineering and computing research. Recent advances in machine learning, deep learning, natural language processing, and intelligent analytics have significantly expanded the ability of digital systems to extract knowledge from large and complex datasets, automate decision-making processes, and support predictive and prescriptive intelligence. The increasing availability of computational resources, cloud infrastructures, and large-scale data repositories has accelerated the deployment of AI across diverse application domains, ranging from industrial automation and business intelligence to healthcare, education, and smart cities. In parallel, emerging developments in foundation models and large language models are enabling more generalized and context-aware forms of intelligence capable of supporting increasingly sophisticated analytical tasks.

Several contributions in this issue reflect the growing importance of intelligent analytics in addressing complex real-world problems. Advanced machine learning techniques are being applied to pattern recognition, sentiment analysis, anomaly detection, knowledge discovery, and decision-support applications. Research involving graph-based learning, social network analytics, and natural language processing demonstrates how intelligent algorithms can uncover meaningful relationships within highly interconnected and unstructured data

environments. At the same time, studies exploring hybrid learning architectures and advanced optimization methods highlight ongoing efforts to improve predictive performance, computational efficiency, and model adaptability. These developments illustrate the continuing evolution of AI from narrow task-specific solutions toward more integrated and context-sensitive analytical frameworks.

Despite remarkable progress, several challenges remain central to the future development of AI systems. Increasing model complexity has raised important concerns regarding interpretability, transparency, fairness, bias mitigation, and robustness. As AI technologies become more deeply integrated into critical infrastructures and societal decision-making processes, ensuring responsible and trustworthy deployment becomes increasingly important. Emerging research on explainable AI, privacy-preserving machine learning, federated learning, and human-centered intelligent systems seeks to address these concerns while maintaining high levels of performance and scalability. Collectively, the studies presented in this issue highlight the expanding role of artificial intelligence and intelligent analytics as key enablers of innovation, while emphasizing the need to balance technological advancement with resilience, accountability, and societal trust.

AI for healthcare, biomedical engineering, and digital health

Healthcare continues to be one of the most impactful application domains for artificial intelligence, intelligent sensing, and advanced computational technologies. The growing availability of medical data, wearable devices, connected health platforms, and intelligent diagnostic systems has accelerated the adoption of AI-driven approaches for disease detection, patient monitoring, clinical decision support, and healthcare management. Recent advances in machine learning and deep learning have enabled the development of more accurate and efficient diagnostic models capable of assisting healthcare professionals in identifying complex medical conditions while supporting earlier intervention and personalized treatment strategies.

Research in biomedical engineering increasingly combines intelligent algorithms with advanced sensing and imaging technologies to improve healthcare accessibility, diagnostic reliability, and patient outcomes. Machine learning techniques are being applied to analyze physiological signals, medical images, clinical records, and population health data, enabling the extraction of meaningful patterns that may be difficult to identify through conventional methods. In parallel, advances in biomedical instrumentation, wireless health monitoring systems, and digital health platforms are creating opportunities for continuous and remote healthcare services. These developments are particularly important in addressing challenges associated with aging populations, chronic disease management, and disparities in healthcare access across different regions.

Emerging trends such as explainable AI, privacy-preserving analytics, federated learning, and human-centered healthcare technologies are further shaping the future of digital health ecosystems. As AI systems become increasingly involved in clinical decision-making, concerns regarding transparency, fairness, reliability, privacy, and regulatory compliance continue to attract significant attention. Addressing these challenges requires interdisciplinary collaboration among engineers, computer scientists, healthcare professionals, and policymakers to ensure that technological innovation remains aligned with clinical needs and ethical standards. The contributions presented in this issue highlight the growing convergence of artificial intelligence, biomedical engineering, and digital health, demonstrating the potential of intelligent technologies to support more accessible, efficient, and patient-centered healthcare systems in the years ahead.

Cybersecurity, cryptography, privacy, and secure digital ecosystems

As digital transformation continues to accelerate, cybersecurity has become a fundamental requirement for modern information systems, communication networks, and critical infrastructures. The increasing interconnection of cloud platforms, IoT devices, cyber-physical systems, and intelligent applications has expanded both the scale and complexity of cyber threats. Traditional perimeter-based security approaches are often insufficient in highly distributed and dynamic environments, creating a growing need for adaptive, intelligence-driven, and resilience-oriented security frameworks. Consequently, cybersecurity is evolving from a supporting function into a strategic component of digital ecosystem design, governance, and operation.

Recent advances in cryptography, privacy-preserving technologies, and intelligent threat detection are reshaping the cybersecurity landscape. Modern security frameworks increasingly incorporate machine learning and artificial intelligence to identify anomalies, detect malicious activities, and respond to emerging threats in real time. At the same time, advances in cryptographic techniques, including homomorphic encryption, secure multi-party computation, and privacy-preserving data analytics, are enabling secure information sharing without compromising sensitive data. The growing adoption of Zero-Trust architectures further reflects a shift toward continuous verification and risk-aware access control, recognizing that trust must be established dynamically rather than assumed based on network location or organizational boundaries.

The development of secure digital ecosystems requires a holistic approach that integrates cybersecurity, privacy protection, resilience, and digital trust throughout the system lifecycle. As intelligent systems increasingly support critical decision-making processes in healthcare, finance, industry, education, and public services, ensuring the confidentiality, integrity, and availability of digital resources becomes essential.

Emerging concepts such as AI-enabled cybersecurity, cyber resilience, privacy-aware computing, and digital trust frameworks are expected to play an increasingly important role in future digital infrastructures. The studies presented in this issue contribute to this evolving landscape by advancing knowledge and innovation in secure computing, privacy preservation, and resilient cyber ecosystems capable of supporting the demands of an increasingly connected world.

Intelligent IoT, edge computing, and cyber-physical systems

The rapid expansion of the IoT is transforming the way physical and digital environments interact. Advances in sensing technologies, wireless communications, embedded systems, and intelligent data processing have enabled the deployment of interconnected devices capable of monitoring, analyzing, and responding to real-world conditions in real time. These developments are driving innovation across a wide range of application domains, including smart cities, industrial automation, environmental monitoring, transportation systems, precision agriculture, and healthcare. As IoT ecosystems continue to grow in scale and complexity, the ability to process data efficiently, securely, and intelligently has become a critical requirement for future connected infrastructures.

Edge computing has emerged as a key enabling technology for addressing many of the limitations associated with centralized cloud-based architectures. By moving computation and intelligence closer to data sources, edge computing reduces communication latency, decreases network congestion, and enhances privacy protection. The integration of edge intelligence with machine learning techniques further enables real-time analytics and autonomous decision-making in resource-constrained environments. Such capabilities are particularly important for applications requiring rapid response, continuous operation, and localized data processing. Combined with advances in distributed computing and intelligent networking, edge-enabled systems are supporting more adaptive and resilient digital ecosystems.

Cyber-physical systems represent another important area where intelligence, connectivity, and control are increasingly converging. These systems integrate computational capabilities with physical processes, enabling closer coordination between sensing, communication, and actuation. As cyber-physical infrastructures become more autonomous and interconnected, ensuring reliability, security, interoperability, and resilience become increasingly important. Emerging research in edge intelligence, distributed coordination, secure IoT architectures, and real-time analytics is helping to address these challenges while supporting the development of more responsive and sustainable environments. The contributions presented in this issue reflect the growing importance of intelligent IoT systems and cyber-physical technologies in shaping future digital infrastructures capable of operating efficiently within highly dynamic and interconnected settings.

Computer vision, multimodal intelligence, and human-centered AI

Computer vision continues to be one of the most dynamic and rapidly advancing areas of artificial intelligence research. Recent developments in deep learning, image analysis, pattern recognition, and visual understanding have significantly improved the ability of intelligent systems to interpret complex visual information. Applications of computer vision now extend far beyond traditional image classification tasks, supporting diverse domains such as healthcare, industrial inspection, autonomous systems, security monitoring, agriculture, and human-computer interaction. Increasing availability of large-scale datasets and advanced computational resources has accelerated innovation while enabling more accurate and robust visual intelligence solutions.

Alongside advances in computer vision, multimodal intelligence is emerging as a transformative paradigm for next-generation AI systems. By integrating information from multiple sources such as images, text, audio, sensor data, and contextual information, multimodal models can achieve richer representations of real-world phenomena and support more sophisticated reasoning capabilities. Recent progress in foundation models and large-scale multimodal architectures has demonstrated the potential of AI systems to process and correlate diverse forms of information within unified analytical frameworks. These capabilities are opening new opportunities for intelligent decision support, content generation, human-machine collaboration, and adaptive learning environments.

As AI technologies become increasingly integrated into everyday life, greater attention is being directed toward human-centered design principles. Future intelligent systems must not only achieve high levels of technical performance but also remain understandable, trustworthy, inclusive, and aligned with human values. Issues such as transparency, explainability, fairness, privacy, and user acceptance are becoming essential considerations in the design and deployment of AI-driven applications. The studies featured in this issue highlight ongoing advances in visual intelligence and multimodal computing while emphasizing the importance of developing AI systems that effectively support human needs, enhance decision-making, and contribute positively to society.

Cloud computing, optimization, and large-scale distributed systems

Cloud computing has become a fundamental enabler of modern digital transformation, providing scalable computational resources, flexible service delivery models, and efficient data management capabilities. The rapid growth of data-intensive applications, artificial intelligence workloads, and interconnected digital services has increased the demand for cloud infrastructures capable of supporting large-scale processing, storage, and communication requirements. Advances in virtualization, containerization, and service orchestration continue to improve the efficiency and adaptability of cloud environments, enabling organizations to deploy and manage complex applications with greater flexibility and reliability.

Optimization techniques play a critical role in enhancing the performance and resource utilization of distributed computing systems. As cloud platforms become increasingly heterogeneous and geographically distributed, efficient scheduling, workload balancing, resource allocation, and energy management have emerged as important research challenges. Machine learning and intelligent optimization methods are increasingly being applied to improve system efficiency, reduce operational costs, and support adaptive decision-making under dynamic conditions. Such approaches are particularly valuable in environments characterized by fluctuating workloads, large-scale data processing requirements, and diverse quality-of-service constraints.

The future of intelligent computing is expected to be shaped by closer integration among cloud platforms, edge infrastructures, and distributed computational resources. Emerging paradigms such as cloud-edge collaboration, federated intelligence, decentralized computing, and autonomous resource management are enabling more resilient and scalable digital ecosystems. These developments support applications requiring real-time responsiveness, high availability, and secure data processing across distributed environments. The contributions presented in this issue reflect ongoing progress in optimization methodologies, intelligent resource management, and large-scale computing architectures that will continue to underpin future advances in artificial intelligence, data analytics, and connected digital services.

Blockchain, decentralized platforms, and digital trust

The increasing reliance on digital services and interconnected platforms has elevated the importance of trust, transparency, and security within modern information ecosystems. Blockchain technology has emerged as a promising approach for supporting decentralized and tamper-resistant digital infrastructures capable of facilitating secure transactions, data sharing, and distributed coordination among multiple stakeholders. By reducing dependence on centralized authorities, blockchain-based systems offer new opportunities for enhancing accountability, traceability, and operational resilience across a wide range of applications.

Beyond cryptocurrencies, blockchain technologies are increasingly being explored in areas such as digital identity management, supply chain monitoring, healthcare data exchange, smart contracts, and secure IoT environments. When combined with advances in cryptography, distributed computing, and intelligent analytics, decentralized platforms can support more transparent and trustworthy digital interactions while reducing vulnerabilities associated with single points of failure. These capabilities are particularly relevant as organizations seek to strengthen digital trust and improve the security of increasingly interconnected systems.

The concept of digital trust extends beyond technical security mechanisms to encompass reliability, transparency, privacy protection, and responsible governance. Future digital ecosystems will require integrated frameworks that balance innovation with accountability while ensuring confidence among users, organizations, and society. The research contributions featured in this issue highlight the growing role of blockchain-enabled solutions and decentralized architectures in supporting secure, resilient, and trustworthy digital environments. As digital transformation continues to evolve, these technologies are expected to become important building blocks for next-generation information systems and connected infrastructures.

Emerging priorities in electrical engineering and computer science for the next decade

The next decade is expected to bring profound changes to the fields of electrical engineering and computer science as intelligent technologies become increasingly integrated into critical infrastructures, industrial systems, public services, and everyday life. While advances in artificial intelligence, cloud computing, communication networks, and digital platforms continue to accelerate innovation, growing concerns regarding resilience, security, sustainability, and responsible technology deployment are reshaping research priorities. Future technological progress will depend not only on achieving higher levels of performance and automation but also on ensuring that intelligent systems remain reliable, transparent, secure, and aligned with societal needs.

One of the most significant priorities will be the development of resilient and trustworthy artificial intelligence. Emerging foundation models, multimodal AI architectures, autonomous systems, and intelligent agents are expected to transform how information is processed, analyzed, and utilized across multiple domains. At the same time, increasing dependence on AI-driven decision-making will require advances in explainability,

fairness, robustness, privacy preservation, and human-centered design. Research in privacy-preserving machine learning, federated learning, trustworthy AI, and AI governance will become increasingly important as organizations seek to balance innovation with accountability and public trust.

Cybersecurity will remain another critical priority as digital ecosystems become more interconnected and distributed. Future infrastructures will increasingly rely on Zero-Trust architectures, AI-enabled threat detection, quantum-resistant cryptography, secure edge computing, and resilient cyber-physical systems. Protecting digital assets, ensuring operational continuity, and safeguarding privacy will require integrated security frameworks capable of adapting to rapidly evolving threat landscapes. Simultaneously, advances in blockchain technologies and decentralized computing will contribute to the development of digital trust ecosystems that support secure information exchange and transparent digital interactions.

Sustainability is also expected to play a central role in future engineering research. Increasing demand for computational resources, data centers, communication networks, and intelligent services highlights the need for energy-efficient technologies and environmentally responsible innovation. Research on green computing, intelligent energy management, sustainable communication infrastructures, and resource-efficient AI models will contribute to reducing environmental impacts while supporting continued technological growth. The integration of intelligent optimization techniques with renewable energy systems and smart infrastructures will further support global efforts toward sustainable development.

Finally, the convergence of cloud computing, edge intelligence, advanced communications, and autonomous systems is expected to redefine future digital environments. Emerging paradigms such as distributed intelligence, digital twins, autonomous networks, human-AI collaboration, and next-generation cyber-physical systems will create new opportunities for innovation while introducing complex technical and societal challenges. Addressing these challenges will require interdisciplinary collaboration among engineers, computer scientists, policymakers, and industry stakeholders. The research themes represented in this issue provide valuable insights into these emerging priorities and illustrate how advances in electrical engineering and computer science are contributing to the development of intelligent, secure, resilient, and sustainable technologies for the future.

Conclusion and SDG-oriented outlook

The articles published in this issue collectively demonstrate the growing convergence of artificial intelligence, cybersecurity, intelligent computing, and digital transformation in addressing complex technological and societal challenges. Advances in machine learning, intelligent analytics, healthcare technologies, cybersecurity, privacy-preserving systems, IoT infrastructures, cloud computing, blockchain applications, and decentralized platforms highlight the increasing importance of resilient, secure, and adaptive digital ecosystems. Beyond technical innovation, many of these contributions support broader societal objectives aligned with the United Nations Sustainable Development Goals (SDGs), including SDG 3 (Good Health and Well-Being), SDG 4 (Quality Education), SDG 9 (Industry, Innovation and Infrastructure), SDG 11 (Sustainable Cities and Communities), and SDG 16 (Peace, Justice and Strong Institutions). Collectively, the research presented in this issue illustrates how advances in electrical engineering and computer science can contribute to more efficient, inclusive, and sustainable digital societies.

Looking ahead, future technological progress will increasingly be shaped by the integration of resilient artificial intelligence, secure digital ecosystems, and intelligent computing infrastructures. Emerging developments in foundation and multimodal AI models, privacy-preserving machine learning, AI-enabled cybersecurity, Zero-Trust architectures, edge intelligence, decentralized computing, and digital trust frameworks are expected to redefine the capabilities and responsibilities of next-generation digital systems. At the same time, growing concerns regarding security, transparency, resilience, sustainability, and human-centered innovation will require continued interdisciplinary collaboration and responsible technology development. Through the dissemination of high-quality research and innovative engineering solutions, IJEECS continues to contribute to the advancement of intelligent, secure, and sustainable technologies that support economic development, societal well-being, and an increasingly connected future.