Introduction to the ICOW3 2025 Special Issue

Yunhee Kang[1], Vijayan Sugumaran[2], Young B. Park[3] and Sooyong Park[4]

[1]*Baekseok University, Cheonan, South Korea*
[2]*Oakland University, Rochester, Michigan, USA*
[3]*Dankook University, Yongin, South Korea*
[4]*Sogang University, Seoul, South Korea*
E-mail: yhkang@bu.ac.kr; sugumara@oakland.edu; ybpark@dankook.ac.kr; sypark@sogang.ac.kr

1 Introduction

Web 3.0 is a term used to describe the next generation of the Internet being built on blockchain technology. It is expected to have a significant impact on society by decentralizing power and control over social media platforms, thereby providing diverse interaction. Meanwhile, Artificial Intelligence (AI) continues to advance, enabling intelligent systems across various domains. The convergence of these two transformative forces–Web 3.0 and AI–holds immense potential to revolutionize our world. Key topics include data sovereignty, blockchain governance, agentic AI, and its infrastructure.

The *Journal of Web Engineering* publishes selected papers from the International Conference on Real World Applications of Agentic AI for Web 3.0 (ICOW3) as a special issue. These papers cover specific themes, including Web 3.0 and AI, that align with the aims and scope of the *Journal of Web Engineering*.

ICOW3 aims to bring together researchers and practitioners from various disciplines in academia and industry to tackle emerging challenges in the engineering of Web 3.0 and AI. ICOW3 2025 took place in Seoul, Korea, on November 5–6, 2025. The conference was also offered to online participants. This special issue includes extended versions of the best papers presented at ICOW3 2025.

2 Selected Papers from ICOW3 Conference

In the paper titled "Agentic AI service architecture based on SOA," Dong Bin Choi et al. introduce a framework for Agentic AI that structures agents. To ensure secure collaboration, the framework integrates Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to manage agent identity and enforce least-privilege access. It presents the design of a verifiable-credentials (VC) architecture and demonstrate its feasibility via a proof-of-concept (PoC). The PoC demonstrates the feasibility of this architecture, validating a blackboard-mediated delegation process where agents solve problems through verified, multi-agent coordination.

Focusing on Natural Language Processing (NLP) for historical texts, the paper titled "Joint Models for Sentence Segmentation and Named Entity Recognition in Literary Sinitic Text" by Dongnyeong Heo et al. proposes a deep learning-based framework for processing and understanding under-resourced Literary Sinitic texts. Analyzing Literary Sinitic texts from the Joseon Dynasty is challenging due to the lack of explicit word separators, which causes significant semantic ambiguity. To overcome this, this paper proposes a Transformer-based analyzer capable of performing sentence segmentation and Named Entity Recognition (NER) simultaneously. The designed architecture integrates a Transformer encoder with dedicated classifiers, optimized specifically for the linguistic characteristics of the Seungjeongwon Ilgi corpus. Experimental results demonstrate that the model achieves high accuracy in both tasks, successfully reducing sentence ambiguity and identifying key historical entities.

The paper titled "PK-PoMLO: Public Key Proof of ML Ownership system" written by Jo Yeon Park, Kyounghwa Do, and Soo Yong Park, proposes a verification framework that combines identity binding via digital signatures with the immutable timestamping of a public blockchain. As large-scale machine learning models become valuable intangible assets, they face increasing risks of unauthorized reproduction and theft that traditional logging methods cannot reliably prevent. Existing watermarking techniques often fail to objectively prove the time of creation or cryptographically bind the model to a specific owner. To address these vulnerabilities, the proposed framework provides a method that embeds a 128-bit mark derived from the owner's signature into the model and commits the model hash on-chain, allowing for independent, third-party verification. This approach establishes a tamper-proof claim of priority and ownership with a negligible false acceptance rate, ensuring robust protection against disputes.

Web 3.0 fundamentally relies on cryptographic private keys to establish user ownership and control over digital assets, making secure key management a critical priority for the industry. While various solutions exist–ranging from commercial centralized and decentralized wallets to academic approaches using secret sharing and threshold signatures–effectively protecting user-side keys against leakage, theft, and loss remains a persistent challenge. In "KeyShield: Leakage-and-Loss-Resilient Private Key Protection for Web3," Ziyang Ji et al. propose a protection scheme, KeyShield, that splits a private key into three shares distributed across a primary device, a secondary device, and a secure storage module to handle the challenge.

The immutability of blockchain technology renders post-minting removal of harmful content impossible, making robust pre-minting moderation essential to prevent the permanent dissemination of unsafe media. Conventional off-chain classifiers fail to provide cryptographic assurances, leaving decentralized ecosystems vulnerable to adversarial manipulation and a lack of binding enforcement. To address this, we propose a hybrid approach that integrates probabilistic AI judgments with cryptographic attestation (EIP-712) and perceptual hashing to ensure tamper-resistant, deterministic prevention of unsafe content. The paper titled "VisionGuard: Cost-Sensitive AI Attestation with Quorum-Verified Blockchain Enforcement" S Prithivraj et al. introduces VisionGuard, a unified framework that operationalizes these principles by deploying Bayes-optimal thresholds and a human-in-the-loop abstention mechanism to minimize expected harm and guarantee verifiable safety.

While research on non-cooperative face recognition has advanced, current methods still struggle with limited facial feature representation and the interference caused by occlusions. The uncertainty of occlusion locations in test samples makes accurate recognition particularly challenging, creating a need for models that can robustly handle partial obstructions while extracting richer feature sets. In "A novel collaboration representation method combining PCANet and occlusion positioning for non-cooperative face recognition," Zhi Zhang and Bingyu Sun propose MSPCANet (Multi-Scale PCANet), which incorporates multi-scale sample information into the standard PCA Network to significantly improve feature expression and optimize filter size selection by utilizing a Markov Random Field (MRF) to precisely locate occluded regions in test samples. Experiments conducted on the AR and LFW datasets demonstrate that combining multi-scale feature fusion with targeted occlusion.

3 Discussion

The keynote session of ICOW3 addressed real-world applications of Agentic AI and the necessity of data sovereignty in Web3, while the conference facilitated technical exchanges between academia and industry regarding the stablecoin-driven reshaping of finance and service integration in multi-agent systems.

This convergence of Web 3.0 and Agentic AI creates the world where Web 3 provides the rails of trust and Agentic AI provides the engine of autonomy. Large Language Models (LLMs) have demonstrated exceptional versatility in generating human-like text and processing vast amounts of information, revolutionizing how we interact with digital systems. However, they remain inherently limited due to their unexplainable parameters in the model and the tendency to hallucinate, often producing confident but factually incorrect outputs without verifiable sources. Despite susceptibility to hallucination, LLMs provide the essential cognitive architecture for Agentic AI, enabled by orchestration layers such as LangChain. LangChain functions as a robust orchestration framework that empowers Large Language Models (LLMs) to interact with external data sources and execute complex, multi-step reasoning tasks. Ensuring the integrity of external data sources and services is increasingly recognized as a key prerequisite in the era of Agentic AI.

The Chain of Trust is a security concept where trust is passed down from a highly secure root to the final application in AI driven society. In Web3, blockchain provides a framework for executing secure transactions and methods, depending on a consensus mechanism for operating decentralized applications from the perspective of the anchor of trust.

The ICOW3 conference served as a venue to address current technical limitations. Through paper presentations and researcher discussions, specific solutions were proposed, including techniques for AI model ownership verification, identity authentication in multi-agent systems, and secure distributed key management. Furthermore, the conference highlighted the emerging challenges and requirements for sustaining Web3 environments in the post-quantum era. Specific research topics that need further exploration are: a) Agentic AI, b) Trusted AI Service, c) Responsible AI, d) AI in Real World Assets, e) Stable coin in Web3, and f) Post Quantum Blockchain. While research on various aspects of artificial intelligence is progressing at a very fast pace, this is only the beginning. There are still a number of issues that have to be explored in terms of the design, implementation and deployment of

AI applications and blockchain based applications for Web 3.0. For example, development of novel and NextGen AI techniques for computational intelligence in support of developing cognitively intensive applications, formal approaches for designing intelligent agentic AI systems, physical AI systems, quantum computing based information systems, and organizational impact of NextGen AI systems are some of the areas in need of further research. Together, these elements define a future in which AI operates as an autonomous and economically active entity, remains legally accountable for its actions, and is sustained by cryptographic trust that endures over decades. Blockchain technology is evolving as the foundational infrastructure to enable, enforce, and preserve this paradigm.

4 Conclusion

The selection of papers included in this special issue demonstrates the quality and topical diversity of the ICOW3 community. Given the significant research reported in these articles, we look forward to new and exciting research to come. Researchers from academia and industry alike are encouraged to continue this momentum and carryout high-quality research and move the field forward with novel applications and tools designed to improve the state of the art and contribute to solving complex societal problems.