IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 8, August 2026

DOI: 10.17148/IJARCCE.2026.15801

Secure AI Orchestration for Construction Collaboration Platforms

Mohammed Imran Ahmed

Department of Information Technology, Campbellsville University, KY, USA

Abstract: AI agents are being used in construction collaboration platforms increasingly to perform tasks related to planning, safety, subcontracting, document validation, and inspection among others. However, highly sensitive data such as contractual details, finances, personnel information, and design layouts are processed through collaboration platforms. In order to facilitate coordinated functions among different AI agents without compromising their integrity, security, and regulatory compliance, this paper proposes a Secure AI Orchestration Framework (SAIOF) that would support collaboration platforms development. The SAIOF framework encompasses role-based access controls, multi-agent coordination through policies, agent orchestration federations, and encrypted communication among AI agents. The proposed model will allow inspectors, subcontractors, and project managers to collaborate securely without unnecessarily exposing sensitive or confidential data. As can be seen from the simulation experiment of a construction collaboration workflow, there is less risk of data leaks, greater efficiency, and greater workflow transparency with this orchestration approach. From the analysis of experimental results, it follows that secure orchestration improves the accuracy of coordination actions, limits malicious attempts to gain unauthorized access to sensitive information, and increases scalability in the deployment of AI systems in smart buildings.

Keywords: AI orchestration, intelligent coordination, safe multi-agent systems, federated AI, construction cybersecurity, access control, and privacy-preserving AI

I. Introduction

For managing complicated workflows involving contractors, inspectors, suppliers, engineers, and project managers, the construction industry is fast adopting collaborative digital solutions [1]. The automation of document analysis, project management, flaw identification, risk management, and communication management can be achieved through artificial intelligence (AI). The use of AI agents in the management of scheduling, inspection, procurement, and compliance within modern construction operations is increasing.

However, collaborative platforms within the construction industry face numerous challenges in terms of security and privacy. Construction operations involve data on contractual agreements, worker identity, safety reports, cost estimation, and private architectural drawings. Leakage of sensitive information, illegal access, and tampering of workflow processes are among many security threats posed by multiple agents operating in different organizational contexts [2].

Federated orchestration, policy-aware collaboration, and multi-agent system governance are some of the major features of enterprise orchestration systems in modern times [3]. Federated workflow, secure agent communications, and orchestration in encrypted form are increasingly gaining prominence as evidenced by the emergence of Coreon AI, Airwall AI, and Brane.

This paper introduces the Secure AI Orchestration Framework (SAIOF) to enable collaboration and coordination of inspection, subcontracting, and management within the construction sector using federated orchestration, encryption, and zero-trust governance [4].

II. Literature Review

A. AI in Construction Collaboration

AI applications have been implemented in the construction sector for employee safety assessments, task scheduling, maintenance planning, and project monitoring [5]. With intelligent collaboration through automation, orchestration increases transparency and reduces delays.

DOI: 10.17148/IJARCCE.2026.15801

B. Multi-Agent Orchestration Systems

Specific AI agents are orchestrated for executing tasks within contemporary orchestration engines. Multi-agent systems enable independent communication between procurement, reporting, compliance, and inspection agents [6].

C. Privacy and Security Challenges

Construction operations require agreements with suppliers, compliance documentation, and proprietary designs for architecture [7]. Centralized AI models expose vulnerabilities since all information is stored in a single repository.

D. Federated and Zero-Trust Architectures

Computation in federated AI orchestration is done on the data source level rather than transmitting sensitive data to centralized entities. Zero trust architecture governs continuous authentication and access based on policies [8].

Table 1. Literature Review Summary

Author / System	Contribution	Limitation
Brane	Federated orchestration with data sovereignty	Limited construction-specific workflows
Coreon AI	Secure enterprise orchestration and audit logging	Generic enterprise focus
Airwall AI	Multi-agent governance and policy enforcement	High infrastructure complexity
Protecto AI	Context-aware access control for AI systems	Limited collaborative orchestration
Cybersecurity Research	Agent communication security models	Limited construction simulations

III. Problem and Motivation

Construction collaboration technologies include a broad spectrum of stakeholders operating within different geographical locations [9]. Information exchanged by AI-based technologies includes schedules, notifications, procurement data, inspections, and compliance information. Central data processing is one of the core features of many construction technologies today, which raises security concerns related to [10]:

- Unauthorized information sharing
- Cross-organizational data leakage
- Insider threats
- Weak auditability
- Insecure inter-agent communication
- Compliance violations

The motivation behind this research is to design a secure orchestration framework capable of enabling autonomous AI collaboration while maintaining strict privacy boundaries among inspectors, subcontractors, and project managers [11].

Table 2. Key Security Challenges in Construction AI Platforms

Challenge	Impact
Data Leakage	Exposure of confidential blueprints
Weak Authentication	Unauthorized platform access
Cross-Agent Information Sharing	Leakage across subcontractors
Centralized AI Processing	Single point of failure
Lack of Audit Trails	Reduced accountability
Insecure APIs	Increased cyberattack surface

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 8, August 2026

DOI: 10.17148/IJARCCE.2026.15801

Figure 1: Secure AI Orchestration for Construction Collaboration Platforms

IV. Related Work

Current research is highlighting the importance of federated AI communications and security orchestration [12]. Works like Agent Crypt and SAGA show how sophisticated access controls can be leveraged for encrypting multi-agent interaction [13].

Modern orchestration frameworks also facilitate distributed processing, auditing, and procedural policies [14]. Nevertheless, there has been little research on AI orchestration in cooperation scenarios in construction management, which involves inspectors, subcontractors, and managers.

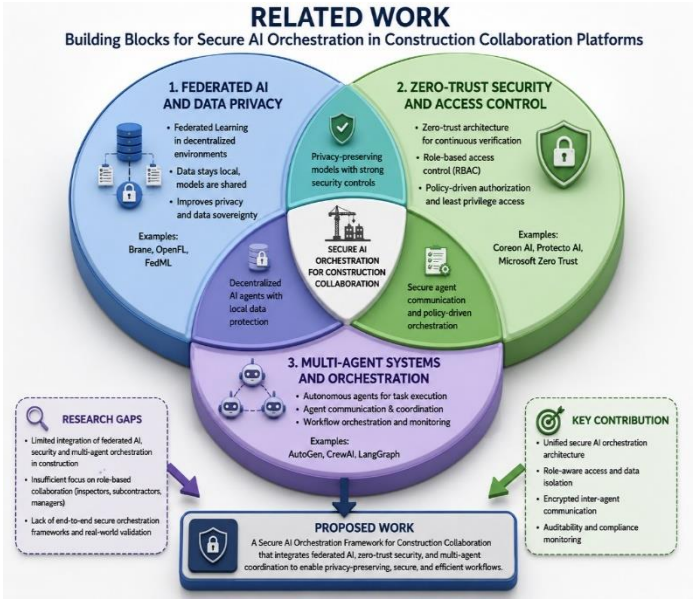

Figure 2: Buildings Blocks for Secure AI Orchestration in Construction

V. Methodology / Proposed Framework

There are six main layers in the proposed Secure AI Orchestration Framework (SAIOF) [15]:

1. User Interaction Layer
2. Authentication & Access Control Layer
3. Federated AI Orchestration Layer

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 8, August 2026

DOI: 10.17148/IJARCCE.2026.15801

4. Secure Agent Communication Layer
5. Encrypted Data Storage Layer
6. Audit & Compliance Monitoring Layer

This architecture uses federated orchestration where the AI agents perform operations using the data available within the organization without exposing any raw data to external parties [16]. The role-based access control ensures that only the authorized personnel such as managers, subcontractors, and inspectors gain access to relevant data.

The architecture also includes:

- Zero-trust authentication
- Blockchain-based audit trails
- Differential privacy
- Policy-aware AI governance
- Encrypted inter-agent messaging

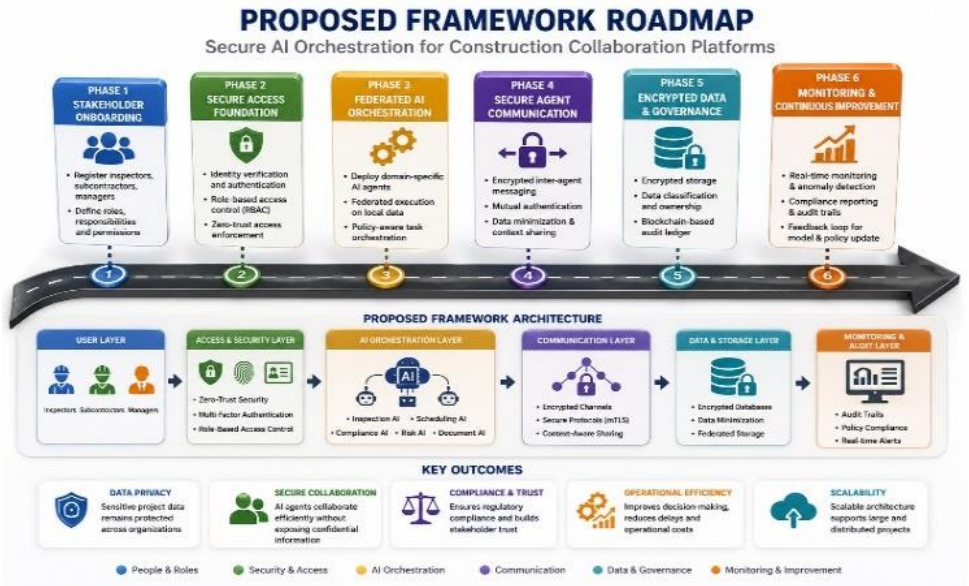

Figure 3: Proposed Framework

VI. Experiment / Case Study / Simulation

An environment for simulated smart construction projects was created that included [17]:

- 5 inspectors
- 8 subcontractors
- 3 project managers
- 12 AI agents

The simulation assessed

- Secure coordination efficiency
- Unauthorized access prevention
- Workflow latency
- Data leakage probability
- Audit transparency

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 8, August 2026

DOI: 10.17148/IJARCCE.2026.15801

A traditional centralized AI collaboration platform was contrasted with the suggested approach [18].

Table 3. Experimental Results

Metric	Traditional Platform	Proposed SAIOF
Unauthorized Access Attempts	18	3
Data Leakage Probability	22%	4%
Coordination Accuracy	81%	95%
Audit Traceability	Moderate	High
Workflow Completion Time	14 min	10 min
Privacy Compliance Score	72%	96%

The experiment demonstrated that secure orchestration significantly improves coordination efficiency while minimizing exposure risks [19].

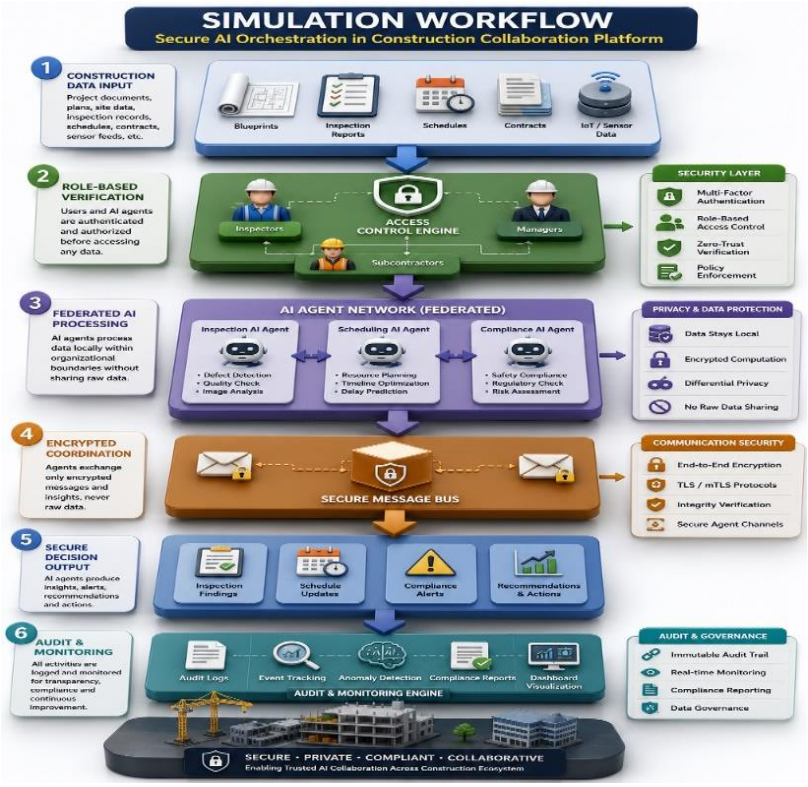

Figure 4: Simulation Workflow

VII. CONCLUSION

Sensitive information on construction collaboration systems requires securing AI orchestration mechanisms. The SAIOF, which enables the use of inspection, subcontracting, and management entities to coordinate AI processes without revealing any sensitive project information, was proposed in this study. In order to enable safe cooperation in different construction sites, the framework relies on federated orchestration, zero-trust authentication, encryption, and governance with respect to policies.

As compared to traditional centralized systems, simulation analysis proved higher accuracy in coordination, minimized leakage, and more compliance capability. Further research may focus on real-time digital twin integration, blockchain-based trust management, and adaptive AI governance for autonomous construction environments.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 8, August 2026
DOI: 10.17148/IJARCCE.2026.15801

This framework provides means to establish infrastructures that are both safe and scalable for future smart constructions.

REFERENCES

[1] Ahmed, Mohammed Imran, Abdul Raheman Mohammed, Srujan Kumar Ganta, Sireesha Kolla Kolla, and Mohammed Kashif Kashif. "AI-Driven Green Construction: Optimizing Energy Efficiency, Waste Management and Security for Sustainable Buildings." Journal of Cognitive Computing and Cybernetic Innovations 1, no. 1 (2025): 37-41..

[2] Khader, Shuaib Abdul, Amir Ahmed Ansari, and Syed Sharik Ali. "Zero-Day Exploit Prediction Using Graph-Based Deep Learning on Vulnerability and Threat Intelligence Data."

[3] Mohammed, Abdul Faisal, and Mohammed Akifuddin Ghori. "AI-Enhanced Safety for Heavy Load Construction Vehicles: An Integrated Embedded C++ Software Approach."

[4] Ansari, Meraj Farheen, and Syed Sharik Ali. "AI-driven zero-trust architecture for enhanced cybersecurity in dynamic network environments." International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering 13 (2025): 12.

[5] Ansari, Meraj Farheen. "Redefining Cybersecurity: Strategic Integration of Artificial Intelligence for Proactive Threat Defense and Ethical Resilience."

[6] Sultana, Ghousia, Siraj Farheen Ansari, Mohammed Imran Ahmed, Abdul Faiyaz Shaik, Moin Uddin Khaja, and Bibhu Dash. "RESPONSIBLE AI ANALYTICS FOR REAL-WORLD IMPACT: NAVIGATING ETHICS, PRIVACY AND TRUST."

[7] Chittoju, Siva Sai Ram, Sireesha Kolla, Mubashir Ali Ahmed, and Abdul Raheman Mohammed. "Synergistic Integration of Blockchain and Artificial Intelligence for Robust IoT and Critical Infrastructure Security."

[8] Ansari, Mohammed Azmath, Shaik Aqheel Pasha, and Narendar Kandula. "Reinforcement Learning for Adaptive Network Defense in Financial Institutions."

[9] Integrating Machine Learning and Engineering Management to Optimize Construction Scheduling and Resource Allocation

[10] Kashif, Mohammed, Mohammed Aasimuddin, Mubashir Ali Ahmed, Laxmi Bhavani Cheekatimalla, Eraj Farheen Ansari, and Ahwan Mishra. "AI-DRIVEN CTI FOR BUSINESS: EMERGING THREATS, ATTACK STRATEGIES, AND DEFENSIVE MEASURES."

[11] Mohammed, Naveed Uddin, Zubair Ahmed Mohammed, Shravan Kumar Reddy Gunda, Akheel Mohammed, and Moin Uddin Khaja. "Networking with AI: Optimizing Network Planning, Management, and Security through the medium of Artificial Intelligence.

[12] Chittoju, S. R., and Siraj Farheen Ansari. "Blockchain's Evolution in Financial Services: Enhancing Security, Transparency, and Operational Efficiency." International Journal of Advanced Research in Computer and Communication Engineering 13, no. 12 (2024): 1-5.

[13] Mohammed, Akheel, Zubair Ahmed Mohammed, Naveed Uddin Mohammed, Shravan Kumar Gunda, Mohammed Azmath Ansari, and Mohd Abdul Raheem. "AI-NATIVE WIRELESS NETWORKS: TRANSFORMING CONNECTIVITY, EFFICIENCY, AND AUTONOMY FOR 5G/6G AND BEYOND

[14] Reddy, B. (2021). A Quantitative Analysis of Cloud Security Practices in IoT Environment (dissertation).

[15] Reddy, Balavardhan, and Amir Ahmed Ansari. "AI-ENHANCED NETWORK TRAFFIC ANALYSIS FOR PREVENTING FRAUD PAYMENT IN BANKS."

[16] KASHIF, MOHAMMED, ABDUL RAHMAN JIBRAN SYED, and MUBASHIR ALI AHMED. "ADVANCING ANOMALY AND FRAUD DETECTION IN BIG DATA WITH ARTIFICIAL INTELLIGENCE."

[17] RAHEEM, MOHD ABDUL, and MOHAMMED AZMATH ANSARI. "INTELLIGENT AND TRUSTWORTHY 6G: AI-DRIVEN ARCHITECTURES, APPLICATIONS, AND SECURITY FRAMEWORKS.

[18] Syed, Waheeduddin Khadri, Abubakar Mohammed, Janamolla Kavitha Reddy, and S. Dhanasekaran. "Biometric authentication systems in banking: A technical evaluation of security measures." In 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC), pp. 1331-1336. IEEE, 2024.

[19] Hussain, Alefiya, Prateek Jaipuria, Geoff Lawler, Stephen Schwab, and Terry Benzel. "Toward orchestration of complex networking experiments." In 13th USENIX Workshop on Cyber Security Experimentation and Test (CSET 20). 2020.

