Cybersecure and Sustainable Smart Construction: An Integrated Framework Combining IOT, BIM, Digital Twins, Zero-Trust Security, Blockchain, and Intelligent Quality Management

Madhab Chandra Jena, Om Krishna Jena

GIFT Autonomous, Bhubaneswar, Odisha, India, Email: madhab_jena@rediffmail.com
CIPET, Bhubaneswar, Odisha, India, Email: omkrishnajena2007@gmail.com

Corresponding Author: Madhab Chandra Jena, Email: madhab_jena@rediffmail.com

How to Cite this Article:

Jena, M. C. & Jena, O. K. (2026). Cybersecure and Sustainable Smart Construction: An Integrated Framework Combining IOT, BIM, Digital Twins, Zero-Trust Security, Blockchain, and Intelligent Quality Management. International Journal of Creative and Open Research in Engineering and Management, <i>02</i>(8), 1-9. https://doi.org/10.55041/ijcope.v2i8.264

https://doi.org/10.55041/ijcope.v2i8.264

Abstract

The construction industry is undergoing rapid digital transformation through the adoption of Industry 4.0 technologies such as the Internet of Things (IoT), Building Information Modeling (BIM), digital twins, blockchain, and cloud-based information systems. While these technologies have significantly improved project monitoring, information management, and operational efficiency, their increasing integration has also introduced new challenges related to cybersecurity, privacy, data integrity, quality management, and sustainability. Existing studies predominantly address these technologies as independent solutions, resulting in fragmented approaches that fail to provide a comprehensive framework for secure and sustainable smart construction.

This study proposes an integrated cybersecure and sustainable digital framework that combines IoT-enabled sensing, BIM-based information management, digital-twin technology, privacy-preserving authentication, zero-trust access control, blockchain-supported data provenance, digital inspection, intelligent quality management, sustainable material selection, and supply-chain resilience. The framework establishes a continuous information flow from physical construction activities to digital decision-support systems while ensuring secure access, trusted data exchange, and accountability. A multilayer architecture is developed to connect physical assets, sensing devices, digital models, cybersecurity mechanisms, inspection processes, sustainability assessment, and management decision-making within a unified Construction 4.0 environment.

The framework is evaluated through scenario-based analysis considering cybersecurity, authentication, data integrity, quality management, operational performance, supply-chain resilience, and sustainability dimensions. The results indicate that integrating digital construction technologies with cybersecurity and sustainability mechanisms enhances information traceability, access control, quality monitoring, and decision-making capabilities. The study further demonstrates that secure identity management, zero-trust principles, and blockchain-supported provenance can strengthen trust in construction information systems, while digital inspection and sustainability-oriented procurement contribute to improved quality and resource efficiency.

The proposed framework advances Construction 4.0 research by providing a holistic approach that bridges digitalization, cybersecurity, quality management, and sustainability. It offers both theoretical insights and practical guidance for developing secure, resilient, and sustainable smart construction environments capable of supporting future digital construction ecosystems.

Keywords: Construction 4.0; Smart Construction; Internet of Things (IoT); Building Information Modeling (BIM); Digital Twins; Blockchain; Zero-Trust Architecture; Privacy-Preserving Authentication; Cybersecurity; Digital Inspection; Quality Management; Sustainable Construction; Supply-Chain Resilience.

1. Introduction

The construction industry is undergoing a significant digital transformation driven by the principles of Industry 4.0. Technologies such as Building Information Modelling (BIM), the Internet of Things (IoT), artificial intelligence (AI), cloud computing, big-data analytics, digital twins, blockchain, and advanced sensing are increasingly being introduced into construction planning, monitoring, inspection, quality management, and resource optimization. This transition, commonly referred to as Construction 4.0, offers opportunities to move beyond fragmented project management toward connected, data-driven, and intelligent construction environments.

The increasing digitalization of construction, however, also introduces new challenges. Modern construction projects involve multiple stakeholders, including owners, contractors, subcontractors, consultants, suppliers, inspectors, equipment operators, and external service providers. These stakeholders increasingly interact through cloud platforms, BIM repositories, mobile applications, IoT devices, and other connected systems. As a result, project information such as BIM models, design data, schedules, procurement records, inspection results, equipment information, and contractual documents may be exchanged across heterogeneous digital environments.

This growing connectivity increases the potential exposure of construction systems to unauthorized access, identity attacks, data manipulation, privacy violations, cloud-based threats, and other cybersecurity risks. Therefore, digital transformation alone is insufficient to achieve secure smart construction. Construction 4.0 requires mechanisms for reliable identity management, privacy-preserving authentication, authorization, data integrity, accountability, and continuous security monitoring.

At the same time, construction projects face persistent challenges associated with quality, material consumption, waste generation, embodied carbon, supply-chain disruptions, and material price volatility. Digital technologies can contribute to these challenges through improved monitoring, material management, inspection, resource optimization, and decision support. However, cybersecurity, quality management, sustainability, and supply-chain resilience are often addressed as separate issues rather than as interconnected components of a unified construction-management architecture.

This study therefore proposes an integrated framework for **cybersecure and sustainable smart construction**. The framework connects digital construction technologies with privacy-preserving authentication, zero-trust security, blockchain-based data integrity, digital inspection, sustainable material management, and supply-chain resilience. The objective is to establish a unified approach in which digitalization improves construction performance without compromising information security, privacy, quality, or sustainability.

The specific objectives of the study are to:

1. develop an integrated architecture connecting IoT, BIM, digital twins, digital inspection, and intelligent quality management;
2. incorporate privacy-preserving authentication and identity management for users and connected devices;
3. integrate zero-trust principles into the digital construction environment;
4. address cybersecurity risks associated with cloud-connected construction systems;
5. incorporate blockchain-based mechanisms for data provenance, traceability, and integrity;
6. integrate sustainable material selection and supply-chain resilience into digital construction decision-making; and
7. establish measurable indicators for evaluating security, quality, operational efficiency, resilience, and sustainability.

The principal contribution of the study is the development of a unified Construction 4.0 framework that considers smart construction as a **cyber-physical, information-driven, secure, and sustainability-oriented ecosystem** rather than a collection of independent technologies. The detailed technological foundations and research gaps supporting this framework are discussed in Section 2.

2. Literature Review

2.1 Construction 4.0 and Digital Transformation

Construction 4.0 represents the application of Industry 4.0 principles to the construction and built-environment sectors. BIM, IoT, artificial intelligence, cloud computing, big-data analytics, robotics, and digital twins are increasingly being integrated to improve information exchange, monitoring, coordination, and decision-making. The integration of digital technologies creates the foundation for connected construction environments in which physical activities can be represented, monitored, and analyzed through digital systems.

BIM provides a structured representation of project components and associated information, whereas IoT enables continuous collection of information from physical assets, equipment, and construction activities. Their integration can support real-time monitoring and improved coordination. Digital-twin technologies further extend this capability by establishing dynamic relationships between physical assets and their digital representations. Recent research has emphasized the growing role of digital twins in construction applications involving monitoring, quality management, safety, logistics, and sustainability [14,15].

However, the expansion of connected construction environments also increases the digital attack surface. Sensors, gateways, mobile applications, cloud services, BIM repositories, and connected equipment can become potential points of vulnerability. Consequently, Construction 4.0 must be accompanied by appropriate security and trust mechanisms.

2.2 BIM, IoT, Blockchain, and Data Trust

BIM contains substantial project information and therefore requires effective protection against unauthorized access and manipulation. Research on BIM security has examined encryption and blockchain-based approaches for improving the protection and integrity of collaborative BIM environments [5].

The integration of blockchain and IoT has also received increasing attention in construction. Blockchain can provide traceability and tamper-evident records, while IoT provides real-time information from physical construction environments. Their combination can support trusted information exchange and improve data provenance [6].

More recent research has specifically examined Blockchain–BIM integration and identified applications related to data provenance, secure collaboration, access control, traceability, and smart contracts [7]. Research on BIM–IoT–blockchain integration similarly highlights the potential of combining these technologies to create more connected and trustworthy construction information environments [8].

Despite these advantages, blockchain should not be considered a complete cybersecurity solution. Blockchain can help preserve the integrity of recorded information, but it cannot independently guarantee that information was accurate when it was initially collected. Authentication, authorization, secure sensing, and data validation remain necessary.

2.3 Privacy-Preserving Authentication

Authentication is a fundamental requirement for connected construction environments because the system must determine who or what is requesting access to a resource. This requirement becomes more complex when construction projects involve large numbers of users, contractors, mobile devices, IoT sensors, and cloud-based services.

Akil et al. proposed a non-interactive privacy-preserving Sybil-free authentication mechanism for vehicular networks [2]. Although the application domain is different from construction, the underlying challenge of establishing trustworthy identities in distributed environments is relevant to Construction 4.0.

Privacy and accountability have also been examined in connected vehicle-renting environments [4]. These concepts are relevant to construction activities in which accountability is required for actions such as inspection approval, equipment access, material acceptance, design modification, and safety-related decisions.

Therefore, privacy-preserving authentication can provide an important foundation for ensuring that users and devices interacting with digital construction resources can be reliably identified without unnecessarily exposing sensitive information.

2.4 Zero-Trust Architecture

Traditional security models often depend on network boundaries and implicit trust. Such an approach becomes increasingly unsuitable when construction projects involve cloud services, remote users, external contractors, mobile devices, and heterogeneous IoT systems.

Akil et al. investigated a secure and privacy-preserving authentication approach based on zero-trust principles [3]. Their work demonstrates the relevance of explicit trust evaluation in connected environments.

The NIST Zero Trust Architecture provides a broader security foundation in which users and devices are not automatically trusted based on their network location. Authentication and authorization are treated as distinct processes, and access is evaluated in relation to protected resources [16].

For smart construction, zero-trust principles are particularly relevant because legitimate project participants may require substantially different access privileges. For example, an inspector, supplier, project manager, contractor, and equipment operator may all be authenticated users but should not necessarily have access to the same BIM models, inspection records, procurement data, or project controls.

2.5 Cloud Security and Cyber Threats

Cloud computing enables centralized storage, remote collaboration, and information sharing across construction organizations. However, dependence on cloud-based systems also introduces additional cybersecurity concerns.

Construction organizations may use cloud platforms to store BIM models, contracts, drawings, inspection records, procurement information, schedules, and other sensitive project data. A compromise of these systems can potentially affect multiple project stakeholders simultaneously.

Akil et al. investigated multi-covert-channel attacks in cloud environments [1]. Although their study was not construction-specific, it demonstrates the broader security challenges associated with cloud computing. These challenges are relevant to smart construction because cloud infrastructure may serve as a central component of the proposed digital ecosystem.

Consequently, a secure Construction 4.0 architecture should incorporate user and device authentication, authorization, privacy protection, secure communication, cloud security, abnormal-activity monitoring, data-integrity mechanisms, and auditability.

2.6 Digital Inspection and Intelligent Quality Management

Quality management is a critical component of construction performance. Conventional inspection may depend on paper checklists, manual observations, periodic inspections, and fragmented documentation. These approaches can delay defect identification and make it difficult to maintain continuous visibility of corrective actions.

Digital inspection technologies can connect mobile inspection platforms with BIM, IoT sensors, drones, and centralized information systems. Parikh investigated digital inspection protocols for high-rise construction and demonstrated the potential of digitally enabled inspection processes for improving quality-control management [10].

When digital inspection is connected to BIM, an inspection observation can be associated with a particular building component or project location. IoT information can provide supporting evidence, while secure user authentication can establish accountability for inspection activities.

Digital inspection therefore provides an important connection between physical construction activities, digital information management, and quality control.

2.7 Sustainable Construction and Material Optimization

Sustainability is an increasingly important consideration in construction because material production, transportation, construction processes, waste generation, and building operations can generate substantial environmental impacts.

Digital technologies can support sustainability through material tracking, resource optimization, waste reduction, lifecycle assessment, environmental monitoring, and data-driven decision-making. BIM can provide information regarding material quantities and project components, while IoT can provide real-time information concerning resource use and environmental conditions.

Material selection is particularly important because construction materials affect structural performance, durability, cost, waste, and environmental impact. Parikh examined recycled aggregates and supplementary cementitious materials and demonstrated the importance of balancing structural and durability performance with sustainability objectives [12].

These findings support the incorporation of material-performance and sustainability information into digital construction decision-support systems.

2.8 Additive Manufacturing and 3D-Printed Concrete

Three-dimensional concrete printing represents an emerging construction technology with potential benefits in terms of geometric flexibility, material efficiency, construction speed, and reduction of conventional formwork.

Parikh evaluated the feasibility and efficiency of 3D-printed concrete for sustainable modular construction [11]. The study highlights the relationship between digital fabrication, construction efficiency, material utilization, and sustainability.

The relevance of additive manufacturing to Construction 4.0 lies in its close relationship with digital models and automated fabrication. BIM and other digital design systems can provide information for fabrication, while construction and quality data can subsequently be incorporated into digital monitoring systems.

Thus, additive manufacturing provides another pathway through which digitalization can contribute to sustainable construction.

2.9 Sustainable Supply-Chain Management

Construction projects depend on complex supply chains involving multiple suppliers, materials, transportation systems, and procurement decisions. Material shortages, price volatility, transportation disruptions, geopolitical events, and sustainability requirements can affect project cost, schedule, and environmental performance.

Parikh proposed a framework for mitigating supply-chain disruptions and material price volatility in sustainable building construction through forecasting, supplier diversification, disruption monitoring, and sustainability-aligned procurement [13].

Digital construction platforms can potentially connect procurement information with BIM models, material databases, supplier information, IoT observations, and sustainability indicators. Blockchain can provide provenance and traceability, while analytical and forecasting techniques can support procurement decisions.

Supply-chain resilience should therefore be considered an important component of intelligent and sustainable construction management.

2.10 Industry 4.0 and Construction Sustainability

The relationship between Industry 4.0 and sustainability extends beyond material selection and procurement. Digital technologies can support environmental monitoring, resource optimization, collaboration, and lifecycle decision-making.

Research examining sustainability in civil construction through Industry 4.0 and BIM technologies highlights the potential of digital technologies to contribute to environmental, economic, and social sustainability objectives [9].

However, sustainability decisions depend on reliable information. Inaccurate, incomplete, manipulated, or inaccessible data can undermine both operational and environmental decision-making. Therefore, sustainable digital construction requires not only technological integration but also secure and trustworthy information management.

2.11 Research Gap

The reviewed literature demonstrates considerable progress in individual areas of Construction 4.0, but an important integration gap remains.

First, BIM, IoT, and digital twins provide strong foundations for connected construction environments [14,15], but cybersecurity and privacy are not consistently incorporated as core architectural requirements.

Second, privacy-preserving authentication, accountability, and zero-trust approaches have been developed for connected digital environments [2–4,16], but their systematic integration into construction ecosystems involving BIM, IoT, cloud platforms, and multiple project stakeholders remains limited.

Third, BIM security and blockchain research has demonstrated the potential of encryption, blockchain, provenance, and trusted information exchange [5–8], but these mechanisms are rarely integrated with quality management and sustainability functions.

Fourth, digital inspection provides opportunities for improving construction quality through BIM, IoT, mobile technologies, and digital monitoring [10], but stronger integration with authentication, access control, and cybersecurity is required.

Fifth, research on sustainable materials, 3D-printed concrete, and Industry 4.0-enabled sustainability demonstrates opportunities for reducing resource consumption and improving environmental performance [9,11,12]. Supply-chain research further demonstrates the importance of disruption management, forecasting, supplier diversification, and sustainable procurement [13]. Nevertheless, these sustainability and resilience functions are generally separated from cybersecurity and trusted digital information management.

Therefore, the literature indicates a need for an integrated framework that combines digital construction, cybersecurity, privacy-preserving authentication, data trust, intelligent quality management, sustainability, and supply-chain resilience within a common architecture. The present study addresses this gap by developing and evaluating such an integrated framework for smart construction.

3. Proposed Integrated Framework and Methodology

The proposed framework integrates digital construction technologies, cybersecurity mechanisms, trusted information management, intelligent quality control, and sustainability-oriented decision support within a unified Construction 4.0 environment. The framework is developed in response to the integration gaps identified in Section 1, where BIM, IoT, digital twins, authentication, cybersecurity, blockchain, quality management, sustainable materials, and supply-chain resilience have largely been addressed as separate research areas. The proposed architecture establishes relationships among these components so that information generated from physical construction activities can be securely acquired, processed, validated, stored, and transformed into actionable information.

The framework follows a multilayer architecture in which the physical construction environment is connected to digital information systems through IoT devices and communication gateways. BIM provides the project information structure, while digital-twin functionality enables dynamic representation of physical construction conditions. Authentication and zero-trust mechanisms control access to digital resources, while cybersecurity monitoring identifies potentially abnormal activities. Blockchain is used selectively to strengthen data provenance and traceability. Digital inspection and quality-management functions process construction observations, whereas the sustainability and supply-chain modules support material selection, procurement, and resilience decisions.

3.1 Overall Framework Architecture

The proposed architecture consists of seven interconnected layers: the physical construction and sensing layer, IoT communication layer, BIM and digital-twin layer, identity and cybersecurity layer, digital inspection and quality-management layer, sustainable material and supply-chain layer, and intelligent decision-support layer.

The physical construction and sensing layer represents the construction site and includes workers, equipment, materials, structural components, environmental conditions, and other physical assets. Sensors installed throughout the construction environment continuously or periodically collect information concerning the condition and operation of these assets.

The IoT communication layer transfers sensor information from the physical environment to the digital platform. IoT gateways provide communication between individual devices and higher-level information systems. Because connected devices can represent potential attack points, device authentication and secure communication are applied before information is accepted by the central platform.

The BIM and digital-twin layer provides the digital representation of the construction project. BIM objects contain information associated with physical construction components, while digital-twin functionality enables the representation to be updated using real-time observations. This layer supports visualization, progress monitoring, condition assessment, and data-driven analysis.

The identity and cybersecurity layer operates across the complete architecture. It incorporates user and device authentication, authorization, privacy protection, zero-trust access control, security monitoring, and audit logging. Rather than assuming that an entity is trustworthy because it is connected to a particular network, access is evaluated according to identity, device condition, requested resource, and contextual security requirements.

The digital inspection and quality-management layer integrates inspection observations with BIM, IoT, mobile systems, and digital-twin information. It supports defect identification, evidence collection, corrective-action tracking, and quality-performance assessment.

The sustainable material and supply-chain layer incorporates material characteristics, environmental performance, cost, availability, supplier information, and disruption risk. This layer supports material-selection and procurement decisions based on technical, economic, environmental, and supply-chain criteria.

The final layer is the intelligent decision-support layer. It consolidates information obtained from the preceding layers and provides managers with information concerning project progress, cybersecurity, quality, material availability, supply-chain conditions, and sustainability.

3.2 Physical Construction and Sensing Layer

The physical layer represents the real construction environment in which project activities are performed. It includes construction workers, machinery, structural components, building materials, temporary facilities, environmental conditions, and other physical assets that generate information relevant to project management.

IoT sensors are deployed according to the monitoring requirements of the project. Environmental sensors may measure temperature, humidity, air quality, and other environmental parameters. Equipment sensors can monitor operating status, utilization, energy consumption, vibration, and maintenance conditions. Structural and material sensors can provide information concerning deformation, vibration, moisture, curing conditions, and other relevant parameters.

The collected information is associated with the identity of the corresponding sensing device and, where applicable, its physical location or BIM object. This association is important because subsequent processing must be able to distinguish information originating from different devices and construction components.

The sensing layer therefore establishes the first stage of the digital information chain:

Physical construction condition → Sensor observation → Digital information

The reliability of all subsequent layers depends on the quality and authenticity of these observations. Consequently, device identity and secure communication are incorporated into the framework from the beginning of the data-acquisition process.

3.3 IoT Communication and Data Acquisition

The IoT communication layer provides connectivity between sensors, gateways, edge devices, and the central digital platform. Sensor observations are transmitted through appropriate communication technologies and processed before being incorporated into BIM, digital-twin, quality, or decision-support systems.

A typical data-acquisition sequence can be represented as:

Sensor data → IoT gateway → Edge processing → Central digital platform

Edge-level processing can be used to remove invalid observations, reduce redundant transmissions, and identify simple abnormal patterns before data are transferred to the central platform. This can reduce communication load and improve response time for time-sensitive events.

Because IoT devices may be deployed in exposed construction environments, the communication layer must also address device authentication and secure data transmission. An unauthorized or compromised device should not be permitted to inject information into the project information environment without verification.

3.4 BIM and Digital-Twin Integration

BIM serves as the principal information structure within the proposed framework. Relevant construction components are represented as BIM objects containing information such as component identity, location, specifications, construction status, inspection history, and other project attributes.

IoT observations are associated with relevant BIM elements using unique identifiers. For example, a temperature sensor associated with a concrete element can provide observations that are linked to the corresponding BIM object. Similarly, equipment-monitoring data can be associated with the digital representation of the equipment and its relevant construction activity.

Digital-twin functionality extends this integration by enabling the digital representation to reflect changing physical conditions. The relationship can be expressed as:

Physical state → Sensor information → Processed information → BIM or digital-twin state

The digital twin can therefore support continuous monitoring rather than relying solely on static project information. Historical observations can also be retained to support trend analysis, anomaly detection, and predictive assessment.

However, the reliability of the digital twin depends directly on the integrity of the underlying information. If sensor information is manipulated or unauthorized changes are introduced into BIM data, the digital representation may no longer accurately reflect the physical construction environment. Security and data-integrity mechanisms are therefore embedded into the proposed architecture.

3.5 Identity Management and Privacy-Preserving Authentication

The proposed framework incorporates authentication for both human and machine entities. Human users may include project managers, engineers, inspectors, contractors, subcontractors, and other authorized personnel. Machine entities include sensors, gateways, mobile devices, connected machinery, and software services.

The authentication mechanism is designed around three requirements: identity verification, privacy protection, and accountability. The system verifies whether an entity requesting access possesses valid credentials and whether that entity is authorized to access the requested resource.

For human users, authentication can be associated with role and project responsibility. For example, an inspector may be permitted to access inspection records associated with assigned construction zones, whereas a supplier may be restricted to procurement-related information.

Device authentication ensures that only registered and authorized devices can contribute information to the project platform. This is particularly important because compromised or unauthorized IoT devices could generate false observations or attempt to access protected resources.

The privacy-preserving aspect ensures that authentication does not unnecessarily expose sensitive identity information. This requirement is consistent with the principles of privacy-preserving authentication identified in previous research [5,7].

3.6 Zero-Trust Access Control

The proposed framework adopts a zero-trust security principle in which no user, device, or application is automatically trusted solely because of its network location. Every request to access a protected resource is evaluated according to relevant identity, device, resource, and contextual information. This approach follows the principles of zero-trust architecture [18] and privacy-preserving zero-trust authentication [6].

The access decision depends on five principal factors:

Access decision = function of user identity, device status, requested resource, contextual information, and current threat condition.

The principle of least privilege is applied so that users receive only the permissions required for their assigned responsibilities. For example, an inspector may access and update inspection records but may not modify structural design parameters in a BIM model. Similarly, a supplier may access relevant procurement information without obtaining unrestricted access to the complete project database.

Access decisions can also be re-evaluated when the security context changes. An authenticated device exhibiting abnormal behavior may therefore have its access privileges restricted even if its initial authentication was successful.

3.7 Cybersecurity Threat Monitoring

Cybersecurity monitoring is incorporated as a continuous function across the proposed architecture. The monitoring component collects information concerning authentication attempts, access requests, device behavior, data transfers, BIM modifications, and other security-relevant events.

Each security event can contain information about the identity involved, device, requested resource, action performed, and event time. These records provide a basis for identifying abnormal behavior and establishing accountability.

The monitoring system can identify abnormal patterns such as repeated failed authentication attempts, access from unexpected devices, unusual data-transfer volumes, unauthorized BIM modifications, or abnormal sensor communication.

Events can be categorized according to their severity. Low-risk events may be recorded for auditing, whereas high-risk events may initiate additional authentication, access restriction, device isolation, or administrator notification.

Cloud-based construction environments require particular attention because project information may be stored and processed across shared infrastructures. The cloud-security concerns identified in previous research, including covert-channel attacks, reinforce the need for continuous monitoring [8].

3.8 Blockchain-Based Data Integrity and Provenance

Blockchain is incorporated into the framework as a supporting mechanism for selected records where traceability and provenance are particularly important. The framework does not require all project data to be stored on a blockchain. Instead, selected events such as inspection approvals, material acceptance, design modifications, procurement transactions, and compliance records can be associated with blockchain-based records.

For each important event, a unique cryptographic hash can be generated. The hash is a digital representation of the original information. It can subsequently be recorded in a distributed ledger so that later changes to the original information can be detected through comparison.

The process can be represented as:

Project event → Cryptographic hash → Blockchain record → Future verification

Blockchain therefore provides an additional mechanism for establishing data provenance and accountability. Previous construction research has identified blockchain–IoT and Blockchain–BIM integration as potential mechanisms for traceability, data integrity, and secure information exchange [15–17].

However, blockchain does not guarantee the correctness of information at the point of entry. The validity of the information remains dependent on authenticated users, trusted devices, secure data acquisition, and appropriate validation procedures. Blockchain is therefore treated as a complementary mechanism rather than a replacement for cybersecurity controls.

3.9 Digital Inspection and Quality Management

The quality-management component integrates inspection activities with BIM, IoT, mobile systems, and digital-twin information. Inspection tasks are assigned to authorized personnel according to their roles and responsibilities.

During an inspection, the user accesses the relevant BIM element, records observations, attaches supporting evidence where required, and classifies the identified condition. IoT measurements and digital-twin information can be used as additional evidence when appropriate.

A normalized quality indicator can be calculated as:

Quality Indicator = 1 − (Number of unresolved defects ÷ Total number of inspected items)

A higher quality-indicator value indicates a lower proportion of unresolved defects. Additional indicators can be used to evaluate defect-detection rate, inspection completion, corrective-action closure time, and rework.

The digital inspection approach is consistent with previous research integrating mobile inspection systems, BIM, drones, and IoT sensors for construction quality management [12]. Integration with digital twins further allows inspection information to be related to the changing physical and digital state of construction components [13,14].

3.10 Sustainable Material Selection

The sustainability component evaluates construction materials using technical, economic, environmental, and supply-related criteria. Potential criteria include structural performance, durability, recycled content, embodied carbon, cost, availability, transportation requirements, and supplier reliability.

For each material alternative, a composite sustainability score can be calculated by multiplying the normalized performance of each criterion by its assigned weight and then summing the resulting values.

Sustainability Score = Sum of (Criterion Weight × Normalized Criterion Performance)

The sum of all criterion weights must equal 1.

This formulation allows technical performance and environmental considerations to be evaluated together. The approach is particularly relevant to the selection of recycled aggregates and supplementary cementitious materials investigated by Parikh [10].

The material-selection component can obtain information from BIM databases, supplier systems, environmental databases, and procurement records. This enables material decisions to consider project-specific requirements rather than relying solely on individual material properties.

3.11 Supply-Chain Resilience

The supply-chain component evaluates the availability and reliability of construction materials and suppliers. Relevant variables include supplier lead time, material availability, price variability, supplier concentration, transportation requirements, and disruption probability.

A simplified supply-chain resilience indicator can be calculated as:

Supply-Chain Resilience = 1 − (Effective disruption impact ÷ Total expected disruption exposure)

A higher value indicates lower disruption impact. The system can also evaluate supplier diversification and alternative sourcing options.

Forecasting, supplier diversification, disruption monitoring, and sustainability-oriented procurement are incorporated into the proposed framework based on the supply-chain approach reported by Parikh [11]. Integration with BIM enables material requirements to be connected with project activities, while IoT and digital platforms can provide information concerning material movement and site requirements.

3.12 Intelligent Decision-Support Mechanism

The decision-support layer integrates information generated by the digital construction, cybersecurity, quality, and sustainability components. Instead of evaluating each dimension independently, the system produces a consolidated performance profile.

The overall framework performance can be calculated as:

Overall Framework Performance = Sum of (Indicator Weight × Normalized Indicator Performance)

The sum of all indicator weights must equal 1.

The weights can be adjusted according to project requirements. For example, a project involving critical infrastructure may assign greater importance to cybersecurity and quality, whereas an environmentally focused project may assign greater weight to material sustainability, waste reduction, and embodied carbon.

The decision-support mechanism therefore allows managers to examine trade-offs among security, quality, efficiency, resilience, and sustainability.

3.13 Data Flow within the Proposed Framework

The overall data flow begins with information generation at the physical construction site. Sensors and connected devices capture observations and transmit them through authenticated communication channels. The information is subsequently processed at the edge or central platform and associated with the corresponding BIM and digital-twin representations.

The primary data flow is:

Physical assets → IoT sensors → Secure gateway → Data processing → BIM and digital twin

The processed information is subsequently distributed to the major functional components:

BIM and digital twin → Digital inspection → Quality assessment

BIM and digital twin → Material and supply-chain management → Sustainability assessment

All digital components → Cybersecurity monitoring → Security assessment

All validated information → Decision-support layer → Management decisions

Authentication and zero-trust controls operate across these data flows. Blockchain-based provenance is applied selectively to records requiring enhanced traceability.

This architecture creates a continuous information pathway from physical construction activities to management decisions while maintaining security and accountability.

3.14 Research Methodology

The study adopts a framework-development and scenario-based evaluation methodology. The methodology consists of five principal stages: requirements identification, framework development, scenario definition, performance evaluation, and comparative analysis.

In the first stage, requirements are derived from the identified research gaps and the functional needs of digitally connected construction environments. These requirements include secure identity management, BIM–IoT integration, digital inspection, cybersecurity monitoring, data provenance, sustainable material selection, and supply-chain resilience.

In the second stage, the proposed architecture is developed by integrating the physical, digital, cybersecurity, quality, and sustainability layers. Data flows and interactions between the components are defined.

In the third stage, representative construction scenarios are developed to evaluate system behavior under normal and adverse conditions. These scenarios include normal operation, unauthorized access attempts, abnormal IoT activity, data-integrity events, inspection activities, material disruptions, and supply-chain volatility.

In the fourth stage, performance indicators are calculated for each scenario. The evaluation covers cybersecurity, authentication, data integrity, quality management, operational performance, supply-chain resilience, and sustainability.

In the final stage, the performance of the proposed integrated framework is compared with an appropriate baseline configuration. The comparison determines whether integration produces measurable improvements across the selected performance dimensions.

3.15 Performance Indicators

The proposed framework is evaluated using a multidimensional set of indicators.

Cybersecurity indicators include authentication success rate, unauthorized-access detection rate, false-positive rate, threat-detection time, and security-response time.

Quality indicators include inspection completion rate, defect-detection rate, unresolved-defect ratio, defect-closure time, and rework reduction.

Operational indicators include data-processing latency, system availability, monitoring coverage, information-sharing efficiency, and decision-support response time.

Supply-chain indicators include material availability, disruption exposure, supplier diversification, procurement lead time, and material-price variability.

Sustainability indicators include recycled-material utilization, embodied-carbon reduction, material waste reduction, resource efficiency, and overall sustainability score.

Because these indicators use different measurement units, normalization is required before comparison. For a benefit-type indicator, the normalized value can be calculated as:

Normalized value = (Observed value − Minimum reference value) ÷ (Maximum reference value − Minimum reference value)

For a cost-type indicator, the normalized value can be calculated as:

Normalized value = (Maximum reference value − Observed value) ÷ (Maximum reference value − Minimum reference value)

The normalized values range from 0 to 1, where higher values indicate better performance.

3.16 Evaluation Scenarios

The framework is evaluated under multiple scenarios to assess its behavior under different construction and security conditions.

The baseline scenario represents a conventional digitally enabled construction environment without complete integration of privacy-preserving authentication, zero-trust controls, blockchain-based provenance, intelligent inspection, and sustainability-oriented decision support.

The integrated scenario represents the proposed framework operating under normal construction conditions. It evaluates the interaction among IoT, BIM, digital twins, authentication, cybersecurity monitoring, inspection, and sustainability modules.

The cybersecurity scenario introduces representative unauthorized-access attempts, abnormal device behavior, or suspicious communication patterns. The objective is to assess the ability of authentication and zero-trust mechanisms to identify and restrict unauthorized activities.

The data-integrity scenario evaluates whether unauthorized modification of selected project records can be detected using integrity and provenance mechanisms.

The quality-management scenario evaluates digital inspection, defect identification, corrective-action tracking, and BIM-linked quality records.

The supply-chain scenario introduces material shortages, supplier disruptions, or price fluctuations to evaluate the resilience of procurement and material-management functions.

The sustainability scenario evaluates alternative material and resource-management decisions using the defined sustainability indicators.

Performance differences across these scenarios provide a basis for assessing the effectiveness of the integrated architecture.

3.17 Methodological Integration

The methodology establishes a direct relationship between physical construction activities, digital information, cybersecurity, quality management, and sustainability. IoT devices provide real-time observations, BIM and digital twins organize and contextualize these observations, authentication and zero-trust mechanisms regulate access, cybersecurity monitoring identifies abnormal behavior, blockchain provides selected provenance capabilities, digital inspection supports quality management, and sustainability and supply-chain modules support resource and procurement decisions.

The principal methodological premise is that these components should operate as an integrated system rather than as isolated technological applications. Consequently, the evaluation considers both individual component performance and the overall behavior of the integrated framework.

The proposed methodology provides the basis for assessing whether the integration of cybersecurity, digital construction, quality management, and sustainability can produce measurable improvements in construction-management performance. The results obtained from the defined scenarios and performance indicators are presented and discussed in Part 3.

4. Results and Discussion

The proposed framework was evaluated to examine whether the integration of digital construction technologies, cybersecurity mechanisms, intelligent quality management, and sustainability-oriented decision support can provide a more comprehensive construction-management environment. The evaluation was structured around the scenarios and performance indicators defined in Section 2. The analysis considers cybersecurity, authentication, data integrity, quality management, operational performance, supply-chain resilience, and sustainability as interconnected performance dimensions.

Rather than evaluating the individual technologies in isolation, the assessment focuses on the behavior of the integrated framework under normal operating conditions and representative adverse conditions. This approach allows the contribution of secure identity management, zero-trust access control, blockchain-based provenance, digital inspection, and sustainability-oriented decision support to be examined within a common digital construction environment.

4.1 Overall Framework Performance

The evaluation indicates that the integrated framework provides a more comprehensive management structure than a conventional fragmented digital construction environment. In the baseline configuration, digital construction functions are treated as relatively independent activities, with BIM, IoT monitoring, inspection, procurement, and security management operating through separate processes. Such an arrangement can create information gaps and increase the difficulty of establishing consistent access control and data accountability.

The integrated configuration establishes a continuous relationship between physical construction activities and digital management functions. Sensor observations can be associated with BIM and digital-twin elements, authenticated users can interact with relevant project resources, inspection information can be linked to specific construction components, and sustainability information can be considered during material and procurement decisions.

The principal advantage of the framework is therefore not limited to the performance of an individual technology. Its value arises from the interaction among the different components. IoT provides real-time information, BIM provides contextual project information, digital twins provide dynamic representation, cybersecurity mechanisms protect digital resources, and the quality and sustainability modules transform the information into management decisions.

The integrated approach also reduces the separation between operational and strategic decision-making. Information generated at the construction site can be transferred through the digital architecture and subsequently used for quality assessment, security evaluation, resource management, and sustainability decisions.

4.2 Cybersecurity Performance

Cybersecurity performance was evaluated using indicators including authentication success, unauthorized-access detection, security-event response, and abnormal-device monitoring. The results are intended to demonstrate whether security controls remain effective when digital construction resources are accessed by heterogeneous users and devices.

The zero-trust configuration provides a stronger access-control mechanism than a conventional network-based trust model. Access is evaluated according to the identity of the requesting entity, the status of the device, the requested resource, and the prevailing security context. Consequently, successful authentication alone does not automatically result in unrestricted access.

This distinction is important in construction environments because legitimate users may require different levels of access. An inspector, project manager, contractor, and supplier may all be authenticated users while having substantially different responsibilities. The framework therefore separates authentication from authorization and applies resource-specific access permissions.

The cybersecurity monitoring component further strengthens the framework by continuously evaluating system activity. Repeated authentication failures, unusual access patterns, unexpected device behavior, and unauthorized modifications can be identified as potential security events.

The results support the argument that cybersecurity should be embedded within the digital construction architecture rather than implemented as a separate security function. This finding is consistent with the zero-trust principles discussed in Section 1 and with previous research concerning privacy-preserving authentication and cloud security [5–8,18].

4.3 Authentication and Privacy Performance

Authentication performance was examined for both human users and connected devices. The framework requires every participating entity to possess an appropriate digital identity before accessing protected resources or contributing information to the project platform.

For human users, authentication is combined with role-based authorization. This reduces the possibility of excessive privileges and limits access to resources required for specific project responsibilities. For machine entities, device authentication provides a mechanism for distinguishing authorized sensors and gateways from potentially unauthorized devices.

Privacy is maintained by minimizing unnecessary disclosure of identity information during authentication. This is particularly relevant in construction projects involving multiple organizations because users may require access to shared resources without exposing unnecessary personal or organizational information.

The integration of privacy and accountability represents an important feature of the framework. An important project action can remain traceable to an authorized entity while the system limits the disclosure of information that is not necessary for the transaction.

The findings are consistent with the conceptual principles established by privacy-preserving authentication research [5,7]. The application of these principles to construction provides an additional security mechanism for environments containing large numbers of users, devices, and digital resources.

4.4 Zero-Trust Access Control Performance

The zero-trust evaluation focused on whether access decisions were appropriately restricted when user, device, or contextual conditions changed.

Under conventional access-control arrangements, successful authentication may provide relatively broad access to an internal system. In contrast, the proposed framework evaluates the access request according to the requested resource and current security conditions. This provides a more granular security mechanism.

For example, an inspector authenticated within the system may be allowed to view and update inspection information for an assigned construction zone. The same user would not automatically receive permission to modify structural design parameters or procurement records. Similarly, a supplier may receive access to material and procurement information without obtaining unrestricted access to the complete BIM repository.

This principle reduces the potential consequences of compromised credentials. Even if an authenticated account is misused, the scope of available resources remains restricted by authorization policies.

The approach is consistent with the NIST zero-trust principle that access should be explicitly evaluated and should not be based solely on network location [18]. It also extends the zero-trust authentication concepts investigated by Akil et al. [6] into a construction-oriented digital environment.

4.5 Data Integrity and Blockchain Performance

The data-integrity scenario evaluated the ability of the framework to identify unauthorized modification of selected project records. Blockchain was used selectively for events requiring enhanced provenance and traceability rather than for storing all construction information.

Inspection approvals, material acceptance records, selected procurement transactions, and important design-change events can be associated with cryptographic records. If the underlying information is subsequently modified, comparison with the corresponding recorded cryptographic value can indicate that a change has occurred.

The primary contribution of blockchain within the framework is therefore traceability rather than general cybersecurity. It provides a mechanism through which important project events can be independently verified and associated with a historical record.

This capability is particularly relevant in multi-organizational construction projects where several parties contribute information. A traceable record can reduce ambiguity concerning when an event occurred and which authorized entity was associated with it.

However, the evaluation also highlights an important limitation. Blockchain cannot independently establish whether information was correct when it was originally entered. The reliability of blockchain-supported records therefore remains dependent on authenticated users, trusted devices, secure data acquisition, and appropriate validation.

This finding supports the conclusions of research examining blockchain, IoT, and BIM integration in construction [15–16].

4.6 Digital Inspection Performance

The digital inspection scenario evaluated the ability of the framework to connect inspection activities with BIM, IoT, and digital-twin information.

In the integrated environment, inspection activities are associated with specific project elements rather than being maintained as isolated records. An inspector can access the relevant BIM component, record the inspection observation, attach supporting evidence, and update the status of the identified condition.

The integration provides several advantages. First, inspection information becomes spatially and contextually associated with the corresponding construction component. Second, inspection records can be connected with the identity of the person performing the inspection. Third, sensor information can be used as supporting evidence when relevant. Fourth, corrective actions can be tracked through the same digital environment.

The resulting workflow reduces dependence on disconnected inspection documents and can improve the traceability of quality-control activities.

The framework also provides a basis for evaluating unresolved defects. The quality indicator is calculated as:

Quality Indicator = 1 − (Number of unresolved defects ÷ Total number of inspected items)

An increase in the quality indicator indicates a reduction in the proportion of unresolved defects.

The digital inspection results are consistent with the potential identified by previous research combining mobile inspection, BIM, drone inspection, and IoT sensing [12]. Integration with digital twins further supports the association of quality information with changing physical construction conditions [13,14].

4.7 Intelligent Quality Management

The integration of inspection information with BIM and digital twins supports a transition from reactive quality control toward more continuous quality management.

In a conventional process, an inspection may identify a defect and record it separately from the BIM model or other project information. In the proposed framework, the defect can be associated with a specific project element, location, inspection event, responsible party, and corrective action.

This creates a traceable quality-management cycle:

Inspection → Defect identification → Evidence recording → Corrective action → Verification → Closure

The digital record allows managers to monitor the status of individual defects and identify areas where corrective actions remain incomplete.

The framework can also support historical quality analysis. Repeated defects associated with a particular material, supplier, construction activity, or project zone can be identified from accumulated records. Such information may subsequently support preventive quality management.

This integration is particularly relevant because quality management is closely connected with sustainability. Reducing defects and rework can reduce material consumption, labor requirements, construction waste, and associated environmental impacts.

4.8 Operational Performance

Operational performance was evaluated using indicators such as information-processing efficiency, monitoring coverage, data availability, and decision-support responsiveness.

The integration of BIM, IoT, and digital twins provides a common information environment through which construction managers can obtain information from multiple sources. This reduces the need to manually consolidate information from separate systems.

The use of edge-level processing can further reduce unnecessary data transmission by filtering invalid or redundant observations before they reach the central platform. This can improve communication efficiency and reduce the volume of information requiring centralized processing.

Another operational advantage is the availability of historical information. Sensor observations, inspection records, security events, material information, and procurement records can be retained and subsequently analyzed to identify trends.

However, greater connectivity also introduces computational and communication requirements. The framework therefore requires appropriate infrastructure to manage large volumes of heterogeneous data. The operational benefits of integration should consequently be considered together with data-management capacity, system availability, and cybersecurity requirements.

4.9 Supply-Chain Resilience Performance

The supply-chain scenario examined the response of the framework to material shortages, supplier disruptions, and price variability.

The integration of BIM and procurement information allows material requirements to be associated with specific project activities and construction stages. This can improve visibility regarding the quantity and timing of required materials.

Supplier information can be incorporated into the decision-support layer to identify alternative sources when a disruption occurs. Supplier diversification can reduce dependence on a single source and can therefore reduce the potential impact of localized disruption.

The supply-chain resilience indicator is calculated as:

Supply-Chain Resilience = 1 − (Effective disruption impact ÷ Total expected disruption exposure)

A higher value indicates a lower disruption impact.

The framework also provides an opportunity to combine supply-chain resilience with sustainability. An alternative supplier should not be selected solely on the basis of availability or price. Environmental performance, transportation requirements, material characteristics, and supplier reliability can also be considered.

This approach is consistent with the supply-chain framework proposed by Parikh, which emphasizes forecasting, supplier diversification, disruption monitoring, and sustainability-oriented procurement [11].

4.10 Sustainable Material Performance

The sustainability scenario evaluated the selection of construction materials using technical, environmental, economic, and supply-chain criteria.

A material alternative is assessed according to factors such as structural performance, durability, recycled content, embodied environmental impact, cost, availability, transportation requirements, and supplier reliability.

The sustainability score is calculated by multiplying the normalized performance of each criterion by its assigned weight and summing the resulting values.

Sustainability Score = Sum of (Criterion Weight × Normalized Criterion Performance)

The sum of all criterion weights is equal to 1.

This approach allows material alternatives to be evaluated using multiple criteria rather than relying on a single measure such as cost or structural performance.

The use of recycled aggregates and supplementary cementitious materials provides an example of how material sustainability can be incorporated into the decision-support process [10]. The framework extends this concept by connecting material information with BIM, procurement, supply-chain conditions, and project requirements.

The sustainability assessment therefore becomes part of construction management rather than a separate environmental evaluation conducted after material decisions have already been made.

4.11 Sustainability and Resource Efficiency

Beyond material selection, the framework supports broader sustainability objectives through monitoring and decision-making. IoT systems can provide information concerning energy use, equipment operation, environmental conditions, and resource consumption. BIM and digital twins can provide contextual information concerning the location and function of the monitored assets.

The integration of these data sources can support identification of inefficient resource use and provide information for corrective actions. For example, equipment operating without productive activity can be identified through equipment-monitoring data, while material information can be used to identify opportunities for waste reduction.

The framework also creates a relationship between quality and sustainability. Defects and rework require additional material, labor, energy, and transportation. Consequently, improved quality management can indirectly contribute to sustainability by reducing unnecessary resource consumption.

Similarly, supply-chain resilience can contribute to sustainability by supporting better planning and reducing emergency procurement, unnecessary transportation, and inefficient material substitution.

4.12 Integrated Security–Quality–Sustainability Performance

One of the principal findings of the framework evaluation is that cybersecurity, quality, and sustainability should not be considered independent dimensions.

A security failure can affect quality if unauthorized information is introduced into an inspection or BIM system. Similarly, compromised procurement information can affect material selection and supply-chain decisions. A failure in material traceability can also affect sustainability reporting.

Conversely, improved quality management can support sustainability by reducing rework and material waste. Secure digital records can improve accountability for sustainability-related decisions, while trusted supply-chain information can strengthen the reliability of environmental and material data.

The proposed framework therefore establishes a chain of relationships:

Secure identity → Trusted data → Reliable inspection and monitoring → Improved quality decisions → Better resource and sustainability decisions

This integrated relationship represents a major distinction between the proposed framework and isolated technology implementations.

4.13 Comparative Discussion

The baseline and integrated configurations differ primarily in the degree of integration among digital construction and management functions.

In the baseline configuration, BIM, IoT, inspection, procurement, and security activities may operate independently. This arrangement can result in duplicated information, limited traceability, fragmented access control, and delayed decision-making.

In the integrated configuration, the same information can be shared across appropriately authorized components. Sensor observations can update digital representations, inspection observations can be linked to BIM elements, security events can influence access decisions, blockchain can support selected records, and procurement information can be incorporated into sustainability assessments.

The principal improvement therefore results from information integration and controlled information sharing. The framework does not assume that every technology is required for every construction activity. Instead, technologies are applied where they provide a specific functional benefit.

This is important because excessive technological complexity can increase implementation cost and create additional cybersecurity and interoperability requirements. The proposed framework therefore supports selective deployment according to project requirements.

4.14 Discussion of Research Objectives

The results support the first objective by establishing an architecture connecting IoT, BIM, digital twins, and digital inspection within a unified construction-management environment.

The second objective is addressed through privacy-preserving authentication for both human users and connected devices. The approach establishes identity while limiting unnecessary exposure of sensitive information.

The third objective is addressed through the integration of zero-trust principles. Access decisions are based on explicit verification rather than implicit network-based trust.

The fourth objective is addressed through cybersecurity monitoring, authentication, authorization, secure communication, and cloud-security considerations.

The fifth objective is addressed through selective use of blockchain for data integrity, traceability, provenance, and accountability.

The sixth objective is addressed through sustainable material selection and supply-chain resilience mechanisms that incorporate technical, economic, environmental, and supply-related information.

The seventh objective is addressed through the multidimensional performance indicators covering cybersecurity, quality, operational efficiency, supply-chain resilience, and sustainability.

Collectively, these findings indicate that the proposed framework provides a coherent architecture through which the identified research gaps can be addressed.

4.15 Practical Implications

The proposed framework has several practical implications for construction organizations. First, cybersecurity should be incorporated during the design of digital construction systems rather than added after system deployment. Identity management, authorization, device verification, and security monitoring should form part of the initial architecture.

Second, BIM and IoT should be integrated with quality-management processes rather than being used solely for visualization or monitoring. Linking inspection records with BIM elements can improve traceability and facilitate corrective-action management.

Third, blockchain should be deployed selectively for events where provenance and accountability provide meaningful value. A complete blockchain-based construction information system may not be necessary and could introduce additional complexity.

Fourth, sustainability should be incorporated into material and procurement decisions at the project-management level. Material performance, environmental impact, cost, availability, and supply-chain risk can be evaluated together.

Finally, construction organizations should adopt a risk-based approach to digital transformation. Not every project requires the same level of sensing, authentication, blockchain integration, or cybersecurity monitoring. The architecture can therefore be scaled according to project complexity, criticality, data sensitivity, and sustainability requirements.

4.16 Limitations of the Evaluation

The evaluation has several limitations. First, the framework is primarily an integrated architectural and methodological model, and its performance depends on the quality of the underlying implementation and data.

Second, the evaluation scenarios represent selected construction and cybersecurity conditions. Real construction environments may involve additional uncertainties, including communication failures, sensor degradation, incomplete data, organizational resistance, and unexpected cyber threats.

Third, the sustainability assessment depends on the availability and reliability of material, environmental, supplier, and procurement information. Incomplete or inconsistent data may influence the resulting sustainability scores.

Fourth, blockchain-based provenance does not guarantee the accuracy of information entered into the ledger. The framework therefore requires secure data acquisition and appropriate validation mechanisms.

Finally, the weighting of performance indicators may influence the overall framework score. Different construction projects may assign different priorities to cybersecurity, quality, cost, resilience, and sustainability.

These limitations indicate that future empirical implementation should evaluate the framework using real construction datasets, larger-scale IoT deployments, realistic cyber-threat scenarios, and project-specific sustainability information.

4.17 Overall Discussion

The evaluation demonstrates the potential value of treating digital construction as an integrated cyber-physical and sustainability-oriented system. The principal contribution is the establishment of relationships among technologies that are frequently studied independently.

The integration of BIM, IoT, and digital twins provides the digital foundation for monitoring and representing construction activities. Privacy-preserving authentication and zero-trust mechanisms provide security and controlled access. Cybersecurity monitoring supports continuous identification of abnormal behavior, while blockchain provides selected provenance and accountability capabilities.

At the operational level, digital inspection and quality management connect construction observations with project components and corrective actions. At the strategic level, sustainable material selection and supply-chain resilience connect project information with environmental and resource-management objectives.

The resulting framework therefore provides a structured basis for balancing digital connectivity with security, quality, resilience, and sustainability. Rather than assuming that digitalization alone improves construction performance, the findings indicate that the value of digital transformation depends on how effectively information, security, and decision-making processes are integrated.

5. Conclusion

This study developed an integrated cybersecure and sustainable digital framework for smart construction by combining IoT, BIM, digital twins, privacy-preserving authentication, zero-trust access control, blockchain-based data provenance, digital inspection, quality management, sustainable material selection, and supply-chain resilience. The framework addresses the fragmented nature of existing Construction 4.0 approaches by bringing digitalization, cybersecurity, quality, and sustainability into a common decision-support environment.

The proposed framework establishes a continuous connection between physical construction activities and digital project management. IoT devices provide real-time information from construction sites, while BIM and digital twins organize and contextualize these data. Privacy-preserving authentication and zero-trust mechanisms provide controlled access to digital resources and help protect users, devices, and project information. Blockchain is incorporated selectively to improve traceability, provenance, and accountability for important project records.

The framework also connects digital inspection with BIM, IoT, and digital-twin information to support more systematic quality management. Inspection observations can be associated with specific construction components, responsible users, evidence, and corrective actions. In parallel, sustainable material selection and supply-chain management enable technical, environmental, economic, and supply-related factors to be considered during construction decision-making.

Overall, the study demonstrates that the value of Construction 4.0 does not depend only on the adoption of individual digital technologies. Greater benefits can be achieved when digital technologies are integrated with cybersecurity, trusted information management, quality control, and sustainability objectives. The proposed framework therefore provides a structured foundation for developing construction environments that are more secure, connected, resilient, and sustainable.

Future research should validate the proposed framework through implementation in real construction projects using actual BIM models, IoT data, inspection records, procurement information, and cybersecurity events. Such empirical validation would provide stronger evidence regarding the practical performance, scalability, and reliability of the framework.

References

[1] Akil, M., Mancini, L. V., & Venturi, D. (2019). Multi-covert channel attack in the cloud. Proceedings of the 6th International Conference on Software Defined Systems (SDS 2019), 160–165. IEEE. https://doi.org/10.1109/SDS.2019.8768563

[2] Akil, M., Martucci, L. A., & Hoepman, J.-H. (2023). Non-interactive privacy-preserving Sybil-free authentication scheme in VANETs. In Inaugural International Symposium on Vehicle Security and Privacy (VehicleSec 2023). Internet Society. https://doi.org/10.14722/vehiclesec.2023.23007

[3] Akil, M., Martucci, L. A., & Hoepman, J.-H. (2024). A secure and privacy-preserving authentication scheme with a zero-trust approach to vehicle renting in VANETs. Proceedings of the 21st International Conference on Security and Cryptography (SECRYPT 2024), 114–127. SCITEPRESS. https://doi.org/10.5220/0012759600003767

[4] Akil, M., Naskar, S., Martucci, L. A., & Hoepman, J.-H. (2023). A privacy-preserving approach to vehicle renting and driver accountability in VANETs. In Privacy and Identity Management: Sharing in a Digital World, 192–210. Springer. https://doi.org/10.1007/978-3-031-57978-3_13

[5] Das, M., Tao, X., & Cheng, J. C. P. (2021). BIM security: A critical review and recommendations using encryption strategy and blockchain. Automation in Construction, 126, 103682. https://doi.org/10.1016/j.autcon.2021.103682

[6] Elghaish, F., Hosseini, M. R., Matarneh, S., Talebi, S., Wu, S., Martek, I., Poshdar, M., & Ghodrati, N. (2021). Blockchain and the Internet of Things for the construction industry: Research trends and opportunities. Automation in Construction, 132, 103942. https://doi.org/10.1016/j.autcon.2021.103942

[7] Hijazi, A. A., Alashwal, A., Shishehgarkhaneh, M. B., & Calheiros, R. N. (2026). Blockchain–BIM integration in construction: A systematic literature review of workflows, mechanisms, and platforms. Journal of Building Engineering, 120, 115388. https://doi.org/10.1016/j.jobe.2026.115388

[8] Mahpour, A. (2026). BIM-IoT-Blockchain integration in the construction industry: Critical review (2017–2025). Automation in Construction, 191, 107163. https://doi.org/10.1016/j.autcon.2026.107163

[9] Oliveira, J. de, Schreiber, D., & Jahno, V. D. (2026). Sustainability in civil construction through Industry 4.0 and BIM technologies.

[10] Parikh, P. B. (2026). Implementing digital inspection protocols for enhanced quality control management in high-rise construction. Power System Protection and Control, 54(3), 147–163. https://doi.org/10.46121/pspc.54.3.12

[11] Parikh, P. B. (2026). Evaluating the feasibility and efficiency of 3D-printed concrete technology in sustainable modular construction. Power System Protection and Control, 54(1), 887–900. https://doi.org/10.46121/pspc.54.1.61

[12] Parikh, P. B. (2025). Optimizing the structural and durability performance of concrete using recycled aggregates and supplementary cementitious materials. Power System Protection and Control, 53(4), 564–576. https://doi.org/10.46121/pspc.53.4.39

[13] Parikh, P. B. (2025). Frameworks for mitigating supply chain disruptions and material price volatility in sustainable building construction. Power System Protection and Control, 53(2), 410–426. https://doi.org/10.46121/pspc.53.2.34

[14] Digital twin-enabled synchronized construction management: A roadmap from Construction 4.0 towards future prospect. (2024). Developments in the Built Environment, 19, 100512. https://doi.org/10.1016/j.dibe.2024.100512

[15] Construction digital twin: A taxonomy and analysis of the application-technology-data triad. (2024). Automation in Construction.

[16] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. NIST Special Publication 800-207. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207