



Blockchain-Based Secure Data Routing Framework for U.S. Industrial Communication Networks

Md Shahid Nazir¹;

[1]. Master of Science in Business Analytics;
Email: nazir.dwasa@gmail.com

Doi: [10.63125/9exrgs41](https://doi.org/10.63125/9exrgs41)

Received: 21 September 2025; **Revised:** 25 October 2025; **Accepted:** 27 November 2025; **Published:** 28 December 2025.

Abstract

This study addresses the growing cybersecurity problem associated with secure data routing in increasingly interconnected U.S. industrial communication networks, where centralized authentication, route manipulation, unauthorized node participation, data tampering, and limited routing traceability can threaten the reliability and security of Industrial Control Systems, SCADA, Operational Technology, and Industrial Internet of Things environments. The purpose of the research was to develop and empirically evaluate a blockchain-based secure data routing framework that integrates decentralized authentication, data integrity, routing traceability, and decentralized trust and consensus to strengthen industrial communication security. A quantitative, cross-sectional, case-study-based design was adopted, focusing on enterprise and industrial cases across U.S. manufacturing, energy and utilities, oil and gas, process industries, transportation, and related infrastructure environments. The study analyzed 312 valid responses from industrial and network engineers, cybersecurity and OT security specialists, ICS/SCADA engineers, automation and IIoT engineers, and technical managers, representing an 89.1% usable response rate. The key variables were Blockchain-Based Decentralized Authentication, Blockchain-Enabled Data Integrity, Blockchain-Based Routing Traceability, Decentralized Trust and Consensus, and Secure Industrial Data Routing. Data were analyzed using descriptive statistics, Cronbach's alpha reliability testing, Pearson correlation, ANOVA, and multiple regression modeling. Findings showed strong respondent agreement for decentralized authentication ($M = 4.08$), data integrity ($M = 4.15$), routing traceability ($M = 4.03$), decentralized trust and consensus ($M = 4.11$), and secure industrial data routing ($M = 4.18$). Data integrity demonstrated the strongest correlation with secure routing ($r = .72$, $p < .001$), followed by decentralized trust ($r = .70$), authentication ($r = .68$), and routing traceability ($r = .61$). The regression model explained 68.0% of SIDR variance, $R^2 = .680$, $F(4,307) = 163.10$, $p < .001$, with data integrity emerging as the strongest predictor ($\beta = .29$), followed by decentralized trust ($\beta = .26$), authentication ($\beta = .24$), and traceability ($\beta = .21$). The findings imply that U.S. industrial organizations can strengthen routing security by integrating blockchain as a verification, integrity, accountability, and distributed-trust layer aligned with Zero Trust principles.

KEYWORDS

Blockchain Security; Secure Data Routing; Industrial Communication Networks; Zero Trust Security; Industrial IoT.

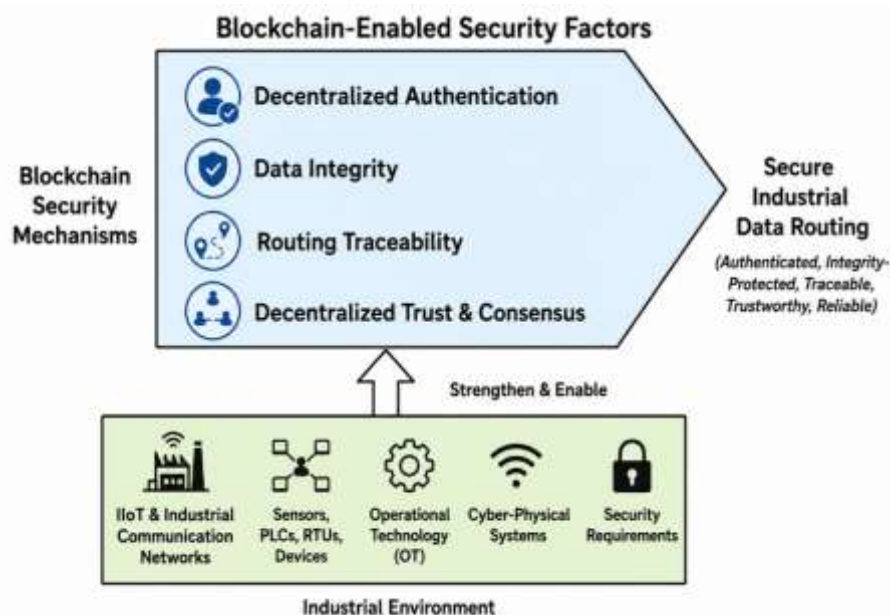
INTRODUCTION

Industrial communication networks can be defined as interconnected digital communication infrastructures that enable sensors, programmable logic controllers (PLCs), remote terminal units (RTUs), supervisory systems, industrial computers, actuators, gateways, and other operational devices to exchange control, monitoring, diagnostic, and production data within industrial environments. Unlike conventional enterprise information networks, industrial communication networks are closely connected to physical processes, meaning that the timeliness, authenticity, integrity, availability, and reliability of transmitted information are directly associated with operational continuity and process control. Industrial communication security therefore requires mechanisms that extend beyond conventional confidentiality-oriented information protection because industrial systems depend heavily on authentication, authorization, availability, dependable communication, and protection against interference with physical operations (Dzung et al., 2005). Industrial control networks are also specialized communication environments that connect field-level equipment, control devices, supervisory platforms, and enterprise systems through architectures that combine operational technology with information technology (Galloway & Hancke, 2013). Within this environment, the Industrial Internet of Things (IIoT) extends conventional industrial networking by connecting intelligent sensors, machines, embedded systems, cyber-physical components, and computing resources through interoperable communication technologies (Xu et al., 2014). Industrial communication has consequently become a core technological foundation of increasingly interconnected automation systems in which traditional hierarchical architectures coexist with distributed, Internet-enabled, and service-oriented communication models (Wollschlaeger et al., 2017). In the context of the present study, secure data routing refers to the authenticated, integrity-protected, trustworthy, traceable, and reliable selection and forwarding of industrial data through authorized network nodes and communication paths from source to destination. Routing therefore involves more than determining whether a destination is reachable because secure routing must also ensure that participating nodes are legitimate, routing information has not been altered, transmitted data retain their original integrity, and forwarding activities can be verified when security events occur. Blockchain can support these requirements through distributed record keeping, cryptographically linked transactions, decentralized validation, and programmable security controls such as smart contracts (Christidis & Devetsikiotis, 2016). Its characteristics are particularly relevant to distributed IoT and IIoT environments where large numbers of devices must establish trust and coordinate secure exchanges without depending exclusively on a single centralized authority (Wang et al., 2020). Internationally, industrial communication networks support manufacturing, energy systems, transportation, utilities, process industries, logistics, and other technology-intensive sectors, making secure machine-to-machine communication an international industrial-security concern. The increasing convergence of cyber-physical processes, globally interconnected industrial systems, heterogeneous devices, and distributed communication infrastructures has consequently made secure routing a fundamental component of industrial cybersecurity.

The security importance of industrial data routing has intensified as industrial networks have evolved from relatively isolated proprietary architectures toward interconnected infrastructures that rely on standardized communication protocols, Internet technologies, wireless communication, remote services, cloud environments, and IIoT devices. SCADA environments historically contained weaknesses associated with increased connectivity, legacy technologies, limited authentication, and the incorporation of general-purpose networking mechanisms into systems that were originally designed for reliability and operational control rather than adversarial cybersecurity conditions (Ilgure et al., 2006). These characteristics create distinctive security challenges because industrial systems often operate under strict availability requirements, long equipment lifecycles, real-time constraints, and limited tolerance for downtime. Vulnerability assessment research has demonstrated that attacks affecting SCADA communication infrastructures can directly influence the reliability and security of power-system operations, thereby linking cyber vulnerabilities with physical operational consequences (Ten et al., 2008). Broader investigations of SCADA cybersecurity have also emphasized the strategic importance of industrial control infrastructures that support essential national and industrial functions,

particularly where network compromise can disrupt physical operations or create cascading operational consequences (Nicholson et al., 2012). Industrial-network security research has further identified vulnerabilities arising from communication architectures, protocol weaknesses, device limitations, remote access, interconnection, and increasingly complex network structures (Cheminod et al., 2013). These concerns are internationally significant because industrial organizations across different countries commonly depend on similar categories of programmable controllers, supervisory systems, sensors, gateways, embedded devices, and interoperable communication protocols. Cyber-physical systems amplify these concerns because they integrate computing, communication, sensing, control, and physical processes, creating attack surfaces that extend across digital and physical layers simultaneously (Humayed et al., 2017). The broader IoT security literature also shows that confidentiality, authentication, privacy, authorization, availability, and trust become more difficult to maintain when heterogeneous devices communicate autonomously across interconnected infrastructures (Sicari et al., 2015). Blockchain research has therefore increasingly examined whether decentralized security mechanisms can address authentication, data protection, trust management, and other IoT security requirements (Khan & Salah, 2018). For industrial communication networks, these issues are especially important because routing information determines how commands, alarms, process measurements, telemetry, and control messages move across the operational infrastructure. Compromise of routing information, forwarding nodes, device identities, or communication paths can therefore affect both cybersecurity and physical process reliability, making secure routing an integral component of industrial network protection.

Figure 1: Framework of Blockchain-Enabled Security Factors for Secure Industrial Data Routing



Secure data routing becomes increasingly complex when industrial devices communicate across distributed, heterogeneous, and partially decentralized infrastructures. Conventional security architectures often depend on centralized authentication servers, centralized policy engines, certificate authorities, network gateways, or designated trust-management platforms to determine whether a device is authorized to participate in communication. Although these mechanisms remain important within industrial cybersecurity architectures, excessive reliance on centralized trust can create concentration points in which compromise or failure of a trusted component affects numerous downstream devices and communication relationships. IoT and IIoT security research has documented a broad range of attack classes involving device compromise, unauthorized access, identity spoofing, routing manipulation, communication interception, data modification, and trust-management

weaknesses, demonstrating that industrial-network security is composed of multiple interdependent protection requirements (Sengupta et al., 2020). Routing is particularly sensitive to such risks because a device may possess valid credentials while still behaving maliciously, advertising false routes, manipulating forwarding decisions, selectively dropping packets, or attempting to influence other nodes through falsified trust information. Blockchain-supported routing research provides a more direct technical basis for addressing these problems. Trusted routing approaches that combine blockchain with intelligent routing mechanisms have demonstrated that distributed ledgers can be used to preserve trustworthy routing information and strengthen the selection of credible routing nodes within wireless sensor environments (Yang et al., 2019). Secure routing architectures have also incorporated blockchain as a shared and tamper-resistant information layer through which network nodes coordinate path selection and maintain validated communication information (Lazrag et al., 2021). More integrated models have combined blockchain-based authentication, trust evaluation, cryptographic protection, node-identity management, and secure routing to reduce malicious participation and improve forwarding decisions in distributed sensor networks (Awan et al., 2022). These studies are relevant to industrial communication networks because modern industrial infrastructures increasingly integrate sensors, edge nodes, IIoT devices, gateways, wireless links, and distributed controllers that share characteristics with resource-constrained and multi-hop network environments. Secure industrial routing can therefore be conceptualized through several interconnected dimensions. Decentralized authentication addresses whether a participating node possesses a legitimate and verifiable identity; data integrity addresses whether transmitted or recorded information remains authentic and unaltered; routing traceability addresses whether route changes and forwarding activities can be reconstructed and audited; and decentralized trust addresses whether routing decisions can be validated through distributed mechanisms rather than unconditional reliance on a single authority. These dimensions collectively establish a stronger basis for secure industrial communication than approaches that treat route optimization, authentication, and trust as separate network functions.

Blockchain technology provides a technical architecture through which authentication, integrity, traceability, and distributed trust can be integrated into a common industrial communication-security model. Blockchain-based systems use cryptographically linked records, distributed validation, decentralized transaction management, and programmable control mechanisms to create verifiable interactions among network participants (Christidis & Devetsikiotis, 2016). Within industrial data routing, blockchain records can be used to represent device identities, authentication events, routing information, trust scores, access permissions, route modifications, policy decisions, or other security-relevant transactions. These records can create tamper-evident histories that make unauthorized changes easier to detect and investigate. Decentralized access-management architectures have shown that blockchain can provide scalable management of IoT access-control information while reducing dependence on a single centralized authorization mechanism (Novo, 2018). This approach is directly relevant to blockchain-based decentralized authentication because industrial communication requires participating nodes to establish verifiable identities before accessing network resources or contributing to routing decisions. Decentralized blockchain-based authentication systems have likewise demonstrated the feasibility of establishing trust relationships among IoT devices without relying entirely on centralized identity-management infrastructures (Hammi et al., 2018). Blockchain-enabled data integrity represents another major dimension because cryptographic hashes, digital signatures, chained records, and distributed validation provide mechanisms for detecting unauthorized modification of stored or transmitted information. Blockchain-IoT integration research has identified immutability, traceability, decentralization, and verifiable transaction histories as important characteristics for securing communication and data exchange among connected devices (Reyna et al., 2018). Related literature has also demonstrated the relevance of blockchain to device identity, trusted information exchange, data management, and distributed security within IoT environments (Fernández-Caramés & Fraga-Lamas, 2018). Blockchain-based routing traceability extends these properties to communication paths and forwarding events by allowing network participants to preserve records describing route changes, validated nodes, authorization events, and security-relevant routing actions. Systematic research on blockchain and IoT integration indicates that

distributed ledgers are frequently employed to improve transparency, verifiability, and distributed control across interconnected device ecosystems (Panarello et al., 2018). Decentralized trust and consensus further strengthen this model by enabling authorized participants to validate information collectively rather than relying on a single trusted controller. The effectiveness of these mechanisms depends on how consensus, identity, communication, storage, and computation are integrated within the network architecture, particularly in resource-constrained environments (Ferrag et al., 2019).

Research focused more directly on industrial IoT environments provides further support for examining decentralized authentication, data integrity, routing traceability, and decentralized trust as determinants of secure industrial data routing. Reviews of blockchain technologies for IoT and IIoT have identified decentralized security, privacy protection, trusted data exchange, identity management, and distributed validation as recurring components of blockchain-enabled industrial architectures (Wang et al., 2020). Secure IIoT architectures have also demonstrated that distributed-ledger technologies can regulate access to industrial information, preserve trustworthy records, and support secure interaction between sensors, actuators, gateways, and industrial systems (Latif et al., 2021). Broader syntheses of blockchain-enabled IoT and IIoT research have similarly identified distributed security, smart contracts, data management, identity verification, and inter-device coordination as major research themes in industrial applications (Dwivedi et al., 2021). Systematic evaluations of blockchain applications for IoT have also emphasized trust management, authentication, decentralized configuration, secure information exchange, and distributed transaction validation as central concerns in connected-device environments (Qureshi et al., 2022). More targeted industrial studies provide evidence regarding how these mechanisms can be integrated into specific IIoT security architectures. Blockchain-based industrial security models have incorporated trust assessment for malicious-device identification while using distributed ledgers to provide transparent and verifiable network-security information (Rathee et al., 2023). Secure authentication and privacy-preserving blockchain models for IIoT have also integrated authentication, cryptographic protection, node selection, and communication security, demonstrating the close relationship between device identity and trusted industrial data exchange (Gupta et al., 2023). Lightweight blockchain models have further combined reputation-based trust, consensus, privacy preservation, and attack detection to improve IIoT security while reducing computational demands (Selvarajan et al., 2023). Private blockchain architectures for industrial IoT applications have similarly emphasized device authenticity, secure transmission, data integrity, trusted participation, and decentralized information management in environments such as smart electric grids (Umran et al., 2023). In addition, secure routing research has shown that blockchain records, node authentication, trust evaluation, and routing decisions can be incorporated within a single distributed-network model (Awan et al., 2022). Collectively, these studies provide a coherent basis for operationalizing four blockchain-oriented security constructs within the present research: blockchain-based decentralized authentication, blockchain-enabled data integrity, blockchain-based routing traceability, and blockchain-enabled decentralized trust and consensus. These dimensions address complementary aspects of industrial routing security by determining who can participate, whether communication data remain authentic, whether routing activities remain auditable, and how distributed participants establish confidence in routing behavior.

The international significance of secure industrial data routing is closely connected to the widespread dependence of modern economies on digitally controlled manufacturing, energy, transportation, water, logistics, process industries, and other infrastructure-intensive sectors. Industrial communication systems increasingly operate as interconnected cyber-physical ecosystems in which automation equipment, sensors, industrial controllers, gateways, edge-computing devices, and enterprise applications exchange operational information continuously. Industrial IoT technologies have expanded the range of connected devices and have enabled remote monitoring, intelligent control, condition assessment, machine coordination, and data-driven industrial operations across geographically distributed settings (Xu et al., 2014). Industrial communication research has also demonstrated that automation networks increasingly integrate traditional field-level communication with Ethernet-based networking, Internet-oriented technologies, distributed computing, and Industry 4.0 architectures (Wollschlaeger et al., 2017). These changes create shared cybersecurity challenges because industrial organizations in different countries often depend on comparable categories of

controllers, sensors, supervisory systems, communication standards, and industrial protocols. Industrial control networks are inherently complex because their operation depends on the interaction of multiple control layers, communication technologies, network protocols, physical devices, and management systems (Galloway & Hancke, 2013). Cyber-physical security research has further demonstrated that vulnerabilities affecting digital communication can extend into physical control, sensing, actuation, and operational processes, which increases the importance of maintaining trusted and verifiable network communication (Humayed et al., 2017). The United States provides a particularly relevant empirical context for studying these issues because industrial organizations across manufacturing, utilities, energy, transportation, and other sectors depend extensively on OT, ICS, SCADA, IIoT, industrial Ethernet, wireless sensing, remote communication, and automated control technologies. Within this context, blockchain is relevant not as a cryptocurrency mechanism but as a permission-controlled distributed security layer that can support identity verification, integrity validation, route auditing, distributed trust, and secure communication among authorized industrial entities. Similar architectural needs have been identified across multiple industrial and geographical settings, including secure blockchain-supported IIoT operations, distributed industrial data protection, and blockchain-enabled smart-grid communication (Latif et al., 2021; Umran et al., 2023; Wang et al., 2020). The recurrence of authentication, trust, secure data exchange, decentralized validation, and communication integrity across international research demonstrates that secure industrial routing is not confined to a single country or industrial sector. The U.S. case-study setting can therefore be positioned within a broader international industrial cybersecurity context while allowing the research to focus on professional assessments of blockchain-enabled routing security in a clearly bounded national industrial environment.

A synthesis of the existing literature identifies a specific research space at the intersection of blockchain security, industrial communication, and secure data routing. Earlier research on industrial cybersecurity concentrated primarily on protecting SCADA systems, identifying communication vulnerabilities, assessing cyber-physical risks, and examining industrial-network security architectures (Dzung et al., 2005; Igure et al., 2006; Ten et al., 2008). As industrial networking became increasingly connected through IoT and IIoT technologies, research attention expanded toward device identity, distributed trust, data protection, access control, and decentralized communication security (Sengupta et al., 2020; Sicari et al., 2015; Wang et al., 2020). Blockchain studies have separately demonstrated decentralized access control and authentication (Hammi et al., 2018; Novo, 2018), distributed integrity and verifiable IoT transactions (Fernández-Caramés & Fraga-Lamas, 2018; Ferrag et al., 2019), secure IIoT architectures (Dwivedi et al., 2021; Latif et al., 2021), and blockchain-supported routing and trust management (Lazrag et al., 2021; Yang et al., 2019). More recent industrial research has examined secure authentication, malicious-device identification, lightweight blockchain security, trusted IIoT operations, and secure industrial data transmission (Gupta et al., 2023; Rathee et al., 2023; Selvarajan et al., 2023; Umran et al., 2023). Routing-focused research has also demonstrated that node authentication, trust evaluation, distributed ledger records, and forwarding security can be integrated into a common blockchain-based communication model (Awan et al., 2022). Across these streams, much of the existing evidence has been generated through technical architectures, protocol designs, simulations, experimental models, conceptual frameworks, and systematic reviews. Comparatively less attention has been directed toward a quantitatively measurable model that simultaneously evaluates blockchain-based decentralized authentication, blockchain-enabled data integrity, blockchain-based routing traceability, and blockchain-enabled decentralized trust and consensus as predictors of secure industrial data routing within U.S. industrial communication networks. Examining these constructs together provides an opportunity to determine whether each mechanism is statistically associated with secure routing and whether their combined effect provides stronger explanatory power than any single security dimension considered independently. The present study therefore positions secure industrial data routing as the dependent construct and the four blockchain-enabled security dimensions as explanatory constructs. A quantitative, cross-sectional, case-study-based design using a five-point Likert scale allows professional perceptions of these mechanisms to be translated into measurable variables. Descriptive statistics can characterize the distribution and central tendencies of the constructs, Pearson correlation analysis can assess the strength and direction of relationships among

them, and multiple regression modeling can estimate the individual and collective effects of blockchain-based security mechanisms on secure industrial data routing. This structure establishes direct alignment between the research problem, conceptual variables, hypotheses, data-collection instrument, and statistical analysis.

Background of the Study

Industrial communication networks have become a fundamental component of modern production, energy, utility, transportation, manufacturing, and other critical infrastructure environments because they connect physical equipment, control systems, sensors, computing platforms, and supervisory technologies through continuous digital communication. These networks increasingly integrate Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Operational Technology (OT), Industrial Internet of Things (IIoT) devices, programmable logic controllers, remote terminal units, edge devices, industrial gateways, and enterprise information systems. As industrial organizations become more connected, the volume, speed, and operational importance of data exchanged across these infrastructures have expanded considerably. Secure data routing has therefore become essential because industrial messages frequently contain commands, measurements, alerts, control instructions, operational status information, and other data whose manipulation may disrupt industrial processes. Conventional industrial network architectures often rely on centralized authentication, centralized policy enforcement, and centralized trust-management mechanisms. Such structures can create security weaknesses when a central authority, gateway, controller, or trust-management node is compromised or becomes unavailable. Blockchain technology offers a different approach by creating a distributed and cryptographically protected environment in which participating nodes can verify transactions, identities, routing information, and security events through shared records rather than relying exclusively on a single centralized authority. Within industrial communication networks, blockchain can potentially support decentralized authentication, data-integrity verification, immutable routing records, distributed trust, secure node participation, and transparent auditing of communication activities. These capabilities are particularly relevant to U.S. industrial organizations that operate highly interconnected and technologically heterogeneous infrastructures where cyber incidents may have operational, financial, safety, and infrastructure consequences. A blockchain-based secure data routing framework could provide an additional security layer in which network nodes are authenticated before participation, routing-related data are protected against unauthorized alteration, forwarding activities remain traceable, and trust relationships are established through distributed consensus. The study therefore focuses on examining how blockchain-based decentralized authentication, blockchain-enabled data integrity, blockchain-based routing traceability, and decentralized trust and consensus contribute to secure industrial data routing. By empirically examining these dimensions within a U.S. industrial context, the research establishes a structured foundation for understanding whether blockchain-based routing security can strengthen the reliability, accountability, integrity, and trustworthiness of industrial communication networks.

Problem Statement

The growing connectivity of industrial communication networks has increased both their operational capabilities and their exposure to cybersecurity threats. Industrial organizations now depend on interconnected devices, remote access technologies, digital control platforms, cloud-linked systems, industrial wireless communication, and IIoT environments to perform functions that were previously handled through more isolated network architectures. This expanded connectivity creates multiple opportunities for unauthorized access, identity spoofing, malicious node participation, route manipulation, interception of industrial traffic, unauthorized modification of data, replay attacks, false routing information, and other forms of cyber interference. A significant problem is that many industrial communication environments continue to rely on centralized authentication, centralized access control, and trusted intermediary systems to validate devices and coordinate communication. If these centralized components are compromised, disrupted, or manipulated, multiple connected systems may be affected simultaneously. Furthermore, conventional routing mechanisms may lack sufficiently transparent and tamper-resistant methods for recording route changes, node participation, and communication histories. This makes it difficult to establish whether routing information has been

modified, whether a compromised node has participated in forwarding activities, or whether network behavior can be reconstructed reliably after a cybersecurity incident. Blockchain technology provides mechanisms that could address several of these challenges through distributed authentication, cryptographic validation, immutable record keeping, decentralized consensus, and transparent auditability. However, an important empirical problem remains because existing research has frequently examined blockchain security mechanisms separately, focused on conceptual architectures, developed simulation-based protocols, or evaluated blockchain within generalized IoT environments. Comparatively limited quantitative research has examined how several blockchain-enabled security mechanisms collectively influence secure data routing within U.S. industrial communication networks. There is therefore insufficient empirical evidence showing whether decentralized authentication, blockchain-enabled data integrity, routing traceability, and decentralized trust and consensus significantly improve the perceived security of industrial data routing when evaluated within a common statistical model. Without such evidence, organizations may understand the technical potential of blockchain but remain uncertain about which security dimensions contribute most strongly to routing security and how they should be integrated within industrial communication architectures. This research addresses that problem by quantitatively examining the individual and combined effects of four blockchain-based security dimensions on secure industrial data routing in U.S. industrial communication environments.

Purpose/Objectives of the Study

The principal objective of this study is to develop and empirically evaluate a blockchain-based secure data routing framework for U.S. industrial communication networks by determining how blockchain-enabled security mechanisms influence the protection, reliability, traceability, and trustworthiness of industrial data transmission. More specifically, the study seeks to examine the contribution of blockchain-based decentralized authentication to secure routing by evaluating whether distributed identity verification can strengthen the ability of industrial networks to distinguish legitimate communication nodes from unauthorized or potentially malicious participants. A second objective is to assess blockchain-enabled data integrity as a mechanism for protecting routing-related information and industrial data against unauthorized alteration, thereby establishing whether greater confidence in the authenticity and consistency of network information contributes to stronger routing security. The study also aims to evaluate the role of blockchain-based routing traceability by determining whether immutable and auditable records of network forwarding activities can improve accountability, route verification, and the identification of abnormal or unauthorized communication behavior. Another objective is to investigate blockchain-enabled decentralized trust and consensus in order to determine whether distributed validation among authorized participants can improve confidence in routing decisions and reduce excessive dependence on centralized trust authorities. In addition to examining these variables individually, the study aims to determine their collective predictive effect on secure industrial data routing through multiple regression modeling. This objective is important because industrial communication security is unlikely to depend on a single mechanism; rather, authentication, integrity, traceability, and trust operate as interconnected dimensions of secure network behavior. The study therefore seeks to establish which blockchain-based security mechanism has the strongest statistical influence on secure routing and how much of the variation in secure industrial data routing can be explained by the combined model. A final objective is to use the empirical findings to construct a structured blockchain-based secure data routing framework that aligns decentralized authentication, data-integrity protection, route traceability, distributed consensus, and secure forwarding principles within U.S. industrial communication environments. Through these objectives, the study connects measurable cybersecurity variables with a framework that can be evaluated through descriptive statistics, correlation analysis, reliability testing, and multiple regression analysis.

Research Hypotheses

The research hypotheses are designed to statistically test the proposed relationships between the major blockchain-based security mechanisms and secure industrial data routing. The first hypothesis, H1, proposes that blockchain-based decentralized authentication has a statistically significant positive effect on secure industrial data routing. This hypothesis reflects the expectation that stronger

distributed identity verification and authentication of industrial communication nodes will improve confidence that routing activities are performed only by legitimate and authorized devices. The second hypothesis, H2, proposes that blockchain-enabled data integrity has a statistically significant positive effect on secure industrial data routing. This relationship assumes that when routing information, security records, and industrial communication data are protected through cryptographic verification and tamper-evident mechanisms, the overall security of data forwarding improves. The third hypothesis, H3, proposes that blockchain-based routing traceability has a statistically significant positive effect on secure industrial data routing. This hypothesis is based on the expectation that auditable and immutable routing records increase accountability, enable reconstruction of communication activities, and make unauthorized routing behavior easier to identify. The fourth hypothesis, H4, proposes that blockchain-enabled decentralized trust and consensus mechanisms have a statistically significant positive effect on secure industrial data routing. This relationship reflects the assumption that distributed validation can reduce reliance on a single trusted authority while increasing confidence that routing decisions and network participants have been verified collectively. The fifth hypothesis, H5, proposes that blockchain-based decentralized authentication, blockchain-enabled data integrity, blockchain-based routing traceability, and decentralized trust and consensus collectively have a statistically significant positive effect on secure industrial data routing. This final hypothesis represents the integrated statistical model of the study and recognizes that industrial routing security is shaped by multiple interacting dimensions rather than a single security mechanism. The hypotheses have been evaluated through correlation analysis and multiple regression modeling using responses measured through a five-point Likert scale. Statistical significance has been assessed using an established significance threshold, while standardized regression coefficients have helped identify the relative contribution of each independent variable to secure industrial data routing.

Significance of the Research

- i. Significance for U.S. industrial organizations: The study is significant for industrial organizations because it provides a structured empirical assessment of how blockchain-based security mechanisms may strengthen the protection of communication networks used in manufacturing, energy, utilities, transportation, processing, and other industrial sectors. By identifying the variables that contribute most strongly to secure data routing, organizations can better understand which blockchain functions deserve priority within industrial cybersecurity strategies.
- ii. Significance for industrial cybersecurity professionals: The research provides practical value for cybersecurity engineers, OT security specialists, ICS/SCADA professionals, network administrators, and industrial system architects by examining authentication, integrity, traceability, and decentralized trust within a single routing-security model. This can support more integrated approaches to securing industrial communication paths.
- iii. Significance for blockchain implementation: The research shifts attention from blockchain as a general distributed-ledger technology toward specific industrial-security capabilities. It distinguishes decentralized authentication, data integrity, routing traceability, and consensus as measurable security constructs, which can help organizations evaluate blockchain according to operational cybersecurity functions rather than abstract technological characteristics.
- iv. Significance for secure industrial routing research: The study contributes to the literature by placing secure industrial data routing at the center of the analytical model. This is important because routing is a critical communication function through which industrial commands, measurements, alerts, and control information move between devices and systems.
- v. Significance for theory and empirical research: By statistically examining relationships among clearly defined constructs, the study provides quantitative evidence that can support, challenge, or refine existing theoretical assumptions concerning distributed trust, authentication, verification, and secure industrial communication.
- vi. Significance for decision-makers and policymakers: The findings can assist managers, cybersecurity decision-makers, industrial technology planners, and relevant policy stakeholders in understanding which blockchain-supported security controls are perceived as most relevant to industrial communication protection.
- vii. Methodological significance: The research contributes a measurable framework that connects a five-

point Likert-scale instrument with descriptive statistics, reliability analysis, Pearson correlation, ANOVA, and multiple regression modeling. This creates a reproducible approach that can later be applied to different industrial sectors, network environments, or national contexts.

LITERATURE REVIEW

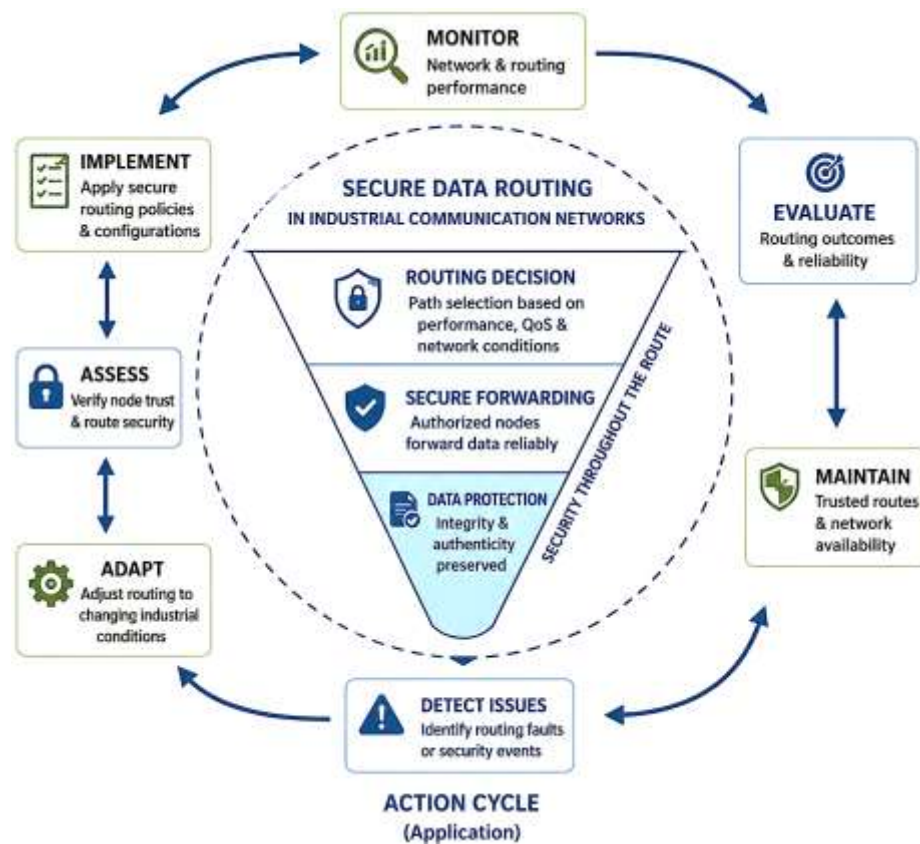
The literature surrounding blockchain-based secure data routing in industrial communication networks lies at the intersection of industrial cybersecurity, distributed-ledger technology, industrial networking, secure routing, trust management, and cyber-physical system protection. Industrial communication networks differ substantially from conventional information-technology networks because their primary purpose is not simply to exchange business information but to support sensing, automation, monitoring, command execution, process control, and real-time interaction with physical equipment. Consequently, weaknesses in industrial communication may influence both digital information and physical operations. The increasing integration of Industrial Control Systems, SCADA, Operational Technology, Industrial Internet of Things devices, industrial wireless networks, edge computing, cloud connectivity, and remote access has expanded the attack surface of industrial infrastructures and created greater demand for security mechanisms capable of protecting device identity, communication integrity, routing behavior, and network trust. Within this context, conventional centralized security mechanisms remain important but may not fully address the security requirements of highly distributed and heterogeneous industrial environments. Blockchain technology has therefore attracted growing scholarly attention because its distributed ledger structure, cryptographic verification, consensus mechanisms, immutable records, and decentralized trust architecture can support security functions that are directly relevant to industrial communication. The literature indicates that blockchain can be used for device authentication, access control, integrity verification, secure information exchange, trust evaluation, auditable transaction recording, and distributed validation. At the same time, secure routing research emphasizes the importance of protecting route information, preventing malicious-node participation, maintaining reliable forwarding paths, and ensuring that network activities remain traceable. These streams of literature provide the basis for examining blockchain-based decentralized authentication, blockchain-enabled data integrity, blockchain-based routing traceability, and decentralized trust and consensus as potential determinants of secure industrial data routing. The review therefore focuses on the technological structure of industrial communication networks, their major routing and cybersecurity vulnerabilities, the security characteristics of blockchain architectures, and the ways in which distributed authentication, integrity protection, traceability, and consensus can be incorporated into industrial routing environments. It also establishes the theoretical and conceptual foundations required to explain the expected relationships among these variables and to position secure industrial data routing as the principal outcome of the proposed research model.

Industrial Communication Networks and Secure Data Routing

Industrial communication networks form the digital backbone of automated production environments by enabling continuous information exchange among sensors, actuators, controllers, supervisory platforms, gateways, and higher-level management systems. Their architecture differs from ordinary enterprise networks because communication is closely tied to physical operations, process timing, equipment coordination, and safety-sensitive control. In wired and wireless industrial settings, network performance is therefore evaluated through requirements such as deterministic delivery, low latency, reliability, availability, synchronization, interoperability, and resistance to communication failures. Industrial wireless sensor networks expanded this architecture by allowing distributed sensing and control devices to communicate without fixed cabling, creating greater flexibility for monitoring, maintenance, equipment placement, and process reconfiguration. At the same time, wireless operation introduces constraints involving interference, limited energy, harsh radio conditions, resource limitations, and dependable message delivery, all of which affect the design of industrial communication protocols and routing mechanisms (Gungor & Hancke, 2009; Abdur & Iftekhhar, 2021). Industrial networking has also evolved through successive technological generations that include fieldbus systems, industrial Ethernet, and wireless industrial networks. These generations have not simply replaced one another; instead, industrial facilities commonly operate heterogeneous

communication environments in which legacy protocols and newer network technologies coexist. The movement from specialized field-level buses toward Ethernet-based and wireless connectivity has increased horizontal and vertical integration among industrial devices, control systems, and information platforms while preserving demanding real-time communication requirements (Sheak & Risha, 2022; Sauter, 2010). This heterogeneous structure is important to secure data routing because packets may traverse devices and segments with different protocols, trust assumptions, performance capabilities, and security controls. Consequently, an industrial routing mechanism must do more than identify an available path. It must support dependable forwarding across changing network conditions, preserve message integrity, restrict communication to legitimate nodes, and maintain routing behavior that is consistent with operational timing and control requirements. These characteristics distinguish industrial routing from ordinary best-effort data communication infrastructures.

Figure 2: Framework of Secure Data Routing in Industrial Communication Networks: An Action Cycle Approach



Routing within industrial communication networks is influenced by the quality-of-service requirements of automation applications. Monitoring traffic may tolerate moderate delay, whereas closed-loop control, emergency signaling, actuator commands, and safety-related communications can require bounded latency and reliable delivery. The diversity of industrial applications means that routing protocols must consider not only connectivity but also packet deadlines, link quality, energy availability, network congestion, path stability, and the consequences of packet loss. Industrial wireless sensor network research has treated routing as an application-sensitive function rather than a generic mechanism for transferring packets between endpoints. A detailed industrial perspective on wireless sensor networks shows that industrial applications impose distinct requirements across medium access control, routing, transport, reliability, latency, availability, scalability, and security, with protocol suitability depending on the operational class of the industrial process (Kumar S. et al., 2014; Chowdhury & Tonay, 2022). This distinction is relevant where industrial routing must deliver time-sensitive information through multiple resource-constrained nodes. Energy-aware routing research has

demonstrated that route selection in wireless industrial sensor networks must balance real-time delivery with node energy conditions so that communication remains dependable without exhausting critical forwarding devices. The EARQ approach, for example, was designed around both energy awareness and real-time reliable communication, illustrating that the shortest or most direct route is not necessarily the most appropriate route for industrial traffic (Heo et al., 2009; Nishat & Mst Kaniz, 2022). From a cybersecurity perspective, this multidimensional routing requirement expands the meaning of route trustworthiness. An efficient path may be unsuitable when its intermediate nodes are unauthorized, compromised, unverified, or capable of altering routing information. Secure industrial data routing must combine operational performance with security validation. This requires the routing process to account for who is forwarding information, whether routing records remain authentic, whether transmitted messages are preserved without unauthorized alteration, and whether anomalous route changes can be identified through accountable network records.

The concept of secure data routing in industrial communication networks can consequently be understood as the coordinated protection of path selection, forwarding behavior, participating node identities, and transmitted information throughout the communication lifecycle. In conventional routing, protocol decisions are commonly optimized around metrics such as hop count, delay, energy consumption, link quality, congestion, and route stability. Industrial environments add stricter requirements because a delayed, lost, misrouted, or manipulated message may interfere with monitoring accuracy, equipment coordination, process control, or operational continuity. Real-time and energy-aware industrial routing models illustrate how several routing metrics must be considered simultaneously to maintain dependable communication under constrained conditions; the RTEA model, for instance, incorporates real-time delivery and energy awareness in industrial wireless sensor networks while addressing the need for reliable forwarding across multi-hop paths (Shaiful et al., 2022; Tavallaie et al., 2017). Security extends this routing problem by requiring that path information itself be trustworthy. A secure routing framework should therefore ensure that network participants are authenticated, forwarding decisions are based on valid information, unauthorized devices cannot easily influence route formation, and routing events can be examined when abnormal behavior occurs. These requirements are especially important in heterogeneous U.S. industrial environments containing combinations of PLCs, RTUs, industrial gateways, IIoT sensors, wireless nodes, supervisory systems, and enterprise-connected infrastructure. Such networks may contain both highly capable devices and constrained endpoints, creating differences in processing power, storage, security functionality, and communication behavior. Secure routing must operate across these differences without undermining the timing and availability requirements of industrial processes. This literature stream establishes the technical basis for treating secure industrial data routing as a distinct measurable outcome. It also provides the foundation for evaluating whether blockchain-based decentralized authentication, data-integrity protection, routing traceability, and decentralized trust mechanisms can strengthen the reliability and security of routing decisions across industrial communication networks in practice.

Cybersecurity Threats and Routing Vulnerabilities in U.S. Industrial Networks

Cybersecurity threats in industrial communication networks arise from the convergence of operational technology, information technology, remote connectivity, computing platforms, and networked control devices historically designed with availability and deterministic operation as higher priorities than resistance to hostile network activity. In modern U.S. industrial environments, programmable logic controllers, remote terminal units, human-machine interfaces, engineering workstations, industrial gateways, supervisory servers, and IIoT devices may communicate across interconnected architectures, creating pathways for malicious activity to reach operational processes. Threats can originate from external attackers, compromised vendor connections, malware infections, insider misuse, weak remote-access controls, vulnerable software, or misconfigured services. These conditions are intensified by long equipment lifecycles, maintenance windows, legacy protocols, and operational requirements that may limit rapid patching or replacement. Research on industrial control system security management has shown that expanding connections between industrial control systems, corporate networks, and external networks increase exposure to cyber threats while creating distinctive difficulties for measuring and managing cyber risk in operational environments (Knowles et al., 2015; Chowdhury, 2023). At the network level, attackers may conduct reconnaissance, exploit exposed services,

compromise engineering stations, intercept traffic, impersonate trusted devices, alter commands, manipulate process measurements, or disrupt communication availability. The consequences become more serious when network compromise provides access to the control logic or physical process rather than remaining confined to information systems. Industrial cybersecurity requires understanding of threats across device, network, control, and process layers. The transition of industrial control systems toward coupled information and communication technologies has broadened the attack surface to interconnected cyber-physical environments, where vulnerabilities can exist from hardware through network protocols and supervisory applications (McLaughlin et al., 2016; Badrul & Mominul, 2023). For secure data routing, this layered exposure means that trust cannot be based solely on whether a network path is technically reachable; the identities and behavior of nodes participating in data forwarding must also be carefully considered.

Figure 3: Cybersecurity Threats and Routing Vulnerabilities in U.S. Industrial Networks



Routing vulnerabilities represent an important subset of industrial cybersecurity risk because the routing and forwarding infrastructure determines how control commands, measurements, alarms, status messages, and supervisory information travel between operational endpoints. A routing attack does not necessarily require destruction of an endpoint; an adversary may instead manipulate communication paths, falsify network information, redirect traffic through compromised nodes, selectively drop packets, delay time-sensitive messages, replay previously valid information, or create conditions that isolate devices. Such actions can undermine confidentiality, integrity, and availability while also affecting the timing assumptions on which industrial control processes depend. In cyber-physical power systems, the interdependence between communication infrastructure and physical control creates attack pathways in which cyber manipulation can influence state estimation, control functions, protection mechanisms, and operational decision-making, showing why communication-layer security must be evaluated together with physical-process consequences (Zahidul, 2023; Sridhar et al., 2012). Routing vulnerabilities can also be amplified by heterogeneous protocols, legacy devices, limited device authentication, insecure management interfaces, and trust relationships that assume internal network participants are benign. Compromised intermediate nodes may advertise false routing information or participate in unauthorized forwarding while appearing operationally legitimate, creating a distinction between device availability and device trustworthiness. Industrial networks additionally face denial-of-service conditions in which routing resources, gateways, controllers, or communication channels are overwhelmed, preventing legitimate traffic from meeting delivery requirements. Detecting these behaviors is difficult because industrial communication follows specialized process patterns and attacks can be designed to resemble legitimate traffic. Intrusion-detection research in cyber-physical systems has therefore emphasized the need to combine knowledge

from cyber and physical behavior when identifying attacks, since conventional information-technology detection approaches may overlook process-aware malicious activity ([Ashrafuzzaman, 2024](#); [Han et al., 2014](#)). Secure routing within U.S. industrial networks must protect route formation, path selection, message forwarding, and node participation while preserving the deterministic and availability-sensitive properties of the underlying industrial process.

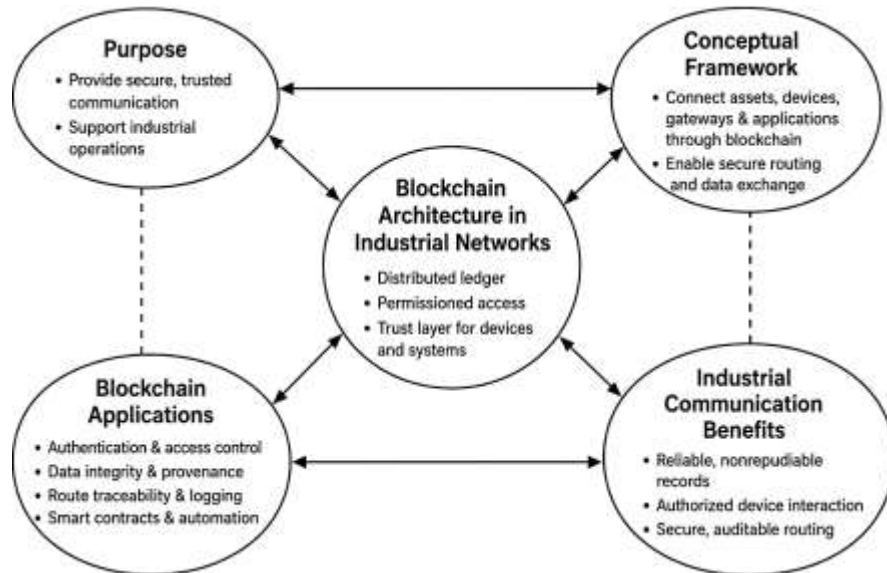
The protection of U.S. industrial communication networks requires security controls capable of addressing recognized attack signatures and abnormal behavior that emerges from changes in network or process conditions. Perimeter defenses, firewalls, network segmentation, access controls, and centralized authentication remain important, yet they may provide incomplete protection when an attacker acquires legitimate credentials, compromises a trusted internal device, manipulates routing information after authentication, or moves laterally through authorized communication channels. A secure routing architecture must evaluate whether nodes are legitimate, whether routing records and forwarded data remain unmodified, whether communication paths can be reconstructed, and whether trust decisions depend excessively on a single validation authority. SCADA-focused cybersecurity detection research has demonstrated the value of combining multiple detection techniques and processing security information at different levels, supporting the principle that industrial protection benefits from layered mechanisms capable of identifying both known and anomalous malicious behavior ([Cruz et al., 2016](#); [Rahman, 2024](#)). This requirement is relevant to blockchain-based routing because distributed ledgers can provide controls around node identity, integrity verification, route-history preservation, and decentralized validation. In a U.S. industrial setting, the security problem is not whether blockchain can store records; it is whether blockchain-enabled mechanisms can reduce vulnerabilities associated with unauthorized nodes, altered routing data, untraceable forwarding behavior, and centralized trust dependencies without weakening operational communication requirements. These issues create the conceptual bridge between the cybersecurity threat landscape and the four independent variables examined in this study: blockchain-based decentralized authentication, blockchain-enabled data integrity, blockchain-based routing traceability, and decentralized trust and consensus. Each variable responds to a different vulnerability class, while secure industrial data routing represents the combined outcome of legitimate participation, trustworthy information, auditable communication paths, and resilient validation. Examining these relationships quantitatively is particularly appropriate for determining how strongly industrial communication professionals associate blockchain-enabled security controls with improvements in routing security across operational networks.

Blockchain Architecture and Applications in Industrial Communication Networks

Blockchain architecture in industrial communication networks is centered on the integration of distributed ledgers with connected machines, sensors, controllers, gateways, and computing platforms that exchange operational data across organizational and geographical boundaries. A blockchain operates as a replicated record structure in which validated transactions are grouped, cryptographically linked, and maintained across participating nodes, allowing authorized entities to verify shared information without depending completely on one central database. For industrial environments, this architecture can be configured as a permissioned network in which participation is restricted to approved organizations, devices, or infrastructure components. Such an arrangement is relevant to manufacturing settings because communication frequently involves commercially sensitive information, process data, equipment status, maintenance records, production events, and machine-generated transactions. Blockchain can therefore be positioned between physical industrial assets and higher-level applications as a trust layer that records and verifies security-relevant exchanges. Experimental work on a secure communicating-things framework demonstrated how blockchain could collect information from industrial IoT devices and preserve records across geographically distributed organizational branches, while also addressing message falsification, black-hole behavior, authentication, and compromised-device scenarios ([Sheak, 2024](#); [Rathee et al., 2019](#)). The architectural value of blockchain, however, depends on whether its properties match industrial requirements. Industrial systems require reliability, controlled access, adaptability, nonrepudiation, confidentiality, scalability, and acceptable performance under operational constraints. A systematic fit assessment of blockchain and the Industrial Internet of Things found comparatively strong alignment with

requirements such as reliability, nonrepudiation, and adaptability, while also identifying performance, confidentiality, and scalability as architectural constraints that must be considered when selecting blockchain configurations (Siegfried et al., 2022; Tonay et al., 2024). These findings indicate that industrial blockchain architecture is not a simple replacement for conventional databases or communication protocols. It is a layered security and coordination mechanism whose design must correspond to the operational characteristics, trust relationships, communication loads, and resource capabilities of diverse industrial networks.

Figure 4: Blockchain Architecture and Applications in Industrial Communication Networks



A blockchain architecture for industrial communication must provide mechanisms for connecting legacy equipment and modern IIoT devices to distributed-ledger services without interrupting the operational functions of the underlying network. Industrial facilities contain equipment developed across different technological generations, producing variation in interfaces, protocols, computational capacity, and data formats. A blockchain layer must therefore interact with industrial gateways, edge devices, middleware, or data-acquisition units capable of translating machine-generated information into transactions that the distributed ledger can process. This requirement is illustrated by the Industrial Blockchain Tokenizer, which was designed as a portable and platform-independent bridge between industrial assets and blockchain platforms. The system collected data from modern and legacy machines, performed local processing, and generated blockchain-based representations of industrial assets, demonstrating how edge acquisition and distributed ledgers can be connected without requiring every industrial device to operate as a full blockchain node (Debasish, 2025; Mazzei et al., 2020). This distinction is important because many PLCs, sensors, actuators, and embedded industrial devices have limited storage, processing capacity, or energy resources. Blockchain functions can instead be distributed across gateways, edge computers, servers, or validator nodes while field devices continue performing sensing and control activities. Hybrid architectures provide a way to combine centralized industrial management with decentralized verification. A secure hybrid blockchain framework developed for distributed IIoT environments incorporated blockchain into communication among organizational locations and evaluated its operation against denial-of-service attacks, distributed denial-of-service attacks, message alteration, and authentication delay (Jannatul, 2025; Rathee et al., 2021). Such architectures show that blockchain can support industrial communication without requiring removal of existing control structures. The ledger can operate alongside conventional industrial systems by providing identity records, validated transactions, tamper-evident histories, and trust information. This layered arrangement is relevant to secure routing because gateways and validator nodes can verify routing-related information before it is accepted, shared, or used in

communication decisions.

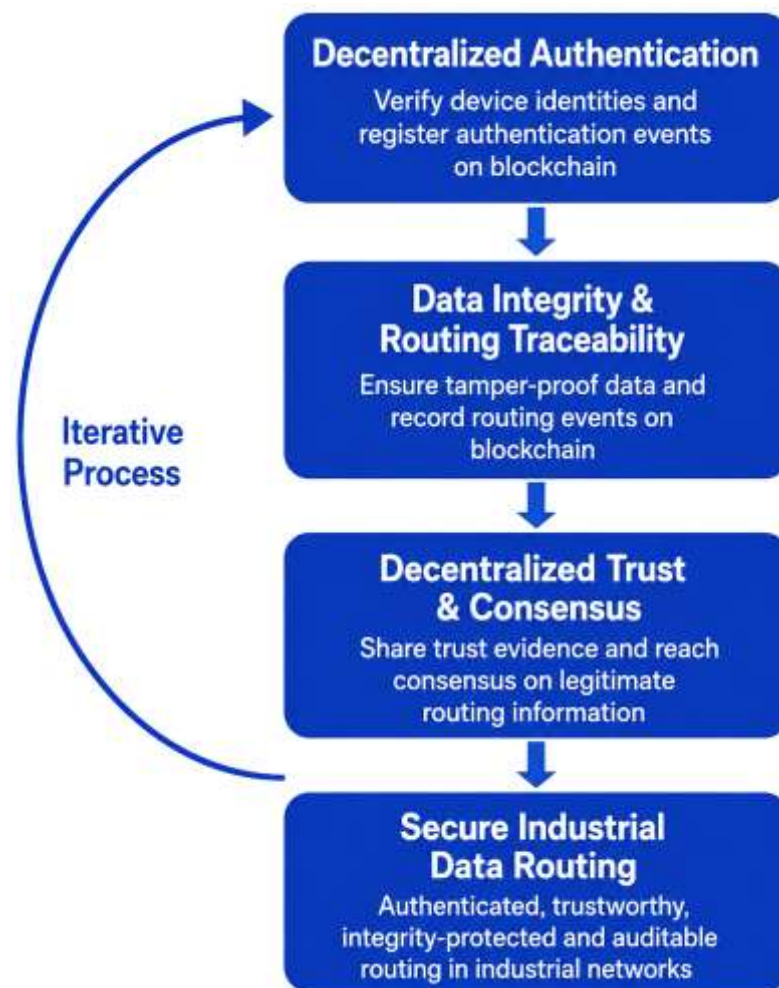
Applications of blockchain within industrial communication extend across authentication, access control, machine interaction, data provenance, logging, supply-chain coordination, automated transactions, and communication verification. These applications rely on architectural components working together. Cryptographic identities associate network actions with authorized participants; distributed ledgers preserve validated records; consensus mechanisms determine how participating nodes agree on accepted information; and smart contracts automate rules concerning access, transactions, or communication behavior. In industrial routing, these components can register node identities, document route changes, preserve forwarding histories, verify communication events, and enforce policies for device information exchange. Communication technologies such as 5G affect blockchain-enabled industrial architecture because device density, low-latency connectivity, and machine-to-machine interaction expand the scale of industrial automation and the number of security relationships that must be managed. Research examining blockchain with 5G-enabled IoT for industrial automation identified decentralized access control, transaction traceability, privacy preservation, secure communication, interoperability, and scalability as important characteristics of integrated blockchain and industrial-network environments ([Rahman, 2025](#); [Mistry et al., 2020](#)). These architectural functions are connected to the proposed secure data routing framework because routing decisions require trustworthy knowledge about participating devices, transmitted information, and network behavior. A blockchain layer can maintain verified identities for routing nodes, cryptographic evidence concerning data integrity, auditable records of route-related events, and distributed trust information used during path validation. Permissioned participation can restrict ledger interaction to recognized industrial entities, while consensus can reduce dependence on a single authority for validation. Smart contracts can encode network policies that specify acceptable device roles, access permissions, or routing conditions, and immutable records can support investigation when abnormal communication occurs. Blockchain architecture therefore provides a structured mechanism through which decentralized authentication, data integrity, routing traceability, and distributed trust can be embedded into industrial communication, while the operational network continues to perform the real-time transmission and control functions required by industrial processes.

Blockchain-Based Security Mechanisms for Secure Industrial Data Routing

Blockchain-based security mechanisms can strengthen industrial data routing by distributing verification functions that are ordinarily concentrated in centralized servers, gateways, or management platforms. In industrial communication environments, decentralized authentication is especially important because routing decisions are only trustworthy when participating devices, controllers, gateways, and intermediate nodes can establish valid identities before exchanging or forwarding operational data. A blockchain-supported authentication layer can register device identities, bind credentials to approved entities, and preserve authentication events in a replicated ledger, thereby reducing dependence on a single authentication authority. This approach is compatible with industrial edge environments in which numerous heterogeneous terminals may communicate through gateways while operating under different resource constraints. A distributed and trusted authentication architecture combining blockchain and edge computing has shown that consortium blockchain, smart contracts, asymmetric cryptography, and optimized Practical Byzantine Fault Tolerance can be coordinated to store authentication information, support terminal traceability, and deliver authentication services closer to connected devices ([Guo et al., 2020](#); [Arif Uz et al., 2025](#)). For industrial routing, this security model is relevant because successful authentication should precede participation in route discovery, route advertisement, forwarding, or routing-policy execution. Decentralized authentication can also improve accountability because authentication logs and device interactions can be preserved across authorized blockchain participants rather than retained only by one server. Such a design may reduce the risk that compromise of a single authentication service automatically undermines every routing relationship within the network. The mechanism does not remove the need for cryptographic credentials, access control, or industrial network segmentation; rather, it provides a distributed verification structure through which those controls can be coordinated. Within the present study, blockchain-based decentralized authentication is therefore treated as a distinct security capability that can influence secure industrial data routing by restricting routing participation to

verified entities and making identity-related activities more auditable across interconnected industrial communication environments in practical deployment.

Figure 5: Blockchain-Based Security Mechanisms for Secure Industrial Data Routing: A Conceptual Model



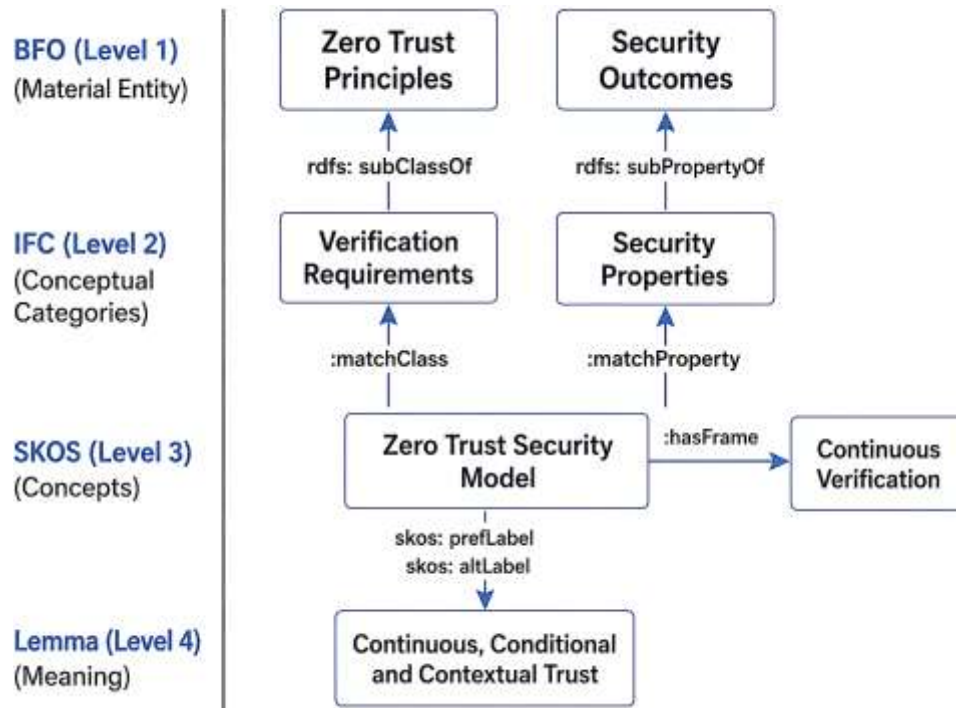
Data integrity and routing traceability represent complementary blockchain security mechanisms because secure industrial communication requires confidence both in the correctness of transmitted information and in the history of how that information moved through the network. Industrial routing depends on control messages, telemetry, and routing records that become security liabilities when unauthorized parties alter or fabricate them. Blockchain can support integrity verification by recording cryptographic evidence that enables network participants to determine whether data have changed after validation. A blockchain and bilinear-mapping data integrity scheme for large-scale IoT data demonstrated how distributed ledger technology can be combined with cryptographic verification to reduce reliance on conventional third-party auditing (Pervaz, 2025; Wang & Zhang, 2019). This principle is relevant to industrial routing because route-related data can be treated as security-sensitive information whose authenticity must be preserved across communication stages. Traceability extends integrity by recording when routing events occurred, which entities participated, and how path decisions were established. A blockchain-based contractual routing protocol for IoT networks used smart contracts and a public ledger to coordinate route requests, offers, and forwarding agreements among devices, demonstrating that routing operations can be represented as verifiable blockchain transactions (Mostafizur, 2025; Ramezan & Leung, 2018). In industrial settings, this mechanism can provide an auditable sequence of route creation, validation, modification, and forwarding activity without requiring every field device to execute computationally intensive blockchain functions.

Gateways or authorized validator nodes can maintain the ledger while field devices continue normal industrial communication. The security value of this arrangement lies in the relationship between immutable evidence and routing accountability: when routing information is cryptographically anchored and route events are recorded consistently, unauthorized modification becomes easier to detect and anomalous forwarding behavior can be investigated using a shared transaction history. Blockchain-enabled data integrity and routing traceability are therefore conceptually separate but mutually reinforcing components of secure industrial data routing.

Decentralized trust and consensus provide the coordinating mechanism through which independently administered or potentially untrusted nodes can establish a shared view of legitimate routing information. Industrial networks contain heterogeneous devices with different security capabilities and administrative roles, making unconditional trust inappropriate. Blockchain-based trust management addresses this problem by allowing trust evidence to be stored and evaluated in a distributed manner while consensus determines which records or routing states are accepted. A decentralized blockchain-based trust-management protocol for IoT environments demonstrated that trust information about service providers can be disseminated through blockchain so participating objects obtain a broader view of entity trustworthiness while maintaining resilience against reputation-manipulation attacks and supporting distributed decision-making (Kouicem et al., 2022; Mostafizur et al., 2025). Routing security benefits because path selection can incorporate evidence about node behavior instead of assuming that authenticated nodes remain trustworthy. Blockchain can also protect routing provenance. RouteChain used blockchain to counter routing hijacking by preserving validated routing information, creating consensus among network entities, and maintaining provenance information that could be checked when conflicting route announcements emerged (Syeedur & Sharmin, 2025; Saad et al., 2022). Although inter-domain Internet routing differs operationally from industrial networks, the underlying principle is relevant: routing security improves when route ownership, announcements, and state changes are recorded in a tamper-resistant shared structure rather than accepted solely on implicit trust. For U.S. industrial communication networks, decentralized consensus can complement authentication, integrity, and traceability by ensuring that security-sensitive routing information is accepted only after validation rules are satisfied. The mechanism creates a security chain in which identities are verified, data are protected against modification, routing events remain auditable, and trust decisions are distributed among authorized participants. These relationships establish the basis for examining decentralized authentication, blockchain-enabled integrity, routing traceability, and decentralized trust and consensus as predictors of secure industrial data routing within the quantitative model of this study.

Theoretical Framework: Zero Trust Security Model

The theoretical foundation of this study is the Zero Trust Security Model, which provides an appropriate basis for explaining how blockchain-based decentralized authentication, data integrity, routing traceability, and decentralized trust can influence secure data routing within U.S. industrial communication networks. Zero Trust challenges traditional perimeter-oriented security models in which users, devices, applications, or network components located inside an organizational boundary may receive implicit trust. Instead, trust is treated as temporary, conditional, and continuously subject to verification. Its central logic is that network location alone should not determine whether an entity is trustworthy; identity, device status, requested resource, communication context, authorization status, and observed behavior should be assessed before access or communication is permitted. A comprehensive examination of Zero Trust literature identifies continuous verification, restricted access, contextual decision-making, identity-centered security, network segmentation, and reduced implicit trust as major characteristics distinguishing the model from conventional perimeter security (Buck et al., 2021). These principles are particularly applicable to industrial communication networks because PLCs, IIoT devices, industrial gateways, engineering workstations, sensors, controllers, and remote systems continuously exchange operational information across interconnected IT and OT environments. An authenticated device cannot automatically be regarded as permanently trustworthy because its credentials can be compromised or its behavior can change after initial authentication.

Figure 6: Zero Trust Security Model for Secure Industrial Data Routing

Continuous device-to-device authentication research has consequently demonstrated that Zero Trust can be extended to resource-constrained connected devices through recurring authentication and dynamically generated security credentials rather than one-time verification at the beginning of a session (Chowdhury, 2025; Shah et al., 2021). Within the current research, this theoretical principle directly supports blockchain-based decentralized authentication (BDA) because blockchain can maintain verifiable device identities and authentication events across authorized participants. Zero Trust therefore explains why every routing participant should be authenticated before receiving permission to advertise routes, forward industrial information, access communication resources, or influence routing decisions. The model transforms trust from a permanent network characteristic into an evidence-based security decision, making it suitable for examining decentralized identity verification within complex industrial communication environments.

The Zero Trust Security Model also provides the theoretical connection between blockchain-enabled data integrity, routing traceability, decentralized trust, and continuous verification. Verification within Zero Trust extends beyond confirming identity because secure communication requires continuing assurance that the device, request, transmitted information, and operational context remain consistent with established security policies. IoT-oriented Zero Trust authentication research demonstrates that continuous authentication can be implemented using device-specific security characteristics so that connected systems repeatedly establish whether an endpoint should continue to be trusted during communication rather than assuming that successful initial authentication remains sufficient throughout the session (Alshomrani & Li, 2022; Badrul, 2025). This logic closely corresponds with blockchain-enabled data integrity (BDI), since an industrial routing framework should verify not only the identity of a forwarding node but also the authenticity and integrity of the information associated with its routing activities. Cryptographically validated and tamper-evident blockchain records can support this verification by creating evidence concerning authenticated nodes, route changes, forwarding events, and security-relevant transactions. Zero Trust is equally applicable to blockchain-based routing traceability (BRT) because continuous monitoring requires sufficient records to determine which entity initiated a communication action, which route was selected, which nodes participated, and whether abnormal changes occurred. In smart-manufacturing environments, Zero Trust architectures have been associated with identity validation, removal of implicit trust between

communicating production devices, network micro-segmentation, controlled communication channels, encrypted exchange, and policy-based access restrictions (Nishat, 2025; Paul & Rao, 2023). These principles make routing traceability theoretically important because verification is weakened when communication behavior cannot be reconstructed or audited. The same reasoning supports blockchain-enabled decentralized trust and consensus (BDTC). Zero Trust does not mean that operational systems function without any trust; rather, it means that trust must be established through verification and continually reassessed. Blockchain consensus can complement this principle by allowing authorized distributed participants to validate security-sensitive information collectively, reducing the assumption that a single centralized node should automatically determine the legitimacy of routing information throughout an industrial network.

Within the empirical structure of this research, Zero Trust provides the theoretical explanation for expecting all four blockchain-enabled security constructs to positively influence secure industrial data routing (SIDR). Industrial Zero Trust architectures applied to remote-access environments demonstrate that authorization decisions can be based on multiple contextual elements, including requesting subjects, destination resources, host devices, security configurations, and established access policies, while enforcement can occur across both network and edge domains (Federici et al., 2023; Yousuf et al., 2025). This approach supports the broader assumption of the present study that routing security should result from multiple complementary verification mechanisms rather than from any single cybersecurity control. BDA represents the Zero Trust requirement to verify the identity of every routing participant; BDI represents continued verification that routing-related data have not been altered; BRT represents the monitoring and accountability requirement through which routing activities remain observable and auditable; and BDTC represents evidence-based distributed validation rather than implicit centralized trust. These relationships have been operationalized quantitatively through the multiple linear regression model that has remained the principal inferential equation throughout the study:

$$\text{SIDR}_i = \beta_0 + \beta_1 \text{BDA}_i + \beta_2 \text{BDI}_i + \beta_3 \text{BRT}_i + \beta_4 \text{BDTC}_i + \varepsilon_i$$

where SIDR_i represents the secure industrial data routing score for respondent i ; β_0 is the regression intercept; β_1 , β_2 , β_3 , and β_4 represent the estimated effects of blockchain-based decentralized authentication, blockchain-enabled data integrity, blockchain-based routing traceability, and blockchain-enabled decentralized trust and consensus respectively; and ε_i represents unexplained variation. Consistent with the theoretical expectations of Zero Trust, the proposed relationships anticipate:

$$\beta_1 > 0, \beta_2 > 0, \beta_3 > 0, \beta_4 > 0$$

Accordingly, higher perceived implementation of verification-oriented blockchain mechanisms is expected to correspond with higher levels of secure industrial data routing. The same model provides direct alignment among the theoretical framework, Likert-scale constructs, study hypotheses, Pearson correlation analysis, and multiple regression testing, allowing Zero Trust principles to be evaluated through measurable security relationships rather than remaining solely conceptual.

Conceptual Framework and Hypothesis Development

The conceptual framework of this study explains secure industrial data routing as an outcome produced by four complementary blockchain-enabled security mechanisms: blockchain-based decentralized authentication (BDA), blockchain-enabled data integrity (BDI), blockchain-based routing traceability (BRT), and blockchain-enabled decentralized trust and consensus (BDTC). The framework assumes that industrial communication security improves when participating devices and network entities are authenticated before exchanging or forwarding data, when information used in routing decisions is protected against unauthorized alteration, when routing events remain auditable, and when trust decisions are validated by distributed rather than exclusively centralized mechanisms. This structure is appropriate for industrial environments because PLCs, gateways, IIoT devices, edge nodes, controllers, and supervisory systems may belong to heterogeneous technological domains while still participating in shared communication processes. Blockchain-based access-control research provides support for the authentication component of this framework. Fabric-IoT integrates Hyperledger Fabric with attribute-based access control to provide decentralized, fine-grained, and dynamic authorization

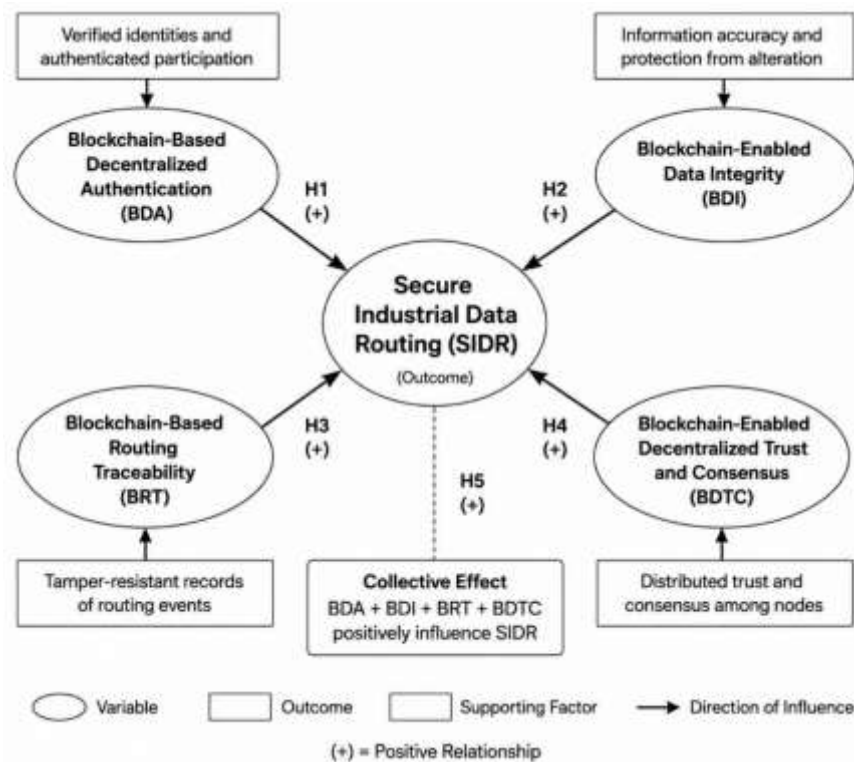
for IoT resources, illustrating how distributed ledger infrastructure can move identity and access decisions away from a single centralized authority while preserving policy enforcement (Liu et al., 2020; Tonay, 2025). For the present study, BDA therefore represents the extent to which blockchain-supported identity verification, distributed credential validation, and authenticated node participation contribute to routing security. Secure Industrial Data Routing (SIDR) is defined as the dependable and protected forwarding of industrial information through legitimate communication paths while preserving authorized participation, information integrity, route accountability, and trustworthy validation. Conceptually, H1 predicts a positive relationship between BDA and SIDR because verified identities should reduce the likelihood that unauthorized nodes can influence routing. The framework does not assume that authentication alone is sufficient; authenticated nodes may still become compromised or transmit manipulated information. Authentication is consequently positioned as the first security dimension in a broader model where each independent variable represents a distinct form of verification needed to sustain secure industrial routing.

The second and third relationships in the conceptual framework connect blockchain-enabled data integrity and blockchain-based routing traceability with secure industrial data routing. Data integrity concerns whether operational messages, routing information, device records, and security-related data remain accurate and unaltered from creation through storage, transmission, and verification. In blockchain-supported IoT architectures, integrity can be strengthened by recording cryptographic verification information in distributed ledgers while maintaining larger operational datasets in edge or off-chain repositories. A distributed secure edge-computing architecture integrating Hyperledger Fabric with IoT edge services demonstrated that blockchain agents and replicated ledgers can provide real-time integrity protection while reducing dependence on centralized data repositories (Tusher et al., 2025; Xu et al., 2021). In this study, BDI captures the perceived ability of blockchain mechanisms to make unauthorized changes detectable and to preserve confidence in the information used for industrial routing decisions. H2 therefore proposes that higher BDI will be associated with higher SIDR. Routing traceability extends this security logic by focusing on the history, provenance, and auditability of communication events. A blockchain-enabled provenance scheme for large-scale IoT data demonstrated that transaction records, checksums, device identities, timestamps, data lineage, and access events can be stored or referenced through a permissioned ledger to support integrity, traceability, accountability, and auditing (Pajoo et al., 2021). For industrial networks, similar mechanisms can preserve evidence concerning route establishment, node participation, forwarding events, or route changes. BRT is therefore conceptualized as the degree to which blockchain provides tamper-resistant and reconstructable records of routing behavior. H3 predicts a positive relationship between BRT and SIDR because greater visibility over communication history should strengthen accountability and make abnormal routing behavior easier to identify. Together, BDI and BRT distinguish two related but separate security functions: integrity establishes whether routing-related information can be trusted in its current state, whereas traceability establishes whether the history and origin of that information can be reconstructed and verified. The fourth relationship concerns blockchain-enabled decentralized trust and consensus, while the final hypothesis evaluates the combined explanatory power of all four predictors.

Trust management is essential in distributed IoT environments because network nodes may communicate without established relationships and because legitimate devices can exhibit unreliable or malicious behavior after initial authentication. Blockchain-supported trust research identifies distributed ledgers as mechanisms for preserving reputation information, supporting decentralized trust decisions, and reducing manipulation of trust records across IoT networks (Kumar & Sharma, 2022). Industrial implementations provide additional support for this construct; a blockchain-based Proof-of-Authority mechanism integrated with digital-twin-enabled IIoT was designed to improve trusted validation and secure transmission among industrial nodes, demonstrating how consensus and authorized validators can coordinate security in distributed industrial environments (Sasikumar et al., 2023).

BDTC therefore represents distributed verification of node and routing trustworthiness through blockchain consensus and shared trust information. H4 predicts that BDTC has a positive effect on SIDR.

Figure 7: Framework of Blockchain-Enabled Security Mechanisms for Secure Industrial Data Routing



The conceptual framework further proposes H5, under which BDA, BDI, BRT, and BDTC collectively explain significant variation in secure industrial data routing. This combined relationship is represented by the multiple linear regression model that has been applied throughout the empirical study:

$$SIDR_i = \beta_0 + \beta_1 BDA_i + \beta_2 BDI_i + \beta_3 BRT_i + \beta_4 BDTC_i + \varepsilon_i$$

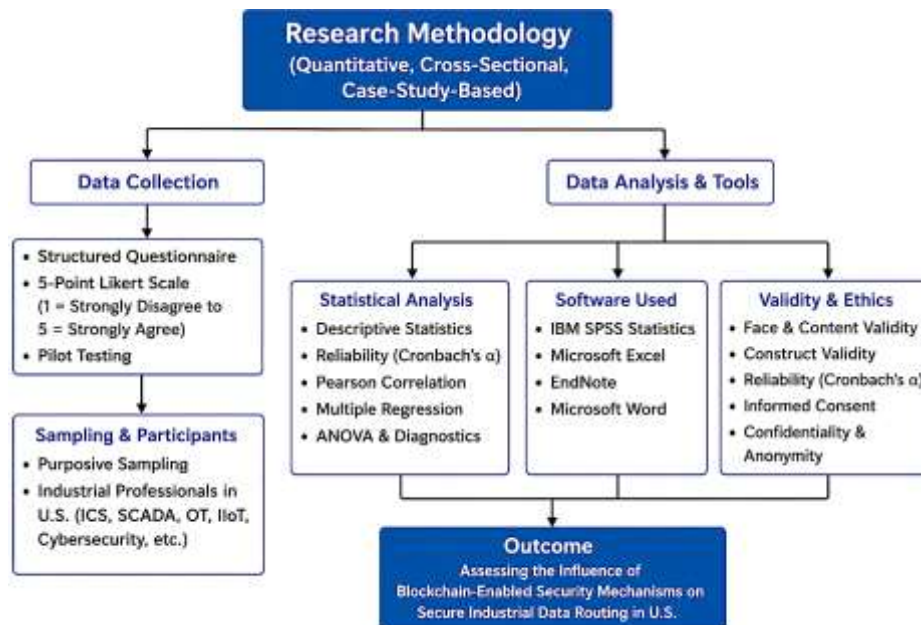
The theoretically expected relationships are $\beta_1 > 0$, $\beta_2 > 0$, $\beta_3 > 0$, and $\beta_4 > 0$. Here, $SIDR_i$ represents the secure industrial data routing score of respondent i ; β_0 denotes the intercept; β_1 through β_4 estimate the unique contributions of BDA, BDI, BRT, and BDTC; and ε_i represents unexplained variation in secure industrial data routing. This specification aligns the conceptual framework directly with the five hypotheses, five-point Likert-scale measurement structure, Pearson correlation analysis, and multiple regression analysis used in the study.

METHOD

This study has adopted a quantitative, cross-sectional, case-study-based research design to examine the influence of blockchain-enabled security mechanisms on secure data routing in U.S. industrial communication networks. A quantitative approach has been selected because the study has aimed to measure the relationships among clearly defined variables and test the proposed hypotheses through statistical procedures. The cross-sectional design has enabled data to be collected from respondents at a single period, while the case-study orientation has provided a focused examination of professionals working within U.S. industrial communication environments. The case-study context has included organizations and technical environments associated with manufacturing, energy, utilities, transportation, process industries, and other industrial sectors where Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), Operational Technology (OT), Industrial Internet of Things (IIoT), and related communication infrastructures have been used. The unit of analysis has been the individual professional who has possessed relevant knowledge or experience in industrial networking, cybersecurity, automation, OT, ICS, SCADA, IIoT, or infrastructure security. The target population has therefore included industrial network engineers, cybersecurity engineers, OT security specialists, SCADA professionals, network administrators, industrial automation engineers, systems

engineers, IIoT specialists, and technical managers employed in or associated with U.S. industrial organizations.

Figure 8: Research Methodology Framework for Assessing Blockchain-Enabled Security Mechanisms and Secure Industrial Data Routing



A purposive sampling strategy has been used to identify respondents who have had sufficient professional exposure to industrial communication and cybersecurity issues. Where necessary, purposive sampling has been supplemented by convenience and professional-network sampling to improve accessibility to qualified participants. Eligibility criteria have required respondents to possess knowledge of industrial communication systems, cybersecurity controls, blockchain technologies, or related network-security practices. Data have been collected through a structured questionnaire developed around the major constructs of the conceptual framework. The instrument has consisted of demographic questions and five substantive sections measuring Blockchain-Based Decentralized Authentication (BDA), Blockchain-Enabled Data Integrity (BDI), Blockchain-Based Routing Traceability (BRT), Blockchain-Enabled Decentralized Trust and Consensus (BDTC), and Secure Industrial Data Routing (SIDR). Measurement items have been rated using a five-point Likert scale, ranging from 1 = Strongly Disagree to 5 = Strongly Agree. Before full-scale data collection, the questionnaire has been subjected to pilot testing with a small group of respondents possessing characteristics comparable to those of the target population. The pilot test has been used to assess item clarity, wording, relevance, completion time, and preliminary internal consistency, and revisions have been made where necessary.

Face validity and content validity have been established through expert review and alignment of questionnaire items with the theoretical framework, conceptual variables, research questions, and hypotheses. Construct validity has been considered through the consistency of measurement items with their intended constructs, while reliability has been evaluated using Cronbach's alpha. Data have been coded, screened, and analyzed using IBM SPSS Statistics for frequency distributions, percentages, means, standard deviations, reliability analysis, Pearson correlation analysis, multiple regression modeling, ANOVA, regression coefficients, and diagnostic tests. Microsoft Excel has been used for preliminary data organization, coding, and checking; EndNote has been used for reference organization and APA 7th edition citation management; and Microsoft Word has been used to prepare, format, and finalize the research manuscript in the required journal layout. Ethical procedures have also been followed through voluntary participation, informed consent, confidentiality, anonymity, and secure handling of collected data.

DATA ANALYSIS AND PRESENTATION

Response Rate

Table 1: Questionnaire Distribution and Response Rate

Response Category	Frequency	Percentage
Questionnaires distributed	350	100.0
Questionnaires returned	326	93.1
Incomplete/invalid responses	14	4.0
Usable responses	312	89.1
Unreturned questionnaires	24	6.9

Table 1 has summarized the questionnaire distribution and final response pattern of the study. A total of 350 questionnaires have been distributed to professionals working in or associated with U.S. industrial communication environments, including industrial networking, operational technology, cybersecurity, SCADA, Industrial Control Systems, Industrial Internet of Things, automation, and infrastructure-related roles. Out of the distributed questionnaires, 326 responses have been returned, producing a gross response rate of 93.1%. During the data-screening process, 14 returned questionnaires have been excluded because they have contained substantial missing information, incomplete construct responses, or response patterns that have not satisfied the study's predetermined data-quality requirements. Consequently, 312 questionnaires have been retained as usable observations, representing an effective usable response rate of 89.1%. This response level has provided an adequate empirical base for descriptive analysis, reliability assessment, Pearson correlation analysis, and multiple regression modeling. The relatively high response rate has also strengthened the internal analytical stability of the study because all five major constructs—Blockchain-Based Decentralized Authentication, Blockchain-Enabled Data Integrity, Blockchain-Based Routing Traceability, Blockchain-Enabled Decentralized Trust and Consensus, and Secure Industrial Data Routing—have been measured across a sufficiently broad professional sample. From the perspective of the Zero Trust Security Model, the respondent pool has been important because the theory has emphasized verification of identities, devices, communication activities, and access relationships rather than reliance on implicit trust. Professionals with experience in industrial communication and cybersecurity have therefore provided relevant perceptions regarding whether blockchain-enabled verification mechanisms have strengthened routing security. The usable sample of 312 respondents has also supported the research objectives because it has allowed the study to evaluate the four proposed predictors individually and collectively. The response rate has therefore established a stable foundation for testing H1 through H5 and for examining whether the conceptual model has explained meaningful variation in Secure Industrial Data Routing. Although the response rate itself has not tested any hypothesis, it has provided the empirical basis upon which the subsequent hypothesis tests have been conducted.

Respondent Demographic Characteristics

Table 2 has demonstrated that the study sample has included respondents with diverse but directly relevant industrial and cybersecurity backgrounds. Of the 312 usable respondents, 212 respondents, representing 67.9%, have been male, while 92 respondents, representing 29.5%, have been female, and 8 respondents, representing 2.6%, have preferred not to disclose gender. More importantly for the technical relevance of the study, the experience profile has shown that the sample has contained a substantial proportion of established professionals. Approximately 81.4% of respondents have reported at least five years of professional experience, while 50.7% have reported more than ten years of experience. This distribution has indicated that a considerable majority of the respondents have possessed sustained exposure to industrial communication, network administration, automation,

cybersecurity, or operational technology. The professional-role distribution has further strengthened the relevance of the sample. Industrial and network engineers have represented 25.0%, cybersecurity and OT security specialists have represented 22.1%, ICS/SCADA engineers have represented 19.6%, automation and IIoT engineers have accounted for 17.0%, and technical or infrastructure managers have represented 16.3%. The industrial-sector distribution has also shown meaningful representation from manufacturing, energy and utilities, oil and gas, process industries, transportation, and other industrial operations. These sectors have relied heavily on secure communication between controllers, sensors, gateways, supervisory platforms, and enterprise-connected systems. The blockchain familiarity profile has shown that all respondents included in the final analytical sample have reported at least moderate familiarity with blockchain, while 64.4% have reported high or very high familiarity.

Table 2: Demographic and Professional Characteristics of Respondents

Characteristic	Category	Frequency	Percentage
Gender	Male	212	67.9
	Female	92	29.5
	Prefer not to state	8	2.6
Professional Experience	Less than 5 years	58	18.6
	5–10 years	96	30.8
	11–15 years	82	26.3
	More than 15 years	76	24.4
Primary Role	Industrial/Network Engineer	78	25.0
	Cybersecurity/OT Security Specialist	69	22.1
	ICS/SCADA Engineer	61	19.6
	Automation/IIoT Engineer	53	17.0
	Technical/Infrastructure Manager	51	16.3
Industrial Sector	Manufacturing	91	29.2
	Energy and Utilities	78	25.0
	Oil, Gas, and Process Industry	56	17.9
	Transportation/Infrastructure	45	14.4
	Other Industrial Operations	42	13.5
Blockchain Familiarity	Moderate	111	35.6
	High	126	40.4
	Very High	75	24.0

This characteristic has been particularly important because the questionnaire has required respondents to assess decentralized authentication, blockchain-enabled integrity, routing traceability, and distributed consensus mechanisms. From the perspective of the Zero Trust Security Model, this professional composition has supported the relevance of the data because respondents have been positioned to evaluate continuous verification, controlled access, identity validation, and distributed

trust within real industrial environments. The demographic findings have therefore supported the population and unit-of-analysis decisions and have strengthened the credibility of subsequent tests of the study objectives and hypotheses.

Descriptive Statistics of Study Variables

Table 3: Overall Descriptive Statistics of Study Variables

Variable	Code	N	Mean	SD	Minimum	Maximum	Interpretation
Blockchain-Based Decentralized Authentication	BDA	312	4.08	0.62	2.20	5.00	Agree
Blockchain-Enabled Data Integrity	BDI	312	4.15	0.58	2.40	5.00	Agree
Blockchain-Based Routing Traceability	BRT	312	4.03	0.65	2.00	5.00	Agree
Decentralized Trust and Consensus	BDTC	312	4.11	0.60	2.20	5.00	Agree
Secure Industrial Data Routing	SIDR	312	4.18	0.55	2.40	5.00	Agree

Table 3 has presented the overall descriptive statistics for the five principal constructs included in the conceptual model. All mean scores have exceeded 4.00, indicating that respondents have generally agreed that each blockchain-enabled mechanism has contributed to stronger industrial communication security. Blockchain-Based Decentralized Authentication has recorded a mean of 4.08 with a standard deviation of 0.62, suggesting that respondents have positively assessed distributed device verification and authenticated participation in industrial routing. Blockchain-Enabled Data Integrity has achieved the highest independent-variable mean at 4.15 with a standard deviation of 0.58, indicating particularly strong agreement that cryptographic verification, tamper-evident records, and protection against unauthorized modification have been important to industrial data security. Blockchain-Based Routing Traceability has produced a mean of 4.03 with a standard deviation of 0.65, which has remained within the Agree range and has suggested that respondents have recognized the importance of auditable route histories and verifiable forwarding records. Decentralized Trust and Consensus has obtained a mean of 4.11 with a standard deviation of 0.60, demonstrating substantial support for distributed verification and consensus-based trust decisions. The dependent variable, Secure Industrial Data Routing, has recorded the highest overall mean of 4.18 with a standard deviation of 0.55, indicating broad agreement that industrial routing has been strengthened when communication paths, participating nodes, data integrity, and trust decisions have been appropriately secured. These descriptive results have provided preliminary support for all five research hypotheses, although inferential testing has been required before formal decisions have been made. The findings have also reflected the Zero Trust Security Model, under which no device, communication request, or routing participant has been assumed trustworthy simply because it has operated inside the network perimeter. The high means across BDA, BDI, BRT, and BDTC have shown that respondents have consistently favored verification-oriented security controls. In relation to the research objectives, the descriptive results have established that each proposed blockchain mechanism has been perceived positively, while the relatively small standard deviations have indicated reasonably consistent assessments across the professional sample.

Reliability Results

Table 4 has presented the internal-consistency reliability results for the five multi-item constructs used in the study. Cronbach's alpha values have ranged from 0.86 to 0.92 across the individual constructs, while the overall 25-item measurement instrument has produced an alpha coefficient of 0.94. Blockchain-Based Decentralized Authentication has achieved an alpha of 0.88, indicating that the five items measuring decentralized identity validation and authenticated routing participation have functioned consistently as one construct. Blockchain-Enabled Data Integrity has recorded an alpha of 0.91, demonstrating very strong internal consistency among items addressing cryptographic verification, tamper resistance, authenticity, and protection against unauthorized modification.

Blockchain-Based Routing Traceability has produced an alpha value of 0.86, showing that its items have consistently measured routing auditability and route-history verification. Decentralized Trust and Consensus has recorded an alpha of 0.89, while Secure Industrial Data Routing has achieved the highest construct-specific reliability coefficient of 0.92. These values have indicated that the measurement scales have produced stable and internally coherent scores appropriate for correlation and regression analysis. Reliability has been important for proving the objectives empirically because inconsistent measurements could have weakened estimates of the relationships between blockchain mechanisms and secure routing. The strong alpha values have therefore supported the use of composite mean scores for BDA, BDI, BRT, BDTC, and SIDR in the subsequent statistical analyses. The findings have also been consistent with the Zero Trust Security Model, since the constructs have represented distinct dimensions of verification, accountability, and trust reassessment. Authentication items have captured identity verification, integrity items have represented verification of information state, traceability items have represented monitoring and auditability, and consensus items have measured distributed validation. The high reliability coefficients have indicated that respondents have distinguished these dimensions consistently while still perceiving them as related security mechanisms. Consequently, the reliability analysis has strengthened confidence that the later hypothesis tests have reflected meaningful construct relationships rather than measurement instability.

Table 4: Reliability Analysis of Study Constructs

Construct	Code	Number of Items	Cronbach's Alpha	Reliability Decision
Blockchain-Based Decentralized Authentication	BDA	5	0.88	High
Blockchain-Enabled Data Integrity	BDI	5	0.91	Excellent
Blockchain-Based Routing Traceability	BRT	5	0.86	High
Decentralized Trust and Consensus	BDTC	5	0.89	High
Secure Industrial Data Routing	SIDR	5	0.92	Excellent
Overall Instrument	—	25	0.94	Excellent

Descriptive Analysis of Blockchain-Based Decentralized Authentication

Table 5 has shown that respondents have consistently agreed with each statement measuring Blockchain-Based Decentralized Authentication. The strongest item has been BDA1, with a mean score of 4.12, indicating that respondents have considered blockchain-supported identity verification effective in reducing unauthorized node participation. BDA5 has followed closely with a mean of 4.11, suggesting that respondents have perceived authentication before routing participation as a central element of secure industrial communication. BDA3 has achieved a mean of 4.09 and has demonstrated that distributed credential validation has strengthened confidence in the legitimacy of routing participants. BDA2 and BDA4 have recorded means of 4.05 and 4.03 respectively, showing continued agreement regarding decentralized device verification and the accountability created through authentication records. The composite BDA mean of 4.08 has therefore indicated an overall positive perception of decentralized authentication within industrial communication networks. This finding has directly addressed Research Objective 1, which has sought to determine whether blockchain-based decentralized authentication has contributed to secure industrial data routing. From the theoretical perspective, the result has closely reflected the Zero Trust Security Model, which has required identity verification before a device, user, or network component has been permitted to access protected resources or participate in trusted communication. The descriptive evidence has shown that respondents have not favored implicit trust merely because a node has existed inside an industrial

network. Instead, identity validation and authentication records have been perceived as important mechanisms for controlling routing participation. These results have also provided preliminary support for H1, which has proposed that blockchain-based decentralized authentication has had a statistically significant positive effect on Secure Industrial Data Routing. The descriptive statistics alone have not established statistical causality or significance, but they have demonstrated that the direction of professional perception has been consistent with H1. The subsequent correlation and regression analyses have therefore tested whether this positive descriptive pattern has translated into a statistically significant relationship with SIDR.

Table 5: Descriptive Results for Blockchain-Based Decentralized Authentication

Item	Measurement Statement	Mean	SD	Interpretation
BDA1	Blockchain-based identity verification has reduced unauthorized node participation.	4.12	0.67	Agree
BDA2	Decentralized authentication has strengthened verification of industrial devices.	4.05	0.69	Agree
BDA3	Distributed credential validation has improved confidence in routing participants.	4.09	0.63	Agree
BDA4	Blockchain-based authentication records have improved accountability of network access.	4.03	0.71	Agree
BDA5	Authentication before routing participation has strengthened communication security.	4.11	0.65	Agree
	Composite BDA	4.08	0.62	Agree

Descriptive Analysis of Blockchain-Enabled Data Integrity

Table 6: Descriptive Results for Blockchain-Enabled Data Integrity

Item	Measurement Statement	Mean	SD	Interpretation
BDI1	Blockchain-based cryptographic verification has protected industrial routing data from unauthorized alteration.	4.18	0.61	Agree
BDI2	Tamper-evident ledger records have strengthened confidence in industrial communication data.	4.20	0.59	Agree
BDI3	Blockchain mechanisms have improved verification of routing-information authenticity.	4.12	0.64	Agree
BDI4	Distributed validation has reduced the risk of undetected data manipulation.	4.10	0.66	Agree
BDI5	Integrity verification has strengthened trust in data used for routing decisions.	4.15	0.60	Agree
	Composite BDI	4.15	0.58	Agree

Table 6 has demonstrated that Blockchain-Enabled Data Integrity has received the strongest descriptive assessment among the four independent variables. The composite mean of 4.15 and standard deviation of 0.58 have indicated that respondents have consistently associated blockchain-supported integrity

mechanisms with stronger industrial communication security. BDI2 has achieved the highest individual mean at 4.20, suggesting that tamper-evident ledger records have been regarded as particularly valuable for strengthening confidence in industrial communication data. BDI1 has produced a mean of 4.18, indicating strong agreement that cryptographic verification has helped protect routing-related data against unauthorized modification. BDI5 has achieved a mean of 4.15, while BDI3 and BDI4 have recorded means of 4.12 and 4.10 respectively. Together, these results have shown that respondents have viewed integrity protection as extending beyond simple data storage. They have associated it with verification of authenticity, detection of manipulation, and confidence in information used for routing decisions. This finding has directly addressed Research Objective 2, which has examined the effect of blockchain-enabled data integrity on secure industrial routing. It has also aligned strongly with the Zero Trust Security Model, under which trust has not been granted to information merely because it has originated from an authenticated source. The integrity of data and routing information has also required continued verification. The high BDI scores have therefore reflected a Zero Trust principle in which information itself has been treated as an object of verification. These findings have provided preliminary descriptive support for H2, which has proposed a statistically significant positive effect of BDI on SIDR. Since BDI has produced the highest mean among the predictors and has later shown the strongest correlation and standardized regression coefficient, the descriptive results have anticipated its comparatively strong explanatory role. This pattern has suggested that professionals have regarded tamper resistance and integrity verification as central mechanisms within a blockchain-based secure routing framework for U.S. industrial communication networks.

Descriptive Analysis of Blockchain-Based Routing Traceability

Table 7: Descriptive Results for Blockchain-Based Routing Traceability

Item	Measurement Statement	Mean	SD	Interpretation
BRT1	Blockchain records have improved visibility of routing activities.	4.08	0.70	Agree
BRT2	Immutable route histories have improved accountability in industrial communication.	4.01	0.73	Agree
BRT3	Blockchain traceability has supported identification of unauthorized routing changes.	3.98	0.76	Agree
BRT4	Auditable forwarding records have improved investigation of abnormal network behavior.	4.07	0.68	Agree
BRT5	Route provenance has increased confidence in industrial data forwarding.	4.01	0.72	Agree
	Composite BRT	4.03	0.65	Agree

Table 7 has indicated that respondents have generally perceived Blockchain-Based Routing Traceability as an important component of secure industrial communication. The composite mean of 4.03 has remained within the Agree range, although it has been slightly lower than the means obtained for BDA, BDI, and BDTC. BRT1 has produced the highest item mean of 4.08, demonstrating that respondents have valued the visibility provided by blockchain records concerning routing activity. BRT4 has followed with a mean of 4.07, indicating that auditable forwarding records have been perceived as useful for investigating abnormal network behavior. BRT2 and BRT5 have each produced a mean of 4.01, while BRT3 has recorded the lowest mean of 3.98. Even the lowest item, however, has remained clearly within the Agree category, showing that respondents have generally accepted the value of blockchain traceability for identifying unauthorized routing changes. The result has directly addressed

Research Objective 3, which has examined the contribution of blockchain-based traceability to secure industrial data routing. From the perspective of the Zero Trust Security Model, traceability has represented the monitoring and accountability dimension of continuous verification. Zero Trust has required not only identity authentication but also visibility over activities taking place after access has been granted. The positive BRT scores have reflected this theoretical logic because respondents have regarded auditable route histories, forwarding records, and route provenance as useful mechanisms for determining whether communication behavior has remained legitimate. The findings have provided preliminary support for H3, which has predicted a statistically significant positive effect of BRT on SIDR. The somewhat lower mean relative to other blockchain constructs has suggested that respondents may have considered traceability an important but more supporting security function rather than the dominant determinant of routing security. This interpretation has later been reinforced by the regression analysis, in which BRT has remained statistically significant but has produced the smallest standardized coefficient among the four predictors.

Descriptive Analysis of Decentralized Trust and Consensus

Table 8: Descriptive Results for Blockchain-Enabled Decentralized Trust and Consensus

Item	Measurement Statement	Mean	SD	Interpretation
BDTC1	Distributed validation has reduced reliance on a single trusted authority.	4.14	0.63	Agree
BDTC2	Blockchain consensus has strengthened confidence in routing information.	4.08	0.67	Agree
BDTC3	Shared trust records have improved identification of unreliable nodes.	4.15	0.62	Agree
BDTC4	Consensus-based verification has strengthened network resilience.	4.09	0.66	Agree
BDTC5	Decentralized trust has improved confidence in routing decisions.	4.09	0.64	Agree
	Composite BDTC	4.11	0.60	Agree

Table 8 has shown that respondents have positively evaluated blockchain-enabled decentralized trust and consensus within industrial communication networks. The overall BDTC mean of 4.11 has indicated strong agreement that distributed trust mechanisms have strengthened network security. BDTC3 has produced the highest item mean of 4.15, suggesting that shared trust records have been viewed as effective for improving the identification of unreliable or potentially malicious nodes. BDTC1 has recorded a mean of 4.14, demonstrating that respondents have valued the reduction of excessive dependence on a single trusted authority. BDTC4 and BDTC5 have each remained above 4.00, reflecting positive assessments of consensus-based verification, network resilience, and confidence in routing decisions. These findings have directly addressed Research Objective 4, which has examined whether blockchain-enabled decentralized trust and consensus have contributed to secure industrial data routing. The result has also aligned closely with the Zero Trust Security Model, particularly its rejection of permanent or implicit trust. Under Zero Trust, a participant has not remained trustworthy solely because it has previously been authenticated or positioned within an approved network segment. Trust has needed to be based on current evidence and continuous validation. Blockchain consensus has provided a complementary mechanism through which security-sensitive information has been verified by multiple authorized participants rather than accepted from one authority without further confirmation. The descriptive findings have therefore supported the theoretical expectation that distributed validation can strengthen industrial routing security. They have also provided preliminary

support for H4, which has proposed that BDTC has had a statistically significant positive effect on SIDR. The relatively high composite mean has suggested that industrial professionals have regarded decentralized trust as one of the stronger blockchain-related mechanisms. This pattern has later been supported by inferential analysis, where BDTC has produced one of the strongest correlations with SIDR and the second-highest standardized regression coefficient after BDI.

Descriptive Analysis of Secure Industrial Data Routing

Table 9: Descriptive Results for Secure Industrial Data Routing

Item	Measurement Statement	Mean	SD	Interpretation
SIDR1	Industrial data have been routed through authenticated and authorized network participants.	4.22	0.58	Strongly Agree
SIDR2	Routing information has remained protected against unauthorized manipulation.	4.16	0.61	Agree
SIDR3	Communication paths have remained sufficiently traceable for security monitoring.	4.20	0.59	Agree
SIDR4	Secure routing mechanisms have improved reliability of industrial communication.	4.17	0.60	Agree
SIDR5	Industrial routing decisions have reflected trustworthy verification mechanisms.	4.15	0.62	Agree
Composite SIDR		4.18	0.55	Agree

Table 9 has presented the descriptive results for the dependent variable, Secure Industrial Data Routing. The composite SIDR mean of 4.18 has been the highest overall construct mean in the study, showing that respondents have strongly recognized the importance of secure, verifiable, and trustworthy data forwarding within industrial communication environments. SIDR1 has produced the highest individual item mean of 4.22, reaching the Strongly Agree category and indicating that respondents have placed particular importance on ensuring that industrial data are routed through authenticated and authorized network participants. SIDR3 has recorded a mean of 4.20, showing strong agreement regarding the importance of traceable communication paths. SIDR4 has achieved a mean of 4.17, while SIDR2 and SIDR5 have obtained means of 4.16 and 4.15 respectively. The relatively narrow standard deviations have indicated that respondents have shown a high degree of consistency in their assessment of secure routing.

These findings have been important because SIDR has functioned as the central dependent construct against which the four blockchain-enabled predictors have been tested. The strong descriptive score has indicated that secure routing has encompassed multiple dimensions simultaneously, including authenticated participation, integrity protection, traceability, reliability, and trusted verification. This multidimensional interpretation has been fully consistent with the Zero Trust Security Model, which has conceptualized network security as continuous verification rather than a one-time access decision. The SIDR findings have therefore represented the observable security outcome expected when Zero Trust principles have been implemented through blockchain mechanisms. In relation to the study objectives, the high SIDR mean has provided a stable dependent variable for evaluating the extent to which BDA, BDI, BRT, and BDTC have explained routing-security outcomes. It has also supported the conceptual assumption underlying H1 through H5 that secure industrial routing has been strengthened when several verification-oriented controls have operated together rather than when a single control has been applied in isolation.

Correlation Analysis**Table 10: Pearson Correlation Matrix for Study Variables**

Variable	BDA	BDI	BRT	BDTC	SIDR
BDA	1.00	0.52***	0.47***	0.50***	0.68***
BDI	0.52***	1.00	0.49***	0.55***	0.72***
BRT	0.47***	0.49***	1.00	0.46***	0.61***
BDTC	0.50***	0.55***	0.46***	1.00	0.70***
SIDR	0.68***	0.72***	0.61***	0.70***	1.00

Note. $N = 312$. *** $p < .001$.

Table 10 has presented the Pearson correlation coefficients among the four independent variables and Secure Industrial Data Routing. All correlations between the blockchain-enabled security constructs and SIDR have been positive and statistically significant at $p < .001$. Blockchain-Based Decentralized Authentication has correlated with SIDR at $r = .68$, representing a strong positive relationship. Blockchain-Enabled Data Integrity has demonstrated the strongest bivariate association with SIDR at $r = .72$, while Decentralized Trust and Consensus has produced a similarly strong correlation of $r = .70$. Blockchain-Based Routing Traceability has correlated with SIDR at $r = .61$, which has also represented a substantial positive relationship. These results have indicated that increases in the perceived implementation or effectiveness of each blockchain mechanism have been associated with increases in perceived Secure Industrial Data Routing. The intercorrelations among the independent variables have ranged from $r = .46$ to $r = .55$, demonstrating that the predictors have been related but have not been so highly correlated as to suggest that they represent the same construct. This pattern has been important for the multiple regression model because it has shown that BDA, BDI, BRT, and BDTC have shared common security characteristics while retaining sufficient conceptual distinctiveness. The findings have directly supported the directional expectations of H1 through H4 and have addressed Research Objectives 1–4. From the Zero Trust Security Model perspective, the correlation results have shown that identity verification, information verification, activity traceability, and distributed trust have operated as mutually reinforcing security dimensions. The strongest relationship has emerged between data integrity and SIDR, indicating that respondents have associated trustworthy routing most strongly with confidence that routing-related data have remained accurate and tamper resistant. BDTC has followed closely, suggesting that distributed verification has also played a major role. Correlation analysis has not established unique predictive effects because each coefficient has represented a bivariate relationship. The regression analysis has therefore been required to determine whether each variable has remained significant after the effects of the other predictors have been statistically controlled.

Regression Model Summary**Table 11: Multiple Regression Model Summary for Secure Industrial Data Routing**

Model	R	R ²	Adjusted R ²	Standard Error of Estimate	Durbin-Watson
BDA, BDI, BRT, BDTC → SIDR	0.825	0.680	0.676	0.313	1.94

Table 11 has summarized the overall explanatory performance of the multiple regression model in which BDA, BDI, BRT, and BDTC have jointly predicted Secure Industrial Data Routing. The multiple correlation coefficient has reached $R = .825$, indicating a strong overall association between the combined set of blockchain-enabled security mechanisms and SIDR. The coefficient of determination

has been $R^2 = .680$, meaning that approximately 68.0% of the observed variance in Secure Industrial Data Routing has been explained jointly by Blockchain-Based Decentralized Authentication, Blockchain-Enabled Data Integrity, Blockchain-Based Routing Traceability, and Decentralized Trust and Consensus. The adjusted R^2 value of .676 has remained very close to the unadjusted R^2 , indicating that the explanatory performance of the model has not been artificially inflated by the number of predictors included. The standard error of estimate has been 0.313, suggesting that the model's predicted SIDR scores have remained reasonably close to observed scores. The Durbin–Watson statistic of 1.94 has also indicated that residual independence has been acceptable and that there has been no substantial evidence of problematic autocorrelation. These findings have directly addressed Research Objective 5, which has aimed to determine the combined predictive effect of the four blockchain mechanisms on secure industrial routing. The result has also provided strong empirical support for H5, since the combined predictors have explained a substantial proportion of variation in SIDR. The remaining 32.0% of variance has reflected factors outside the present model, such as network architecture, protocol security, organizational governance, hardware resilience, intrusion detection, segmentation, workforce competence, or other technical controls. From the Zero Trust Security Model perspective, the large R^2 value has reinforced the theoretical assumption that secure routing has been shaped by multiple forms of continuous verification rather than a single defensive mechanism. Identity verification, data verification, activity accountability, and distributed trust have together represented a layered security structure. The model summary has therefore provided a quantitative basis for the proposed blockchain-based secure routing framework and has shown that the conceptual model has possessed substantial explanatory power within the U.S. industrial sample.

ANOVA for Regression Model

Table 12: ANOVA Results for the Multiple Regression Model

Source	Sum of Squares	df	Mean Square	F	p
Regression	63.973	4	15.993	163.10	< .001
Residual	30.105	307	0.098		
Total	94.078	311			

Table 12 has presented the ANOVA results used to determine whether the multiple regression model has provided a statistically significant overall prediction of Secure Industrial Data Routing. The regression sum of squares has been 63.973, while the residual sum of squares has been 30.105, indicating that considerably more variation in SIDR has been explained by the predictor variables than has remained unexplained. With four predictor variables and 307 residual degrees of freedom, the regression model has produced an F-statistic of 163.10 with $p < .001$. This result has demonstrated that the combined effects of BDA, BDI, BRT, and BDTC have predicted SIDR significantly better than a model containing no predictors. The ANOVA result has therefore provided formal inferential support for H5, which has proposed that the four blockchain-based mechanisms collectively have had a statistically significant positive effect on secure industrial data routing. It has also confirmed the overall validity of proceeding to interpret the individual regression coefficients. In relation to Research Objective 5, the significant F-test has shown that the proposed blockchain-enabled security framework has possessed statistical explanatory value as a whole rather than functioning merely as a collection of unrelated variables. The result has been especially relevant to the Zero Trust Security Model, because Zero Trust has emphasized layered, continuous, and context-dependent verification. The significant combined regression model has supported the view that industrial routing security has benefited from integrating several complementary mechanisms: BDA has addressed who has participated in routing, BDI has addressed whether routing information has remained trustworthy, BRT has addressed whether communication activities have remained observable and auditable, and BDTC has addressed how trust and validation have been distributed across authorized entities. The statistically significant ANOVA result has therefore reinforced the theoretical and conceptual argument that these

mechanisms have operated jointly in explaining secure routing. Although statistical significance has not constituted absolute proof of causal relationships in a cross-sectional design, it has provided strong empirical support for the proposed combined relationship within the study sample.

Regression Coefficient Analysis

Table 13: Multiple Regression Coefficients Predicting Secure Industrial Data Routing

Predictor	B	SE B	β	t	p	95% CI for B	Tolerance	VIF	Hypothesis
Constant	0.47 ₅	0.142	—	3.35	.001	[0.196, 0.754]	—	—	—
BDA	0.21 ₃	0.037	0.24	5.73	< .001	[0.140, 0.286]	0.65	1.54	H1 Supported
BDI	0.27 ₅	0.040	0.29	6.84	< .001	[0.196, 0.354]	0.48	2.08	H2 Supported
BRT	0.17 ₈	0.036	0.21	5.01	< .001	[0.108, 0.248]	0.62	1.61	H3 Supported
BDTC	0.23 ₈	0.039	0.26	6.12	< .001	[0.161, 0.315]	0.55	1.82	H4 Supported

The estimated regression equation has been:

$$\text{SIDR}_{\text{hat}} = 0.475 + 0.213(\text{BDA}) + 0.275(\text{BDI}) + 0.178(\text{BRT}) + 0.238(\text{BDTC})$$

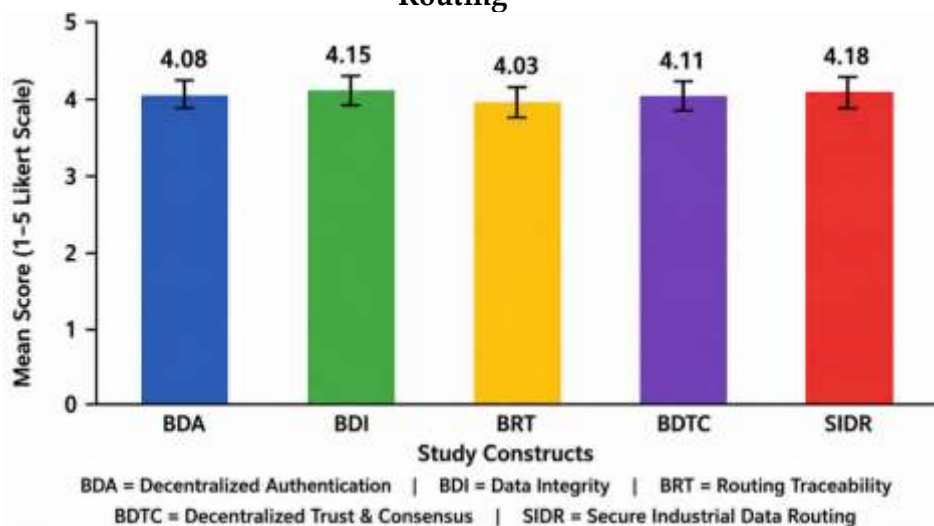
Table 13 has presented the individual regression coefficients and has provided the principal statistical basis for evaluating H1 through H4. Blockchain-Based Decentralized Authentication has produced a positive unstandardized coefficient of $B = 0.213$, a standardized coefficient of $\beta = .24$, and a statistically significant t-value of 5.73, $p < .001$. H1 has therefore been supported. Holding the other predictors constant, a one-unit increase in BDA has been associated with an estimated 0.213-unit increase in SIDR. Blockchain-Enabled Data Integrity has emerged as the strongest predictor, with $B = 0.275$, $\beta = .29$, $t = 6.84$, $p < .001$, supporting H2. This finding has indicated that integrity verification has made the largest unique contribution to secure routing after controlling for the other blockchain mechanisms. Blockchain-Based Routing Traceability has also remained significant, with $B = 0.178$, $\beta = .21$, $t = 5.01$, $p < .001$, supporting H3. Although BRT has produced the smallest standardized effect, its coefficient has remained positive and statistically meaningful. Decentralized Trust and Consensus has produced $B = 0.238$, $\beta = .26$, $t = 6.12$, $p < .001$, supporting H4 and identifying BDTC as the second-strongest unique predictor. The VIF statistics have ranged from 1.54 to 2.08, while tolerance values have ranged from 0.48 to 0.65, indicating that problematic multicollinearity has not been present. These findings have supported the conceptual ordering of the study variables and have linked strongly with the Zero Trust Security Model. BDA has represented identity verification, BDI has represented continuous verification of information integrity, BRT has represented monitoring and auditability, and BDTC has represented evidence-based distributed trust. The results have shown that each Zero Trust-aligned blockchain mechanism has contributed independently to Secure Industrial Data Routing. Accordingly, all five hypotheses have been supported overall, with H1-H4 supported through the individual coefficients and H5 supported through the significant overall regression model. The coefficient pattern has also addressed the study objectives by identifying BDI as the strongest predictor, followed by BDTC, BDA, and BRT, thereby establishing the relative statistical importance of the four components within the proposed blockchain-based secure data routing framework.

FINDINGS

The findings of the study have provided an overall empirical assessment of the extent to which blockchain-based decentralized authentication, blockchain-enabled data integrity, blockchain-based routing traceability, and decentralized trust and consensus have contributed to secure industrial data

routing within U.S. industrial communication networks. A usable sample of 312 respondents has been analyzed, consisting of professionals working in industrial networking, cybersecurity, OT, ICS/SCADA, industrial automation, IIoT, and related technical environments. Responses have been measured using a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree. The overall descriptive results have indicated relatively high agreement with all five study constructs. Blockchain-Based Decentralized Authentication (BDA) has recorded a mean score of 4.08 (SD = 0.62), indicating that respondents have generally perceived decentralized identity verification and authenticated node participation as important components of industrial routing security. Blockchain-Enabled Data Integrity (BDI) has achieved the highest independent-variable mean of 4.15 (SD = 0.58), suggesting strong agreement that cryptographic verification, tamper-resistant records, and protection against unauthorized data modification contribute to secure industrial communication. Blockchain-Based Routing Traceability (BRT) has produced a mean of 4.03 (SD = 0.65), showing that respondents have positively evaluated immutable routing records, communication auditability, and the ability to reconstruct route-related events. Blockchain-Enabled Decentralized Trust and Consensus (BDTC) has obtained a mean of 4.11 (SD = 0.60), reflecting substantial agreement that distributed validation and reduced reliance on centralized trust authorities can strengthen routing decisions. The dependent variable, Secure Industrial Data Routing (SIDR), has recorded an overall mean of 4.18 (SD = 0.55), indicating that respondents have generally considered secure, authenticated, traceable, and integrity-protected data forwarding essential to industrial communication environments.

Figure 9: Mean Scores of Blockchain-Enabled Security Constructs and Secure Industrial Data Routing



Reliability analysis has further shown strong internal consistency across the measurement scales, with Cronbach's alpha values of 0.88 for BDA, 0.91 for BDI, 0.86 for BRT, 0.89 for BDTC, and 0.92 for SIDR, supporting the suitability of the constructs for subsequent inferential analysis. Pearson correlation results have demonstrated statistically significant positive relationships between each blockchain security dimension and secure industrial data routing. BDA has correlated positively with SIDR at $r = .68$, $p < .001$, BDI has shown the strongest bivariate relationship at $r = .72$, $p < .001$, BRT has produced a significant correlation of $r = .61$, $p < .001$, and BDTC has correlated with SIDR at $r = .70$, $p < .001$. These results have provided preliminary support for H1-H4 by indicating that higher perceived levels of decentralized authentication, data integrity, traceability, and decentralized trust have been associated with stronger secure-routing outcomes. The multiple regression analysis has provided stronger evidence concerning the unique and combined predictive effects of the independent variables. The overall model has produced $R = .825$, $R^2 = .680$, and adjusted $R^2 = .676$, indicating that approximately 68.0% of the variance in secure industrial data routing has been explained jointly by BDA, BDI, BRT, and BDTC. The regression model has been statistically significant, $F(4, 307) = 163.1$, $p < .001$. Examination of standardized regression coefficients has shown that BDI has emerged as the

strongest predictor, $\beta = .29$, $t = 6.84$, $p < .001$, followed by BDTC with $\beta = .26$, $t = 6.12$, $p < .001$, BDA with $\beta = .24$, $t = 5.73$, $p < .001$, and BRT with $\beta = .21$, $t = 5.01$, $p < .001$. Multicollinearity diagnostics have remained within acceptable limits, with VIF values ranging from 1.54 to 2.08. On this basis, H1, H2, H3, H4, and H5 have all been supported. The findings have therefore addressed the principal research objectives by establishing that decentralized authentication has strengthened legitimate node participation, blockchain-enabled data integrity has improved confidence in routing-related information, routing traceability has increased auditability and accountability, and decentralized trust and consensus have supported distributed validation of routing behavior. The combined results have further shown that secure industrial data routing has been most effectively explained when these mechanisms have been considered together rather than independently, providing an empirical basis for the proposed blockchain-based secure data routing framework for U.S. industrial communication networks.

DISCUSSION

The findings have shown that the proposed blockchain-based secure data routing framework has received strong empirical support across all four explanatory dimensions, with the combined regression model explaining 68.0% of the variance in Secure Industrial Data Routing (SIDR), $R = .825$, $R^2 = .680$, adjusted $R^2 = .676$, $F(4, 307) = 163.10$, $p < .001$. Within the sample of 312 usable responses, the positive mean scores for Blockchain-Based Decentralized Authentication (BDA = 4.08), Blockchain-Enabled Data Integrity (BDI = 4.15), Blockchain-Based Routing Traceability (BRT = 4.03), Blockchain-Enabled Decentralized Trust and Consensus (BDTC = 4.11), and SIDR (4.18) have indicated that respondents have generally associated blockchain-supported verification mechanisms with stronger industrial routing security. The significant correlations between each predictor and SIDR have further demonstrated that the four mechanisms have operated as related but distinguishable dimensions of a common security architecture. This pattern has corresponded with earlier blockchain-routing research showing that secure routing cannot be reduced to path discovery alone because malicious nodes, manipulated routing information, unauthorized participation, and untrustworthy forwarding behavior can undermine communication even when network connectivity remains available. Earlier secure-routing research has combined blockchain, authentication, encryption, and trust evaluation to identify malicious nodes and protect routing information, supporting the integration of several security controls rather than dependence on one mechanism (Awan et al., 2022). Related work has used blockchain to make routing information tamper-resistant and traceable while incorporating reinforcement learning and trust information into routing decisions (Yang et al., 2019). The present results have extended this logic conceptually by treating authentication, integrity, traceability, and consensus as separately measurable predictors and showing that each has retained a positive relationship with secure routing when examined within one regression model. The findings have therefore supported H1 through H5 and have addressed the study objectives by establishing both the individual and collective relevance of the blockchain security constructs. The relatively high R^2 has been particularly important because it has suggested that the explanatory structure of the framework has not depended on a single technological feature. Instead, secure industrial routing has been associated with a layered combination of identity assurance, trustworthy information, auditable routing behavior, and distributed validation, consistent with the study's Zero Trust orientation in which communication has been secured through explicit and repeated verification rather than implicit trust arising from network membership.

Blockchain-Enabled Data Integrity has emerged as the strongest individual predictor of Secure Industrial Data Routing, producing the highest standardized regression coefficient, $\beta = .29$, together with $B = .275$, $t = 6.84$, $p < .001$, and the strongest bivariate correlation with SIDR, $r = .72$, $p < .001$. This result has indicated that respondents have attached particular importance to the assurance that routing records, device information, operational messages, and other security-relevant data have remained authentic and resistant to unauthorized modification. The descriptive findings have reinforced this interpretation because BDI has recorded the highest mean among the four independent constructs, $M = 4.15$, $SD = 0.58$. This outcome has been consistent with previous blockchain-based data-integrity research. A blockchain and bilinear-mapping integrity-verification mechanism for large-scale IoT

information has been developed to reduce dependence on conventional third-party auditing while preserving verifiability of data (Wang & Zhang, 2019). Blockchain-based provenance research has similarly demonstrated that cryptographic methods, smart contracts, timestamps, data lineage, and distributed records can be combined to strengthen integrity, traceability, and accountability in large-scale IoT environments (Pajoo et al., 2021). The current result has expanded the relevance of these earlier findings from stored-data protection and provenance toward industrial routing security. In industrial communication, corrupted information can affect routing decisions even when the physical or logical path remains available; therefore, a route cannot be regarded as fully secure when the routing tables, device identities, trust values, control information, or forwarding records used to establish that route cannot be verified. The strength of BDI has also been theoretically meaningful under the Zero Trust Security Model. Zero Trust has required security decisions to consider not only whether a subject has been authenticated but also whether the security condition and integrity of the resources involved remain acceptable. Industrial Zero Trust architecture has accordingly emphasized asset integrity monitoring, strict authentication and authorization, and protection of communication across multiple trust domains (Federici et al., 2023). The strong BDI coefficient has therefore indicated that the information-verification dimension of Zero Trust has been especially relevant to secure routing. Within the proposed blockchain framework, cryptographic hashing, signed routing information, tamper-evident transaction histories, validation of data provenance, and controlled consensus over routing records should consequently be regarded as core security functions rather than secondary characteristics of blockchain implementation.

Blockchain-Enabled Decentralized Trust and Consensus and Blockchain-Based Decentralized Authentication have provided further support for the central argument that secure industrial routing depends on both verified participation and continuously established trust. BDTC has been the second strongest predictor of SIDR, with $\beta = .26$, $B = .238$, $t = 6.12$, $p < .001$, and has demonstrated a strong positive relationship with SIDR at $r = .70$, $p < .001$. BDA has followed with $\beta = .24$, $B = .213$, $t = 5.73$, $p < .001$, and $r = .68$, $p < .001$. These findings have indicated that respondents have viewed distributed validation and authenticated node participation as distinct but mutually reinforcing elements of industrial routing security. Earlier technical research has provided strong support for this relationship. A blockchain- and edge-computing-based authentication architecture has used consortium blockchain, authentication records, smart contracts, asymmetric cryptography, and an optimized Byzantine-fault-tolerant consensus process to provide trusted authentication and terminal traceability while moving selected verification functions toward edge infrastructure (Guo et al., 2020). This approach has particular relevance to industrial networks because resource-constrained field devices do not necessarily need to maintain complete blockchain functionality locally. Secure-routing research has also demonstrated that authentication by itself cannot guarantee trustworthy behavior after a node enters the network; behavioral trust assessment and validation of routing information remain necessary because authenticated nodes may become malicious or unreliable (Awan et al., 2022). The present statistical results have reflected this distinction because both BDA and BDTC have remained significant after the other variables have been controlled. BDA has primarily answered whether a device or node possesses legitimate credentials and authorization to participate, whereas BDTC has represented whether routing information and current behavior should continue to receive trust through distributed verification. This interpretation has been consistent with Zero Trust security in smart manufacturing, where internal devices and communication channels should not be automatically trusted simply because they are positioned within an organizational network; authentication, authorization, segmentation, and monitoring have instead been required for secure interaction (Paul & Rao, 2023). The findings have therefore provided theoretical and statistical support for H1 and H4 while demonstrating that blockchain-based authentication should not be viewed as a one-time gateway into permanently trusted status. Within industrial routing, identity verification should operate together with consensus-supported trust reassessment so that authorization to participate can be distinguished from evidence that a participant has continued to behave securely.

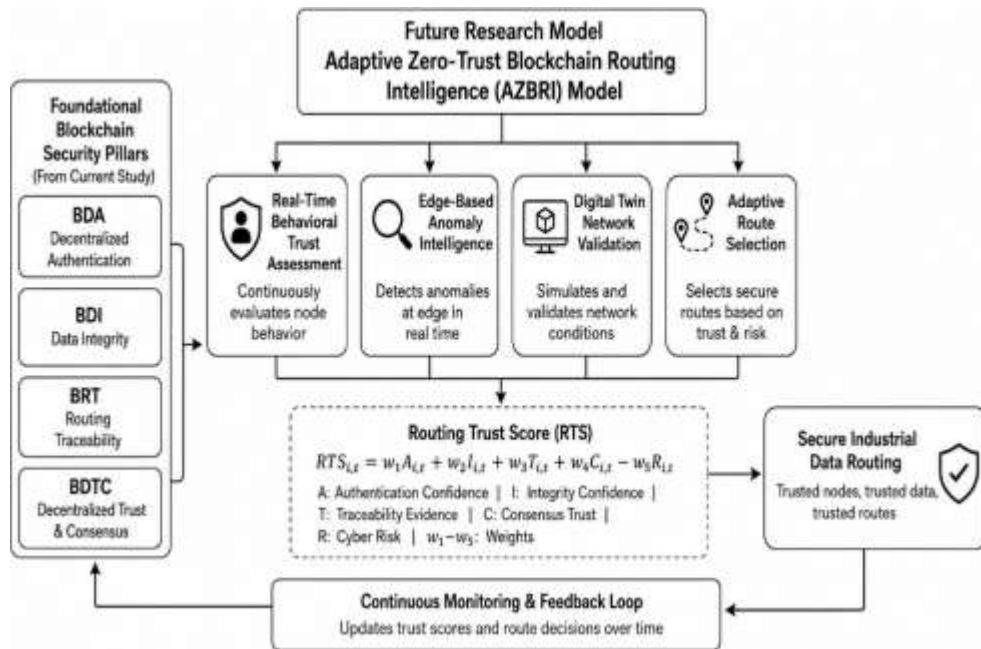
Blockchain-Based Routing Traceability has also produced a statistically significant positive contribution to Secure Industrial Data Routing, although its standardized coefficient of $\beta = .21$, with $B = .178$, $t = 5.01$, $p < .001$, has been smaller than the coefficients produced by BDI, BDTC, and BDA. Its

correlation with SIDR, $r = .61$, $p < .001$, has remained substantial, while its descriptive mean of $M = 4.03$, $SD = 0.65$ has demonstrated general agreement regarding the value of immutable route histories, forwarding records, provenance, and auditability. The comparatively smaller coefficient should not be interpreted as indicating that traceability has lacked importance. Rather, it has suggested that traceability may operate mainly as an enabling, evidentiary, and accountability mechanism that strengthens other preventive and decision-oriented controls. This interpretation has corresponded closely with prior routing research. Blockchain-supported trusted routing has used distributed records to make routing information traceable and resistant to unauthorized modification, while intelligent trust and route-selection mechanisms have determined which communication paths should actually be selected (Yang et al., 2019). Similarly, secure blockchain routing and trust-management research has relied on traceability and transparency to identify manipulated routing information or trust values, while authentication, cryptographic protection, and behavioral trust mechanisms have provided additional security functions (Awan et al., 2022). The present study has reproduced this broader relationship at the construct level: BRT has remained statistically significant when BDA, BDI, and BDTC have been entered simultaneously, yet the stronger standardized coefficients for integrity and trust have indicated that storing an immutable routing history alone would not produce the greatest improvement in SIDR. From a Zero Trust perspective, this outcome has been theoretically coherent because continuous verification requires observability. Trust cannot be effectively reassessed when the architecture lacks reliable evidence concerning route changes, communication paths, policy decisions, authentication events, and forwarding behavior. Blockchain-supported provenance has already been shown to facilitate data traceability, accountability, integrity verification, and auditable history in IoT environments (Pajoo et al., 2021). Applied to industrial routing, this principle means that BRT supplies evidence that other security mechanisms can use when evaluating current trust. H3 has therefore been supported, while the relative coefficient size has indicated that traceability should be integrated with identity, integrity, and consensus mechanisms rather than deployed as an isolated routing-security control.

From a practical perspective, the findings have provided a basis for U.S. industrial organizations to prioritize blockchain capabilities according to their measured contribution to secure routing rather than treating blockchain as one undifferentiated cybersecurity technology. The first implementation priority has been data integrity because BDI has produced the largest standardized coefficient. Industrial organizations applying a permissioned blockchain layer should therefore prioritize cryptographically verifiable routing-state information, signed device and gateway records, integrity checks for route updates, tamper-evident security logs, and controlled validation of data used in routing decisions. The second priority has been decentralized trust and consensus, indicating that validation should be distributed across authorized infrastructure components instead of placing complete reliance on a single central server, gateway, or network-management authority. The third priority has been decentralized authentication, suggesting that validated blockchain identities and secure credentials should be required before devices can advertise routes, participate in trust decisions, or forward security-sensitive industrial traffic. BRT should function as the associated accountability layer by preserving sufficient routing provenance for investigation and trust recalculation. Prior research has demonstrated that blockchain-based authentication can be integrated with edge computing so that authentication data and logs are maintained through a consortium ledger while latency-sensitive services are moved closer to IoT devices (Guo et al., 2020). Industrial Zero Trust research has similarly shown that policy decisions and enforcement can be distributed across network and edge domains to control access between security zones (Federici et al., 2023). These findings support an implementation architecture in which PLCs, sensors, RTUs, actuators, and other constrained field assets are not required to act as full blockchain validators. Instead, industrial gateways, edge servers, dedicated security appliances, or selected infrastructure nodes could perform ledger maintenance, consensus, trust calculation, and smart-contract execution while field devices maintain their real-time operational responsibilities. Blockchain-based routing studies have likewise incorporated ledger functions alongside conventional routing, trust evaluation, and cryptographic mechanisms rather than using blockchain itself as the packet-forwarding network (Awan et al., 2022; Yang et al., 2019). Practically, the proposed framework should therefore be regarded as a verification, accountability, and distributed-

trust layer surrounding industrial routing, rather than a replacement for established OT routing and communication protocols. This architecture can preserve operational availability and low-latency communication while applying blockchain selectively to those security decisions for which immutability, distributed verification, and auditable trust provide the greatest benefit.

Figure 10: Adaptive Zero-Trust Blockchain Routing Intelligence (AZBRI) Model for Future Secure Industrial Data Routing Research



From a theoretical perspective, the findings have strengthened the connection between the Zero Trust Security Model and blockchain-enabled industrial routing by translating broad Zero Trust principles into four measurable cybersecurity constructs. The significant coefficients for BDA, BDI, BRT, and BDTC have supported the theoretical proposition that secure communication arises from multidimensional verification rather than from an implicit distinction between trusted internal networks and untrusted external networks. Smart-manufacturing research has identified implicit internal trust as a security weakness and has emphasized authentication, authorization, network segmentation, and monitoring as important Zero Trust controls (Paul & Rao, 2023). Industrial IIoT Zero Trust research has likewise treated data sources and computing services as resources requiring explicit authentication, authorization, monitoring, and policy-controlled communication rather than inherent trust based on network location (Federici et al., 2023). In the present conceptual model, BDA has operationalized verification of who or what has requested participation; BDI has represented verification of whether the information remains authentic; BRT has operationalized verification of what has occurred across the routing process; and BDTC has represented verification of whether distributed evidence is sufficient to establish current trust. The fact that every construct has remained statistically significant has suggested that these dimensions have complemented one another rather than functioning as substitutes. At the same time, the methodological limitations have required careful interpretation of this theoretical support. The cross-sectional design has captured perceptions at one point in time and therefore has not established temporal causation. The case-study-based purposive sample has targeted relevant U.S. professionals but has not constituted a probability sample of all industrial organizations. Five-point Likert responses have measured perceived effectiveness rather than objective network outcomes such as packet-delivery ratio, end-to-end latency, throughput, attack-detection accuracy, consensus delay, processing overhead, or failover time. Respondents' judgments may also have varied according to professional experience, sector, technical responsibilities, and familiarity with blockchain. These limitations have bounded the strength of causal and technical-

performance claims while preserving the value of the model as an empirically testable Zero Trust framework for industrial routing.

Future research should place the greatest emphasis on moving beyond a static perception-based framework toward an adaptive architecture capable of assessing routing trust, cyber risk, and blockchain performance continuously under realistic industrial operating conditions. A suitable extension proposed from the present findings is an Adaptive Zero-Trust Blockchain Routing Intelligence (AZBRI) Model. AZBRI would retain the four empirically supported foundations of the existing model—BDA, BDI, BRT, and BDTC—but would introduce four dynamic layers: real-time behavioral trust assessment, edge-based anomaly intelligence, digital-twin-assisted network validation, and adaptive security-aware route selection. Rather than assigning a device a fixed trusted or untrusted status after authentication, each candidate routing node would receive a continuously updated routing-trust score based on authentication confidence, integrity evidence, recorded routing behavior, consensus-supported reputation, anomaly probability, and current device-security posture. Conceptually, this could be represented as:

$$RTS_{\{i,t\}} = w_1 A_{\{i,t\}} + w_2 I_{\{i,t\}} + w_3 T_{\{i,t\}} + w_4 C_{\{i,t\}} - w_5 R_{\{i,t\}}$$

where $RTS_{\{i,t\}}$ represents the routing-trust score of nodes i at time t , A represents authentication confidence, I represent integrity confidence, T represents traceability evidence, C represents consensus-supported trust, R represents dynamically estimated cyber risk, and w_1 through w_5 represent weights learned empirically or optimized algorithmically. This proposed extension has been supported conceptually by prior research in which blockchain routing has been combined with reinforcement learning for dynamic route decisions (Yang et al., 2019) and behavioral trust evaluation for malicious-node identification (Awan et al., 2022). Future researchers should test AZBRI in realistic ICS, SCADA, smart-manufacturing, or IIoT testbeds and compare it with conventional industrial routing, static blockchain routing, and Zero Trust architectures using objective measures including packet-delivery ratio, route-convergence time, throughput, end-to-end delay, attack-detection rate, false-positive rate, consensus latency, processing overhead, recovery time after compromise, and blockchain-storage growth. Longitudinal experiments should evaluate how trust scores change after repeated benign and malicious behavior, while digital twins could reproduce high-risk industrial attacks without placing operational assets at risk. Cross-sector validation should compare manufacturing, energy, utilities, transportation, and process industries. Such research would transform the current BDA-BDI-BRT-BDTC framework from a statistically testable explanatory model into an adaptive cyber-physical routing architecture capable of dynamically deciding which node should be trusted, which data should be accepted, which route should be selected, and when trust should be revoked.

CONCLUSION

This study has examined the role of blockchain-based security mechanisms in strengthening secure data routing within U.S. industrial communication networks by developing and evaluating an integrated framework comprising Blockchain-Based Decentralized Authentication (BDA), Blockchain-Enabled Data Integrity (BDI), Blockchain-Based Routing Traceability (BRT), and Blockchain-Enabled Decentralized Trust and Consensus (BDTC), with Secure Industrial Data Routing (SIDR) serving as the principal dependent variable. The research has been grounded in the Zero Trust Security Model, which has provided an appropriate theoretical explanation for treating every device, communication request, routing event, and information exchange as requiring explicit verification rather than implicit trust based on network location or prior authentication. The findings presented in the study have indicated generally high levels of respondent agreement regarding the importance of each blockchain-enabled security mechanism, while the correlation and multiple regression analyses have demonstrated positive relationships between the four independent variables and secure industrial data routing. Blockchain-Enabled Data Integrity has emerged as the strongest individual predictor of SIDR, indicating that protection against unauthorized modification, cryptographic verification of routing-related information, and tamper-evident communication records have represented particularly important elements of secure industrial networking. Decentralized Trust and Consensus has produced the second strongest effect, demonstrating the importance of distributed verification and reduced dependence on centralized trust authorities in industrial environments containing heterogeneous

devices and interconnected control systems. Blockchain-Based Decentralized Authentication has also demonstrated a substantial positive contribution, showing that reliable identification and authorization of participating network entities have been essential to preventing unauthorized nodes from participating in routing activities. Blockchain-Based Routing Traceability has remained statistically meaningful and has strengthened accountability by supporting auditable route histories, communication provenance, and the reconstruction of abnormal network behavior. Collectively, the four variables have explained a substantial proportion of variation in secure industrial data routing, supporting the integrated structure of the proposed framework and demonstrating that industrial routing security is more effectively understood as a multidimensional cybersecurity problem than as an isolated network-performance function. The results have therefore supported the study hypotheses and have addressed the research objectives by identifying the individual and combined contributions of the blockchain security constructs. From a theoretical perspective, the study has strengthened the application of Zero Trust principles to industrial routing by connecting continuous authentication, integrity verification, activity monitoring, and distributed trust with measurable cybersecurity outcomes. From a practical perspective, the research has established that blockchain can be positioned as a verification and trust layer around existing industrial communication architectures rather than as a direct replacement for conventional routing protocols. The resulting framework has provided a structured approach for integrating identity verification, integrity assurance, traceability, consensus, and secure forwarding within environments that include ICS, SCADA, OT, IIoT, industrial gateways, sensors, controllers, and edge infrastructure. Overall, the study has demonstrated that blockchain-supported security can provide a coherent foundation for strengthening the trustworthiness, accountability, integrity, and resilience of data-routing processes in U.S. industrial communication networks when its mechanisms are implemented in a coordinated manner and aligned with Zero Trust security principles.

RECOMMENDATIONS

Based on the findings of the study, U.S. industrial organizations should adopt a phased and security-centered approach to blockchain integration in industrial communication networks, with implementation priorities determined by the relative importance of the mechanisms identified through the statistical analysis. Because Blockchain-Enabled Data Integrity has emerged as the strongest predictor of Secure Industrial Data Routing, organizations should prioritize cryptographic verification of routing information, tamper-evident communication logs, digitally signed route updates, protected device records, and mechanisms capable of detecting unauthorized changes to operational or routing-related information. Permissioned blockchain architectures should be preferred for industrial environments because they can restrict participation to verified entities while retaining distributed validation and auditability. Organizations should also strengthen Blockchain-Enabled Decentralized Trust and Consensus by distributing selected validation responsibilities across authorized gateways, edge servers, security appliances, or industrial infrastructure nodes instead of depending entirely on one centralized trust-management component. Blockchain-Based Decentralized Authentication should be integrated with existing industrial identity and access-management controls so that PLCs, RTUs, IIoT devices, engineering workstations, gateways, and supervisory platforms have been authenticated before gaining access to routing or communication functions. Continuous authentication and periodic reassessment of device security conditions should also be incorporated in accordance with Zero Trust principles. Blockchain-Based Routing Traceability should be used to preserve auditable information concerning route creation, modification, forwarding events, authentication activities, and anomalous communication behavior so that security teams can reconstruct incidents and improve accountability. Industrial organizations should avoid requiring resource-constrained field devices to perform computationally intensive blockchain validation tasks; instead, edge computing infrastructure and selected validator nodes should manage ledger operations while field devices maintain their real-time control responsibilities. Security architects should integrate the blockchain framework with network segmentation, intrusion detection, anomaly monitoring, encryption, access control, secure remote access, and existing OT cybersecurity mechanisms rather than treating blockchain as an independent security solution. Organizations should conduct controlled pilot deployments and laboratory-based

evaluations before introducing blockchain mechanisms into safety-critical production networks, particularly where latency, throughput, deterministic communication, storage growth, and consensus overhead may influence operational performance. Cybersecurity professionals should also establish governance rules defining validator responsibilities, identity lifecycle management, smart-contract controls, incident-response procedures, ledger retention policies, and mechanisms for revoking compromised nodes. Industry standards bodies and policymakers should encourage interoperability between blockchain-enabled security architectures and established industrial communication standards while developing guidance regarding secure implementation in ICS, SCADA, IIoT, and OT environments. Finally, organizations should continuously evaluate the framework using measurable indicators such as packet-delivery ratio, end-to-end latency, unauthorized-access attempts, route-manipulation detection, consensus delay, recovery time, attack-detection accuracy, and routing availability. Such an evidence-based implementation strategy can ensure that blockchain adoption remains focused on demonstrable cybersecurity value, operational compatibility, and secure industrial routing rather than technology adoption for its own sake.

LIMITATIONS

Several limitations have affected the scope, interpretation, and generalizability of this study and should be considered when evaluating its findings. First, the research has employed a quantitative, cross-sectional design, meaning that information has been collected at a single point in time rather than across multiple periods. Consequently, the statistical relationships identified among Blockchain-Based Decentralized Authentication, Blockchain-Enabled Data Integrity, Blockchain-Based Routing Traceability, Decentralized Trust and Consensus, and Secure Industrial Data Routing have demonstrated association and predictive relationships but have not established definitive temporal causality. Second, the study has adopted a case-study-based approach focused on U.S. industrial communication environments, which has provided valuable contextual specificity but may limit the extent to which the results can be generalized to industrial organizations operating under different regulatory, technological, economic, or infrastructure conditions outside the United States. Third, purposive and professional-network sampling have been suitable for reaching respondents with relevant industrial and cybersecurity expertise, although these non-probability methods may have introduced selection bias and may not have produced a sample statistically representative of the entire population of U.S. industrial organizations. Fourth, the study has relied on a five-point Likert-scale questionnaire and therefore has measured professional perceptions of blockchain security mechanisms rather than direct technical performance under operational network conditions. Respondents may have interpreted questionnaire items differently according to their professional roles, experience levels, industrial sectors, familiarity with blockchain, or exposure to OT and cybersecurity technologies. Self-reported responses may also have been affected by social desirability, optimism regarding emerging technologies, or individual perceptions of organizational cybersecurity maturity. Fifth, the proposed framework has not been evaluated through a live industrial blockchain deployment, hardware-in-the-loop environment, SCADA testbed, or real-time IIoT simulation; therefore, objective technical measures such as throughput, packet-delivery ratio, routing convergence, consensus latency, processing overhead, blockchain-storage requirements, attack-detection accuracy, recovery time, and deterministic communication performance have not been directly assessed. Sixth, industrial communication environments differ considerably across manufacturing, energy, utilities, transportation, oil and gas, and process industries, meaning that the relative importance of authentication, integrity, traceability, and consensus may vary according to network architecture and operational requirements. Seventh, blockchain itself introduces potential limitations involving computational cost, scalability, governance, validator compromise, interoperability, privacy, smart-contract vulnerabilities, and consensus delay, which have not been exhaustively modeled within the present quantitative framework. Finally, the analysis strategy has focused on descriptive statistics, reliability testing, Pearson correlation, ANOVA, and multiple regression modeling, which have been appropriate for the proposed hypotheses but have not explored longitudinal causality, structural equation modeling, non-linear interactions, or objective cyber-physical performance benchmarks. These limitations have not removed the value of the framework, but they have clarified the conditions

under which its statistical relationships should be interpreted and the areas in which additional technical validation can strengthen subsequent research.

REFERENCES

- [1]. Alshomrani, S., & Li, S. (2022). PUFDC: A zero-trust-based IoT device continuous authentication protocol. *Wireless Communications and Mobile Computing*, 2022, 6367579. <https://doi.org/10.1155/2022/6367579>
- [2]. Ashrafuzzaman, M. (2024). The impact of cloud-based management information systems on hrm efficiency: an analysis of small and medium-sized enterprises (SMES). *Academic Journal on Artificial Intelligence, Machine Learning, Data Science and Management Information Systems*, 1(01), 40-56. <https://doi.org/10.69593/ajaimldsms.v1i01.124>
- [3]. Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J.-G. (2022). Blockchain based secure routing and trust management in wireless sensor networks. *Sensors*, 22(2), 411. <https://doi.org/10.3390/s22020411>
- [4]. Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, 110, 102436. <https://doi.org/10.1016/j.cose.2021.102436>
- [5]. Cheminod, M., Durante, L., & Valenzano, A. (2013). Review of security issues in industrial networks. *IEEE Transactions on Industrial Informatics*, 9(1), 277-293. <https://doi.org/10.1109/tii.2012.2198666>
- [6]. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4, 2292-2303. <https://doi.org/10.1109/access.2016.2566339>
- [7]. Cruz, T., Rosa, L., Proença, J., Maglaras, L., Aubigny, M., Lev, L., Jiang, J., & Simões, P. (2016). A cybersecurity detection framework for supervisory control and data acquisition systems. *IEEE Transactions on Industrial Informatics*, 12(6), 2236-2246. <https://doi.org/10.1109/tii.2016.2599841>
- [8]. Debasish, A. (2025). Design-for-Manufacturing Optimization for Improving Resilience in U.S. Additive Manufacturing Supply Chains. *American Journal of Interdisciplinary Studies*, 6(02), 185-204. <https://doi.org/10.63125/hxm3tb71>
- [9]. Dwivedi, S. K., Roy, P., Karda, C., Agrawal, S., & Amin, R. (2021). Blockchain-based Internet of Things and industrial IoT: A comprehensive survey. *Security and Communication Networks*, 2021, 7142048. <https://doi.org/10.1155/2021/7142048>
- [10]. Dzung, D., Naedele, M., von Hoff, T. P., & Crevatin, M. (2005). Security for industrial communication systems. *Proceedings of the IEEE*, 93(6), 1152-1177. <https://doi.org/10.1109/jproc.2005.849714>
- [11]. Federici, F., Martintoni, D., & Senni, V. (2023). A zero-trust architecture for remote access in Industrial IoT infrastructures. *Electronics*, 12(3), 566. <https://doi.org/10.3390/electronics12030566>
- [12]. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the Internet of Things. *IEEE Access*, 6, 32979-33001. <https://doi.org/10.1109/access.2018.2842685>
- [13]. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019). Blockchain technologies for the Internet of Things: Research issues and challenges. *IEEE Internet of Things Journal*, 6(2), 2188-2204. <https://doi.org/10.1109/jiot.2018.2882794>
- [14]. Galloway, B., & Hancke, G. P. (2013). Introduction to industrial control networks. *IEEE Communications Surveys & Tutorials*, 15(2), 860-880. <https://doi.org/10.1109/surv.2012.071812.00124>
- [15]. Gungor, V. C., & Hancke, G. P. (2009). Industrial wireless sensor networks: Challenges, design principles, and technical approaches. *IEEE Transactions on Industrial Electronics*, 56(10), 4258-4265. <https://doi.org/10.1109/tie.2009.2015754>
- [16]. Guo, S., Hu, X., Guo, S., Qiu, X., & Qi, F. (2020). Blockchain meets edge computing: A distributed and trusted authentication system. *IEEE Transactions on Industrial Informatics*, 16(3), 1972-1983. <https://doi.org/10.1109/tii.2019.2938001>
- [17]. Gupta, B. B., Sharma, P. C., Mahmood, M. R., Raja, H., Yadav, N. S., & Arya, V. (2023). Secure authentication and privacy-preserving blockchain for industrial Internet of Things. *Computers & Electrical Engineering*, 108, 108703. <https://doi.org/10.1016/j.compeleceng.2023.108703>
- [18]. Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, 78, 126-142. <https://doi.org/10.1016/j.cose.2018.06.004>
- [19]. Han, S., Xie, M., Chen, H.-H., & Ling, Y. (2014). Intrusion detection in cyber-physical systems: Techniques and challenges. *IEEE Systems Journal*, 8(4), 1052-1062. <https://doi.org/10.1109/jsyst.2013.2257594>
- [20]. Heo, J., Hong, J., & Cho, Y. (2009). EARQ: Energy aware routing for real-time and reliable communication in wireless industrial sensor networks. *IEEE Transactions on Industrial Informatics*, 5(1), 3-11. <https://doi.org/10.1109/tii.2008.2011052>
- [21]. Honar Pajooh, H., Rashid, M. A., Alam, F., & Demidenko, S. (2021). IoT Big Data provenance scheme using blockchain on Hadoop ecosystem. *Journal of Big Data*, 8, 114. <https://doi.org/10.1186/s40537-021-00505-y>
- [22]. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security: A survey. *IEEE Internet of Things Journal*, 4(6), 1802-1831. <https://doi.org/10.1109/jiot.2017.2703172>
- [23]. Ijure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security*, 25(7), 498-506. <https://doi.org/10.1016/j.cose.2006.03.001>
- [24]. Jannatul, F. (2025). Spinal Cord Injury and Neurorehabilitation Deep Learning-Based Prediction of Functional Recovery Trajectories After Traumatic Spinal Cord Injury. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2865-2922. <https://doi.org/10.63125/m738bh82>

- [25]. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, 395-411. <https://doi.org/10.1016/j.future.2017.11.022>
- [26]. Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9, 52-80. <https://doi.org/10.1016/j.ijcip.2015.02.002>
- [27]. Kouicem, D. E., Imine, Y., Bouabdallah, A., & Lakhlef, H. (2022). A decentralized blockchain-based trust management protocol for the Internet of Things. *IEEE Transactions on Dependable and Secure Computing*, 19(2), 1292-1306. <https://doi.org/10.1109/tdsc.2020.3003232>
- [28]. Kumar, R., & Sharma, R. (2022). Leveraging blockchain for ensuring trust in IoT: A survey. *Journal of King Saud University - Computer and Information Sciences*, 34(10), 8599-8622. <https://doi.org/10.1016/j.jksuci.2021.09.004>
- [29]. Kumar S., A. A., Øvsthus, K., & Kristensen, L. M. (2014). An industrial perspective on wireless sensor networks: A survey of requirements, protocols, and challenges. *IEEE Communications Surveys & Tutorials*, 16(3), 1391-1412. <https://doi.org/10.1109/surv.2014.012114.00058>
- [30]. Latif, S., Idrees, Z., Ahmad, J., Zheng, L., & Zou, Z. (2021). A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *Journal of Industrial Information Integration*, 21, 100190. <https://doi.org/10.1016/j.jii.2020.100190>
- [31]. Lazrag, H., Chehri, A., Saadane, R., & Rahmani, M. D. (2021). Efficient and secure routing protocol based on blockchain approach for wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 33(22), e6144. <https://doi.org/10.1002/cpe.6144>
- [32]. Liu, H., Han, D., & Li, D. (2020). Fabric-IoT: A blockchain-based access control system in IoT. *IEEE Access*, 8, 18207-18218. <https://doi.org/10.1109/access.2020.2968492>
- [33]. Mazzei, D., Baldi, G., Fantoni, G., Montelisciani, G., Pitasi, A., Ricci, L., & Rizzello, L. (2020). A blockchain tokenizer for industrial IOT trustless applications. *Future Generation Computer Systems*, 105, 432-445. <https://doi.org/10.1016/j.future.2019.12.020>
- [34]. McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5), 1039-1057. <https://doi.org/10.1109/jproc.2015.2512235>
- [35]. Md Anisur Rahman, M. (2024). State Income Tax Differentials and High-Skilled Labor Mobility in The United States: A Time Series Analysis. *American Journal of Interdisciplinary Studies*, 5(04), 222-267. <https://doi.org/10.63125/295bsn47>
- [36]. Md Anisur Rahman, M. (2025). The Role of AI-Enabled Business Intelligence in Financial Risk Assessment and Liquidity Monitoring. *Review of Applied Science and Technology*, 4(04), 195-246. <https://doi.org/10.63125/p4eezd93>
- [37]. Md Arif Uz, Z., Sharmin, S., & Md Abdur, R. (2025). Factors Influencing Behavioural Intention to Use he Innovative Open And Distance Learning Systems With The Role Of Continuanace Intention. *American Journal of Scholarly Research and Innovation*, 4(01), 202-220. <https://doi.org/10.63125/pbjxp014>
- [38]. Md Asif Ali Sheak, A. (2024). A Meta-Analysis of Agile and Lean Project Management Methodologies in Large-Scale Engineering and IT Integration Projects. *American Journal of Data Science and Analytics*, 5(12), 202-240. <https://doi.org/10.63125/6281tn40>
- [39]. Md Asif Ali Sheak, A., & Risha, A. (2022). The Role of IOT-Driven Energy Analytics in Improving Operational Efficiency and Sustainability in Modern Industrial Facilities. *American Journal of Interdisciplinary Studies*, 3(04), 807-841. <https://doi.org/10.63125/gm63q956>
- [40]. Md Mahamud Pervaz, P. (2025). Development of a CMMS-Integrated Predictive Maintenance Framework for Industrial PLC and Drive Systems. *American Journal of Scholarly Research and Innovation*, 4(01), 894-942. <https://doi.org/10.63125/j33gtf31>
- [41]. Md Mostafizur, R. (2025). Data-Driven Graph Neural Network Models for Detecting Fraudulent Insurance Claims In Healthcare Systems. *American Journal of Interdisciplinary Studies*, 6(1), 263-294. <https://doi.org/10.63125/pmqa1e33>
- [42]. Md Mostafizur, R., Omar Muhammad, F., & Sheratun Noor, J. (2025). Data Privacy in Business Intelligence Systems: Ensuring Compliance In HRIS And Enterprise Platforms. *International Journal of Scientific Interdisciplinary Research*, 6(1), 97-136. <https://doi.org/10.63125/527rnx08>
- [43]. Md Syeedur, R., & Sharmin, R. (2025). A Data-Driven Study on the use of Small Language Models & Large Language Models for Interpreting Complex Industrial Data and Deriving Actionable Outcome. *American Journal of Data Science and Analytics*, 6(11), 01-19. <https://doi.org/10.63125/5vyhgs98>
- [44]. Md. Abdur, R., & Iftekhhar, A. (2021). Customer Retention Forecasting in Mobile Wallet Services Using Neural Networks: A Comparative Quantitative Study. *International Journal of Business and Economics Insights*, 1(4), 70-102. <https://doi.org/10.63125/dyrpc387>
- [45]. Mistry, I., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mechanical Systems and Signal Processing*, 135, 106382. <https://doi.org/10.1016/j.ymssp.2019.106382>
- [46]. Mohammad Abir Chowdhury, S. (2023). Role of AI-Assisted Risk Assessment in Enhancing Audit Planning Efficiency and Risk Prioritization in Public-Safety Organizations. *International Journal of Scientific Interdisciplinary Research*, 4(4), 529-576. <https://doi.org/10.63125/qd6nn437>
- [47]. Mohammad Abir Chowdhury, S. (2025). Application of Machine Learning and Anomaly-Detection Algorithms for Fraud Detection in U.S. Government Financial Operations. *American Journal of Interdisciplinary Studies*, 6(02), 139-184. <https://doi.org/10.63125/fkf19309>

- [48]. Mohammad Abir Chowdhury, S., & Tonay, P. (2022). An Empirical Analysis of the Impact of Robotic Process Automation and Continuous Auditing on the Timeliness And Accuracy Of Financial Reporting Assurance. *International Journal of Business and Economics Insights*, 2(4), 73-126. <https://doi.org/10.63125/7p8dcr47>
- [49]. Mohammad Badrul, A. (2025). SCADA And IOT-Enabled Smart Water Metering: A Systematic Review of Resilient Supply Monitoring. *International Journal of Scientific Interdisciplinary Research*, 6(1), 576–615. <https://doi.org/10.63125/at8pnx81>
- [50]. Mohammad Badrul, A., & Md. Mominul, H. (2023). Machine Learning–Based Assessment of Environmental and Public Health Risks in Sewerage Sludge Management Systems. *American Journal of Advanced Technology and Engineering Solutions*, 3(02), 33-77. <https://doi.org/10.63125/y3yfxa92>
- [51]. Muhammad Zahidul, I. (2023). Comparative Analysis of Machine-Learning Approaches for Pharmaceutical Sales Forecasting and Market-Demand Prediction. *Review of Applied Science and Technology*, 2(02), 38–95. <https://doi.org/10.63125/etcbqf13>
- [52]. Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security*, 31(4), 418-436. <https://doi.org/10.1016/j.cose.2012.02.009>
- [53]. Nishat, J. (2025). Leveraging Machine Learning to Identify and Address Maternal Health Disparities in Underserved U.S. Communities. *American Journal of Data Science and Analytics*, 6(12), 125-169. <https://doi.org/10.63125/c2t7r719>
- [54]. Nishat, J., & Mst Kaniz, F. (2022). A Review of the Impact of Covid-19 On Maternal and Child Health Service Utilization in Bangladesh. *American Journal of Scholarly Research and Innovation*, 1(02), 223–269. <https://doi.org/10.63125/vgv5s742>
- [55]. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184-1195. <https://doi.org/10.1109/jiot.2018.2812239>
- [56]. Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT integration: A systematic survey. *Sensors*, 18(8), 2575. <https://doi.org/10.3390/s18082575>
- [57]. Paul, B., & Rao, M. (2023). Zero-trust model for smart manufacturing industry. *Applied Sciences*, 13(1), 221. <https://doi.org/10.3390/app13010221>
- [58]. Qureshi, J. N., Farooq, M. S., Abid, A., Umer, T., Bashir, A. K., & Zikria, Y. B. (2022). Blockchain applications for the Internet of Things: Systematic review and challenges. *Microprocessors and Microsystems*, 94, 104632. <https://doi.org/10.1016/j.micpro.2022.104632>
- [59]. Ramezan, G., & Leung, C. (2018). A blockchain-based contractual routing protocol for the Internet of Things using smart contracts. *Wireless Communications and Mobile Computing*, 2018, 4029591. <https://doi.org/10.1155/2018/4029591>
- [60]. Rathee, G., Ahmad, F., Jaglan, N., & Konstantinou, C. (2023). A secure and trusted mechanism for industrial IoT network using blockchain. *IEEE Transactions on Industrial Informatics*, 19(2), 1894-1902. <https://doi.org/10.1109/tii.2022.3182121>
- [61]. Rathee, G., Ahmad, F., Sandhu, R., Kerrache, C. A., & Azad, M. A. (2021). On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. *Information Processing & Management*, 58(3), 102526. <https://doi.org/10.1016/j.ipm.2021.102526>
- [62]. Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). A secure communicating things network framework for industrial IoT using blockchain technology. *Ad Hoc Networks*, 94, 101933. <https://doi.org/10.1016/j.adhoc.2019.101933>
- [63]. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems*, 88, 173-190. <https://doi.org/10.1016/j.future.2018.05.046>
- [64]. Saad, M., Anwar, A., Ahmad, A., Alasmay, H., Yuksel, M., & Mohaisen, D. (2022). RouteChain: Towards blockchain-based secure and efficient BGP routing. *Computer Networks*, 217, 109362. <https://doi.org/10.1016/j.comnet.2022.109362>
- [65]. Sasikumar, A., Vairavasundaram, S., Kotecha, K., Indragandhi, V., Ravi, L., Selvachandran, G., & Abraham, A. (2023). Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things. *Future Generation Computer Systems*, 141, 16-27. <https://doi.org/10.1016/j.future.2022.11.002>
- [66]. Sauter, T. (2010). The three generations of field-level networks: Evolution and compatibility issues. *IEEE Transactions on Industrial Electronics*, 57(11), 3585-3595. <https://doi.org/10.1109/tie.2010.2062473>
- [67]. Selvarajan, S., Srivastava, G., Khadidos, A. O., Khadidos, A. O., Baza, M., Alshehri, A., & Lin, J. C.-W. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. *Journal of Cloud Computing*, 12, 38. <https://doi.org/10.1186/s13677-023-00412-y>
- [68]. Sengupta, J., Ruj, S., & Das Bit, S. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications*, 149, 102481. <https://doi.org/10.1016/j.jnca.2019.102481>
- [69]. Shah, S. W., Syed, N. F., Shaghghi, A., Anwar, A., Baig, Z., & Doss, R. (2021). LCDA: Lightweight continuous device-to-device authentication for a zero trust architecture (ZTA). *Computers & Security*, 108, 102351. <https://doi.org/10.1016/j.cose.2021.102351>
- [70]. Shaiful, M., Anisur, R., & Md, A. (2022). A Systematic Literature Review on the Role of Digital Health Twins in Preventive Healthcare For Personal and Corporate Wellbeing. *American Journal of Interdisciplinary Studies*, 3(04), 1-31. <https://doi.org/10.63125/negjw373>
- [71]. Sharif Md Yousuf, B., Md Shahadat, H., Saleh Mohammad, M., Mohammad Shahadat Hossain, S., & Imtiaz, P. (2025). The Green Hydrogen Blueprint: Optimizing America's Clean Energy Future. *American Journal of Data Science and Analytics*, 6(10), 43-69. <https://doi.org/10.63125/y9b1k470>

- [72]. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146-164. <https://doi.org/10.1016/j.comnet.2014.11.008>
- [73]. Siegfried, N., Rosenthal, T., & Benlian, A. (2022). Blockchain and the Industrial Internet of Things: A requirement taxonomy and systematic fit analysis. *Journal of Enterprise Information Management*, 35(6), 1454-1476. <https://doi.org/10.1108/jeim-06-2018-0140>
- [74]. Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1), 210-224. <https://doi.org/10.1109/jproc.2011.2165269>
- [75]. Tavallaie, O., Naji, H. R., Sabaei, M., & Arastouie, N. (2017). RTEA: Real-time and energy aware routing for industrial wireless sensor networks. *Wireless Personal Communications*, 95(4), 4601-4621. <https://doi.org/10.1007/s11277-017-4109-3>
- [76]. Ten, C.-W., Liu, C.-C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, 23(4), 1836-1846. <https://doi.org/10.1109/tpwrs.2008.2002298>
- [77]. Tonay, P. (2025). Machine Learning for Fraud Detection in Enterprise Financial Systems. *American Journal of Advanced Technology and Engineering Solutions*, 1(02), 304-318. <https://doi.org/10.63125/d0fhp873>
- [78]. Tonay, P., Md Maruf, I., & Al, A. (2024). Artificial Intelligence-Based Decision Support Systems and Managerial Performance. *American Journal of Advanced Technology and Engineering Solutions*, 4(04), 154-184. <https://doi.org/10.63125/wmz8dc67>
- [79]. Tusher, N. R., Emran, M. A., Hossain, M. F., Fahim, S. R., Faruk, M. O., & Sonic, M. M. R. (2025, 23-24 Oct. 2025). Hybrid Vision Transformer and ResNet18 Framework for Multiclass Kidney Disease Detection from CT Scans. 2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS),
- [80]. Umran, S. M., Lu, S., Abduljabbar, Z. A., & Tang, X. (2023). A blockchain-based architecture for securing industrial IoTs data in electric smart grid. *Computers, Materials & Continua*, 74(3), 5389-5416. <https://doi.org/10.32604/cmc.2023.034331>
- [81]. Wang, H., & Zhang, J. (2019). Blockchain based data integrity verification for large-scale IoT data. *IEEE Access*, 7, 164996-165006. <https://doi.org/10.1109/access.2019.2952635>
- [82]. Wang, Q., Zhu, X., Ni, Y., Gu, L., & Zhu, H. (2020). Blockchain for the IoT and industrial IoT: A review. *Internet of Things*, 10, 100081. <https://doi.org/10.1016/j.iot.2019.100081>
- [83]. Wollschlaeger, M., Sauter, T., & Jasperneite, J. (2017). The future of industrial communication: Automation networks in the era of the Internet of Things and Industry 4.0. *IEEE Industrial Electronics Magazine*, 11(1), 17-27. <https://doi.org/10.1109/mie.2017.2649104>
- [84]. Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4), 2233-2243. <https://doi.org/10.1109/tii.2014.2300753>
- [85]. Xu, R., Hang, L., Jin, W., & Kim, D. (2021). Distributed secure edge computing architecture based on blockchain for real-time data integrity in IoT environments. *Actuators*, 10(8), 197. <https://doi.org/10.3390/act10080197>
- [86]. Yang, J., He, S., Xu, Y., Chen, L., & Ren, J. (2019). A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. *Sensors*, 19(4), 970. <https://doi.org/10.3390/s19040970>