Management Strategies and Engineering Sciences 2027; 9(5):1-19

A Strategic Framework for Managing Smart Contract–Driven Access Control in Industrial Internet of Things Ecosystems

Hourieh Alsadat Hosseini[1], Alireza Hedayati [1*] Vahe Aghazarian [1]

[1] Department of Computer Engineering, CT.C., Islamic Azad University, Tehran, Iran

*** Corresponding author email address**: Hedayati@iau.ac.ir

Received: 2026-02-10 **Revised:** 2026-07-21 **Accepted:** 2026-07-28 **Initial Publish:** 2026-07-29 **Final Publish:** 2027-09-01

Abstract

The objective of this study was to develop and empirically validate a strategic framework for managing smart contract–driven access control in Industrial Internet of Things (IIoT) ecosystems by integrating organizational, technological, governance, identity-management, security, and risk-management dimensions into a comprehensive model. This study employed an exploratory sequential mixed-methods design conducted in Tehran, Iran. In the qualitative phase, 21 Industrial Internet of Things experts were selected using purposive and snowball sampling, and semi-structured interviews were conducted until theoretical saturation was achieved. The qualitative findings were analyzed using thematic analysis through open, axial, and selective coding in MAXQDA. The extracted themes were subsequently transformed into a researcher-developed questionnaire. In the quantitative phase, 246 Industrial Internet of Things experts participated in the survey. The reliability and validity of the measurement instrument were assessed using Cronbach's alpha, composite reliability, average variance extracted, and discriminant validity. The proposed framework was evaluated using Partial Least Squares Structural Equation Modeling (PLS-SEM) in SmartPLS, while bootstrapping with 5,000 resamples was used to test the significance of the structural relationships. The structural model demonstrated that all hypothesized relationships were statistically significant. Continuous monitoring, auditability, and risk management had the strongest direct effect on effective management of smart contract–driven access control ($\beta = 0.284$, $p < 0.001$), followed by security and privacy assurance ($\beta = 0.257$, $p < 0.001$), smart contract governance and policy management ($\beta = 0.214$, $p < 0.001$), decentralized identity and trust management ($\beta = 0.146$, $p = 0.003$), organizational and regulatory readiness ($\beta = 0.138$, $p = 0.003$), and technological infrastructure and interoperability ($\beta = 0.119$, $p = 0.012$). Organizational and regulatory readiness significantly predicted smart contract governance and policy management ($\beta = 0.412$, $p < 0.001$), while security and privacy assurance ($\beta = 0.391$, $p < 0.001$) and technological infrastructure and interoperability ($\beta = 0.367$, $p < 0.001$) significantly predicted continuous monitoring, auditability, and risk management. Significant indirect effects confirmed the mediating roles of governance and monitoring. The proposed model explained 68.4% of the variance in effective management of smart contract–driven access control. The findings demonstrate that effective smart contract–driven access control in Industrial Internet of Things ecosystems requires an integrated strategic approach that combines decentralized identity management, smart contract governance, organizational readiness, technological interoperability, security and privacy assurance, and continuous monitoring within a unified governance framework.

Keywords: *Industrial Internet of Things; Smart Contracts; Blockchain; Access Control; Identity and Access Management; Cybersecurity; Distributed Ledger Technology*

How to cite this article:

Hosseini, H. A., Hedayati, A., & Aghazarian, V. (2027). A Strategic Framework for Managing Smart Contract–Driven Access Control in Industrial Internet of Things Ecosystems. Management Strategies and Engineering Sciences, 9(5), 1-19.

1. Introduction

The rapid expansion of the Industrial Internet of Things has transformed industrial production, logistics, energy systems, transportation, healthcare infrastructure, and other cyber-physical environments by connecting sensors, actuators, controllers, machines, gateways, and enterprise platforms through continuously interacting digital networks. This transformation enables real-time monitoring, predictive maintenance, process automation, adaptive production, and

data-driven decision-making, yet it also introduces substantial security and governance challenges because highly heterogeneous devices and systems must exchange sensitive operational data across distributed and often weakly protected environments. Unlike conventional information systems, Industrial Internet of Things ecosystems integrate resource-constrained devices, legacy industrial control systems, cloud platforms, edge nodes, mobile interfaces, and third-party applications, thereby creating a broad and dynamic attack surface. As industrial systems become increasingly interconnected, conventional centralized access-control mechanisms face difficulties in maintaining trust, scalability, resilience, transparency, and policy consistency across multiple administrative and technological domains [1-3].

Access control is a foundational security requirement in Industrial Internet of Things environments because it determines which users, devices, applications, and services are authorized to access particular resources, under what conditions, and for what purposes. In industrial settings, access decisions may influence physical processes, equipment safety, data confidentiality, production continuity, and human well-being. Unauthorized commands, compromised credentials, or incorrectly assigned privileges can therefore cause consequences that extend beyond information loss to include equipment damage, operational disruption, environmental hazards, and safety incidents. Traditional access-control approaches, including role-based, attribute-based, capability-based, and policy-based mechanisms, remain important, but their centralized design may create single points of failure, administrative bottlenecks, limited auditability, and difficulties in enforcing dynamic policies across organizational boundaries. Existing reviews indicate that IoT authorization mechanisms frequently struggle with scalability, device heterogeneity, contextual sensitivity, policy updating, credential revocation, and the management of highly dynamic relationships among users, devices, and services [4, 5].

Blockchain and distributed ledger technologies have emerged as promising mechanisms for addressing several of these limitations. Blockchain can provide decentralized trust, tamper-resistant transaction records, distributed consensus, traceability, and transparent enforcement without requiring all participants to depend on a single central authority. In IoT and industrial environments, these capabilities may be used to record device identities, verify credentials, document access requests, preserve authorization histories, and coordinate policy enforcement across multiple stakeholders. The growing literature on blockchain integration with IoT highlights its potential to enhance authentication, data integrity, accountability, and resilience, while also emphasizing unresolved concerns involving latency, scalability, energy consumption, privacy, interoperability, and governance [6-9]. Therefore, blockchain should not be treated as a universally sufficient security solution, but rather as one component within a broader socio-technical architecture.

Smart contracts extend blockchain functionality by enabling predefined rules and conditions to be encoded as executable programs. Once deployed, smart contracts can automatically validate requests, verify conditions, issue or deny permissions, document decisions, and trigger responses without continuous manual intervention. This capacity makes them particularly relevant to Industrial Internet of Things access control, where authorization decisions may need to be executed rapidly and consistently across large numbers of devices and services. Smart contracts can support policy automation, reduce administrative overhead, improve transparency, and provide an auditable record of access-control events. Research on blockchain-based smart contracts has demonstrated their applicability across digital transactions, distributed services, data management, and automated trust relationships, while also identifying risks related to code vulnerabilities, inflexibility, erroneous logic, oracle dependence, and irreversible execution [10, 11].

A central advantage of smart contract–driven access control is the possibility of translating organizational authorization policies into machine-executable logic. Attribute-based access control can, for example, be implemented through smart contracts that evaluate user attributes, device properties, location, time, operational state, and environmental conditions before granting access. Blockchain-based attribute models can also improve traceability because authorization rules and decisions are recorded on a distributed ledger rather than maintained exclusively by a central administrator. Zaidi et al. developed an attribute-based access-control approach using blockchain and smart contracts, illustrating how decentralized policy enforcement can increase transparency and reduce dependency on centralized authorities [12]. Similarly, domain-sensitive access-control approaches have incorporated spatial and temporal attributes into smart contract logic, demonstrating that IoT permissions can be adjusted according to contextual conditions rather than assigned permanently or statically [13]. Such dynamic

capabilities are especially important in industrial settings, where access requirements may vary according to production stage, machine status, maintenance schedules, emergency conditions, and personnel responsibilities.

Recent smart contract–based frameworks have further shown that decentralized access control can support direct authorization among IoT devices and service providers. Hasan et al. proposed a smart contract–based access-control framework for IoT devices that emphasized decentralized permission management, transparent decision-making, and resistance to unauthorized access [14]. Albulayhi and Alsukayti presented a blockchain-centric IoT architecture in which smart contracts were used to manage data communications and regulate interactions among IoT entities [15]. Other research has combined blockchain-based access control with trusted execution technologies, such as Intel Software Guard Extensions, to protect sensitive computations and enhance confidentiality in IoT systems [16]. These studies demonstrate the technical feasibility of smart contract–driven authorization, but they predominantly focus on architectural design, protocol performance, or proof-of-concept implementation rather than the development of a comprehensive strategic management framework.

Identity management is another essential component of access-control architecture. Effective authorization depends on the ability to establish who or what is requesting access and whether the presented identity remains trustworthy. Industrial Internet of Things ecosystems involve not only human users but also machines, embedded devices, sensors, robots, gateways, software agents, and external service platforms. These entities may be deployed for long periods, transferred between operational domains, updated remotely, or compromised without immediate detection. Blockchain-based identity systems can provide decentralized identifiers, verifiable credentials, cryptographic authentication, and immutable registration histories. Surveys of distributed ledger–based identity and access management suggest that blockchain can improve control over digital identities and reduce reliance on centralized identity providers, although challenges remain in credential recovery, privacy, governance, interoperability, and revocation [17, 18].

Several studies have addressed identity authentication and device onboarding more specifically. Venkatraman and Parvin proposed an IoT identity-management system using blockchain to improve identity validation and trust among connected entities [19]. Wang et al. examined IoT device authentication through hashing and digital signatures within blockchain environments, emphasizing the need for cryptographic mechanisms that can verify device identities and protect registration records [20]. Secure onboarding and key management are equally important because even a well-designed access-control policy can be undermined if initial credentials are issued insecurely or cryptographic keys are exposed. Research on federated IoT environments has therefore highlighted secure onboarding, credential distribution, key renewal, and lifecycle management as fundamental requirements [21]. For industrial deployments, these mechanisms must also support device replacement, ownership transfer, maintenance access, emergency revocation, and the isolation of compromised nodes.

Privacy represents a further challenge because blockchain transparency can conflict with the confidentiality requirements of industrial operations. Although immutable ledgers enhance auditability, they may expose metadata regarding device behavior, communication patterns, transaction frequency, operational schedules, and organizational relationships. Even when payload data are encrypted, repeated or linkable transactions may permit inference attacks. Blockchain privacy research therefore emphasizes the importance of pseudonymization, encryption, selective disclosure, zero-knowledge techniques, off-chain storage, and permissioned participation models [22]. Privacy-preserving mechanisms have been proposed for smart homes, smart cities, vehicular networks, and other IoT environments, but many of the underlying concerns are equally relevant to industrial ecosystems. Qashlan et al. demonstrated how blockchain could be integrated into privacy-preserving smart-home systems, while Padma and Ramaiah proposed a blockchain-based framework for protecting privacy in smart-city environments [23, 24]. A broader survey of privacy-preserving architectures for IoT and vehicular data sharing further identifies recurring tensions among data utility, decentralization, confidentiality, computational overhead, and regulatory compliance [25].

The integration of blockchain, edge computing, and Industrial Internet of Things infrastructure offers one possible response to these performance and privacy concerns. Edge computing enables data processing and policy evaluation to occur closer to industrial devices, thereby reducing latency, bandwidth consumption, and exposure of raw operational data. Blockchain can then be used selectively for identity verification, policy synchronization, event logging, and consensus rather than for storing or processing every IoT interaction. Research has

suggested that combining blockchain with edge computing can improve security and distribute trust across IoT environments [26]. Similar approaches have been explored in beyond-5G and federated learning settings, where privacy-preserving mechanisms and incentive structures are required to coordinate decentralized edge participants [27]. The anticipated convergence of blockchain with 6G communication technologies may further support massive device connectivity, decentralized resource sharing, low-latency services, and secure machine-to-machine transactions [28]. Nevertheless, industrial deployment remains constrained by the computational limitations of embedded devices, inconsistent network connectivity, consensus delays, and integration difficulties with legacy infrastructure.

Interoperability is particularly significant because industrial organizations often operate a mixture of modern IoT devices and older supervisory control, programmable logic, manufacturing execution, and enterprise resource-planning systems. A smart contract–driven access-control framework must therefore support diverse communication protocols, identity formats, policy models, and trust domains. Blockchain and IoT integration platforms continue to face implementation challenges involving incompatible architectures, limited standards, cross-chain communication, data synchronization, and platform dependence [3]. Hyper-connected smart-city platforms have demonstrated that blockchains, smart contracts, and complex sensor-management systems can be combined to support decentralized data marketplaces and multi-stakeholder services [29]. However, such environments also show that technical integration must be accompanied by clear rules concerning data ownership, service responsibilities, dispute resolution, pricing, consent, and accountability.

The broader convergence of blockchain with artificial intelligence, digital assets, and autonomous systems further increases the strategic importance of trustworthy access control. Blockchain can support provenance, automation, data integrity, model sharing, and accountable decision-making in artificial intelligence systems [30]. Bibliometric and conceptual research also indicates growing interest in combining artificial intelligence and blockchain for business automation, secure data exchange, and decentralized governance [31]. In metaverse and digital-asset environments, blockchain-based identity, ownership, and smart contract mechanisms are becoming central to the management of virtual resources and cross-platform interactions [32]. Although these developments extend beyond Industrial Internet of Things applications, they demonstrate that smart contract–based access control will increasingly operate within interconnected digital ecosystems rather than within isolated industrial networks.

Security threats remain a major barrier to such integration. Blockchain may protect ledger integrity, but it does not automatically secure endpoints, communication channels, smart contract code, external data sources, or cryptographic keys. Surveys of blockchain in IoT cybersecurity identify vulnerabilities involving consensus attacks, smart contract exploitation, denial-of-service attacks, key compromise, privacy leakage, malicious nodes, and insecure interfaces [1]. Cloud–IoT and cyber-physical systems additionally require lightweight security protocols because many devices cannot support computationally intensive cryptographic operations. Recent work on blockchain-enhanced lightweight protocols shows that hybrid approaches can strengthen authentication and key exchange while remaining suitable for constrained environments [33]. Nevertheless, a strategic access-control framework must determine which security functions should be executed on-chain, off-chain, at the edge, in secure hardware, or through conventional industrial-security mechanisms.

These technical issues are inseparable from governance and organizational readiness. Smart contracts encode decisions that may have legal, operational, financial, and safety implications, yet their execution can be difficult to modify after deployment. Organizations must therefore establish procedures for policy design, contract validation, auditing, updating, suspension, emergency override, and accountability. They must also determine who has authority to register devices, issue credentials, approve access rules, modify contracts, interpret logs, and respond to incidents. Access-control governance should address separation of duties, least privilege, revocation, human oversight, and alignment with organizational risk appetite. The literature on authorization and distributed identity frequently acknowledges such requirements, but governance relationships are often treated as secondary to architectural performance [4, 18].

A further limitation of the current literature is its fragmented treatment of access-control dimensions. Some studies emphasize blockchain architecture, others focus on identity management, smart contracts, privacy preservation, trusted hardware, dynamic policies, or cryptographic protocols. For example, existing research has separately examined blockchain-based data communication [15],

spatio-temporal access policies [13], trusted execution environments [16], attribute-based authorization [12], and device-level smart contract frameworks [14]. These contributions are valuable, yet industrial adoption requires an integrated view in which technological infrastructure, identity assurance, smart contract governance, security, privacy, auditability, organizational readiness, and regulatory compliance are treated as mutually dependent components.

The need for integration is reinforced by the dynamic character of Industrial Internet of Things systems. Devices may join or leave networks, user responsibilities may change, production conditions may shift, vulnerabilities may emerge, and threat levels may increase unexpectedly. Static access policies are therefore insufficient. Dynamic access control requires continuous assessment of identity, context, trust, device state, location, time, risk, and operational necessity [5]. Smart contracts can automate policy execution, but the policies themselves must remain adaptable and subject to governance. Continuous monitoring, immutable logging, anomaly detection, and risk-based policy revision are consequently necessary to prevent automation from becoming rigid or unsafe.

From a strategic perspective, the central question is not merely whether blockchain and smart contracts can technically enforce access decisions, but how organizations should manage these capabilities across the full lifecycle of design, deployment, operation, monitoring, and revision. A viable framework must reconcile decentralization with accountability, automation with human oversight, transparency with privacy, immutability with policy change, and security with operational efficiency. It must also account for resource constraints, legacy integration, stakeholder coordination, legal responsibility, and the long-term maintenance of smart contract code. Without such a framework, organizations may implement technically sophisticated access-control mechanisms that remain fragmented, difficult to govern, or incompatible with industrial risk-management practices.

Accordingly, the aim of this study was to develop and validate a strategic framework for managing smart contract–driven access control in Industrial Internet of Things ecosystems.

2. Methodology

This study employed an exploratory sequential mixed-methods design to develop and validate a strategic framework for managing smart contract–driven access control in Industrial Internet of Things ecosystems. The research was conducted in Tehran, Iran, in two consecutive qualitative and quantitative phases. The qualitative phase was undertaken to identify the principal dimensions, components, implementation requirements, governance mechanisms, security considerations, and strategic relationships associated with blockchain-enabled access control in industrial IoT environments. The quantitative phase was subsequently conducted to evaluate the validity of the qualitatively derived framework and examine the relationships among its major constructs. The target population comprised experts with professional or academic experience in Industrial Internet of Things architecture, blockchain technology, smart contract development, cybersecurity, access control systems, industrial automation, distributed systems, information technology governance, and digital transformation. Participants were recruited from technology companies, industrial organizations, research centers, universities, cybersecurity firms, blockchain development teams, and information technology departments located in Tehran. In the qualitative phase, 21 experts were selected through purposive and snowball sampling. Recruitment continued until theoretical saturation was reached and additional interviews no longer produced substantively new concepts or categories. Eligibility criteria included holding at least a master's degree in computer engineering, information technology, industrial engineering, cybersecurity, software engineering, telecommunications engineering, technology management, or a closely related discipline; having at least five years of relevant professional, managerial, research, or technical experience; possessing direct knowledge of IoT security, blockchain-based systems, smart contracts, industrial digital infrastructures, or access control mechanisms; and expressing willingness to participate in an in-depth interview. Experts who lacked direct experience in the study domain, provided incomplete responses, or withdrew before completion of the interview were excluded.

The quantitative phase included exactly 246 Industrial IoT experts from Tehran. Participants were selected using a combination of purposive and stratified sampling to ensure the representation of specialists from industrial enterprises, technology companies, academic institutions, cybersecurity organizations, and blockchain-related development teams. The quantitative sample included experts in system architecture, industrial automation, network and information security, software development, smart contract

programming, blockchain implementation, IoT infrastructure, risk management, data governance, and technology strategy. To be included in this phase, respondents were required to have at least three years of relevant work or research experience and sufficient familiarity with at least two of the following domains: Industrial Internet of Things, smart contracts, blockchain networks, cybersecurity, access control, industrial information systems, or technology governance. Questionnaires with substantial missing data, uniform response patterns, or inconsistent answers to control questions were removed before the final analysis. Participation in both phases was voluntary. Before data collection, the objectives and procedures of the research were explained to the participants, and informed consent was obtained. Participants were assured that their identities and organizational affiliations would remain confidential, that the collected information would be used exclusively for research purposes, and that they could withdraw from the study at any stage without penalty.

Qualitative data were collected using a researcher-developed semi-structured interview guide. The initial interview questions were formulated through a review of the conceptual literature on Industrial Internet of Things security, blockchain-based identity and access management, smart contract governance, role-based and attribute-based access control, zero-trust architecture, decentralized authorization, interoperability, privacy protection, scalability, auditability, and organizational technology strategy. The interview guide was reviewed by five specialists in Industrial Internet of Things, blockchain security, qualitative research, and technology management to assess the clarity, relevance, comprehensiveness, and logical sequence of the questions. Based on their comments, ambiguous questions were revised, overlapping questions were combined, and additional prompts were included to obtain more detailed explanations of implementation barriers, strategic requirements, and governance mechanisms. The interviews began with general questions concerning the participants' professional experiences with industrial connected systems and gradually progressed toward more specific questions about the advantages, risks, architectural requirements, organizational conditions, security controls, and managerial implications of smart contract–driven access control. Participants were also asked to explain how access permissions should be defined, verified, updated, revoked, monitored, and audited within a distributed Industrial IoT environment. Further questions explored identity authentication, device registration, policy enforcement, blockchain selection, on-chain and off-chain data management, interoperability with legacy industrial systems, smart contract vulnerabilities, privacy preservation, emergency access, regulatory compliance, accountability, and incident response. Probing questions were used when clarification or elaboration was required. Each interview lasted approximately 50 to 75 minutes and was conducted either face-to-face at the participant's workplace or through a secure online communication platform. With the participants' permission, interviews were digitally recorded and subsequently transcribed verbatim.

The quantitative data collection instrument was a researcher-made questionnaire developed from the themes, categories, and subcategories extracted during the qualitative phase. The preliminary item pool was created by converting the qualitative findings into measurable statements representing the proposed framework's strategic, technological, security, organizational, operational, and governance dimensions. Items were formulated to assess constructs such as decentralized identity management, smart contract–based authorization, dynamic policy enforcement, trust management, security and privacy protection, interoperability, scalability, auditability, organizational readiness, governance and accountability, risk management, and the effectiveness of access control within Industrial IoT ecosystems. Responses were recorded on a five-point Likert scale ranging from 1, representing strongly disagree, to 5, representing strongly agree. To establish face validity, the preliminary questionnaire was reviewed by eight Industrial IoT professionals who assessed the clarity, readability, technical appropriateness, and interpretability of the items. Content validity was subsequently examined by a panel of 10 experts in blockchain, cybersecurity, industrial systems, technology management, and research methodology. The experts evaluated the necessity, relevance, simplicity, and clarity of each item. Items that were considered conceptually redundant, technically ambiguous, or insufficiently related to the intended construct were revised or eliminated. The content validity ratio and content validity index were calculated to support decisions regarding item retention.

A pilot study was conducted with 30 Industrial IoT specialists who were not included in the final quantitative sample. The pilot study was used to assess the questionnaire's administration procedure, completion time, internal consistency, and preliminary construct structure. Reliability was evaluated using Cronbach's alpha and composite reliability coefficients. Coefficients of 0.70 or

greater were considered acceptable. Convergent validity was assessed through factor loadings and average variance extracted, while discriminant validity was evaluated by comparing the square roots of the average variance extracted with inter-construct correlations and by examining the heterotrait–monotrait ratio. Items with weak factor loadings or substantial cross-loadings were examined and removed when their elimination improved the psychometric quality of the instrument without weakening its conceptual coverage. The final questionnaire was administered electronically and, where organizational access permitted, in printed form. A brief explanation of the study, instructions for completing the questionnaire, and a confidentiality statement were provided at the beginning of the instrument.

Qualitative data were analyzed using thematic analysis with a systematic coding procedure. Immediately after each interview, the audio recording was transcribed verbatim, and the transcript was compared with the recording to ensure accuracy. The researchers repeatedly read the transcripts to become familiar with the data and identify meaningful statements related to smart contract–driven access control in Industrial IoT ecosystems. During open coding, relevant words, sentences, and paragraphs were assigned initial conceptual labels. Similar codes were compared, merged, differentiated, or refined through constant comparison. During axial coding, conceptually related codes were organized into subcategories and broader categories reflecting causal conditions, contextual factors, intervening conditions, strategic actions, implementation mechanisms, and anticipated outcomes. During selective coding, the principal categories were integrated around the central phenomenon of strategically managing smart contract–based access control in Industrial IoT ecosystems. Analytical memos were maintained throughout the coding process to document conceptual decisions, emerging relationships, and revisions to the developing framework. MAXQDA software was used to organize the transcripts, codes, categories, and supporting excerpts.

The trustworthiness of the qualitative findings was established using credibility, dependability, confirmability, and transferability criteria. Credibility was enhanced through prolonged engagement with the data, purposive recruitment of experts from different professional backgrounds, iterative interviewing, and member checking. A summary of the initial interpretations and extracted categories was returned to selected participants so that they could evaluate whether the findings accurately represented their experiences and viewpoints. Peer debriefing was performed by two researchers familiar with qualitative analysis and Industrial IoT security. They independently reviewed a portion of the transcripts, examined the coding structure, and discussed disagreements until consensus was achieved. Dependability was supported by maintaining an audit trail containing interview protocols, coding decisions, category revisions, analytical notes, and framework development records. Confirmability was strengthened by grounding the categories in participants' statements and documenting the analytical procedures. Transferability was addressed by providing detailed descriptions of the participants' expertise, the research setting, the data collection process, and the technological context of the study.

Quantitative data were analyzed using SPSS and SmartPLS software. Before testing the proposed framework, the dataset was screened for missing values, outliers, response-pattern irregularities, and distributional characteristics. Descriptive statistics, including frequency, percentage, mean, standard deviation, skewness, and kurtosis, were calculated to summarize the participants' characteristics and responses to the study variables. The measurement model was evaluated by examining indicator loadings, Cronbach's alpha, composite reliability, rho_A, average variance extracted, and discriminant validity. Indicator loadings of 0.70 or greater were preferred, although items with moderately lower loadings were retained when they had strong theoretical relevance and did not adversely affect construct reliability or convergent validity. An average variance extracted value of at least 0.50 and reliability coefficients of at least 0.70 were regarded as evidence of acceptable measurement quality. Discriminant validity was assessed using the Fornell–Larcker criterion, cross-loadings, and the heterotrait–monotrait ratio.

After establishing the adequacy of the measurement model, partial least squares structural equation modeling was used to evaluate the structural relationships among the framework's constructs. Collinearity was assessed using variance inflation factor values. The significance of the proposed paths was examined through a bootstrapping procedure with 5,000 resamples. Path coefficients, t statistics, confidence intervals, and probability values were used to determine the significance and direction of the relationships. The explanatory power of the model was assessed using the coefficient of determination, and predictive relevance was evaluated through the Stone–Geisser Q^2 criterion. Effect-size coefficients were calculated to determine the contribution of each exogenous construct to

the explained variance of the endogenous constructs. Model fit was additionally examined using the standardized root mean square residual. The final strategic framework was developed by integrating the qualitative categories with the statistically supported relationships obtained from the quantitative analysis. Qualitative findings defined the substantive dimensions and components of the framework, while quantitative findings established the reliability, validity, relative importance, and structural relationships of those dimensions. This integration enabled the development of a context-sensitive and empirically validated framework for managing secure, transparent, scalable, auditable, and strategically governed smart contract–driven access control in Industrial Internet of Things ecosystems.

3. Findings and Results

The findings were obtained by integrating the qualitative results derived from interviews with 21 Industrial Internet of Things experts and the quantitative results obtained from 246 experts working in Tehran. In the qualitative phase, the participants included university faculty members, cybersecurity specialists, blockchain developers, Industrial Internet of Things architects, industrial automation professionals, information technology managers, and technology-governance experts. Their professional experience ranged from 6 to 24 years, with a mean professional experience of 12.71 years. Of the 21 interviewees, 16 were men and 5 were women. Eight participants held doctoral degrees, 11 held master's degrees, and 2 held professional or postgraduate technical qualifications relevant to the research domain. Regarding their principal field of expertise, 5 participants specialized in cybersecurity and access control, 4 in blockchain and smart contract development, 4 in Industrial Internet of Things architecture and industrial automation, 3 in software and distributed systems, 3 in technology strategy and governance, and 2 in telecommunications and network infrastructure. The diversity of participants' professional backgrounds enabled the study to examine smart contract–driven access control from technical, security, managerial, organizational, and regulatory perspectives.

The quantitative sample consisted of 246 Industrial Internet of Things experts from universities, industrial organizations, technology firms, cybersecurity companies, research centers, and blockchain development teams located in Tehran. Among the respondents, 184 participants, representing 74.8% of the sample, were men, and 62 participants, representing 25.2%, were women. The participants' ages ranged from 27 to 59 years, with a mean age of 39.46 years and a standard deviation of 7.38 years. In terms of educational attainment, 41 participants, or 16.7%, held bachelor's degrees or equivalent professional qualifications, 139 participants, or 56.5%, held master's degrees, and 66 participants, or 26.8%, held doctoral degrees. The respondents had between 3 and 28 years of relevant professional experience, with a mean of 10.84 years and a standard deviation of 5.79 years. Concerning organizational affiliation, 72 participants, or 29.3%, were employed by industrial and manufacturing organizations; 61 participants, or 24.8%, worked in technology and software companies; 43 participants, or 17.5%, were affiliated with universities and research institutions; 38 participants, or 15.4%, worked in cybersecurity and information-security organizations; and 32 participants, or 13.0%, were employed by blockchain, telecommunications, or digital-infrastructure companies. The largest group of respondents specialized in cybersecurity and access management, followed by Industrial Internet of Things architecture, blockchain and smart contract development, industrial automation, software engineering, network infrastructure, technology governance, and risk management. This distribution indicated that the quantitative sample possessed substantial technical and managerial expertise relevant to the development and validation of the proposed framework.

Table 1. Qualitative Themes, Subthemes, and Representative Concepts Extracted from Expert Interviews

Main Theme	Subthemes	Representative Concepts	Number of Related Initial Codes	Number of Participants Referring to the Theme
Smart Contract Governance and Policy Management	Policy formalization; authorization rule design; contract updating; revocation mechanisms; emergency intervention; governance responsibilities	Machine-readable access policies, predefined authorization logic, contract version control, revocation of outdated permissions, emergency override procedures, separation of technical and managerial authority	47	21
Decentralized Identity and Trust Management	Device identity; user identity; credential verification; trust scoring;	Cryptographic device identifiers, decentralized identifiers, verifiable credentials, device	42	20

	lifecycle management; identity revocation	registration, continuous trust evaluation, identity renewal, compromised-device isolation		
Security and Privacy Assurance	Smart contract security; transaction confidentiality; key management; attack resistance; privacy preservation; incident response	Formal verification, vulnerability testing, secure key storage, protection against replay attacks, prevention of unauthorized contract execution, privacy-preserving authentication, anomaly detection	51	21
Technological Infrastructure and Interoperability	Blockchain architecture; on-chain and off-chain processing; scalability; latency management; integration with legacy systems; cross-platform compatibility	Permissioned blockchain, edge computing, off-chain storage, lightweight consensus, gateway integration, protocol translation, interoperability with supervisory control and data acquisition systems	45	19
Organizational and Regulatory Readiness	Organizational capabilities; specialist knowledge; management support; regulatory compliance; accountability; stakeholder coordination	Technical training, executive sponsorship, legal responsibility, data-governance policies, compliance monitoring, cross-functional implementation teams, allocation of financial resources	38	18
Continuous Monitoring, Auditability, and Risk Management	Real-time monitoring; immutable auditing; risk assessment; anomaly detection; performance evaluation; recovery planning	Traceable authorization decisions, event logging, continuous contract monitoring, access-pattern analysis, audit trails, risk-based policy adjustment, business-continuity procedures	44	20
Strategic Outcomes of Smart Contract–Driven Access Control	Security improvement; operational efficiency; transparency; accountability; adaptive control; resilience	Reduction in unauthorized access, automated authorization, reduced administrative burden, transparent policy enforcement, rapid response to security incidents, increased industrial-system resilience	36	21

The qualitative analysis generated 303 initial codes, which were progressively compared, refined, and integrated into 39 subcategories and 7 main themes. Smart contract governance and policy management emerged as a central dimension of the proposed framework because all 21 participants emphasized that the technical deployment of smart contracts would be ineffective without clearly defined governance rules. Participants explained that access-control policies should be formally translated into executable smart contract logic, but the authority to design, approve, update, suspend, and revoke these policies should remain explicitly assigned to accountable organizational actors. They also emphasized the need for contract version control, emergency override mechanisms, predefined dispute-resolution procedures, and separation between the individuals who develop smart contracts and those who authorize their operational use. Decentralized identity and trust management constituted another major theme, reflecting the importance of establishing reliable identities for industrial devices, human users, applications, gateways, and organizational units. Participants argued that identity management should extend beyond initial authentication and should include the complete lifecycle of registration, credential issuance, verification, renewal, suspension, and revocation.

Security and privacy assurance produced the largest number of initial codes. Experts repeatedly referred to coding vulnerabilities, insecure external data feeds, compromised private keys, replay attacks, unauthorized contract execution, transaction-data exposure, and malicious manipulation of access conditions. The interviews indicated that smart contracts should undergo formal verification, independent security auditing, penetration testing, and continuous runtime monitoring before and after deployment. Technological infrastructure and interoperability were also identified as essential because Industrial Internet of Things environments commonly contain resource-constrained devices, heterogeneous communication protocols, real-time operational requirements, and legacy industrial equipment. Participants recommended permissioned blockchain architectures, edge-based processing, off-chain data storage, lightweight consensus mechanisms, and gateway-level integration to reduce latency and computational overhead. Organizational and regulatory readiness emphasized that successful implementation depended on management support, skilled personnel, legal clarity, financial resources, interdepartmental coordination, and compliance with data-protection and industrial-security requirements. Continuous monitoring, auditability, and risk management were regarded as necessary for detecting abnormal access behavior, documenting authorization decisions, supporting forensic investigation, and adjusting access policies in response to emerging risks. Finally, the strategic outcomes theme demonstrated that experts expected smart contract–driven access control to improve security, transparency, accountability, efficiency, adaptability, and operational resilience when all preceding dimensions were implemented in a coordinated manner.

Table 2. Measurement Model Evaluation for the Constructs of the Strategic Framework

Construct	Number of Retained Items	Standardized Loading Range	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted
Smart Contract Governance and Policy Management	7	0.724–0.872	0.902	0.906	0.923	0.632
Decentralized Identity and Trust Management	6	0.731–0.881	0.889	0.895	0.916	0.646
Security and Privacy Assurance	8	0.742–0.893	0.927	0.931	0.940	0.663
Technological Infrastructure and Interoperability	7	0.708–0.861	0.894	0.901	0.917	0.616
Organizational and Regulatory Readiness	6	0.719–0.864	0.881	0.887	0.910	0.629
Continuous Monitoring, Auditability, and Risk Management	7	0.736–0.886	0.913	0.917	0.932	0.663
Effective Management of Smart Contract–Driven Access Control	7	0.751–0.901	0.925	0.929	0.940	0.692

The measurement model was evaluated before examining the structural relationships among the research constructs. The initial questionnaire contained 54 items developed from the qualitative findings. Following expert review, pilot testing, and preliminary measurement-model analysis, 6 items were removed because of low factor loadings, excessive conceptual overlap, or substantial cross-loadings. The final model therefore contained 48 items distributed across 7 constructs. As shown in Table 2, standardized indicator loadings ranged from 0.708 to 0.901. All retained items exceeded the minimum acceptable loading level, and most loadings were greater than 0.75, indicating that the items adequately represented their intended latent constructs. The highest loading was observed for an item assessing the capacity of the access-control framework to provide traceable and automatically enforceable authorization decisions, whereas the lowest retained loading was associated with an interoperability item addressing the integration of blockchain-based access control with older industrial communication systems.

Cronbach's alpha coefficients ranged from 0.881 for organizational and regulatory readiness to 0.927 for security and privacy assurance. These results indicated a high degree of internal consistency for all constructs. The rho_A coefficients ranged from 0.887 to 0.931, while composite reliability values ranged from 0.910 to 0.940. Because all reliability coefficients were higher than 0.70 and remained below levels suggesting excessive item redundancy, the internal reliability of the measurement model was considered satisfactory. Average variance extracted values ranged from 0.616 to 0.692 and therefore exceeded the recommended threshold of 0.50 for every construct. These findings demonstrated that each construct explained more than half of the variance in its associated indicators and provided evidence of convergent validity. Security and privacy assurance, continuous monitoring and risk management, and effective access-control management exhibited particularly strong measurement properties, reflecting the high coherence of items related to protection mechanisms, traceability, monitoring, risk-based adaptation, and authorization effectiveness. Overall, the measurement-model findings confirmed that the researcher-developed questionnaire possessed adequate reliability and convergent validity for evaluating the strategic framework.

Table 3. Fornell–Larcker Assessment of Discriminant Validity

Construct	SCG	DIT	SPA	TII	ORR	CMR	EMA
Smart Contract Governance and Policy Management (SCG)	0.795						
Decentralized Identity and Trust Management (DIT)	0.584	0.804					
Security and Privacy Assurance (SPA)	0.623	0.601	0.814				
Technological Infrastructure and Interoperability (TII)	0.518	0.546	0.571	0.785			
Organizational and Regulatory Readiness (ORR)	0.556	0.491	0.529	0.503	0.793		
Continuous Monitoring, Auditability, and Risk Management (CMR)	0.608	0.577	0.648	0.562	0.551	0.814	
Effective Management of Smart Contract–Driven Access Control (EMA)	0.676	0.632	0.711	0.617	0.602	0.729	0.832

The discriminant validity results presented in Table 3 showed that the square root of the average variance extracted for each construct, displayed on the main diagonal, was greater than its correlations with all other constructs. The

square roots of the average variance extracted ranged from 0.785 for technological infrastructure and interoperability to 0.832 for effective management of smart contract–driven access control. The highest inter-construct correlation was observed between continuous monitoring, auditability, and risk management and effective management of smart contract–driven access control, with a coefficient of 0.729. This relationship was theoretically reasonable because continuous monitoring, immutable auditing, anomaly detection, and risk-based policy adjustment were expected to contribute directly to the effectiveness of the access-control framework. Nevertheless, the correlation remained lower than the square roots of the average variance extracted for both constructs, indicating that they represented related but empirically distinct concepts.

The correlation between security and privacy assurance and effective access-control management was 0.711, suggesting that the protection of smart contract logic, transaction confidentiality, cryptographic keys, identities, and device communications was strongly associated with effective access-control implementation. Smart contract governance and policy management was also strongly correlated with effective access-control management, with a coefficient of 0.676, reflecting the importance of policy formalization, governance accountability, contract updating, and revocation procedures. The remaining correlations ranged from 0.491 to 0.648 and did not indicate problematic construct overlap. In addition to the Fornell–Larcker criterion, heterotrait–monotrait ratios were examined. These values ranged from 0.516 to 0.824 and remained below the conservative threshold of 0.85. The cross-loading analysis similarly indicated that each item loaded more strongly on its intended construct than on other constructs. Taken together, these findings established satisfactory discriminant validity and confirmed that smart contract governance, decentralized identity, security and privacy, technological infrastructure, organizational readiness, monitoring and risk management, and effective access-control management were empirically distinguishable dimensions of the strategic framework.

Table 4. Structural Model Results for the Proposed Strategic Framework

Hypothesized Relationship	Standardized Path Coefficient	Standard Error	t Value	p Value	95% Confidence Interval	Effect Size
Smart Contract Governance and Policy Management → Effective Access-Control Management	0.214	0.052	4.115	<0.001	0.113–0.316	0.081
Decentralized Identity and Trust Management → Effective Access-Control Management	0.146	0.049	2.980	0.003	0.052–0.243	0.041
Security and Privacy Assurance → Effective Access-Control Management	0.257	0.055	4.673	<0.001	0.151–0.364	0.105
Technological Infrastructure and Interoperability → Effective Access-Control Management	0.119	0.047	2.532	0.012	0.029–0.213	0.030
Organizational and Regulatory Readiness → Effective Access-Control Management	0.138	0.046	3.000	0.003	0.049–0.228	0.039
Continuous Monitoring, Auditability, and Risk Management → Effective Access-Control Management	0.284	0.056	5.071	<0.001	0.176–0.393	0.127
Organizational and Regulatory Readiness → Smart Contract Governance and Policy Management	0.412	0.058	7.103	<0.001	0.302–0.527	0.205
Technological Infrastructure and Interoperability → Continuous Monitoring, Auditability, and Risk Management	0.367	0.061	6.016	<0.001	0.247–0.484	0.156
Security and Privacy Assurance → Continuous Monitoring, Auditability, and Risk Management	0.391	0.059	6.627	<0.001	0.277–0.506	0.178
Organizational and Regulatory Readiness → Smart Contract Governance → Effective Access-Control Management	0.088	0.026	3.385	0.001	0.042–0.145	—
Security and Privacy Assurance → Continuous Monitoring and Risk Management → Effective Access-Control Management	0.111	0.030	3.700	<0.001	0.060–0.177	—
Technological Infrastructure and Interoperability → Continuous Monitoring and Risk Management → Effective Access-Control Management	0.104	0.029	3.586	<0.001	0.053–0.167	—

The structural model was assessed after confirming the reliability and validity of the measurement model. Collinearity diagnostics showed that the variance inflation factor values for the predictor constructs ranged from 1.48 to 2.67, remaining below the critical threshold and indicating that multicollinearity did not distort the estimated structural relationships. Bootstrapping with 5,000 resamples demonstrated that all proposed direct relationships were statistically significant. Continuous monitoring, auditability, and risk management had the strongest direct effect on

effective management of smart contract–driven access control, with a standardized path coefficient of 0.284, a t value of 5.071, and a probability value below 0.001. This finding indicated that real-time monitoring, immutable audit trails, abnormal-access detection, performance evaluation, risk assessment, and recovery planning were the most influential direct contributors to the effectiveness of the proposed framework.

Security and privacy assurance had the second strongest direct effect, with a standardized coefficient of 0.257. This result demonstrated that the strategic framework depended substantially on secure smart contract code, reliable cryptographic mechanisms, protected identity credentials, transaction confidentiality, attack resistance, and effective incident response. Smart contract governance and policy management also exerted a significant direct effect on access-control effectiveness, with a coefficient of 0.214. Therefore, the formalization of access rules, contract updating, permission revocation, emergency intervention, and assignment of governance responsibilities constituted essential strategic mechanisms rather than merely administrative considerations. Decentralized identity and trust management had a significant coefficient of 0.146, showing that verifiable identities, device registration, credential management, and continuous trust assessment improved the reliability of authorization decisions. Organizational and regulatory readiness had a direct coefficient of 0.138, while technological infrastructure and interoperability had a coefficient of 0.119. Although these coefficients were smaller than those associated with security, governance, and monitoring, both effects were statistically significant and demonstrated that technical compatibility, organizational capabilities, managerial support, specialist knowledge, regulatory alignment, and stakeholder coordination remained necessary for effective implementation.

The analysis also identified significant relationships among the framework's antecedent and intermediary dimensions. Organizational and regulatory readiness had a strong positive effect on smart contract governance and policy management, with a coefficient of 0.412. This result indicated that organizations with stronger leadership support, clearer accountability structures, more developed data-governance procedures, adequate technical competence, and greater regulatory awareness were more capable of translating access-control requirements into formally governed smart contracts. Security and privacy assurance had a coefficient of 0.391 in predicting continuous monitoring, auditability, and risk management, while technological infrastructure and interoperability had a coefficient of 0.367. These findings suggested that continuous monitoring could not be established independently of secure technical foundations, compatible infrastructure, reliable communication mechanisms, and appropriately integrated blockchain and edge-computing components.

The indirect effects were also statistically significant. Organizational and regulatory readiness influenced effective access-control management through smart contract governance and policy management, with an indirect coefficient of 0.088. Because both the direct and indirect effects were significant, smart contract governance functioned as a partial mediator of the relationship between organizational readiness and access-control effectiveness. Security and privacy assurance indirectly affected effective access-control management through continuous monitoring and risk management, with a coefficient of 0.111. Technological infrastructure and interoperability also produced a significant indirect effect of 0.104 through the same mediating construct. These results indicated that secure and interoperable technical foundations improved access-control effectiveness partly by enabling stronger monitoring, auditing, anomaly detection, and risk-management capabilities.

The model explained 68.4% of the variance in effective management of smart contract–driven access control. It also explained 17.0% of the variance in smart contract governance and policy management and 44.9% of the variance in continuous monitoring, auditability, and risk management. The coefficient of determination for the primary dependent construct indicated substantial explanatory power. The Stone–Geisser predictive relevance value for effective access-control management was 0.452, demonstrating strong predictive relevance. The Q^2 values for smart contract governance and continuous monitoring were 0.097 and 0.286, respectively, and were greater than zero, confirming that the model possessed predictive capability for all endogenous constructs. The standardized root mean square residual was 0.061, which indicated an acceptable overall model fit. The normed fit index was 0.912, providing additional support for the adequacy of the proposed structural model.

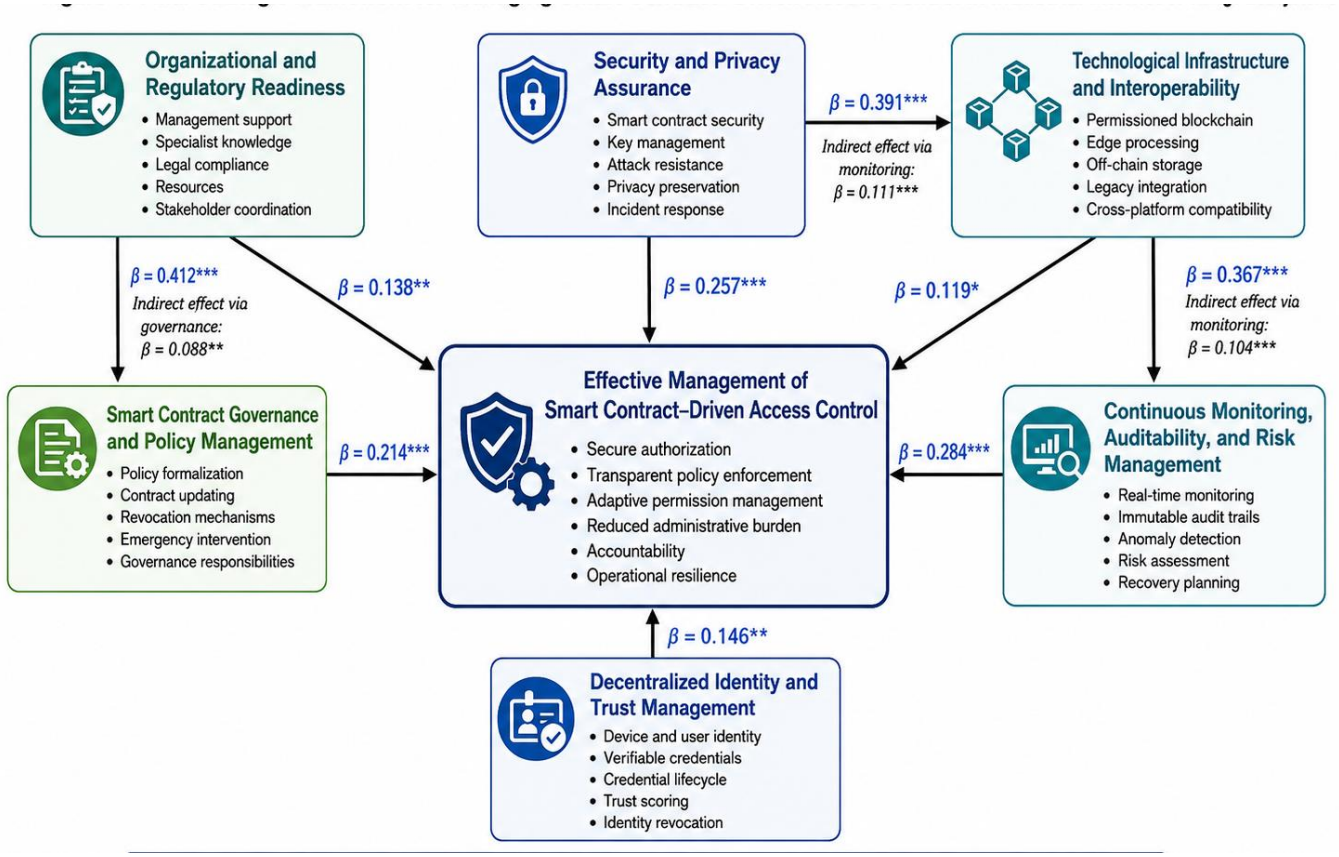

Figure 1. Final Strategic Framework for Managing Smart Contract–Driven Access Control in Industrial Internet of Things Ecosystems

The final integrated framework illustrated that effective management of smart contract–driven access control resulted from the coordinated interaction of six principal strategic dimensions rather than from the isolated implementation of blockchain technology. At the center of the framework was effective access-control management, defined by secure authorization, transparent policy enforcement, adaptive permission management, reduced administrative burden, accountable decision-making, and increased operational resilience. Smart contract governance and policy management, decentralized identity and trust management, security and privacy assurance, technological infrastructure and interoperability, organizational and regulatory readiness, and continuous monitoring, auditability, and risk management were positioned as the major determinants of this central outcome.

The framework further demonstrated that organizational and regulatory readiness provided the institutional foundation for smart contract governance. Management support, skilled personnel, financial resources, legal clarity, data-governance procedures, and stakeholder coordination enabled organizations to define access policies and convert them into executable, reviewable, and accountable smart contract rules. Technological infrastructure and interoperability, together with security and privacy assurance, formed the technical foundation for continuous monitoring and risk management. Permissioned blockchain architecture, edge processing, lightweight consensus, off-chain storage, secure gateways, protected cryptographic keys, contract auditing, and vulnerability testing enabled organizations to monitor authorization events and identify abnormal behavior without imposing unacceptable latency or computational burdens on industrial devices.

The final framework also indicated that access-control management should be understood as a continuous lifecycle. The process begins with the registration and verification of users, devices, applications, and gateways. It then proceeds through the assignment of decentralized identities and verifiable credentials, the formalization of access policies, and the deployment of smart contracts that automatically enforce authorization conditions. After deployment, access decisions are continuously monitored, logged, audited, and evaluated. Changes in device behavior, user roles, operational conditions, threat levels, or regulatory requirements trigger policy reassessment and, where necessary, contract updating, permission suspension, or

identity revocation. Emergency access and recovery procedures remain available for exceptional industrial conditions, but their use is documented and subjected to subsequent review. The framework therefore combines automation with human accountability and strategic oversight.

The integration of qualitative and quantitative findings confirmed that no single technological component was sufficient to ensure effective access control. Blockchain immutability alone could not guarantee secure authorization if vulnerable smart contracts, compromised identities, inadequate governance, or incompatible legacy systems remained unaddressed. Similarly, strong organizational policies could not be implemented effectively in the absence of scalable infrastructure, secure identity mechanisms, and continuous technical monitoring. The findings therefore supported a multilayered strategic approach in which technical architecture, security controls, identity management, organizational governance, regulatory compliance, and continuous risk management operate as interconnected elements. This integrated structure constituted the final strategic framework for managing smart contract–driven access control in Industrial Internet of Things ecosystems.

4. Discussion and Conclusion

The present study developed and validated a strategic framework for managing smart contract–driven access control in Industrial Internet of Things ecosystems. The qualitative findings identified seven principal themes: smart contract governance and policy management, decentralized identity and trust management, security and privacy assurance, technological infrastructure and interoperability, organizational and regulatory readiness, continuous monitoring, auditability, and risk management, and the strategic outcomes of effective access-control management. The quantitative findings supported the reliability and validity of these dimensions and showed that all six antecedent constructs exerted significant direct effects on effective access-control management. The model explained 68.4% of the variance in the principal outcome, indicating that the proposed framework possessed substantial explanatory power. Among the direct predictors, continuous monitoring, auditability, and risk management had the strongest effect, followed by security and privacy assurance, smart contract governance and policy management, decentralized identity and trust management, organizational and regulatory readiness, and technological infrastructure and interoperability. Significant indirect effects further showed that smart contract governance partially mediated the influence of organizational readiness, while continuous monitoring and risk management partially mediated the effects of security assurance and technological infrastructure.

The strongest direct relationship was observed between continuous monitoring, auditability, and risk management and effective management of smart contract–driven access control. This result indicates that the effectiveness of blockchain-based authorization depends not only on the initial design of access policies but also on the ability to supervise their ongoing execution, detect abnormal behavior, preserve traceable records, and adapt controls in response to emerging risks. In Industrial Internet of Things environments, access relationships are highly dynamic because devices join and leave networks, user roles change, operational conditions fluctuate, and vulnerabilities may emerge after deployment. Therefore, immutable transaction records and automated policy enforcement are insufficient unless organizations can continuously examine whether smart contracts are functioning as intended. This finding aligns with studies emphasizing dynamic access policies, contextual authorization, and continuous assessment as essential requirements for IoT access control [4, 5]. It is also consistent with the literature on distributed ledger–based authentication and access control, which highlights auditability and traceability as major advantages of blockchain integration [18].

The importance of monitoring can also be explained by the irreversible or difficult-to-modify nature of deployed smart contracts. An incorrectly coded authorization rule may repeatedly execute without human intervention, producing systematic rather than isolated access-control failures. Continuous contract monitoring, anomaly detection, event logging, and post-deployment auditing therefore serve as compensatory mechanisms that reduce the risks associated with automated enforcement. The significant predictive role of this dimension is consistent with research showing that smart contracts provide strong automation capabilities while also introducing risks related to coding errors, inflexibility, external dependencies, and unintended execution [10]. The result further supports blockchain-centric IoT architectures in which access transactions and communication events are recorded in a transparent and verifiable manner, enabling subsequent review and accountability [15]. Thus, monitoring should be interpreted not as an auxiliary

operational function but as a core strategic component of smart contract governance.

Security and privacy assurance had the second strongest direct effect on effective access-control management. This finding confirms that blockchain does not automatically eliminate the broader security risks of Industrial Internet of Things environments. Although a distributed ledger can protect the integrity of recorded transactions, it cannot independently secure compromised devices, poorly written smart contracts, exposed cryptographic keys, malicious gateways, vulnerable interfaces, or insecure external data sources. The result is consistent with comprehensive reviews showing that blockchain–IoT integration remains vulnerable to smart contract attacks, key compromise, denial-of-service incidents, malicious nodes, privacy leakage, and consensus-related threats [1, 2]. It also aligns with recent lightweight blockchain-enhanced security protocols demonstrating that authentication, key exchange, and cryptographic efficiency remain central concerns in cloud–IoT and cyber-physical systems [33].

The strong effect of security and privacy assurance also reflects the sensitivity of industrial data and operational commands. Access-control transactions may reveal production schedules, maintenance activities, user responsibilities, device relationships, and patterns of system utilization. Even when the underlying data are not directly stored on-chain, transactional metadata can expose sensitive organizational information. The finding therefore supports research emphasizing encryption, pseudonymity, selective disclosure, off-chain storage, and privacy-preserving access mechanisms in blockchain systems [22, 23]. Similar concerns have been reported in smart-city and IoT data-sharing architectures, where transparency must be balanced against confidentiality and regulatory requirements [24, 25]. The present results extend these observations to industrial ecosystems by showing that security and privacy protections directly shape the effectiveness of access-control management rather than merely influencing user acceptance or technical compliance.

Smart contract governance and policy management also significantly predicted effective access-control management. This finding suggests that access-control performance depends on how authorization rules are designed, approved, encoded, updated, suspended, and revoked. Smart contracts can automatically enforce predefined conditions, but the legitimacy and safety of their execution depend on organizational decisions made before and after deployment. The result is consistent with prior studies demonstrating that smart contracts can operationalize attribute-based, context-aware, and device-level authorization policies [12-14]. However, the present study extends this literature by demonstrating that policy formalization alone is insufficient. Effective governance additionally requires version control, separation of duties, emergency intervention, accountability, and clearly assigned authority for modifying contract logic.

The significance of governance is particularly important in industrial environments because access-control errors can affect physical processes and safety-critical operations. A technically valid but organizationally inappropriate rule may deny essential emergency access or permit actions outside an operator's legitimate responsibility. The framework therefore supports a controlled balance between automation and human oversight. This interpretation corresponds with broader analyses of smart contract applications that identify automation and trust reduction as major benefits while warning that immutable or self-executing code may reproduce flawed assumptions at scale [10, 11]. The findings imply that smart contracts should be treated as governed organizational instruments rather than autonomous substitutes for managerial responsibility.

Decentralized identity and trust management had a positive and significant effect on effective access-control management. This result was expected because authorization cannot be reliable unless the identities of users, devices, gateways, software agents, and services can be established and maintained throughout their operational lifecycles. Industrial Internet of Things systems contain numerous nonhuman entities whose identities may change because of maintenance, ownership transfer, software updates, credential expiration, or compromise. Blockchain-based identity mechanisms offer decentralized registration, verifiable credentials, cryptographic authentication, and tamper-resistant histories, but they must also support revocation, recovery, and trust reevaluation. The present result aligns with surveys showing that distributed ledger technology can strengthen identity and access management while reducing reliance on centralized identity providers [17]. It is also consistent with blockchain-based identity systems designed for IoT environments [19] and authentication approaches using hashing and digital signatures for connected devices [20].

The qualitative emphasis on credential lifecycle management and compromised-device isolation further supports research on secure onboarding and key management in federated IoT environments [21]. Initial

identity registration is insufficient when devices remain operational for long periods and may be exposed to physical tampering, malware, or unauthorized reassignment. The significant structural path therefore indicates that identity management should be continuous and risk-sensitive. In practice, access permissions should be linked not only to static identifiers but also to the current validity of credentials, behavioral trust indicators, operational context, and device status. This conclusion also aligns with dynamic and spatio-temporal authorization models that evaluate contextual attributes before granting permission [5, 13].

Organizational and regulatory readiness directly influenced effective access-control management and also exerted an indirect effect through smart contract governance. This mediation result is theoretically important because it shows that organizational readiness produces stronger access-control outcomes when it is translated into formal governance procedures. Management support, legal awareness, specialist expertise, financial resources, and stakeholder coordination do not improve access control automatically; they do so by enabling organizations to establish clear policy authority, contract-development standards, validation procedures, and accountability arrangements. This result addresses a limitation in much of the existing literature, which often concentrates on technical architectures while treating organizational capacity as an external implementation issue. The present findings demonstrate that institutional readiness is part of the causal structure of effective blockchain-based access control.

The result also reflects the multi-stakeholder character of Industrial Internet of Things ecosystems. Industrial organizations may depend on equipment vendors, cloud providers, telecommunications operators, software developers, cybersecurity teams, regulators, and external maintenance contractors. These actors may possess different legal responsibilities and operational priorities. Blockchain platforms and smart contracts can coordinate transactions among multiple parties, as demonstrated in hyper-connected smart-city and IoT marketplace environments [29]. However, technological coordination does not remove the need for clear data ownership, liability allocation, dispute-resolution procedures, and regulatory compliance. The present framework therefore positions organizational and regulatory readiness as the institutional foundation for trustworthy smart contract deployment.

Technological infrastructure and interoperability had the smallest but still significant direct effect on effective access-control management. Its smaller coefficient should not be interpreted as evidence of limited importance. Rather, the result suggests that infrastructure functions partly through other strategic mechanisms, particularly continuous monitoring and risk management. This interpretation is supported by the significant indirect effect of technological infrastructure through the monitoring construct. Permissioned blockchains, edge processing, off-chain storage, gateway integration, and lightweight consensus mechanisms improve access-control effectiveness because they enable timely policy evaluation, reliable logging, anomaly detection, and scalable supervision.

This finding aligns with studies arguing that blockchain integration with edge computing can reduce latency, distribute trust, and support secure IoT processing [26]. It is also compatible with emerging beyond-5G and 6G architectures that combine decentralized communication, privacy-preserving computation, and large-scale device connectivity [27, 28]. At the same time, research continues to identify interoperability, scalability, platform fragmentation, and legacy-system integration as major barriers to blockchain–IoT deployment [3, 7, 8]. The current results reinforce the argument that technological architecture must be designed as an enabling layer rather than as the complete access-control solution.

The significant indirect effect of security and privacy assurance through continuous monitoring and risk management further clarifies the internal logic of the framework. Strong security controls make monitoring more reliable by protecting logs, identities, communication channels, and contract execution. At the same time, monitoring allows organizations to identify failures that preventive controls cannot eliminate. This reciprocal functional relationship explains why both dimensions emerged as the strongest determinants of effective access-control management. The result supports hybrid architectures that combine blockchain with trusted hardware and secure execution environments to protect sensitive authorization processes [16]. It also corresponds with research emphasizing that blockchain should be integrated with other security mechanisms rather than deployed as a standalone solution [1].

The overall explanatory power of the model indicates that effective smart contract–driven access control is a multidimensional strategic outcome. No single determinant was sufficient on its own. Identity without governance could produce valid credentials governed by inappropriate policies; governance without secure infrastructure could formalize rules that remain technically vulnerable;

blockchain immutability without privacy could expose sensitive industrial patterns; and automation without monitoring could perpetuate flawed decisions. The framework therefore contributes an integrated perspective that connects technological design with governance, organizational capability, continuous supervision, and risk management. This integration is consistent with the broader evolution of blockchain from a transaction-recording technology toward a platform for trust, automation, digital assets, artificial intelligence, and decentralized service coordination [9, 30-32].

In summary, the findings demonstrate that smart contract–driven access control should be managed as a continuously governed socio-technical system. The proposed framework suggests a lifecycle beginning with organizational preparation and infrastructure design, followed by identity registration, policy formalization, contract deployment, authorization execution, continuous monitoring, risk evaluation, policy revision, and credential revocation. This lifecycle approach reconciles automation with oversight, decentralization with accountability, transparency with privacy, and immutability with operational adaptability. The validated framework therefore provides a structured basis for organizations seeking to implement secure, scalable, auditable, and strategically governed access control across Industrial Internet of Things ecosystems.

This study had several limitations that should be considered when interpreting its findings. The participants were recruited exclusively from Tehran, and although they represented multiple industrial, academic, cybersecurity, blockchain, and technology-management backgrounds, the results may not fully reflect the conditions of other cities, countries, or industrial sectors. The quantitative findings were based on expert perceptions rather than operational measurements obtained from a deployed Industrial Internet of Things platform. Consequently, the estimated relationships represent validated professional judgments about the framework rather than direct evidence of system performance under real-time industrial conditions. The cross-sectional design also prevented examination of how organizational readiness, access-control maturity, and smart contract governance evolve over time. In addition, the framework was developed at a strategic level and did not compare the performance of specific blockchain platforms, consensus mechanisms, smart contract languages, or industrial communication protocols.

Future research should validate the framework in different geographical, regulatory, and industrial contexts and should include participants from manufacturing, energy, transportation, healthcare, mining, and critical-infrastructure sectors. Longitudinal studies could examine how the framework performs across different stages of blockchain adoption and whether the importance of its dimensions changes as organizations gain experience. Experimental and simulation-based investigations should test the framework using operational indicators such as authorization latency, throughput, energy consumption, attack-detection accuracy, revocation time, contract-execution cost, and recovery performance. Comparative studies could evaluate permissioned and public blockchain architectures, alternative consensus mechanisms, edge-assisted designs, and different smart contract platforms. Future studies should also investigate the effects of artificial intelligence–based anomaly detection, zero-knowledge proofs, decentralized identifiers, post-quantum cryptography, and cross-chain interoperability on the proposed framework.

Industrial organizations should begin implementation by establishing a cross-functional governance team that includes cybersecurity specialists, operational technology engineers, blockchain developers, legal experts, risk managers, and senior decision-makers. Access policies should be formally documented before being translated into smart contract code, and every contract should undergo independent review, vulnerability testing, and controlled deployment. Organizations should use permissioned blockchain architectures where confidentiality, performance, and organizational accountability are priorities, while sensitive operational data should generally remain off-chain. Device identities, credentials, and cryptographic keys should be managed throughout their complete lifecycles, including onboarding, renewal, suspension, replacement, and revocation. Real-time monitoring, immutable audit trails, anomaly detection, emergency override procedures, and periodic policy reviews should be established before large-scale deployment. Pilot implementation in a limited industrial domain is recommended before the framework is extended across the entire ecosystem.

Authors' Contributions

Authors equally contributed to this article.

Acknowledgments

Authors thank all participants who participate in this study.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

References

[1] L. A. C. Ahakonye, C. I. Nwakanma, and D. S. Kim, "Tides of Blockchain in IoT Cybersecurity," *Sensors,* vol. 24, no. 10, p. 3111, 2024, doi: 10.3390/s24103111.

[2] Y. I. Alzoubi, A. Al-Ahmad, H. Kahtan, and A. Jaradat, "Internet of Things and Blockchain Integration: Security, Privacy, Technical, and Design Challenges," *Future Internet,* vol. 14, no. 7, p. 216, 2022, doi: 10.3390/fi14070216.

[3] C. Nartey *et al.*, "On Blockchain and IoT Integration Platforms: Current Implementation Challenges and Future Perspectives," *Wireless Communications and Mobile Computing,* vol. 2021, no. 1, 2021, doi: 10.1155/2021/6672482.

[4] A. Khan, A. Ahmad, M. Ahmed, J. Sessa, and M. Anisetti, "Authorization Schemes for Internet of Things: Requirements, Weaknesses, Future Challenges and Trends," *Complex & Intelligent Systems,* vol. 8, no. 5, pp. 3919-3941, 2022, doi: 10.1007/s40747-022-00765-y.

[5] K. Ragothaman, Y. Wang, B. P. Rimal, and M. Lawrence, "Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions," *Sensors,* vol. 23, no. 4, p. 1805, 2023, doi: 10.3390/s23041805.

[6] M. A. Şimşek, "A Study of Blockchain in Iot Architecture," *International Journal of Engineering and Innovative Research,* vol. 3, no. 2, pp. 163-174, 2021, doi: 10.47933/ijeir.851109.

[7] C. Trivedi, U. P. Rao, K. Parmar, P. Bhattacharya, S. Tanwar, and R. Sharma, "A Transformative Shift Toward Blockchain-based<scp>IoT</Scp>environments: Consensus, Smart Contracts, and Future Directions," *Security and Privacy,* vol. 6, no. 5, 2023, doi: 10.1002/spy2.308.

[8] C. Trivedi, U. P. Rao, K. Parmar, P. Bhattacharya, and S. Tanwar, "A Transformative Shift Towards Blockchain-Based IoT Environments: Consensus, Smart Contracts, and Future Directions," 2024, doi: 10.22541/au.170663514.49171896/v1.

[9] Z. Ullah, F. M. A. Turjman, A. waqas, N. Saeed, and A. Coronato, "A Comprehensive Survey of Blockchain Applications in Communication Networks," 2026, doi: 10.21203/rs.3.rs-8622215/v1.

[10] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on Blockchain Based Smart Contracts: Applications, Opportunities and Challenges," *Journal of Network and Computer Applications,* vol. 177, p. 102857, 2021, doi: 10.1016/j.jnca.2020.102857.

[11] H. Chen, N. Wei, L. Wang, W. Mobarak, M. A. Albahar, and Z. A. Shaikh, "The Role of Blockchain in Finance Beyond Cryptocurrency: Trust, Data Management, and Automation," *Ieee Access,* vol. 12, pp. 64861-64885, 2024, doi: 10.1109/access.2024.3395918.

[12] S. Y. A. Zaidi *et al.*, "An Attribute-Based Access Control for IoT Using Blockchain and Smart Contracts," *Sustainability,* vol. 13, no. 19, p. 10556, 2021, doi: 10.3390/su131910556.

[13] F. Guo, G. Shen, Z. Huang, Y. Yang, M. Cai, and L. Wei, "DABAC: Smart Contract-Based Spatio-Temporal Domain Access Control for the Internet of Things," *Ieee Access,* vol. 11, pp. 36452-36463, 2023, doi: 10.1109/access.2023.3257027.

[14] M. R. Hasan *et al.*, "Smart Contract-Based Access Control Framework for Internet of Things Devices," *Computers,* vol. 12, no. 11, p. 240, 2023, doi: 10.3390/computers12110240.

[15] A. S. Albulayhi and I. S. Alsukayti, "A Blockchain-Centric IoT Architecture for Effective Smart Contract-Based Management of IoT Data Communications," *Electronics,* vol. 12, no. 12, p. 2564, 2023, doi: 10.3390/electronics12122564.

[16] J. Han *et al.*, "A Blockchain-Based and SGX-Enabled Access Control Framework for IoT," *Electronics,* vol. 11, no. 17, p. 2710, 2022, doi: 10.3390/electronics11172710.

[17] F. Ghaffari, K. Gilani, E. Bertin, and N. Crespi, "Identity and Access Management Using Distributed Ledger Technology: A Survey," *International Journal of Network Management,* vol. 32, no. 2, 2021, doi: 10.1002/nem.2180.

[18] F. Ghaffari, E. Bertin, N. Crespi, and J. Hatin, "Distributed Ledger Technologies for Authentication and Access Control in Networking Applications: A Comprehensive Survey," *Computer Science Review,* vol. 50, p. 100590, 2023, doi: 10.1016/j.cosrev.2023.100590.

[19] S. Venkatraman and S. Parvin, "Developing an IoT Identity Management System Using Blockchain," *Systems,* vol. 10, no. 2, p. 39, 2022, doi: 10.3390/systems10020039.

[20] L. Wang, Y. Yuan, and Y. Ding, "Analysis and Design of Identity Authentication for IoT Devices in the Blockchain Using Hashing and Digital Signature Algorithms," *International Journal of Distributed Sensor Networks,* vol. 2023, pp. 1-12, 2023, doi: 10.1155/2023/2524051.

[21] K. Kanciak, K. Wrona, and M. Jarosz, "Secure Onboarding and Key Management in Federated IoT Environments," vol. 30, pp. 627-634, 2022, doi: 10.15439/2022f173.

[22] A. Chhabra, R. Saha, G. Kumar, and T.-h. Kim, "Navigating the Maze: Exploring Blockchain Privacy and Its Information Retrieval," *Ieee Access,* vol. 12, pp. 32089-32110, 2024, doi: 10.1109/access.2024.3370857.

[23] A. Qashlan, P. Nanda, X. He, and M. Mohanty, "Privacy-Preserving Mechanism in Smart Home Using Blockchain," *Ieee Access,* vol. 9, pp. 103651-103669, 2021, doi: 10.1109/access.2021.3098795.

[24] A. Padma and M. Ramaiah, "Blockchain Based an Efficient and Secure Privacy Preserved Framework for Smart Cities," *Ieee Access,* vol. 12, pp. 21985-22002, 2024, doi: 10.1109/access.2024.3364078.

[25] P. T. Tran-Truong, V. T. P. Nguyen, H. X. Son, P. Nguyen-Ngoc, K. H. Vo, and T. M. Nguyen, "Systematic Survey on Privacy-Preserving Architectures for IoT and Vehicular Data Sharing: Techniques, Challenges, and Future Directions," 2026, doi: 10.48550/arxiv.2603.01876.

[26] T. S. Gupta and H. Patel, "Integrating Blockchain Technology With Internet of Things and Edge Computing to Achieve Security," *Journal of Ecohumanism,* vol. 3, no. 7, 2024, doi: 10.62754/joe.v3i7.4620.

[27] N. A. Jalali and H. Chen, "Federated Learning Incentivize With Privacy-Preserving for IoT in Edge Computing in the Context of B5G," 2024, doi: 10.21203/rs.3.rs-4513308/v1.
[28] T. Nguyen, L. Lovén, J. Partala, and S. Pirttikangas, "The Intersection of Blockchain and 6G Technologies," pp. 393-417, 2021, doi: 10.1007/978-3-030-72777-2_18.
[29] G. Palaiokrassas *et al.*, "Combining Blockchains, Smart Contracts, and Complex Sensors Management Platform for Hyper-Connected SmartCities: An IoT Data Marketplace Use Case," *Computers,* vol. 10, no. 10, p. 133, 2021, doi: 10.3390/computers10100133.
[30] R. Wang, M. Luo, Y. Wen, L. Wang, K. K. R. Choo, and D. He, "The Applications of Blockchain in Artificial Intelligence," *Security and Communication Networks,* vol. 2021, pp. 1-16, 2021, doi: 10.1155/2021/6126247.
[31] S. Kumar, W. M. Lim, U. Sivarajah, and J. Kaur, "Artificial Intelligence and Blockchain Integration in Business: Trends From a Bibliometric-Content Analysis," *Information Systems Frontiers,* 2022, doi: 10.1007/s10796-022-10279-0.
[32] V. T. Truong, L. B. Le, and D. Niyato, "Blockchain Meets Metaverse and Digital Asset Management: A Comprehensive Survey," *Ieee Access,* vol. 11, pp. 26258-26288, 2023, doi: 10.1109/access.2023.3257029.
[33] A. U. Rehman *et al.*, "IBS-ECDHE: A Blockchain-Enhanced Lightweight Protocol for Secure Cloud-IoT in Biomedical HCPS," *Computational and Structural Biotechnology Journal,* vol. 28, pp. 564-591, 2025, doi: 10.1016/j.csbj.2025.10.059.