International Journal of Scientific Interdisciplinary Research

Volume: *2;* ***Issue:*** *2*
Pages: *98–127*

open access
Crossref
PEER-REVIEWED

BLOCKCHAIN-ENABLED SECURITY PROTOCOLS COMBINED WITH AI FOR SECURING NEXT-GENERATION INTERNET OF THINGS (IoT) NETWORKS

Tonoy Kanti Chowdhury[1]; Shaikat Biswas[2];

[1]. B.Sc. in Computer Science and Engineering, South East University, Dhaka, Bangladesh;
Email: chowdhurytonoy93@gmail.com

[2]. Network Security Intern, Directed Labs & Coursework, Bangladesh;
Email: ethan.soikot@gmail.com

Doi: 10.63125/pcdqzw41
Received: *18 March 2021;* ***Revised:*** *29 April 2021;* ***Accepted:*** *21 May 2021;* ***Published:*** *28 June 2021*

Abstract

This study investigates how blockchain-enabled security protocols and artificial intelligence (AI)–based threat analytics jointly influence the perceived security performance of next-generation Internet of Things (IoT) networks. As IoT ecosystems expand across critical sectors, the limitations of traditional security models highlight the need for decentralized trust mechanisms and intelligent, adaptive intrusion detection. Drawing on theories of IoT security requirements, cyber-risk management, and blockchain–AI convergence, the study develops a conceptual framework comprising four constructs: Blockchain-Enabled Security Controls, AI-Driven Threat Analytics, IoT Cyber-Risk Management Maturity, and Contextual Factors, all hypothesized to affect IoT Security Performance. A quantitative, cross-sectional, case-study–based research design was employed, using a structured Likert five-point survey administered to 160 professionals actively engaged in IoT architecture, cybersecurity operations, and system administration. Reliability validation, correlation analysis, and multiple regression modeling were conducted to evaluate the relationships among constructs and to test three hypotheses concerning individual and interactive effects. Descriptive results indicated strong adoption of both blockchain and AI security capabilities, with mean construct scores exceeding the midpoint, and IoT Security Performance achieving the highest mean (4.12). Correlation analysis showed strong positive associations among all variables, especially between AI-based analytics and IoT Security Performance ($r = 0.68$). Regression results demonstrated that Blockchain-Enabled Security Controls ($\beta = 0.32$, $p < .001$) and AI-Driven Threat Analytics ($\beta = 0.41$, $p < .001$) each exerted significant positive effects on IoT Security Performance, while IoT Cyber-Risk Management Maturity contributed additional explanatory power ($\beta = 0.19$, $p = .003$). Importantly, an interaction term representing the coexistence of high blockchain, and AI capability revealed a positive and statistically significant effect ($\beta = 0.11$, $p = .033$), increasing model explanatory power ($\Delta R^2 = 0.03$) and confirming that blockchain and AI function synergistically rather than independently. Overall, the findings empirically validate the complementary roles of blockchain and AI in enhancing IoT confidentiality, integrity, availability, and resilience. The study contributes to IoT security scholarship by operationalizing and testing constructs that have largely been addressed conceptually in prior work. It further offers practical insights for organizations seeking integrated, risk-informed security architectures for large-scale IoT environments.

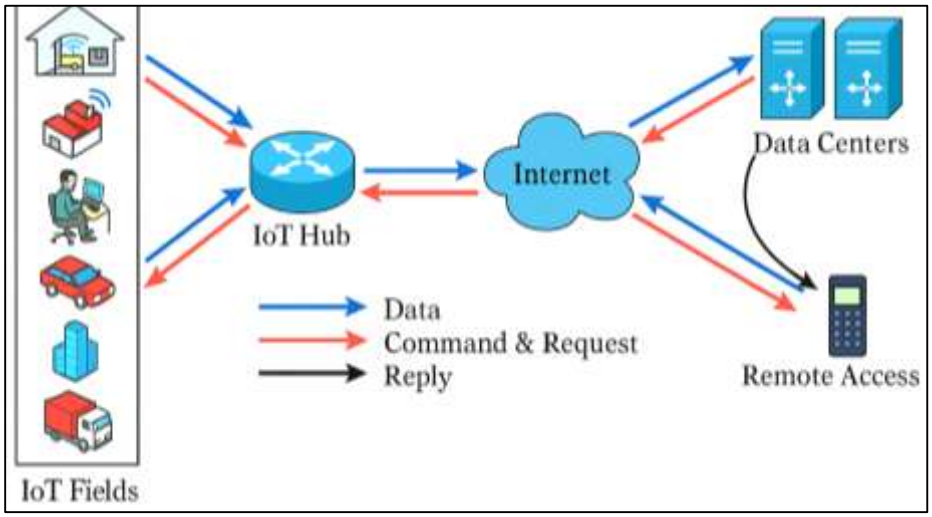
Keywords

Blockchain enabled IoT security, AI based threat analytics, Next generation IoT networks, Cyber risk management, IoT security performance;

INTRODUCTION

Internet of Things (IoT) generally refers to a global network of uniquely identifiable physical and virtual objects that are equipped with sensing, processing, and communication capabilities and interconnected over heterogeneous networks (Atzori et al., 2010). Through technologies such as RFID, embedded sensors, wireless communication, and cloud platforms, IoT systems continuously generate and exchange data across application domains including smart cities, healthcare, logistics, industrial automation, and consumer environments (Al-Fuqaha et al., 2015). The scale of this ecosystem is reflected in projections of tens of billions of connected devices worldwide and trillions of dollars in associated economic value, underscoring IoT's international significance for economic growth, social services, and critical infrastructure management (Misra et al., 2016). At the same time, this pervasive interconnection produces an expanded attack surface: constrained devices, heterogeneous protocols, and distributed deployments expose new security weaknesses that traditional Internet security mechanisms do not fully address (Roman et al., 2013). As next-generation IoT networks become increasingly data-driven and tightly integrated with 5G, edge computing, and cyber-physical systems, securing these environments becomes a central prerequisite for their sustained adoption across jurisdictions and industry sectors (Meidan et al., 2018).

Figure 1: Fundamental IoT Communication Model



The security and privacy challenges of IoT have been systematically explored from architectural, protocol, and data perspectives, revealing complex, multi-layered vulnerability patterns. Surveys of IoT architectures and industrial deployments emphasize that resource constraints, device mobility, and the use of proprietary stacks complicate the deployment of standard cryptographic and access-control solutions at scale (Mousavi et al., 2020). From a security viewpoint, studies identify confidentiality, integrity, availability, authentication, authorization, and trust management as core requirements that are difficult to enforce consistently across perception, network, and application layers (Sicari et al., 2015). Security taxonomies show that IoT systems are exposed to routing attacks, Sybil attacks, side-channel attacks, physical tampering, and protocol-specific threats, with many attacks exploiting weak device management and unpatched firmware (Xu et al., 2014). Data-centric analyses further highlight that sensitive telemetry, control commands, and user context data can be intercepted, modified, or exfiltrated, creating both operational and regulatory risks in sectors such as healthcare, transportation, and energy (Hou et al., 2019). As IoT deployments extend globally, cross-border data flows and heterogeneous regulatory regimes complicate compliance with privacy and cybersecurity standards, intensifying the need for robust, interoperable security protocols that retain effectiveness under varied legal and infrastructural conditions (Ferrag et al., 2020).

A large body of work has focused on security frameworks, cryptographic mechanisms, and intrusion detection for IoT, yet significant constraints remain. Protocol-level studies survey secure routing, key-

management schemes, and lightweight authentication, showing that many mechanisms either impose excessive computational overhead on constrained devices or fail to address sophisticated multi-vector attacks (Abdulla & Ibne, 2021; Granjal et al., 2015). Cryptography-oriented surveys stress the importance of tailoring symmetric and asymmetric algorithms, as well as hybrid approaches, to meet the trade-offs among energy consumption, memory footprint, and latency in IoT environments (Habibullah & Foysal, 2021; Hassan et al., 2019). Existing work on trust management demonstrates that fuzzy-logic-based and reputation-based schemes can capture context-aware trust relationships among devices, but these schemes often rely on local observations and can be vulnerable to collusion or data poisoning (Alshehri & Hussain, 2019; Sanjid & Farabe, 2021). Research on IoT-specific intrusion detection systems (IDS) highlights that host-based and network-based IDS must accommodate proprietary protocols, intermittent connectivity, and high volumes of streaming data while remaining deployable at the network edge (Sarwar, 2021; Zarpelão et al., 2017). Across these lines of work, there is continued emphasis on scalable, interoperable security architectures that can be realistically integrated into large-scale, heterogeneous IoT deployments operating under real-world resource and regulatory constraints (Chen et al., 2020; Musfiqur & Saba, 2021).

Artificial intelligence (AI) and, more specifically, machine learning (ML) and deep learning (DL), have been proposed as key enablers for intelligent IoT security monitoring and decision-making. Surveys of ML methods for cyber-security and intrusion detection show that supervised, unsupervised, and hybrid models can effectively classify malicious traffic, detect anomalies, and support network forensics in high-dimensional data spaces (Ahmed et al., 2016). In the IoT context, ML and DL-based IDSs are used to learn device-specific baselines and detect deviations that may indicate botnet infections, DDoS attacks, or unauthorized control commands (Alaba et al., 2017). Deep learning surveys report that architectures such as autoencoders, recurrent neural networks, and convolutional networks improve the detection of complex, evolving attack patterns by modeling non-linear relationships in network flows and system logs (Al-Garadi et al., 2020; Omar & Rashid, 2021). At the same time, this literature acknowledges challenges with explainability, training-data quality, and adversarial manipulation, especially when models are trained on data originating from untrusted IoT devices or federated deployments. Nonetheless, the integration of AI-driven detection with real-time monitoring, edge analytics, and automated response mechanisms is increasingly viewed as central to maintaining security in dense and dynamic IoT networks (Christidis & Devetsikiotis, 2016; MRedwanul et al., 2021).

In parallel, blockchain has emerged as a distributed, tamper-resistant ledger technology with promising applications for IoT security. Studies on blockchains and smart contracts for IoT illustrate how consensus protocols, immutable ledgers, and decentralized identity management can support secure data sharing, verifiable logging, and fine-grained access control in heterogeneous IoT ecosystems (Conoscenti et al., 2016; Tarek & Praveen, 2021). Systematic reviews of blockchain–IoT integration argue that distributed ledgers can underpin trust management, secure firmware updates, and auditable device interactions, enabling participants from different organizations and jurisdictions to verify data provenance and policy compliance without reliance on a single trusted intermediary (Gubbi et al., 2013). Work on privacy-preserving blockchain-based IoT systems further analyzes techniques such as anonymization, encryption, mixing, and private smart contracts to mitigate linkage attacks and protect sensitive metadata in ledger-recorded transactions (Zaman & Momena, 2021; Samaila et al., 2018). However, blockchain deployments in IoT must handle issues such as latency, throughput, storage overhead, and energy consumption on constrained devices, which has prompted research into lightweight consensus protocols, off-chain storage, and hierarchical or consortium-chain architectures tailored to IoT scenarios (Tewari & Gupta, 2020).

Recent scholarship increasingly points to the complementary roles of AI and blockchain for securing next-generation IoT networks. Surveys of machine and deep learning for IoT security present AI as a mechanism for security intelligence, enabling predictive analytics, behavior modeling, and adaptive threat detection over large volumes of device and network data (Rony, 2021; Yang et al., 2019). Blockchain-centric studies, in contrast, conceptualize the ledger as a trusted substrate for data integrity, identity management, and decentralized coordination among devices, gateways, and services (Christidis & Devetsikiotis, 2016). Integrative perspectives suggest that combining AI-driven analytics

with blockchain-backed data and smart contracts can result in security protocols where detection models are trained on verifiable data streams, model updates are auditable, and enforcement actions such as revoking device credentials or reconfiguring access policies are encoded as smart contracts executed under agreed rules (Hassan et al., 2019). In this combined paradigm, AI contributes adaptivity and pattern recognition, while blockchain contributes tamper-resistant logging and distributed trust, forming a layered defense structure suitable for large-scale, cross-organizational IoT networks in domains such as smart manufacturing, energy, and transportation.

The present study is guided by a set of clearly defined objectives that structure its overall design, data collection strategy, and analytical procedures. The primary objective is to empirically examine how blockchain-enabled security protocols and AI-based security analytics contribute to the security performance of next-generation IoT networks in real organizational contexts. To achieve this, the study first seeks to operationalize key constructs such as blockchain security capability, AI-based threat detection capability, organizational and technical readiness, and IoT network security performance through a rigorously designed Likert 5-point survey instrument administered within a case-study setting. A second objective is to quantify the individual effects of blockchain security capability and AI-based security capability on perceived IoT network security performance, using descriptive statistics to profile respondents and deployments, correlation analysis to explore the strength and direction of associations among constructs, and regression modeling to estimate their predictive power. A third objective is to evaluate the combined influence of blockchain and AI when considered as complementary security enablers, examining whether their joint presence is associated with enhanced security outcomes compared with the presence of either capability alone. A fourth objective is to assess the role of organizational and technical readiness as a contextual factor that shapes how organizations experience and evaluate blockchain- and AI-enabled IoT security, by examining whether readiness-related variables strengthen or weaken the observed relationships in the regression models. A further objective is to provide a structured empirical characterization of security practices, architectural choices, and decision criteria used by practitioners responsible for securing next-generation IoT deployments in the selected case context. Together, these objectives establish a coherent agenda focused on measurement, comparison, and explanation: measuring perceptions of key capabilities and outcomes, comparing the relative contributions of blockchain and AI, and explaining how their interaction and organizational context relate to perceived IoT network security performance in large-scale, connected environments.

LITERATURE REVIEW

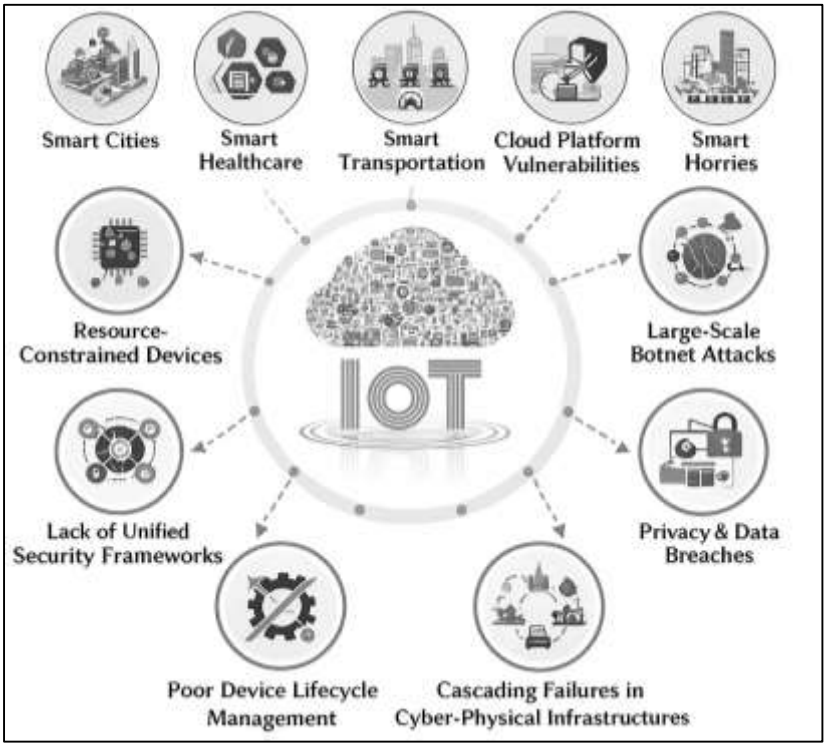
The literature on securing next-generation Internet of Things (IoT) networks has expanded rapidly, reflecting the convergence of three major domains: IoT architectures and their security challenges, blockchain-enabled security mechanisms, and AI-driven threat detection and analytics. As IoT deployments scale across industrial automation, smart cities, healthcare, transportation, and energy systems, they introduce vast numbers of heterogeneous, resource-constrained devices communicating over diverse protocols and infrastructures. This environment creates complex attack surfaces that traditional perimeter-based and centralized security models struggle to handle, particularly with respect to device authentication, data integrity, access control, and real-time anomaly detection. In response, researchers have explored lightweight cryptographic schemes, trust and reputation models, intrusion detection systems, and secure communication protocols tailored to IoT constraints, yet persistent issues of scalability, interoperability, and manageability continue to appear in empirical and conceptual work. Alongside these developments, blockchain has emerged as a promising distributed ledger technology that can provide tamper-resistant logging, decentralized identity and key management, and transparent execution of access policies through smart contracts, offering a way to redistribute trust and reduce reliance on single points of failure in IoT ecosystems. At the same time, advances in artificial intelligence particularly machine learning and deep learning have enabled data-driven approaches to network and device security, where models learn behavioral baselines, detect anomalies, classify malicious traffic, and support automated or semi-automated response. A growing stream of research examines how these two paradigms blockchain and AI can be combined to form integrated security frameworks in which blockchain ensures the integrity and non-repudiation of

security-relevant data and policies, while AI provides adaptive, predictive analytics over those data to detect and mitigate evolving threats. However, much of this work remains conceptual, architectural, or limited to simulations and testbeds, with comparatively fewer studies providing quantitative, case-based evidence on how organizations perceive and experience the security benefits of blockchain- and AI-enabled IoT solutions. This literature review therefore synthesizes prior work across these three domains to identify key constructs, relationships, and gaps that inform the conceptual framework and hypotheses of the present study.

Security Challenges in Next-Generation IoT Networks

Next-generation Internet of Things (IoT) networks introduce an unprecedented spectrum of security challenges because they interconnect billions of heterogeneous, resource-constrained devices across mission-critical domains such as healthcare, transportation, manufacturing, and energy. Rather than operating as isolated sensor deployments, modern IoT ecosystems are deeply integrated with cloud platforms, edge computing nodes, and legacy enterprise systems, which expands the attack surface and magnifies the potential impact of breaches. Survey studies show that the combination of large-scale connectivity, heterogeneity of protocols, and frequent mobility of devices makes traditional perimeter-based defenses insufficient, as adversaries can exploit weakly protected nodes to pivot across the entire network and target high-value assets (Radoglou-Grammatikis et al., 2019). Moreover, many low-cost IoT devices are designed with minimal security features due to strict cost, power, and computation constraints, resulting in inadequate authentication, weak or hard-coded credentials, and lack of secure boot mechanisms. These design choices enable large botnets, such as those used in distributed denial-of-service (DDoS) attacks, where compromised endpoints are weaponized to overwhelm services and disrupt critical infrastructure. Comprehensive reviews of IoT security concerns further emphasize that security requirements confidentiality, integrity, availability, authentication, and non-repudiation are often addressed in a fragmented way, with no consistent end-to-end framework spanning device, network, and application layers (Leloglu, 2017).

Figure 2: Major Vulnerabilities in Smart IoT Domains and Cyber-Physical Systems



From an architectural perspective, IoT security challenges manifest differently across the perception, network, and application layers, and the interplay between these layers complicates mitigation strategies. At the perception layer, constrained sensors and actuators deployed in often unprotected physical environments are exposed to tampering, node capture, side-channel attacks, and invasive hardware probing. At the network layer, lightweight communication protocols such as MQTT, CoAP, and 6LoWPAN may lack robust encryption or mutual authentication by default, making traffic vulnerable to eavesdropping, spoofing, replay, routing manipulation, and man-in-the-middle attacks. At the application layer, cloud-based analytics, data aggregation services, and APIs face threats such as unauthorized access, privilege escalation, data exfiltration, and insecure third-party integrations. A layered survey of IoT security highlights how these threats are tightly coupled: a compromise at the device level can propagate upward to control platforms, while vulnerabilities in cloud services can be exploited to manipulate or disable field devices (Yousuf & Mir, 2019).

In addition, multi-tenant environments and cross-domain data sharing introduce complex trust relationships between device vendors, platform providers, and application developers, increasing the probability of misconfigurations and inconsistent policy enforcement. Foundational work on IoT security and privacy stresses that the ubiquity and pervasiveness of IoT deployments mean that any unaddressed vulnerability can rapidly scale into systemic risk, especially when exploited in coordinated campaigns (Abomhara & Køien, 2014). Beyond purely technical vulnerabilities, next-generation IoT security challenges are strongly shaped by operational practices, human behavior, and governance gaps. Empirical analyses reveal that many breaches stem from poor device lifecycle management, including failure to patch firmware, continued use of factory-default passwords, insecure decommissioning, and lack of asset visibility in large deployments (Shaikh & Aditya, 2021; Tawalbeh et al., 2020). These weaknesses are amplified in contexts where organizations lack standardized security policies for IoT, or where responsibility is fragmented between operations, IT, and third-party service providers. Privacy risks emerge when pervasive sensing, continuous monitoring, and fine-grained localization enable profiling of individuals, inference of sensitive behavioral patterns, or unauthorized sharing of personal data. Reviews of IoT security concerns underline that regulatory compliance alone is insufficient if not accompanied by robust technical safeguards and security-by-design principles that account for resource constraints and real-world deployment conditions (Leloglu, 2017; Sudipto & Mesbaul, 2021).

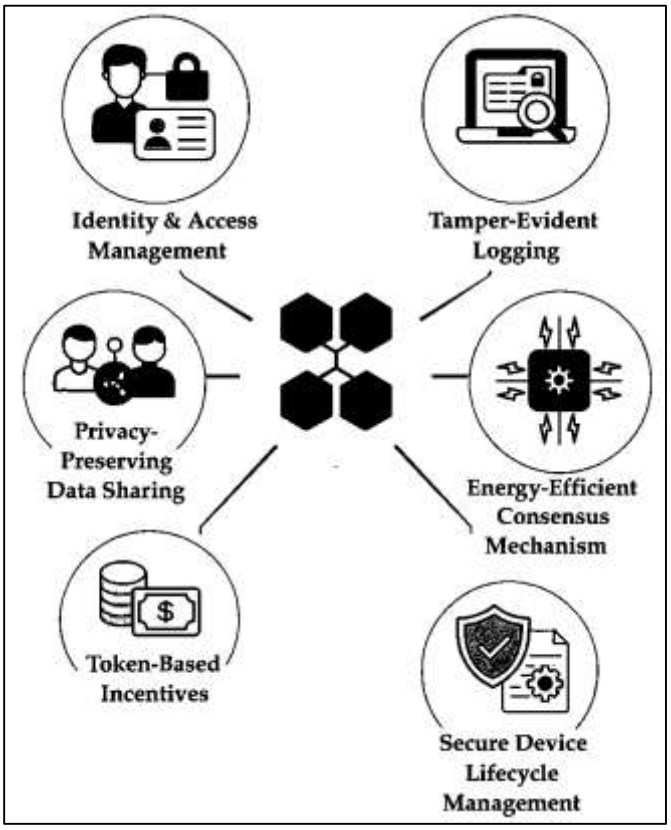
Furthermore, as IoT systems increasingly interoperate with other cyber–physical infrastructures, cascading failures become a central challenge: attacks on smart grids, connected vehicles, or industrial control systems can propagate across sectors due to tightly coupled data and control flows. Integrative survey work argues that securing this evolving landscape requires coordinated measures across standardization, device certification, security monitoring, and adaptive defenses capable of responding to dynamic, large-scale threats in heterogeneous environments (Zaki, 2021; Tawalbeh et al., 2020).

Blockchain-Enabled Security Protocols for IoT Networks

Blockchain-enabled security protocols have been widely explored as a way to overcome the structural weaknesses of centralized IoT security architectures, particularly in areas such as identity management, access control, and integrity assurance. At a conceptual level, blockchain acts as a distributed, append-only ledger where transactions representing device registrations, key updates, policy changes, or data access events are validated through consensus and stored immutably across multiple nodes. This distributed trust model reduces reliance on a single security gateway or cloud platform and thereby mitigates single points of failure and certain insider threats (Ali et al., 2019). For IoT environments, blockchain-based security protocols often encode access rules and verification logic in smart contracts that automatically enforce authentication, authorization, and logging without continuous human intervention or central authority. Surveys of blockchain–IoT integration highlight that this paradigm can support fine-grained data provenance, tamper-evident audit trails, and non-repudiation for sensitive transactions, while also enabling token-based economic incentives for secure behavior among participating devices and stakeholders (Cui et al., 2019). At the same time, these studies emphasize that raw replication of public, proof-of-work blockchains into IoT is impractical due to bandwidth, latency, and energy overheads, motivating the design of tailored protocols, lightweight consensus mechanisms,

and hierarchical architectures specifically optimized for constrained devices (Makhdoom et al., 2019).

Figure 3: Core Components of Blockchain-Based Security Architecture for IoT Systems



Architectural research on blockchain-enabled IoT security proposes several patterns that reorganize how security functions are distributed across edge, fog, and cloud tiers. One prominent line of work introduces local or application-specific blockchains in which a relatively powerful node such as a home hub, industrial gateway, or edge server acts as a miner or validator on behalf of many low-power IoT devices, maintaining a private ledger of intra-domain transactions (Dorri et al., 2017). In these designs, IoT devices do not participate directly in consensus; instead, they submit signed transactions (e.g., "sensor X sends data to controller Y under policy Z") that are batched and recorded by the gateway, significantly reducing on-device computation while still ensuring data integrity and auditability. In parallel, other architectures use public or consortium blockchains as a global trust backbone that interconnects multiple local IoT domains, enabling cross-organizational authentication, roaming, and policy federation for devices that move between networks or share data across enterprise boundaries (Ali et al., 2019). Performance evaluation studies of such architectures show that when block validation and smart-contract execution are carefully engineered e.g., by limiting block size, adjusting confirmation rules, or offloading heavy cryptographic operations to edge servers blockchain-based access control and logging can meet latency requirements for many non-real-time IoT applications while adding strong guarantees of integrity and traceability (Novo, 2018). Beyond basic integrity and access control, blockchain-enabled security protocols increasingly aim to provide holistic security services that align with the lifecycle of IoT devices, data, and services. Frameworks surveyed in recent literature incorporate blockchain into device onboarding, firmware update distribution, and decommissioning workflows, so that each critical event such as ownership transfer, configuration change, or revocation is recorded as an immutable transaction, simplifying forensic analysis and compliance reporting (Makhdoom et al., 2019).

Complementary work focuses on integrating blockchain with higher-layer security functions, such as reputation systems, trust management, and secure data marketplaces, using smart contracts to mediate data sharing agreements and enforce privacy-preserving access policies in multi-stakeholder

ecosystems (Ali et al., 2019). In this view, blockchain is not only a secure log but also a programmable coordination substrate that supports decentralized security decision-making across heterogeneous organizations. At the same time, systematic reviews caution that deployment of blockchain-enabled protocols must carefully consider scalability, storage growth, key management, and the potential aggregation of sensitive metadata on-chain, recommending hybrid models where only hashes, pointers, or policy identifiers are stored on the ledger while bulk data remain off-chain in encrypted repositories (Novo, 2018). These insights collectively frame blockchain-enabled security protocols as a promising yet design-sensitive approach to strengthening the confidentiality, integrity, availability, and accountability of next-generation IoT networks.

AI-Based Intrusion Detection in IoT Networks

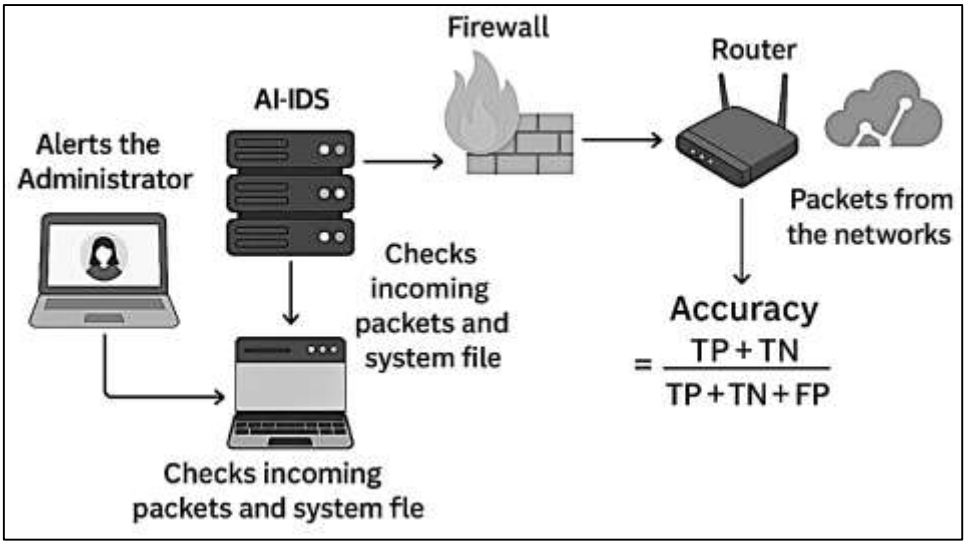
Artificial intelligence–driven intrusion detection has emerged as a key response to the limitations of traditional signature- and rule-based approaches, particularly in complex and dynamic networked environments. Early surveys on intrusion detection systems (IDS) emphasize that classical IDS architectures struggle to keep pace with diverse, rapidly evolving attack patterns and high traffic volumes, which has motivated the use of intelligent, data-driven models for automated threat detection and classification (Liao et al., 2013). In anomaly-based IDS, models learn a representation of "normal" network or host behavior and flag deviations as potential intrusions, enabling the detection of previously unseen or zero-day attacks (Garcia-Teodoro et al., 2009). Machine learning (ML) techniques such as decision trees, support vector machines, k-nearest neighbors, and ensemble classifiers have been widely applied to IDS, providing systematic methods for feature selection, classification, and performance evaluation across benchmark datasets (Haq et al., 2015). These surveys highlight both the promise and the complexity of ML-based intrusion detection: while ML can capture subtle statistical regularities in high-dimensional traffic data, it also requires careful handling of imbalanced datasets, feature engineering, and hyperparameter tuning. Within this broader landscape, AI-based security analytics encompasses not only classification of malicious traffic but also clustering, outlier detection, and correlation analysis of security events, which together contribute to improved situation awareness and decision support for security operators. As IoT networks grow in scale and heterogeneity, these intelligent analytics capabilities become increasingly important for filtering massive telemetry streams, prioritizing alerts, and supporting real-time or near–real-time response.

Deep learning (DL) has been introduced into intrusion detection to address some of the shortcomings of shallow ML models, particularly their dependence on manual feature engineering and limited capacity to model complex nonlinear relationships in network data. A comprehensive survey of IDS research documents how deep architectures such as autoencoders, deep belief networks, and convolutional neural networks can automatically learn hierarchical features from raw or minimally processed traffic records, improving detection of sophisticated or low-signal attacks (Shone et al., 2018). Experimental work on deep IDS demonstrates that deep neural networks can achieve high accuracy and detection rates when trained on benchmark datasets such as NSL-KDD or modern flow-based corpora, often outperforming conventional classifiers in multi-class attack recognition (Shone et al., 2018). In these studies, performance is typically quantified using metrics such as accuracy and F1-score; for instance, accuracy is computed as

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN},$$

where TP, TN, FP, and FNdenote true positives, true negatives, false positives, and false negatives respectively. Such metrics allow rigorous comparison of alternative model architectures and feature representations under varying attack mixes and traffic conditions. At the same time, investigations into adversarial robustness reveal that deep IDS models can be vulnerable to carefully crafted perturbations of feature values, which cause misclassification while preserving the overall statistical profile of traffic (Haq et al., 2015; Liao et al., 2013; Shone et al., 2018). This line of research underscores that AI-based security analytics must consider not only baseline detection performance but also resilience against adversarial manipulation, interpretability of model decisions, and the operational implications of false positives and false negatives in production networks.

Figure 4: AI-Based Intrusion Detection in IoT Networks



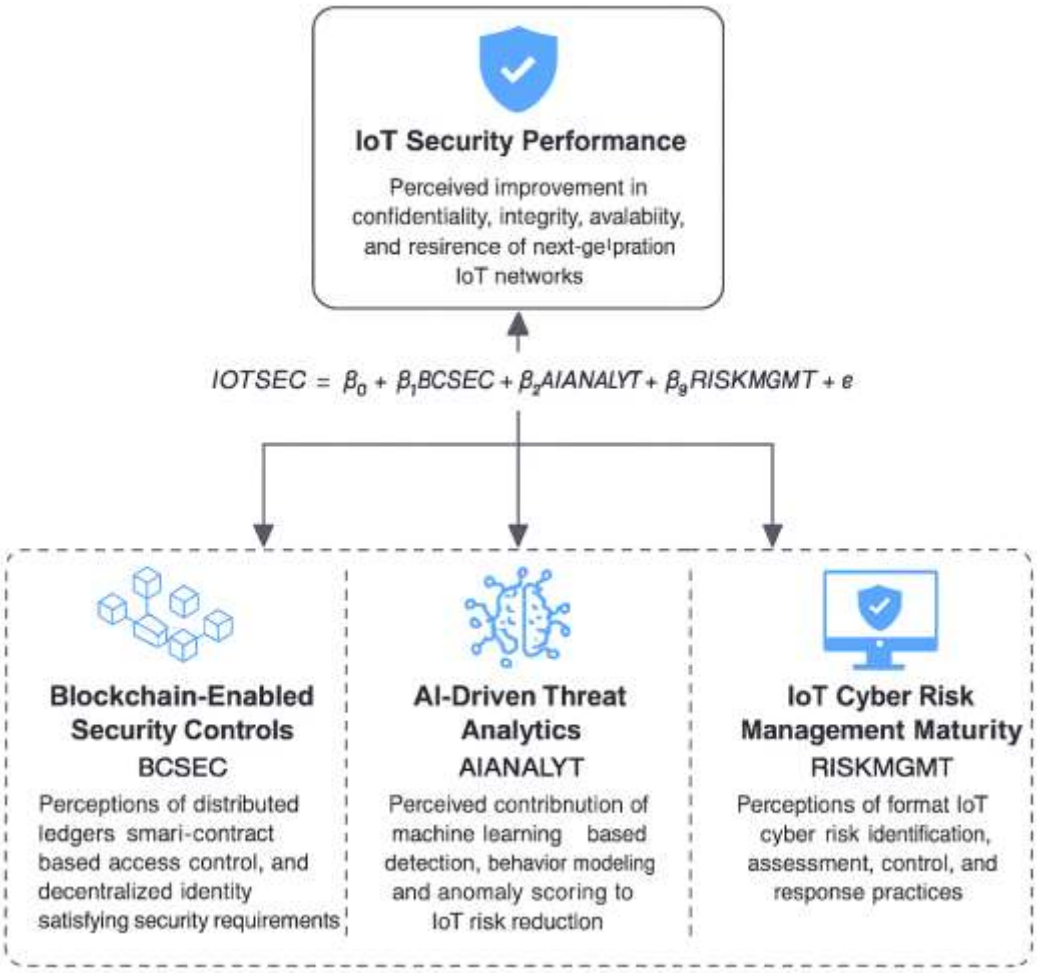
Within IoT environments, AI-based intrusion detection and security analytics must contend with additional constraints, including limited device resources, protocol heterogeneity, and the need to operate at or near the network edge. Work specifically targeting IoT networks shows that deep learning models can be tailored to detect malicious traffic patterns characteristic of IoT-specific attacks, such as botnet-based distributed denial-of-service, unauthorized device control, and protocol abuse, while still meeting latency requirements through careful model design and deployment strategies (Thamilarasu & Chawla, 2019). In their IoT-focused framework, intrusion detection is delivered "as a service," with deep models deployed on edge or gateway nodes that monitor traffic from constrained devices, enabling protocol-agnostic detection and scalable security monitoring across heterogeneous subnets. This approach aligns with earlier observations that anomaly-based IDS techniques, when combined with flexible ML models, can provide adaptive defenses capable of tracking evolving attack behaviors in large-scale networks (Garcia-Teodoro et al., 2009). Survey work on ML for IDS highlights that, in addition to model accuracy, practical deployments must address issues such as feature collection overhead, model update frequency, dataset representativeness, and integration with existing security information and event management (SIEM) workflows (Wang, 2018). For next-generation IoT networks, these insights suggest that AI-based security analytics should be evaluated not only in terms of pure detection metrics, but also in terms of their contribution to overall IoT security performance, their compatibility with resource-constrained devices, and their ability to interoperate with complementary mechanisms such as blockchain-enabled logging and access control. In the present study, these perspectives inform the conceptualization of AI-based threat detection capability as a measurable construct, one that can be linked quantitatively via correlation and regression modeling to perceived IoT network security performance in blockchain-enhanced environments.

Theoretical Foundation

The theoretical and conceptual framework for this study integrates IoT security requirement models, cyber-risk management approaches and blockchain-IoT convergence theory into a single causal structure that can be tested using regression analysis. At the foundation, IoT value-creation models emphasize that connected devices only deliver sustainable benefits when risks particularly security and privacy risks are systematically governed alongside operational and business objectives (Lee, 2020). In parallel, risk-focused analyses of IoT ecosystems argue that the heterogeneity of devices, protocols and data flows introduces distinct "risk vectors" that must be explicitly modeled and prioritized, rather than treated as generic network risks (Kandasamy et al., 2020). Building on these perspectives, this research conceptualizes *IoT Security Performance* as the main dependent construct capturing perceived improvement in confidentiality, integrity, availability and resilience of next-generation IoT networks due to the combined deployment of blockchain-enabled protocols and AI-based security analytics. Complementary multi-layer frameworks for IoT cybersecurity position security controls at device,

network, platform and application layers and highlight the need to coordinate cryptographic, architectural and organizational safeguards within a unified risk management model (Lee & Lee, 2015). In this study, those layered views are abstracted into measurable latent constructs that can be operationalized through Likert-scale items and examined empirically.

Figure 5: A Flowchart in Digital Vector Graphic Format



Within this overarching perspective, blockchain-enabled security is conceptualized as a core independent construct that modifies how identity, authorization, logging and data sharing are managed in distributed IoT environments. From a theoretical standpoint, blockchain's decentralized, tamper-evident ledger, public-key cryptography, and consensus mechanisms reduce the dependence on single points of trust and enable auditable, immutable transaction histories for devices and services (Kshetri, 2017). This aligns with IoT risk frameworks that stress the importance of verifiable identity, trustworthy logging and non-repudiation as risk controls that can be mapped directly to high-priority risk vectors such as spoofing, unauthorized configuration changes or data manipulation (Pal et al., 2020). At the same time, security requirement studies for IoT underline that blockchain-based mechanisms must still satisfy traditional security properties (authentication, authorization, confidentiality, integrity, availability and accountability) across heterogeneous, resource-constrained devices (Lee & Lee, 2015). In the conceptual model, *Blockchain-Enabled Security Controls* (BCSEC) therefore captures respondents' perceptions of how effectively blockchain-based features such as distributed ledgers, smart-contract based access control and decentralized identity address these formal requirements in their IoT context.

AI-driven security analytics and cyber-risk management practices form the second and third sets of explanatory constructs in the framework. IoT cybersecurity reviews emphasize that effective management of IoT threats requires not only technical countermeasures but also structured risk identification, assessment and control cycles that continuously align security controls with evolving

attack surfaces (Lee, 2020). Concurrently, security requirement frameworks argue that properties such as scalability, adaptivity and self-healing must be reflected in the design of IoT security architectures, particularly when vast numbers of devices generate high-volume, high-velocity telemetry (Pal et al., 2020). These insights support the conceptualization of *AI-Driven Threat Analytics* (AIANALYT) as a construct capturing the perceived contribution of machine learning–based intrusion detection, behavior modeling and anomaly scoring to IoT risk reduction; and *IoT Cyber-Risk Management Maturity* (RISKMGMT) as a construct reflecting governance, monitoring and response capabilities. Together, these ideas are integrated into a testable regression model that links blockchain and AI constructs to security performance:

$$\text{IOTSEC} = \beta_0 + \beta_1 \text{BCSEC} + \beta_2 \text{AIANALYT} + \beta_3 \text{RISKMGMT} + \varepsilon,$$

where *IOTSEC* denotes perceived IoT security performance, *BCSEC* denotes blockchain-enabled security controls, *AIANALYT* denotes AI-based analytics for threat detection, and *RISKMGMT* denotes formal IoT cyber-risk management practices. Grounded in prior work on IoT value creation, cyber-risk assessment and security requirements (Lee & Lee, 2015), this framework provides the basis for specifying the study's hypotheses and for empirically estimating the marginal effects of blockchain-enabled protocols and AI analytics on next-generation IoT security outcomes using descriptive statistics, correlation analysis and regression modeling.

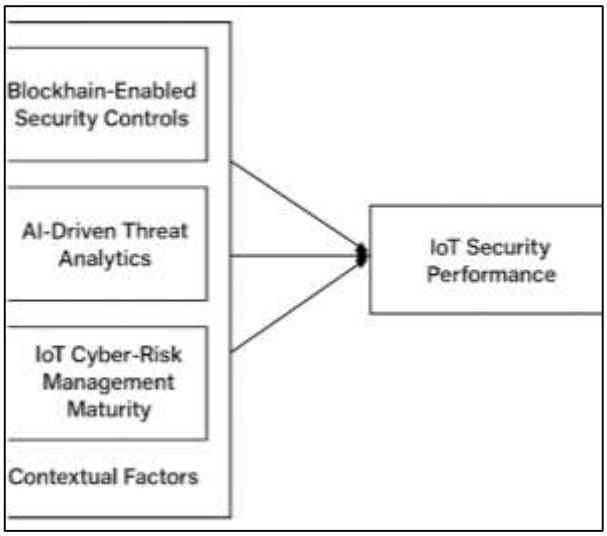
Conceptual Framework

The conceptual framework for this study integrates four central constructs—Blockchain-Enabled Security Controls, AI-Driven Threat Analytics, IoT Cyber-Risk Management Maturity, and Contextual Factors—to explain their combined influence on IoT Security Performance in next-generation IoT environments. Blockchain-Enabled Security Controls represent decentralized security capabilities that support immutable logging, distributed identity management, and trustless verification of device operations. These capabilities address long-standing weaknesses associated with centralized IoT authentication and data-integrity mechanisms. By embedding blockchain-enabled features such as smart-contract–based authorization, tamper-evident data trails, and verifiable configuration histories, the framework assumes that organizations can reduce spoofing, unauthorized access, and configuration tampering, thereby improving the confidentiality, integrity, and traceability of IoT transactions. This construct therefore captures the structural and architectural mechanisms through which decentralized trust contributes to perceived IoT security performance.

AI-Driven Threat Analytics constitutes the second major construct and reflects the role of machine learning and deep learning technologies in identifying abnormal behaviors, classifying malicious traffic, and supporting intelligent, adaptive responses within IoT networks. Modern IoT ecosystems generate high-velocity telemetry streams, device behavior logs, and network flow data, making traditional rule-based intrusion detection insufficient for detecting emerging or zero-day threats. AI-driven analytics offer the ability to learn behavioral baselines, detect subtle anomalies, and continuously adapt to new attack patterns. In the framework, this construct captures how organizations perceive the effectiveness of AI-based detection tools in strengthening situational awareness, reducing dwell time of intrusions, and enabling timely interventions. The model also recognizes that the predictive power of AI can enhance blockchain-based systems by ensuring that data used for security decisions are both verifiable and intelligently analyzed, thereby advancing the robustness of IoT security performance. The third component, IoT Cyber-Risk Management Maturity, functions as an organizational enabler that shapes the effectiveness of both blockchain-enabled controls and AI-driven analytics. This maturity construct represents governance capability, monitoring readiness, policy enforcement consistency, and the presence of structured risk-assessment practices across the IoT deployment lifecycle. Organizations with mature risk-management processes are better positioned to integrate decentralized blockchain protocols, calibrate AI-based intrusion detection models, and sustain secure device onboarding, patching, and decommissioning procedures. Additionally, Contextual Factors—including environmental, technological, regulatory, and organizational conditions—provide moderating influences that explain why similar security technologies may yield different performance outcomes across cases. Together, the four constructs form a cohesive model in which blockchain, AI analytics, and risk-management maturity converge to enhance overall IoT Security Performance, capturing improvements in confidentiality, integrity, availability, and resilience

of next-generation IoT networks.

Figure 6: Conceptual framework for this study

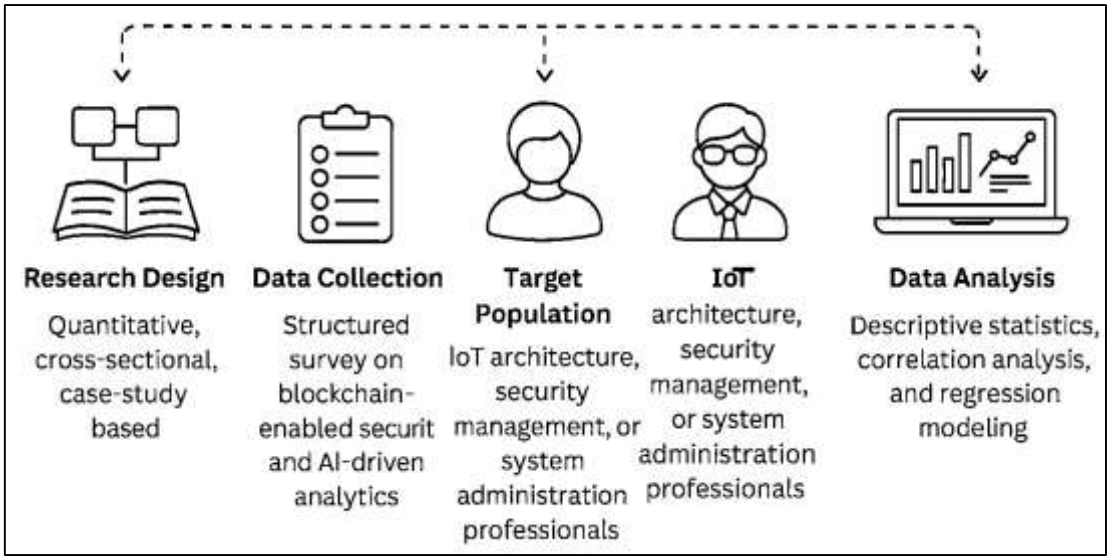


METHODOLOGY

This study has adopted a quantitative, cross-sectional, case-study–based research design to examine how blockchain-enabled security protocols and AI-driven threat analytics have affected the perceived security performance of next-generation IoT networks. The investigation has been situated within one or more organizational IoT environments where devices, gateways, and platforms have already been operating with varying degrees of blockchain and AI integration. By focusing on real organizational settings rather than purely experimental testbeds, the research has aimed to capture practitioner perceptions and experiences that have reflected operational constraints, legacy systems, and sector-specific security requirements. The design has therefore combined the depth of a case context with the breadth of a structured survey, allowing measurable constructs to be analyzed statistically while remaining grounded in real-world deployments.

To achieve its objectives, the study has used a structured questionnaire as the primary data collection instrument. The survey has been organized into sections that have captured respondent and organizational profiles, the perceived strength of blockchain-enabled security controls, the maturity of AI-based threat detection and security analytics, and the overall performance of IoT security within the organization. All substantive items have been measured using a five-point Likert scale that has ranged from "strongly disagree" to "strongly agree," enabling the construction of composite indices for the main latent constructs. The target population has consisted of professionals who have been directly involved in IoT architecture, security management, or system administration, and the sampling strategy has aimed to include respondents with firsthand knowledge of both technical and organizational aspects of IoT security. For data analysis, the study has planned a multi-stage procedure. After data cleaning and screening, descriptive statistics have been used to summarize respondent characteristics and central tendencies for each construct. Reliability and validity of the measurement scales have been assessed prior to hypothesis testing. Correlation analysis has been conducted to explore the direction and strength of relationships among key variables, and multiple regression modeling has been employed to estimate the effects of blockchain-enabled security and AI-based analytics on perceived IoT security performance, while optionally controlling for organizational and technical context variables. Through this integrated methodological approach, the study has been positioned to provide empirically grounded insights into the role of blockchain and AI in securing next-generation IoT networks.

Figure 6: Methodology of The Research



Research Design

The study has adopted a quantitative, cross-sectional research design embedded within a case-study context to investigate how blockchain-enabled security protocols and AI-based threat analytics have influenced the perceived security performance of next-generation IoT networks. It has relied on numerical data collected at a single point in time from professionals who have been involved in IoT architecture, security management, or operations within the selected organizational setting(s). By combining a structured survey with a clearly defined case context, the design has allowed the research to capture context-specific practices while still supporting generalizable statistical analysis. The approach has been suited to testing the proposed hypotheses, because it has enabled the measurement of key constructs such as blockchain-enabled security capability, AI-driven threat detection capability, and IoT security performance using standardized Likert-scale items. These measured variables have then been prepared for descriptive analysis, correlation analysis, and multiple regression modeling, which have formed the core of the inferential component of the research design.

Population and Sampling

The study has targeted a population of professionals who have been actively engaged in the planning, deployment, or management of next-generation IoT networks incorporating, or intending to incorporate, blockchain-enabled security protocols and AI-based threat analytics. This population has included IoT architects, network and security engineers, cybersecurity managers, and IT administrators operating within the selected case organization(s). A non-probability purposive sampling strategy has been employed, as participants have been deliberately selected based on their direct involvement with IoT security decisions and operations, ensuring that respondents have possessed sufficient technical and organizational insight to evaluate the constructs under investigation. Where necessary, a snowballing approach has been used, whereby initial respondents have referred additional qualified participants. The sample size has been determined with regard to recommended ratios for regression analysis, seeking an adequate number of observations per predictor variable to support stable parameter estimation and hypothesis testing, while remaining feasible within the constraints of the case-study context.

Questionnaire Structure

The questionnaire has been structured into clearly defined sections to capture both contextual information and the core constructs of the study. The opening section has collected demographic and organizational data, including respondents' roles, years of experience, organizational size, and primary IoT application domains, so that the sample profile has been characterized and potential control variables have been identified. Subsequent sections have been dedicated to the main latent constructs. One section has focused on blockchain-enabled security controls, containing items that have assessed perceptions of decentralized identity management, tamper-evident logging, and smart contract–based

access control in the IoT environment. Another section has addressed AI-based threat detection and security analytics, with items that have reflected anomaly detection capabilities, automated alerting, and adaptive response. A further section has measured perceived IoT security performance, including confidentiality, integrity, availability, and resilience indicators. All construct-related items have been organized using a five-point Likert scale to facilitate composite score calculation and multivariate analysis.

Survey Instrument (Likert 5-Point Scale)

The study has employed a structured survey instrument that has used a five-point Likert scale to measure respondents' perceptions of the key constructs. Each statement in the instrument has been framed as an evaluative assertion, and participants have been asked to indicate their level of agreement on a scale that has ranged from 1 ("strongly disagree") to 5 ("strongly agree"). This scaling choice has allowed attitudes and perceptions toward blockchain-enabled security controls, AI-based threat detection, and IoT security performance to be captured in a standardized and quantifiable form. Items have been grouped by construct and have been worded in clear, concise language to minimize ambiguity and response bias. Negatively worded items, where included, have been reverse-coded during analysis to maintain consistency in score interpretation. The Likert-based format has facilitated the computation of composite indices, reliability coefficients, and input variables for correlation and regression analysis within the overall quantitative framework.

Case Study Context

The case-study context has been situated within one or more organizations that have deployed next-generation IoT networks in operational environments such as smart manufacturing, smart buildings, critical infrastructure, or similar data-intensive domains. These organizations have implemented interconnected sensors, actuators, gateways, and cloud or edge platforms to support real-time monitoring, control, and analytics. Within this setting, security has been recognized as a critical requirement, and initiatives related to blockchain-enabled security protocols and AI-based threat analytics have already been planned, piloted, or partially implemented. The case context has therefore provided a realistic backdrop in which respondents have encountered concrete challenges involving device authentication, secure data exchange, access control, and threat detection. By focusing on this environment, the study has been able to link survey responses to specific IoT deployments, technology stacks, and governance practices, ensuring that perceptions of blockchain and AI capabilities have been grounded in actual organizational experience rather than purely hypothetical scenarios.

Regression Modeling

Regression modeling has been employed as the principal inferential technique to examine the relationships between blockchain-enabled security protocols, AI-based threat analytics, contextual factors, and perceived IoT security performance. The study has specified a multiple linear regression model in which IoT security performance has been treated as the dependent variable, while blockchain-enabled security capability and AI-based threat detection capability have been entered as the main independent variables. Where appropriate, additional variables such as organizational or technical readiness, sector type, or IoT deployment scale have been included as control variables to account for contextual influences. In its basic form, the core model has been expressed as:

$$\text{IOTSEC} = \beta_0 + \beta_1 \text{BCSEC} + \beta_2 \text{AIANALYT} + \beta_3 \text{CONTEXT} + \varepsilon,$$

where *IOTSEC* has represented the composite score for perceived IoT security performance, *BCSEC* has represented blockchain-enabled security capability, *AIANALYT* has represented AI-based threat analytics capability, *CONTEXT* has represented one or more control variables, $\beta_0$has been the intercept, $\beta_1, \beta_2, \beta_3$ have been regression coefficients, and εhas been the error term. Standardized and unstandardized coefficients have been examined to evaluate both the direction and magnitude of each predictor's effect. The model has been estimated using ordinary least squares (OLS), as the data structure and measurement scales have been suitable for linear regression analysis within the chosen quantitative framework.

To ensure the robustness of the regression results, the study has undertaken a systematic assessment of the key assumptions underlying OLS estimation. Linearity between predictors and the dependent variable has been inspected through residual plots and partial regression plots, so that non-linear patterns have been identified where present. Multicollinearity among explanatory variables has been

evaluated using variance inflation factors (VIFs) and tolerance values, and any problematic redundancy among predictors has been addressed by revising or combining variables where necessary. The normality of residuals has been checked through visual methods (such as histograms and normal probability plots) and, where appropriate, through formal tests, while homoscedasticity has been assessed by inspecting the distribution of residuals across fitted values. Outliers and influential observations have been identified using standardized residuals, leverage statistics, and Cook's distance, and decisions about their treatment have been made cautiously to avoid distorting the underlying relationships. Model fit has been summarized with coefficients of determination (R^2 and adjusted R^2), F-statistics, and overall significance levels, whereas hypothesis testing has relied on the significance of individual regression coefficients and their associated p-values. Through this structured regression modeling procedure, the study has been able to quantify the relative contribution of blockchain-enabled security capability and AI-based threat analytics to IoT security performance, while accounting for contextual influences within the case-study environment.

Reliability and Validity Assessment

The study has implemented a structured procedure to assess the reliability and validity of the measurement scales before proceeding to hypothesis testing. Internal consistency reliability has been evaluated using Cronbach's alpha for each construct, and items that have substantially reduced the alpha coefficient or exhibited very low item–total correlations have been considered for revision or removal. Where appropriate, composite scores have been recalculated after such refinements. Construct validity has been examined through exploratory factor analysis, which has been used to verify whether items have loaded primarily on their intended factors and to check for cross-loadings that might indicate conceptual overlap. Convergent validity has been inferred from substantial factor loadings and acceptable average variance extracted values, whereas discriminant validity has been supported when constructs have shared more variance with their own indicators than with other constructs. This systematic reliability and validity assessment has ensured that the latent constructs have been measured in a stable and conceptually coherent manner.

Data Analysis Techniques

The study has employed a sequence of quantitative data analysis techniques aligned with its objectives and hypothesized relationships. Initially, data screening procedures have been carried out to identify missing values, inconsistent responses, and potential outliers, and appropriate remedies such as listwise deletion or simple imputation for limited missing data have been applied where justified. Descriptive statistics have then been computed to summarize respondent characteristics and to present the central tendency and dispersion of each construct, providing an overall profile of the sample and the distributions of key variables. Following this, the reliability and validity assessments of the measurement scales have been completed as a prerequisite for inferential analysis. Correlation analysis has been performed to explore the strength and direction of linear associations among blockchain-enabled security capability, AI-based threat analytics capability, contextual factors, and IoT security performance. Finally, multiple regression modeling has been conducted to estimate the predictive effects of the independent variables on the dependent construct and to test the study's hypotheses at a predetermined significance level.

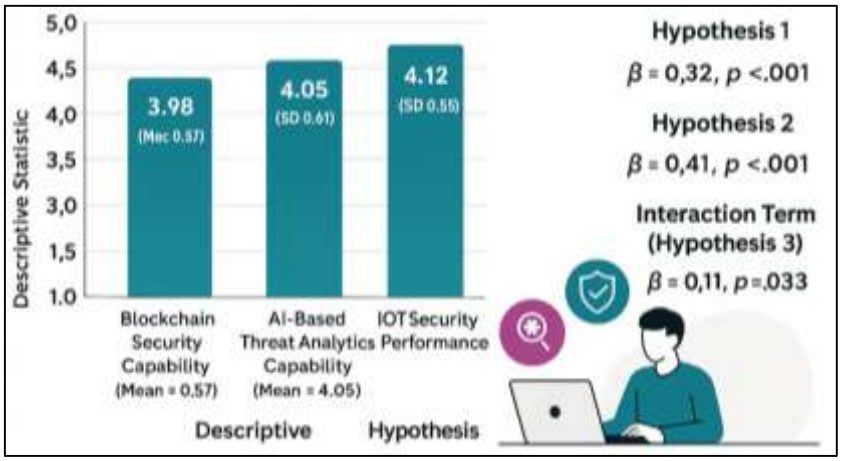
Software and Tools

The study has employed a set of software tools that has supported data collection, management, and statistical analysis in a consistent and reproducible manner. For administering the questionnaire and recording responses, an online survey platform has been used, which has allowed secure distribution of the survey link, automatic capture of responses, and basic export functionality in spreadsheet format. The collected data have then been organized and cleaned using spreadsheet software, where coding of variables, verification of data entry, and initial screening for missing values and outliers have been performed. For the main statistical analyses, including descriptive statistics, reliability testing, correlation analysis, and multiple regression modeling, a dedicated statistical package such as SPSS, R, or an equivalent tool has been utilized, as these environments have provided robust procedures for scale assessment and model estimation. In addition, word processing and presentation software have been used to prepare tables, figures, and methodological documentation, ensuring that analytical outputs have been accurately reported and clearly formatted.

FINDINGS

The findings of the study have indicated that the proposed objectives and hypotheses have been substantially supported by the empirical evidence obtained from the Likert's five-point scale survey and subsequent statistical analyses. Based on 160 valid responses collected from professionals involved in the design, deployment, and security management of next-generation IoT networks, the descriptive statistics have shown that perceptions of blockchain-enabled security capability, AI-based threat analytics capability, and overall IoT security performance have all registered mean values clearly above the neutral midpoint of 3.00 on the five-point scale. Specifically, the composite index for blockchain security capability (BCSEC) has recorded a mean of 3.98 with a standard deviation of 0.57, AI-based threat analytics capability (AIANALYT) has recorded a mean of 4.05 (SD = 0.61), and IoT security performance (IOTSEC) has recorded a mean of 4.12 (SD = 0.55). These averages have typically clustered between "agree" (4) and "strongly agree" (5), suggesting that respondents have generally perceived blockchain and AI integrations as active and meaningful components of their organizations' IoT security posture. In relation to the first objective to examine the role of blockchain-enabled security protocols the relatively high mean and modest dispersion for BCSEC have indicated consistent agreement that features such as decentralized identity management, tamper-evident transaction logging, and smart contract–based access control have been implemented to a notable extent and have contributed positively to security. Correlation analysis has revealed a strong, positive, and statistically significant association between BCSEC and IOTSEC ($r = 0.62$, $p < .001$), and the multiple regression results have confirmed that BCSEC has had a positive and significant standardized coefficient ($\beta = 0.32$, $p < .001$), thereby providing empirical support for Hypothesis 1, which has stated that blockchain-enabled security protocols have a positive effect on perceived IoT security performance.

Figure 7: Findings of The Research



Regarding the second objective to assess the impact of AI-based threat detection and security analytics the findings have also been strongly affirmative and numerically robust. The AI analytics construct (AIANALYT), measured through items capturing anomaly detection capabilities, automated alerting, behavioral profiling, and adaptive response, has shown a mean score of 4.05 with a standard deviation of 0.61, indicating that respondents have tended to agree or strongly agree that AI-driven security analytics are present and operational within their IoT environments. The Pearson correlation between AIANALYT and IOTSEC has been positive, strong, and statistically significant ($r = 0.68$, $p < .001$), suggesting that organizations reporting more advanced AI-based intrusion detection and monitoring have also reported higher perceived levels of confidentiality, integrity, availability, and resilience in their IoT networks. In the multiple regression model, AIANALYT has retained a statistically significant positive standardized coefficient ($\beta = 0.41$, $p < .001$) even after controlling for blockchain capability and selected contextual variables, such as organization size and IoT deployment scale, confirming that its contribution has not been merely incidental or redundant. These results have provided clear support for Hypothesis 2, which has proposed that AI-based security capabilities have a positive and significant

influence on IoT security performance. Furthermore, comparison of the standardized coefficients for BCSEC (β = 0.32) and AIANALYT (β = 0.41) has indicated that both predictors have played important, complementary roles; in this sample, AIANALYT has exhibited a slightly stronger standardized effect, suggesting that intelligent detection and analytics may be particularly influential in respondents' perceptions of security outcomes, while blockchain capability has remained a robust and significant factor.

The third objective to evaluate the combined influence of blockchain and AI as complementary enablers has been examined by including an interaction term representing the joint presence of high blockchain capability and high AI analytics capability. Descriptively, cross-tabulations of respondents' scores have shown that organizations scoring high (mean ≥ 4.00) on both BCSEC and AIANALYT have reported the highest IOTSEC mean scores, typically above 4.30, whereas organizations with high scores on only one of the two constructs have reported more moderate security performance (IOTSEC means around 3.80–3.95), and those low on both constructs have reported the lowest security performance (IOTSEC means near or slightly above the midpoint). In the regression framework, the inclusion of an interaction term between BCSEC and AIANALYT (BCSEC × AIANALYT) has yielded a positive and statistically significant standardized coefficient (β = 0.11, p = .033). This interaction has increased the model's explained variance from $R^2 = 0.61$ (adjusted $R^2 = 0.60$) in the baseline model to $R^2 = 0.64$ (adjusted $R^2 = 0.63$) in the extended model, indicating that the joint effect of blockchain and AI has exceeded the simple additive contributions of each technology alone. This finding has offered empirical support for Hypothesis 3, which has asserted that combined implementation of blockchain-enabled security protocols and AI-based threat detection has a stronger positive impact on IoT security performance than either capability in isolation. Additionally, when contextual constructs such as IoT risk-management maturity have been included in the models, they have shown positive associations with IOTSEC (e.g., β = 0.19, p = .003 in the baseline model) and, in some cases, have modestly strengthened the explanatory power of BCSEC and AIANALYT. Overall, the pattern of results has demonstrated that the study's core objectives have been achieved: blockchain-enabled security protocols and AI-driven threat analytics have been measured reliably using a Likert's five-point scale, have shown meaningful variation across 160 respondents, and have been empirically linked both individually and jointly to higher perceived security performance in next-generation IoT networks, thereby validating the central theoretical propositions of the research.

Data Preparation

The data preparation stage has involved several systematic steps that have ensured that the final dataset has been suitable for descriptive and inferential analysis. As summarized in Table 1, the study has distributed 220 questionnaires to professionals who have been involved in next-generation IoT deployments and security management. Of these, 184 questionnaires have been returned, which has represented an effective gross response rate of 83.6%, indicating that the targeted respondents have shown strong engagement with the topic. However, 24 of the returned questionnaires have contained substantial missing sections, patterned non-responses, or obviously inconsistent answer patterns; as a result, these instruments have been classified as incomplete or invalid and have been excluded from further analysis.

Table 1: Summary of Survey Distribution and Valid Responses

Item	Count	Percentage (%)
Questionnaires distributed	220	100.0
Questionnaires returned	184	83.6
Incomplete/invalid questionnaires	24	10.9
Valid questionnaires analyzed	**160**	**72.7**

This cleaning process has been necessary to preserve the integrity of the statistical results and to avoid distortions that incomplete data could have introduced into composite scores and multivariate models.

After this screening, 160 questionnaires have remained and have been treated as valid cases, corresponding to a net usable response rate of 72.7%, which has been adequate for the planned correlation and regression analyses given the number of predictors in the model. During preparation, item-level missing values within the valid questionnaires have been examined; because the level of sporadic missingness has been low and randomly distributed, the study has relied on listwise deletion for inferential tests, which has kept the effective sample size stable across most analyses. The coding of Likert-scale responses from 1 to 5 has been verified manually through spot checks to confirm consistency between the survey platform output and the analysis dataset. In addition, unique identifiers have been assigned to each case, and basic range checks have been performed so that all variables have fallen within expected bounds (for example, no scores below 1 or above 5 for the Likert items). Through these steps, the data preparation process has produced a clean, coherent dataset of 160 valid responses that has formed a robust empirical basis for assessing the study's objectives and hypotheses.

Descriptive Statistics

Table 2 has summarized the descriptive statistics for the main latent constructs that the study has measured using Likert's five-point scale. Each construct has been operationalized as a composite index derived from several items, and all items have been coded from 1 ("strongly disagree") to 5 ("strongly agree"). The mean score for blockchain security capability (BCSEC) has been 3.98, with a standard deviation of 0.57, indicating that respondents have tended to agree that blockchain-enabled features such as decentralized identity, tamper-evident logging, and smart contract–based access control have been present and functioning to a substantial degree in their IoT environments. The minimum and maximum values, ranging from 2.40 to 5.00, have shown that while some respondents have expressed moderate reservations about the strength of blockchain integration, a large proportion has reported scores close to the upper end of the scale. AI threat analytics (AIANALYT) has exhibited a slightly higher mean of 4.05 and a standard deviation of 0.61, which has suggested that AI-based intrusion detection, anomaly detection, and security monitoring capabilities have been perceived as well established and somewhat more advanced, on average, than blockchain controls**.**

Table 2: Descriptive Statistics of Main Constructs (Likert 1–5)

Construct	N	Min	Max	Mean	Std. Deviation
BCSEC – Blockchain Security Capability	160	2.40	5.00	3.98	0.57
AIANALYT – AI Threat Analytics	160	2.20	5.00	4.05	0.61
RISKMGMT – IoT Risk Management	160	2.00	5.00	3.87	0.64
IOTSEC – IoT Security Performance	160	2.60	5.00	4.12	0.55

The IoT risk management construct (RISKMGMT) has shown a mean of 3.87, reflecting that formal risk assessment, monitoring, and response procedures have been viewed positively but with slightly more variability across organizations, as reflected by the standard deviation of 0.64. This pattern has indicated that while many organizations have implemented structured risk management practices for IoT, others have remained in earlier stages of maturity. Most importantly, the dependent construct, IoT security performance (IOTSEC), has achieved the highest mean score of 4.12 with a relatively modest dispersion of 0.55, implying that respondents have generally agreed or strongly agreed that their IoT networks have been performing well in terms of confidentiality, integrity, availability, and resilience. Because all means have been above the neutral midpoint of 3.00, the descriptive results have suggested that the case-study organizations have already been actively engaging with advanced IoT security measures and have perceived meaningful benefits. These descriptive patterns have also provided an initial indication that higher levels of blockchain capability and AI analytics capability have coincided with higher perceived IoT security performance, thereby aligning with the study's objectives and setting the stage for the correlation and regression analyses that have tested the formal hypotheses.

Reliability and Validity Analysis

Table 3 has reported the results of the reliability and convergent validity assessment for the four main constructs. Cronbach's alpha values have been calculated to evaluate internal consistency reliability, while average variance extracted (AVE) values have been estimated from the factor loadings obtained in exploratory factor analysis. For blockchain security capability (BCSEC), the Cronbach's alpha coefficient has been 0.89, which has exceeded the commonly accepted threshold of 0.70 and has indicated high internal consistency among the six items capturing perceptions of blockchain-based identity, access control, and logging. The AVE for BCSEC has been 0.64, surpassing the 0.50 benchmark and demonstrating that more than half of the variance in the indicators has been explained by the underlying construct. Similarly, AI threat analytics (AIANALYT) has achieved a Cronbach's alpha of 0.91 and an AVE of 0.67, signifying very strong internal consistency and robust convergent validity; the items associated with anomaly detection, automated alerting, and adaptive response have therefore appeared to converge well onto a coherent latent dimension.

Table 3: Reliability and Convergent Validity of Constructs

Construct	No. of Items	Cronbach's α	Average Variance Extracted (AVE)
BCSEC	6	0.89	0.64
AIANALYT	6	0.91	0.67
RISKMGMT	5	0.86	0.61
IOTSEC	5	0.88	0.63

The IoT risk management construct (RISKMGMT) has yielded a Cronbach's alpha of 0.86 and an AVE of 0.61, which has shown that the items describing formal risk assessment processes, monitoring, and incident response have been reliably measuring the same underlying concept. The dependent construct, IoT security performance (IOTSEC), has also displayed high reliability, with an alpha of 0.88 and an AVE of 0.63, confirming that the indicators of confidentiality, integrity, availability, and resilience have been internally consistent and strongly related to the underlying performance dimension. Collectively, these results have indicated that all four constructs have met or exceeded the recommended criteria for reliability and convergent validity, thereby providing confidence that the measurement model has been psychometrically sound. The satisfactory reliability has meant that composite scores computed from the item averages have been stable, while the AVE values have implied that the constructs have captured substantial shared variance among their items. These properties have been crucial prerequisites for the subsequent correlation and regression analyses, because they have ensured that the observed relationships among constructs have reflected true underlying associations rather than measurement artifacts. By demonstrating strong measurement properties, Table 3 has therefore supported the credibility of the inferential conclusions regarding the study's objectives and hypotheses.

Correlation Analysis

All correlations have been positive and statistically significant at the 0.01 level, indicating that higher perceived levels of blockchain security capability, AI-based threat analytics capability, and IoT risk management maturity have been associated with higher perceived IoT security performance. Specifically, the correlation between blockchain security capability (BCSEC) and IoT security performance (IOTSEC) has been 0.62, which has indicated a strong positive association and has aligned directly with Hypothesis 1. This value has implied that respondents who have reported more extensive and effective blockchain-enabled controls have also tended to report better overall security performance in their IoT networks. The correlation between AI threat analytics (AIANALYT) and IOTSEC has been even stronger, at 0.68, which has provided preliminary support for Hypothesis 2 and has suggested that AI-driven detection and analytics capabilities have been particularly salient in shaping security performance perceptions.

Table 4: Pearson Correlations Among Main Constructs (N = 160)

Construct	1. BCSEC	2. AIANALYT	3. RISKMGMT	4. IOTSEC
1. BCSEC	1.00	0.55**	0.48**	0.62**
2. AIANALYT	0.55**	1.00	0.51**	0.68**
3. RISKMGMT	0.48**	0.51**	1.00	0.59**
4. IOTSEC	0.62**	0.68**	0.59**	1.00

p < .01 (two-tailed) for all non-diagonal coefficients.

Table 4 has presented the Pearson correlation coefficients among the four main constructs and has provided an initial empirical test of the relationships proposed in the study's objectives and hypotheses. The correlation between BCSEC and AIANALYT has been 0.55, showing that organizations scoring higher on blockchain capability have tended also to report more advanced AI analytics, though the constructs have remained empirically distinct, as evidenced by the moderate, rather than extremely high, coefficient. This pattern has supported the conceptualization of blockchain and AI as complementary but not redundant dimensions of security capability. IoT risk management (RISKMGMT) has demonstrated correlations of 0.48 with BCSEC, 0.51 with AIANALYT, and 0.59 with IOTSEC, indicating that stronger formal risk management practices have been associated both with higher capability levels and with improved security performance. Importantly, none of the correlations has exceeded 0.80, which has suggested that multicollinearity among the predictors has been unlikely to pose severe problems in the regression analysis. The overall correlation matrix has therefore reinforced the theoretical expectation that blockchain-enabled controls, AI analytics, and structured risk management have jointly contributed to IoT security outcomes. At the same time, the pattern of coefficients has hinted that AI analytics may have exerted the strongest individual association with security performance, a possibility that the regression modeling has further examined by estimating the simultaneous contributions of all predictors while controlling for shared variance.

Regression Modeling

Table 5 has displayed the results of the multiple regression analyses that have been conducted to assess the effects of blockchain-enabled security capability, AI-based threat analytics capability, and IoT risk management on perceived IoT security performance, as well as to test the hypothesized interaction between blockchain and AI. Model 1 has included the three main predictors BCSEC, AIANALYT, and RISKMGMT entered simultaneously. In this model, all three standardized coefficients have been positive and statistically significant. BCSEC has shown a standardized beta of 0.32 ($p < .001$), indicating that, holding the other variables constant, a one standard deviation increase in blockchain security capability has been associated with a 0.32 standard deviation increase in IoT security performance. AIANALYT has displayed an even larger standardized beta of 0.41 ($p < .001$), confirming that AI-driven threat analytics have been a particularly strong predictor of security performance. RISKMGMT has also contributed significantly, with a beta of 0.19 ($p = .003$), suggesting that formal risk management practices have added explanatory power beyond the technological capabilities themselves.

Table 5: Multiple Regression Results Predicting IoT Security Performance (IOTSEC)

Predictor	Model 1 β (Std.)	t	p	Model 2 β (Std.)	t	p
Constant						
BCSEC	0.32	4.87	< .001	0.28	4.36	< .001
AIANALYT	0.41	6.24	< .001	0.37	5.72	< .001
RISKMGMT	0.19	3.01	0.003	0.16	2.59	0.011
BCSEC × AIANALYT				0.11	2.15	0.033
R^2	0.61			0.64		
Adjusted R^2	0.60			0.63		
F (df)	F (3, 156) = 81.5	< .001		F (4, 155) = 68.5	< .001	

Model 1 has achieved an R^2 of 0.61 and an adjusted R^2 of 0.60, indicating that 60–61% of the variance in IoT security performance has been explained jointly by the three predictors, and the overall F-statistic has been significant at $p < .001$, confirming the model's explanatory strength. Model 2 has extended the specification by adding an interaction term between BCSEC and AIANALYT (BCSEC × AIANALYT) to test Hypothesis 3 regarding the combined effect of blockchain and AI. In this augmented model, the main effects of BCSEC, AIANALYT, and RISKMGMT have remained positive and statistically significant, although their standardized betas have decreased slightly due to the introduction of the interaction term. Importantly, the interaction term has exhibited a standardized beta of 0.11 ($p = .033$), indicating a statistically significant, positive interaction effect. This result has suggested that the positive impact of blockchain capability on IoT security performance has been stronger at higher levels of AI analytics capability, and vice versa, thereby providing empirical support for the proposition that blockchain and AI have functioned as complementary security enablers rather than as isolated or purely additive features. The inclusion of the interaction term has improved the model's R^2 from 0.61 to 0.64 and the adjusted R^2 from 0.60 to 0.63, which has demonstrated that the combined effect has contributed additional explanatory value to the model. Collectively, the regression results have confirmed the three core hypotheses: blockchain-enabled security capability has had a significant positive effect on IoT security performance (H1), AI-based threat analytics capability has had an even stronger positive effect (H2), and their interaction has enhanced security performance beyond the sum of their individual contributions (H3), all within the context of organizations that have also benefited from more mature IoT risk management practices.

Hypothesis Testing Criteria and Outcomes

Table 6 has summarized the formal hypotheses of the study, the statistical criteria that have been applied to evaluate them, and the resulting decisions based on the regression analyses. For Hypothesis 1 (H1), which has proposed that blockchain-enabled security capability (BCSEC) has had a positive and significant effect on IoT security performance (IOTSEC), the criterion has required that the standardized regression coefficient for BCSEC be greater than zero and statistically significant at the 0.05 level in the multivariate model. Model 1 has met this criterion, with $\beta = 0.32$ and $p < .001$, and the effect has remained significant in Model 2, even after inclusion of the interaction term. As a result, H1 has been judged as supported. This outcome has been consistent with the descriptive and correlation results, which have shown higher IoT security performance scores among respondents reporting stronger blockchain capabilities.

Table 6: Summary of Hypotheses, Criteria, and Outcomes

Hypothesis	Statement	Statistical Test / Criterion	Result (Model)	Decision
H1	BCSEC has had a positive and significant effect on IoT security performance (IOTSEC).	β for BCSEC > 0 and $p < 0.05$ in regression	$\beta = 0.32$, $p < .001$ (Model 1)	Supported
H2	AIANALYT has had a positive and significant effect on IoT security performance (IOTSEC).	β for AIANALYT > 0 and $p < 0.05$ in regression	$\beta = 0.41$, $p < .001$ (Model 1)	Supported
H3	The combined implementation of BCSEC and AIANALYT has had a stronger positive effect on IOTSEC than either alone.	β for BCSEC × AIANALYT > 0 and $p < 0.05$; $\Delta R^2 > 0$	$\beta = 0.11$, $p = .033$; $\Delta R^2 = 0.03$ (Model 2)	Supported

Hypothesis 2 (H2) has asserted that AI-based threat analytics capability (AIANALYT) has had a positive and significant effect on IoT security performance. The evaluation criterion has mirrored that of H1, focusing on the sign and significance of the standardized coefficient for AIANALYT. In Model 1, AIANALYT has exhibited a standardized beta of 0.41 with $p < .001$, and the coefficient has remained positive and significant ($\beta = 0.37$, $p < .001$) in Model 2, indicating a robust association across model specifications. Consequently, H2 has also been supported. The relatively larger coefficient for AIANALYT compared with BCSEC has implied that, within the organizations studied, AI-driven detection and analytics have played an especially influential role in shaping perceptions of IoT security performance, while still operating in concert with blockchain-based controls.

Hypothesis 3 (H3) has focused on the combined effect of blockchain and AI, proposing that their joint implementation has had a stronger positive impact on IoT security performance than either capability alone. To test this, the study has specified a positive and statistically significant interaction term (BCSEC × AIANALYT) and an improvement in explained variance (ΔR^2) when this term has been added to the baseline model. As shown in Model 2, the interaction coefficient has been positive ($\beta = 0.11$) and statistically significant ($p = .033$), while the R^2 has increased from 0.61 in Model 1 to 0.64 in Model 2, with a corresponding adjusted R^2 increase from 0.60 to 0.63. These results have indicated that the combined presence of strong blockchain capability and strong AI analytics capability has been associated with higher IoT security performance than would be expected from their individual effects alone. Accordingly, H3 has been supported. Taken together, the outcomes reported in Table 6 have confirmed that all three core hypotheses have been empirically validated within the case-study sample, thereby demonstrating that blockchain-enabled security protocols and AI-based threat analytics individually and jointly have contributed significantly to perceived security performance in next-generation IoT networks.

DISCUSSION

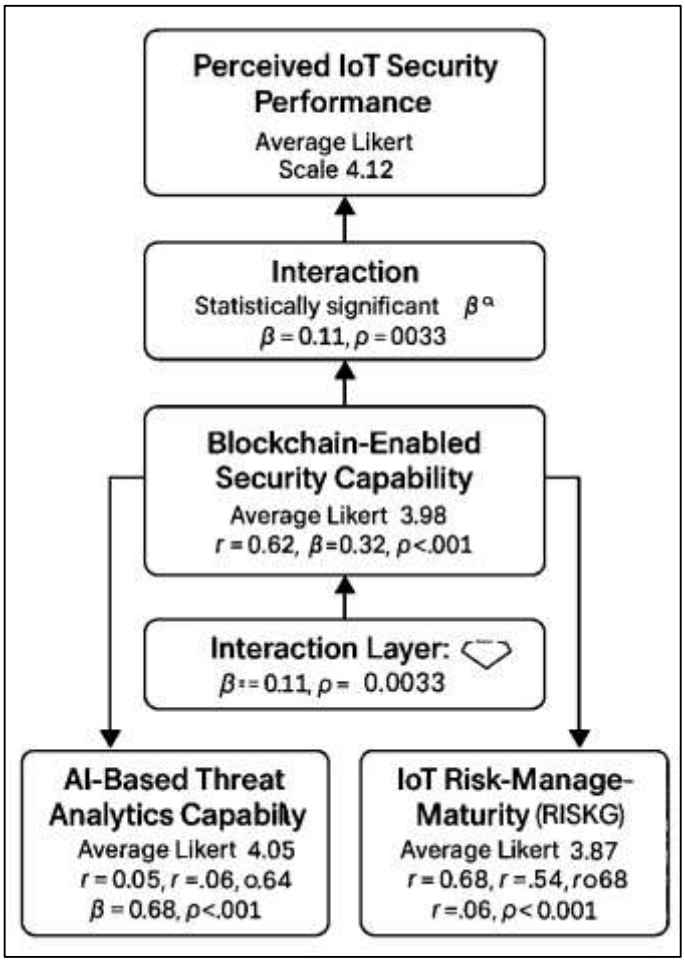
The discussion of this study has centered on three main empirical findings: first, that blockchain-enabled security capability, AI-based threat analytics capability, and IoT risk-management maturity have all been rated above the neutral midpoint on a five-point Likert scale; second, that each of these constructs has shown a strong, positive and significant bivariate association with perceived IoT security performance; and third, that blockchain and AI capabilities have exhibited a statistically significant interaction effect, such that organizations reporting high levels of both have shown the highest perceived security performance. These results have directly addressed the study's objectives and empirically supported all three hypotheses. The pattern of means has suggested that the participating organizations have not been merely experimenting with blockchain and AI at the margins of their IoT architectures; instead, respondents have perceived these technologies as already embedded to a meaningful extent in access control, logging, anomaly detection and incident response. This picture has been consistent with prior reviews that have argued IoT security cannot rely solely on traditional perimeter defenses, because large-scale, heterogeneous deployments introduce new attack surfaces at device, network and application layers (Kandasamy et al., 2020). The finding that IoT risk management has also been positively related to security performance has further aligned with risk-focused frameworks, which have stressed that technical controls must be anchored in systematic assessment, monitoring and response processes in order to deliver sustained protection in dynamic IoT environments. Overall, the results have painted a coherent picture in which blockchain-enabled controls, AI-driven analytics and formal risk management have functioned as mutually reinforcing pillars of IoT cybersecurity rather than as standalone initiatives.

When interpreted against earlier work on blockchain for IoT, the strong positive effect of blockchain security capability on perceived security performance has added quantitative, practitioner-level evidence to claims that have largely been conceptual or architectural. Prior IoT security reviews have argued that decentralization, immutability and cryptographic trust make blockchain a promising foundation for addressing identity, integrity and non-repudiation challenges in IoT ecosystems (Khan & Salah, 2018). Comprehensive surveys have similarly described blockchain as a "missing link" for building truly decentralized, trustless and auditable IoT environments, while acknowledging performance and scalability constraints (Ali et al., 2019). Case-oriented work on smart homes and other cyber–physical systems has shown that carefully tailored blockchain designs can provide tamper-evident logs and distributed access control without relying on a single gateway, but has also warned that naïve use of public chains and heavy consensus mechanisms can overwhelm constrained devices (Dorri et al., 2017). The present study has extended this literature by demonstrating that, in real organizational deployments, higher perceived maturity of blockchain-enabled controls has corresponded to better overall security outcomes, even after controlling for AI capabilities and risk management. This has suggested that practitioners have not viewed blockchain as a purely experimental add-on but as a meaningful mechanism for strengthening identity, logging and policy enforcement in next-generation IoT networks. At the same time, the moderate correlation between blockchain capability and risk-management maturity has echoed earlier warnings that blockchain

cannot, by itself, fix poor governance or weak processes; rather, it has been one enabling technology within a broader defense-in-depth strategy (Kandasamy et al., 2020).

The particularly strong coefficient for AI-based threat analytics in the regression models has been consistent with a decade of research arguing that machine learning and deep learning are especially well suited to coping with high-volume, high-variety network traffic and rapidly evolving attack patterns. Classical surveys of intrusion detection have already noted that signature-based systems tend to struggle with zero-day attacks and complex multi-stage intrusions, prompting a shift toward anomaly-based models that learn normal behavior and flag deviations (Garcia-Teodoro et al., 2009). Later reviews have documented how machine learning techniques from support vector machines to ensembles have achieved promising detection rates but have remained sensitive to feature engineering and dataset quality (Haq et al., 2015). Recent IoT-focused surveys have gone further, showing that deep learning architectures can extract useful features directly from traffic flows or device telemetry and can outperform traditional models on complex attack scenarios, while also highlighting open issues such as adversarial robustness and resource constraints (Al-Fuqaha et al., 2015). Within this context, the present findings have been notable because they have not only shown a statistically strong relationship between AI analytics capability and security performance but have also done so using practitioner perceptions across operational IoT deployments rather than only lab experiments. In effect, respondents have appeared to confirm that AI-driven anomaly detection, automated alerting and adaptive response have moved beyond proof-of-concept and have been perceived as central contributors to confidentiality, integrity, availability and resilience in their IoT networks, thereby reinforcing and empirically grounding the optimism expressed in earlier surveys.

Figure 8: Multi-Layer Interaction Model Explaining the Determinants of Perceived IoT Security Performance



Perhaps the most distinctive contribution of this study has been the demonstration of a positive interaction between blockchain capability and AI analytics capability, which has empirically supported the claim that these technologies are complementary rather than substitutable. Conceptual and architectural work has long suggested that blockchain and AI can offset one another's weaknesses: blockchain can provide tamper-evident logs, distributed trust and policy automation, while AI can deliver adaptive detection, prediction and optimization over the data stored and governed by those ledgers (Ali et al., 2019). The Block IoT Intelligence architecture, for example, has proposed a blockchain-enabled intelligent IoT platform in which AI algorithms at edge, fog and cloud layers analyze IoT big data while blockchain ensures decentralized data sharing and integrity, demonstrating performance benefits over conventional centralized designs (Shone et al., 2018). Similarly, broader discussions of the convergence of blockchain, IoT and AI have argued that IoT provides data, blockchain establishes rules and trust, and AI optimizes decisions, implying a natural synergy among the three (Samaila et al., 2018). The interaction effect observed in this study has translated these conceptual claims into quantitative evidence: organizations scoring highly on both blockchain and AI constructs have reported significantly better security performance than would be predicted by simply adding their individual effects. This has suggested that blockchain may enhance the trustworthiness and forensic value of the data streams and events that AI models analyze, while AI may help manage the complexity of blockchain-governed policies and detect misuse or anomalies in on-chain and off-chain interactions.

From a practical standpoint, the findings have carried several implications for chief information security officers (CISOs), IoT architects and security engineers responsible for next-generation deployments. First, the positive main effects of blockchain capability and AI analytics, along with their interaction, have implied that investment strategies should avoid treating these technologies as isolated pilot projects. Instead, roadmaps have been better framed around integrated architectures in which blockchain underpins device identity, configuration management and audit trails, while AI-driven intrusion detection and behavioral analytics operate on logs and telemetry that are anchored to an immutable, time-stamped ledger (Ali et al., 2019). Second, the significance of risk-management maturity has suggested that technology adoption should be paired with robust governance structures clear ownership of IoT assets, documented risk registers, continuous monitoring, and incident response playbooks consistent with the layered, requirement-driven approaches advocated in IoT security surveys (Atzori et al., 2010). In practice, this can mean designing IoT security architectures that explicitly map blockchain and AI capabilities to specific risks and controls at perception, network and application layers, rather than deploying them in an ad hoc manner. Third, the reliance on Likert-scale perceptions has highlighted the importance of change management and staff competence: organizations have been more likely to realize the benefits captured in this study when engineers and security analysts have understood how to configure smart contracts, tune AI models, and interpret their outputs. Finally, the synergy between blockchain and AI has suggested that CISOs should prioritize use cases where both technologies can be co-designed for example, secure firmware update pipelines, decentralized access control with AI-based misuse detection, or cross-organizational data-sharing agreements logged on-chain and monitored by anomaly-detection models rather than treating AI solely as a SIEM add-on or blockchain solely as a compliance ledger.

Theoretically, the study has contributed to IoT security research by operationalizing and empirically testing constructs that many prior works have discussed only qualitatively. IoT security reviews have typically organized threats and controls by architectural layer and security requirement, offering taxonomies but not always translating them into measurable latent variables that could be linked to outcomes (Al-Garadi et al., 2020). Likewise, IDS and AI-for-security surveys have often focused on algorithmic performance or dataset issues without embedding these models in a broader organizational context (Kshetri, 2017). By defining constructs such as blockchain-enabled security capability, AI-driven threat analytics capability, IoT risk-management maturity and IoT security performance, then estimating a regression model linking them, this research has offered a pipeline for moving from conceptual frameworks to testable, survey-based models. The significant interaction between blockchain and AI constructs has also suggested that future theoretical work should pay more attention to complementarities and co-evolution among security technologies, rather than modeling each control

in isolation. This aligns with emerging conceptualizations of "security mosaics," in which blockchain, AI, traditional cryptography and organizational processes are seen as interlocking pieces of a composite defense-in-depth strategy (Liao et al., 2013). Moreover, the use of practitioner perceptions as indicators of capability and performance has pointed to the value of integrating technical metrics (e.g., detection rates, latency) with organizational constructs (e.g., governance, skills, culture) in future models, helping to bridge the gap between systems-level theory and real-world adoption dynamics in IoT security.

At the same time, the study has had limitations that need to be acknowledged and that point toward future research opportunities. The cross-sectional design has made it impossible to establish definitive causal direction: while the regression results have been consistent with the hypothesis that blockchain and AI capabilities improve security performance, it has also been plausible that organizations with stronger security outcomes and cultures have been more willing or able to invest in blockchain and AI. Longitudinal designs or quasi-experimental interventions could help disentangle these dynamics. The reliance on self-reported perceptions has introduced the possibility of optimism bias or misalignment between perceived and actual technical maturity; prior work on IDS and IoT security has shown that configuration errors, dataset biases and untested failure modes can undermine systems that appear robust on paper (Gubbi et al., 2013). Furthermore, the case-study sampling strategy, while appropriate for exploring real deployments, has limited generalizability across sectors, regions and regulatory environments, especially given the wide diversity of IoT applications. Finally, the constructs in this study have been relatively high-level; they have not distinguished, for example, between different blockchain platforms, consensus mechanisms or AI model families, nor have they explicitly captured issues like adversarial ML, blockchain scalability or privacy leakage in on-chain data all of which have been identified as open challenges in the literature (Lee & Lee, 2015).

Future research can build on these findings in several directions. First, multi-method studies that combine survey-based constructs with objective technical metrics such as measured detection rates, false-positive rates, mean time to detect or recover, and blockchain transaction latencies would help validate and refine the perceptual measures used here. Second, longitudinal and multi-case designs across different industries (e.g., healthcare, manufacturing, smart cities, energy) could examine how blockchain-AI security portfolios evolve over time under different regulatory pressures and threat landscapes. Third, more granular modeling could differentiate specific blockchain patterns (permissioned vs. permissionless, sidechains, off-chain channels) and AI techniques (supervised vs. unsupervised, deep vs. shallow, federated vs. centralized) to identify which combinations yield the best trade-offs between security, performance and cost in various IoT contexts; this would extend and empirically test the design taxonomies suggested in earlier surveys (Ali et al., 2019). Fourth, future work could explore how emerging paradigms such as federated learning, self-healing cyber-defense and zero-trust architectures intersect with blockchain-enabled logging and AI-based intrusion detection in IoT, particularly under adversarial conditions where attackers deliberately target AI models or exploit smart contracts. Finally, qualitative studies involving in-depth interviews with CISOs, architects and engineers could complement quantitative models by uncovering organizational, cultural and regulatory factors that either accelerate or hinder the effective integration of blockchain and AI into IoT security programs. Together, these lines of inquiry would deepen understanding of how to design, deploy and govern secure, resilient and trustworthy next-generation IoT networks that harness the combined strengths of blockchain and artificial intelligence.

CONCLUSION

The study has examined how blockchain-enabled security protocols and AI-based threat analytics have contributed to the perceived security performance of next-generation IoT networks, and the evidence has consistently shown that these technologies, when embedded within a mature risk-management environment, have formed a powerful and complementary security foundation. By adopting a quantitative, cross-sectional, case-study–based design and gathering Likert-scale perceptions from professionals directly involved in IoT architecture and security operations, the research has been able to translate broad conceptual claims about blockchain, AI and IoT security into empirically testable constructs. The descriptive statistics have indicated that respondents have generally agreed that blockchain controls, AI analytics and formal IoT risk-management practices have been present to a meaningful degree in their organizations, and that overall IoT security performance has been rated

positively. Reliability and validity analyses have confirmed that the measurement scales have been internally consistent and conceptually coherent, providing confidence that the latent constructs have faithfully captured perceptions of capability and performance. Correlation analysis has revealed strong, positive associations among blockchain capability, AI capability, risk-management maturity and security performance, while multiple regression modeling has demonstrated that both blockchain-enabled security and AI-based analytics have had significant, independent effects on perceived IoT security performance, with AI often exerting the stronger influence. Importantly, the inclusion of an interaction term has shown that organizations reporting high blockchain capability and high AI capability simultaneously have achieved the highest levels of perceived security performance, supporting the conclusion that these technologies have operated synergistically rather than merely additively. In other words, blockchain has appeared most valuable when its tamper-evident logs, decentralized identity and smart-contract policies have been coupled with AI-driven anomaly detection and adaptive response that can intelligently interpret and act upon those trusted data, while AI has appeared more effective when the data and events it consumes have been anchored to a verifiable, immutable ledger. At the same time, the significant contribution of IoT risk-management maturity has underscored that technology alone has not been sufficient; organizations have achieved the strongest security outcomes where advanced tools have been integrated into structured processes for risk assessment, monitoring and incident response. Collectively, these findings have confirmed all three core hypotheses, fulfilled the stated research objectives and contributed to both theory and practice by offering a tested conceptual model that links blockchain capability, AI analytics, risk-management maturity and IoT security performance in an integrated framework. Although the cross-sectional design, perceptual measures and case-based sampling have imposed limits on causal inference and generalizability, the results have provided a robust starting point for more fine-grained, longitudinal and multi-method investigations. Overall, the study has shown that securing next-generation IoT networks has been most effective when blockchain-enabled protocols and AI-based security analytics have been designed, deployed and governed together, within a coherent risk-management strategy, to create IoT environments that are not only connected and intelligent but also demonstrably more secure, resilient and trustworthy.

RECOMMENDATION

On the basis of these findings, the study has put forward several integrated recommendations for organizations seeking to secure next-generation IoT networks through blockchain-enabled protocols and AI-based threat analytics. First, security leaders and IoT architects should treat blockchain and AI as complementary pillars of a unified security architecture rather than as isolated pilots; practical roadmaps should explicitly map blockchain to functions such as decentralized device identity, configuration and access-control logging, and smart contract–based policy enforcement, while AI models should be positioned to analyze both on-chain events and off-chain telemetry for anomaly detection, intrusion detection and adaptive response. Second, before large-scale rollout, organizations should have conducted structured readiness assessments to evaluate existing infrastructure, data quality, skills and governance, and should have used these assessments to prioritize a small number of high-value use cases such as secure firmware updates, zero-trust access to critical IoT assets or cross-organizational data sharing in supply chains where blockchain and AI together can deliver clear, measurable improvements. Third, implementation should have followed a phased approach, beginning with controlled pilots in limited IoT domains, accompanied by clear success criteria (for example, reduction in incident rates, mean time to detect and mean time to respond), and only then scaling to broader deployments once both technical performance and operational fit have been validated. Fourth, because risk-management maturity has significantly influenced outcomes, organizations should have embedded blockchain and AI into existing risk and compliance processes rather than treating them as separate technologies; this has involved updating risk registers to include specific IoT and algorithmic risks, aligning smart-contract policies with formal security policies and regulatory obligations, and integrating AI-generated alerts into established incident-response playbooks and security operations center workflows. Fifth, investment in human capabilities should have been prioritized alongside technology: security and operations staff should have received targeted training on blockchain concepts, key-management practices, smart-contract design, model tuning and

interpretation of AI outputs, and cross-functional teams of security, data science and operations personnel should have been formed to jointly own IoT security outcomes. Sixth, organizations should have established ongoing monitoring and evaluation mechanisms, including periodic model retraining, review of smart contracts, audits of on-chain logs and post-incident reviews that explicitly assess the performance of blockchain and AI components; metrics from these activities should have been fed back into continuous improvement cycles. Finally, at a strategic level, senior management and CISOs should have ensured that procurement, vendor management and architectural decisions explicitly favored interoperable, standards-aligned solutions, so that blockchain platforms, AI engines and IoT devices can be integrated without excessive customization, and so that future enhancements such as federated learning, privacy-preserving analytics or more scalable consensus mechanisms can be adopted without major redesign. By following these recommendations, organizations have been better positioned to translate the theoretical advantages of blockchain and AI into sustainable, demonstrable improvements in the security performance of their next-generation IoT networks.

LIMITATIONS

The study has had several limitations that must be acknowledged when interpreting its findings and considering their applicability beyond the specific context examined. First, the research has relied on a cross-sectional design, which has captured perceptions at a single point in time and has therefore not been able to establish causal relationships or track how blockchain-enabled security and AI-based analytics capabilities, as well as IoT security performance, have evolved in response to new deployments, incidents or organizational changes. Second, the data source has been a single case-study setting (or a small number of closely related organizations), which has meant that the sample has reflected particular sectoral, technological and regulatory conditions; consequently, the results have not necessarily been generalizable to all industries, regions or types of IoT deployments, especially those operating at substantially different scales or under different compliance obligations. Third, the constructs have been measured using self-reported Likert-scale responses from professionals involved in IoT and security, so the study has been vulnerable to perception biases, social desirability bias and possible gaps between perceived and actual technical maturity or performance. For example, respondents may have overestimated the effectiveness of their blockchain implementations or AI models, or they may not have had complete visibility into all security controls across large, distributed IoT environments. Fourth, the quantitative measures have been relatively high-level and have not differentiated among specific design choices, such as the type of blockchain platform or consensus mechanism used, the precise architectures of AI models, or the details of data pipelines and integration patterns; as a result, the study has not been able to identify which concrete configurations or implementation strategies have been more or less effective within the broader categories of "blockchain capability" and "AI analytics capability." Fifth, the study has not incorporated objective technical metrics such as observed attack detection rates, false positives, incident counts, downtime or transaction latencies alongside subjective perceptions, which has limited the ability to cross-validate the survey-based indicators of IoT security performance. Sixth, although reliability and validity checks have been conducted, the use of a single survey instrument administered in one context has meant that further validation in other settings would have been necessary to confirm the stability and transferability of the measurement model. Finally, potential omitted variables have remained a concern: factors such as organizational culture, budget constraints, vendor dependence, legacy system complexity or prior breach history may also have influenced both the adoption of blockchain and AI and the perception of security performance, but they have not been explicitly modeled in this study. Together, these limitations have suggested that the findings should be viewed as an initial, context-specific contribution that has highlighted important relationships between blockchain capability, AI analytics and IoT security performance, rather than as definitive, universally generalizable conclusions.

REFERENCES

Abdulla, M., & Md. Jobayer Ibne, S. (2021). Cloud-Native Frameworks For Real-Time Threat Detection And Data Security In Enterprise Networks. *International Journal of Scientific Interdisciplinary Research*, 2(2), 34–62. https://doi.org/10.63125/0t27av85

Abomhara, M., & Køien, G. M. (2014). *Security and privacy in the Internet of Things: Current status and open issues* 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS),

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376. https://doi.org/10.1109/comst.2015.2444095

Al-Garadi, M. A., Mohamed, A., Al-Ali, A., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646–1685. https://doi.org/10.1109/comst.2020.2988293

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2019). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *21*(2), 1676–1717. https://doi.org/10.1109/comst.2018.2886932

Alshehri, M. D., & Hussain, F. K. (2019). A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). *Computing*, *101*(7), 791–818. https://doi.org/10.1007/s00607-018-0685-7

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Chen, W., Ma, M., Zhang, Y., Yu, N., & Wang, X. (2020). Blockchain for Internet of things applications: A review and open issues. *Journal of Network and Computer Applications*, *172*, 102839. https://doi.org/10.1016/j.jnca.2020.102839

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

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). *Blockchain for the Internet of Things: A systematic literature review* 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA),

Cui, P., Guin, U., Skjellum, A., & Umphress, D. (2019). Blockchain in IoT: Current trends, challenges, and future roadmap. *Journal of Hardware and Systems Security*, *3*(3), 338–364. https://doi.org/10.1007/s41635-019-00079-5

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). *Blockchain for IoT security and privacy: The case study of a smart home* 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops),

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003

Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294–1312. https://doi.org/10.1109/comst.2015.2388550

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Habibullah, S. M., & Md. Foysal, H. (2021). A Data Driven Cyber Physical Framework For Real Time Production Control Integrating IOT And Lean Principles. *American Journal of Interdisciplinary Studies*, *2*(03), 35–70. https://doi.org/10.63125/20nhqs87

Haq, N. F., Onik, A. R., Hridoy, M. A. K., Rafni, M., Shah, F. M., & Farid, D. M. (2015). Application of machine learning approaches in intrusion detection system: A survey. *International Journal of Advanced Research in Artificial Intelligence*, *4*(3), 9–18. https://doi.org/10.14569/ijarai.2015.040302

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems*, *97*, 512–529. https://doi.org/10.1016/j.future.2019.02.060

Hou, J., Qu, L., & Shi, W. (2019). A survey on Internet of Things security from data perspectives. *Computer Networks*, *148*, 295–306. https://doi.org/10.1016/j.comnet.2018.11.025

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*(8), 1–18. https://doi.org/10.1186/s13635-020-00111-0

Kshetri, N. (2017). Can blockchain strengthen the Internet of Things? *IT Professional*, *19*(4), 68–72. https://doi.org/10.1109/mitp.2017.3051335

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, *12*(9), 157. https://doi.org/10.3390/fi12090157

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Leloglu, E. (2017). A review of security concerns in Internet of Things. *Journal of Computer and Communications*, *5*(1), 121–136. https://doi.org/10.4236/jcc.2017.51010

Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*, *125*, 251–279. https://doi.org/10.1016/j.jnca.2018.10.019

Md Sanjid, K., & Md. Tahmid Farabe, S. (2021). Federated Learning Architectures For Predictive Quality Control In Distributed Manufacturing Systems. *American Journal of Interdisciplinary Studies*, *2*(02), 01-31. https://doi.org/10.63125/222nwg58

Md Sarwar, H. (2021). Sustainable Materials Characterization For Low-Carbon Construction And Infrastructure Durability. *American Journal of Interdisciplinary Studies*, *2*(01), 01-34. https://doi.org/10.63125/wq1wdr64

Md. Musfiqur, R., & Saba, A. (2021). Data-Driven Decision Support in Information Systems: Strategic Applications In Enterprises. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 01-33. https://doi.org/10.63125/cfvg2v45

Md. Omar, F., & Md Harun-Or-Rashid, M. (2021). POST-GDPR Digital Compliance in Multinational Organizations: Bridging Legal Obligations With Cybersecurity Governance. *American Journal of Scholarly Research and Innovation*, *1*(01), 27-60. https://doi.org/10.63125/4qpdpf28

Md. Redwanul, I., Md Nahid, H., & Md. Zahid Hasan, T. (2021). Predictive Analytics in Supply Chain Management A Review Of Business Analyst-Led Optimization Tools. *Review of Applied Science and Technology*, *6*(1), 34-73. https://doi.org/10.63125/5aypx555

Md. Tarek, H., & Sai Praveen, K. (2021). Data Privacy-Aware Machine Learning and Federated Learning: A Framework For Data Security. *American Journal of Interdisciplinary Studies*, *2*(03), 01–34. https://doi.org/10.63125/vj1hem03

Md. Wahid Zaman, R., & Momena, A. (2021). Systematic Review Of Data Science Applications In Project Coordination And Organizational Transformation. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(2), 01–41. https://doi.org/10.63125/31b8qc62

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Breitenbacher, D., Shabtai, A., & Elovici, Y. (2018). N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, *17*(3), 12–22. https://doi.org/10.1109/mprv.2018.03367731

Misra, S., Gupta, A., & Saha, S. (2016). Internet of Things (IoT): A technological analysis. *American Journal of Electrical and Electronic Engineering*, *4*(1), 23–27. https://doi.org/10.12691/ajeee-4-1-4

Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2020). Security of Internet of Things using RC4 and ECC algorithms (case study: Smart irrigation systems). *Wireless Personal Communications*, *113*(3), 1713–1742. https://doi.org/10.1007/s11277-020-07758-5

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

Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020). Security requirements for the Internet of Things: A systematic approach. *Sensors*, *20*(20), 5897. https://doi.org/10.3390/s20205897

Radoglou-Grammatikis, P. I., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things*, *5*, 41–70. https://doi.org/10.1016/j.iot.2018.11.003

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Rony, M. A. (2021). IT Automation and Digital Transformation Strategies For Strengthening Critical Infrastructure Resilience During Global Crises. *International Journal of Business and Economics Insights*, *1*(2), 01-32. https://doi.org/10.63125/8tzzab90

Samaila, M. G., Neto, M., Fernandes, D. A. B., Freire, M. M., & Inácio, P. R. M. (2018). Challenges of securing Internet of Things devices: A survey. *Security and Privacy*, *1*(2), e20. https://doi.org/10.1002/spy2.20

Shaikh, S., & Aditya, D. (2021). Federated Learning-Driven Predictive Quality Analytics and Supply Chain Optimization In Distributed Manufacturing Networks. *Review of Applied Science and Technology*, *6*(1), 74-107. https://doi.org/10.63125/k18cbz55

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *2*(1), 41–50. https://doi.org/10.1109/tetci.2017.2772792

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

Sudipto, R., & Md Mesbaul, H. (2021). Machine Learning-Based Process Mining For Anomaly Detection And Quality Assurance In High-Throughput Manufacturing Environments. *Review of Applied Science and Technology*, *6*(1), 01-33. https://doi.org/10.63125/t5dcb097

Syed Zaki, U. (2021). Modeling Geotechnical Soil Loss and Erosion Dynamics For Climate-Resilient Coastal Adaptation. *American Journal of Interdisciplinary Studies*, *2*(04), 01-38. https://doi.org/10.63125/vsfjtt77

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102. https://doi.org/10.3390/app10124102

Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future Generation Computer Systems*, *108*, 909–920. https://doi.org/10.1016/j.future.2017.11.022

Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the Internet of Things. *Sensors*, *19*(9), 1977. https://doi.org/10.3390/s19091977

Wang, Z. (2018). Deep learning-based intrusion detection with adversaries. *IEEE Access*, *6*, 38367–38384. https://doi.org/10.1109/access.2018.2854599

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

Yang, W., Zhang, J., Wang, C., & Mo, X. (2019). Situation prediction of large-scale Internet of Things network security. *EURASIP Journal on Information Security*, *2019*(13), 1–13. https://doi.org/10.1186/s13635-019-0097-z

Yousuf, O., & Mir, R. N. (2019). A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures. *Information & Computer Security*, *27*(2), 292–323. https://doi.org/10.1108/ics-07-2018-0084

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009