IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

Blockchain-Enabled Secure Wireless Sensor Networks for Transparent E-Governance: An Analysis of Data Integrity, Trust Management, and Service Efficiency

Vivek Kumar and Sumit Lal
Government Engineering College, Vaishali
Assistant Professor, Government Engineering College, Vaishali

Abstract: *The use of a wireless sensor network is increasingly supporting e-governance functions such as municipal utility monitoring, environmental monitoring, grievance-based field reporting, and smart public service delivery. Most wireless sensor network architectures rely on a gateway or database. However, this introduces vulnerabilities to data integrity, node accountability, and auditability. This study examines transparency through a blockchain-enabled WSN architecture for e-governance. The study applies a reproducible Python-based Monte Carlo simulation with a fixed random seed, five node densities, three architectural scenarios, and 450 observations. The scenarios that are compared in this work are a normal WSN, a centralized secure WSN, and a permissioned blockchain-enabled WSN with smart-contract-based identity registration, hash-linked data records, trust scoring, and tamper verification. Descriptive statistics, one-way ANOVA, Welch t-tests, Pearson correlation, and multiple linear regression analysis. The blockchain-assisted WSN, as evidenced by the simulation findings of our project, produced the highest mean data integrity score, tampering detection rate, trust score, malicious node detection rate, and packet delivery ratio. The architecture also improved the composite service efficiency index relative to the conventional baseline, even though it introduced higher latency, transaction confirmation time, and energy consumption. The research indicates that the permissioned blockchain can enhance public-sector WSN transparency with edge aggregation and lightweight cryptographic operations along with carefully tuned endorsement rules. The methods presented in this study allow for scrutiny of secure WSN designs tailored for e-governance.*

Keywords: Blockchain; wireless sensor networks; e-governance; data integrity; trust management; IoT security; service efficiency

I. INTRODUCTION

Wireless sensor networks (WSNs) have become a useful infrastructure for field data collection in smart cities or digital government. Sensor nodes can send information about water quality, electricity consumption, air pollution, road conditions, and waste-bin levels. They can also provide flood information and building energy use, as well as other service variables needed by public agencies for evidence-based administration. In such situations, the sensor stream is not just any technical telemetry; it can affect public spending, service prioritization, grievance redressal, compliance monitoring and accountability. The most recent literature on digital government develops the view that public systems should combine connection with trust, transparency, and accountable data governance instead of viewing digitalisation as merely a service improvement at the front end (United Nations Department of Economic and Social Affairs [UN DESA] 2024).

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-38040

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

A major issue is that many (so-called) collaborative WSN deployments still use a gateway-centric or database-centric trust model. Data collection is performed by various low-power nodes; however, this information can only be accepted, modified, verified, or rejected by a central authority. While this design is operationally convenient, it introduces risks of single-point compromise, insider manipulation, delayed detection of false data injection, and weak public auditability. According to Ramasamy et al. (2021) and Xia et al. (2022), security research in Wireless Sensor Networks (WSN) has shown that the exploitation of vulnerable issues due to their offering of wireless communication, unattended physical deployment, energy constraints, and multi-hop routing renders sensor networks vulnerable to various attacks.

An article suggests that blockchain can help in attaining distributed trust because it employs hash-linked storage, offers chronological verification and shared validation, as well as smart-contract-driven enforcement. The technology should not be viewed as a one-size-fits-all substitute for standard controls for cyber-security. Bankers should be able to place their trust in the technology. However, that does not mean all bets are off on database operators that can be hacked, or that the technology will not benefit when the same dishonest actor has control of each database. NIST defines blockchain as a tamper-evident and tamper-resistant digital ledger, the distributed implementation of which has properties that are relevant to situations where sensors must be able to verify records after collection (Yaga et al., 2018). In the realm of IoT and Wireless Sensor Network (WSN), the application of blockchain can facilitate identity registration, decentralized audit logs, as well as data provenance, along with transparent validation workflows provided by Da Xu et al. (2021) and Khan et al. (2022) in the WSN and IoT.

1.1 Background of E-Governance Wireless Sensor Networks

Cyber-physicalsensing is important for e-governance applications. Sensors can identify abnormal pressure or contamination in smart water management. Low-cost nodes can generate spatially distributed streams of air-quality data or flood alarms. Field sensors can monitor asset operation and service availability in rural public-service monitoring. Applications in this reference need trustworthy and timely data as values reported may be acted on by government dashboards, citizen-facing portals, and administrative escalation systems (UN DESA, 2024). WSNs are appealing in this regard as they are scalable, low-cost, and can be deployed where wired instrumentation is unfeasible.

Nonetheless, the qualities which make WSNs attractive make them vulnerable too. Nodes can be physically accessible to the attacker, may be resource-constrained, may be intermittently connected, and dependent on multi-hop routing through neighbouring nodes. Conventional cryptographic security offers some assistance in addressing the trust issue. However, it does not completely resolve the matter. If a node is legitimately registered but compromised. It can still send fake measurements or route manipulation messages. As per Awan et al. (2022); Xia et al. (2022), trust-management schemes evaluate node behaviours over time. In this regard, reputation, forwarding success, residual energy, and consistency indicators support routing and data validation decisions.

1.2 Data Integrity and Trust Problems in Conventional WSNs

Corrupted sensor data has the potential to distort public decisions. Thus, e-governance requires data integrity. In regular WSNs, the integrity may be compromised at the node, link, gateway, database and application layers. An attacker can inject false values, replay old packets, masquerade as a legitimate node, thwart packets from honest nodes and adjust records after they reach a central server. While access control and backups can protect centralized logs, these logs do not usually offer independent verifiability by citizens, government auditors, or other departments. As a result, studies regarding WSN security based on blockchain has highlighted as the important research direction malicious node detection, secure routing, and tamper-resistant reporting (Hsiao & Sung, 2021; Ramasamy et al., 2021).

Trust management refers closely to the integrity of data and the credibility of the data source. A record that's cryptographically signed can still be misleading if the signing node is compromised or behaving strategically. Trust management is more effective when nodes are evaluated, abnormal reporting is detected, and malicious nodes cannot affect routes or the public dashboard.While blockchain cannot determine sensor truth, it allows auditing trust evidence.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

Furthermore, blockchain will not retroactively change trust scores. Also, smart contract enforce rules for node registration and penalty execution (Awan et al., 2022; Abd El-Moghith & Darwish, 2021).

1.3 Functionality of Blockchain Technology in Secure Public Digital Infrastructure

Permissioned blockchain is applicable for public-service WSN because the validators can be known institution, department, utility or district administration node. A permissioned architecture lessens the computing load implied by public proof-of-work chains and provides governance rules to be encoded through endorsement policies and smart contracts. For example, Hyperledger Fabric uses an execute-order-validate transaction model and endorsement policies, which specify the peers that must endorse a transaction before it is deemed valid (Hyperledger Fabric Documentation, n.d.-a; Piao et al., 2023).

As per suggested e-governance scheme, the blockchain ledger will not save all raw sensor streams.In lieu of that, edge gateways will aggregate records, run hashes of confirmed sensor readings, submit integrity metadata, update node trust scores, and trigger smart-contract events on detecting data anomalies. It preserves auditability while simultaneously limiting ledger bloat. It is also in accordance with IoT Security Baselines to implement device identity, data protection, integrity of configuration and update (Fagan et al., 2020).

1.4 Research Gap

The existing works of literature can provide some models for WSN authentication and secure routing using blockchain. Still, three gaps exist. To begin, a lot of the literature on blockchain-WSN specially the technical security metrics is very detail-oriented and not conceptualize. Many conceptual papers discuss using blockchain for public-sector services, but they do not evaluate the trade-off in WSN-level performance, such as latency, packet delivery ratio, energy consumption, transaction confirmation time, etc. Moreover, few efforts combine data integrity, trust management, and service efficiency within a quantitative framework that allows comparison of conventional, centralised, and permissioned blockchain-enabled architectures (Awan et al., 2022; Khan et al., 2022; Rathod et al., 2022).

1.5 Research Objectives

- To design a blockchain-enabled WSN architecture for transparent e-governance applications.
- To compare conventional WSN, centralized secure WSN, and blockchain-enabled WSN scenarios under the same simulated attack and node-density conditions.
- To evaluate data integrity, tamper detection, trust management, malicious node detection, packet delivery ratio, latency, throughput, energy consumption, and service efficiency.
- To statistically test whether architecture choice significantly affects security and service-performance outcomes.
- To identify implementation trade-offs for public-sector deployment of blockchain-enabled WSNs.

1.6 Research Questions

- RQ1: How does blockchain integration improve data integrity in WSN-based e-governance systems?
- RQ2: How does blockchain-based trust management affect malicious node detection and network reliability?
- RQ3: What is the impact of blockchain integration on service efficiency indicators such as latency, throughput, packet delivery ratio, and energy consumption?
- RQ4: Is blockchain-enabled WSN significantly more secure and transparent than conventional WSN architecture?

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

II. LITERATURE REVIEW

2.1 Wireless Sensor Networks for Public Sector and Smart Governance

The WSNs convert geographically distributed physical events into signals which can be monitored by public sectors. This will permit real-time observation of infrastructure, while also providing an evidence layer for service delivery in smart-governance. Government use of WSN deployments goes beyond technical sensor fields and includes citizen trust, departmental accountability, and regulatory compliance as socio-technical systems.The analysis of UN DESA's Digital government highlights the broader movement toward the integration, the inclusion and the data-driven public service which make the reliability of data – a governance problem rather than a narrow network-management issue (UN DESA, 2024).

The value of WSNs to the public sector is dependent on continuity, traceability, and value. A municipal water-level sensor that gives a falsely low value may delay flood warnings; a smart-metering sensor that is tampered with will misreport billing or subsidy data; an environmental sensor that is silenced selectively will weaken enforcement action by regulators. These examples show why secure data acquisition, verifiable logging as well as service-level analytics need to be considered together (Khan & Salah, 2018; Ramasamy et al., 2021).

2.2 Security Issues within WSNs

Limited battery power, small memory, low computation capacity, and exposure to untrusted physical environments constrain WSN security. The following is a list of usual attacks that an ad hoc network may be subject to: node capture, false data injection, replay, spoofing, sybil behavior, sinkhole routing, selective forwarding and packet dropping.Denial of service attacks can undermine the integrity of systems. In recent reviews it was emphasized that conventional cryptographic protection is necessary; however, it is not sufficient (Ramasamy et al., 2021; Xia et al., 2022). This means that compromised internal nodes may behave maliciously while holding valid credentials.

Overcoming this limit is a behavioral evidence evaluation. Routing that is trust-aware evades nodes that drop packets or report inconsistent values. While reputation aggregation can enhance resilience, centralized trust tables risk manipulation or bottlenecks. The aim of blockchain-based trust management is to ensure that recorded decisions regarding approval and routing are tamper-evident (Awan et al., 2022; Abd El-Moghith & Darwish, 2021).

2.3 Blockchain Security for IoT and WSN

A thorough investigation into Blockchain-IoT interfaces was carried out due to weaknesses of centralized trust and data integrity. Research papers analyzing blockchain for IoT suggest that they could potentially perform provenance, authentication, access control, automated execution, and tamper-evident storage. However, scaling and energy consumption constraints nonetheless remain important (Dai et al., 2019; Da Xu et al., 2021; Khan et al., 2022). The blockchain is most suitable in WSNs when it is not used extensively on sensor nodes to make them perform costly consensus operations. The edge devices or gateway validators can interact with the ledger instead.

According to Hsiao and Sung, blockchain integration can be vital in enhancing the security of data transfer in WSNs. Also, Ramasamy et al. have reviewed the approaches concerning malicious node detection using blockchain integrated WSN.Awan et al. (2022) further work on blockchain (BC) based secure routing and trust management which link authentication and trust evaluation to improve routing performance. The findings of these studies are in line with present paper's assumption about the implementation of blockchain to the gateway and validation layers rather than the constrained end nodes directly.

2.4 Trust Management in Decentralized Sensor Networks

Within a Wireless Sensor Network (WSN), trust management is employed to check whether nodes act reliably, such as if they forward packets, if they report values within expected bounds, and if they avoid making malicious routing announcements. Trust scores can be calculated from many parameters like direct interaction, indirect recommendation, residual energy, communication success and an anomaly indicator. As per Xia et al. (2022), trust mechanisms can

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

address behavioral threats in WSN security that cannot be handled merely by cryptography. The schemes are secured further through the ability of blockchain to make trust updates transparent and difficult to alter in hindsight.

Trust management in e-governance has an added institutional dimension. Citizens, municipal officers, utilities, regulators, and third-party auditors can make use of sensor data. A trust score that is saved exclusively on an internal server may not be accountable. Using a permissioned blockchain can permit access to the sequence of trust-score changes to authorized stakeholders while also providing a verifiable artefact of auditability in the event of contesting automated decisions (Yaga et al. 2018; UN DESA 2024).

2.5 Data Integrity, Auditability and Transparency in E-Governance

The integrity of data in e-governance means that the data that is collected is reliable. It is accurate, complete and consistent, etc. It is also resistant to unauthorized interference and changes. Through hash chaining and digital signatures, blockchain can facilitate timestamping and distributed validation.In a 34-word overview NIST explains that, blockchain systems allow a community of users to record transactions in a shared ledger such that, under normal operating conditions, recorded transactions are not capable of being modified after they are published (Yaga et al. 2018). This property can be used to generate tamper-evident audit logs for sensors in public sector WSNs.

The transparency advantage doesn't occur automatically. A blockchain ledger may faithfully store poor-quality data, which calls for the adoption of validation rules, anomaly detection, node authentication, and governance processes. In this paper, it is understood that only authorized stakeholders should be able to trace how a sensor record was generated, validated, stored, and acted upon. According to digital-government principles linking technology with accountability, service quality and data responsibility (UN DESA, 2024).

2.6 Service Efficiency and Performance Trade-offs

Integrating blockchain can help foster integrity trust in the construction supply chain, but it may also add latency and more. According to documentation of Hyperledger Fabric, endorsement policies are an important component of transaction validity and empirical work suggests that endorsement policy choice can affects latency in permissioned networks (Hyperledger Fabric Documentation, n.d.-a; Piao et al., 2023). The Hyperledger Caliper emphasizes throughput and latency as the fundamental performance metrics for blockchain networks (n.d.) (Performance and Scale Working Group, 2018).

As a result, blockchain-enabled WSN should be evaluated as a security-efficiency trade-off rather than purely a superior architecture. The design has to balance tamper resistance, public auditability, packet delivery, transaction delay, throughput, energy cost, service response time. This paper strives to achieve that balance by creating a service efficiency index from security, network and operational indicators.

2.7 Gap in Literature and Conceptual Positioning

As has been established by the literature reviewed, blockchain can improve IoT and WSN security, trust management can help reduce malicious routing behaviour, and e-governance requires reliable and auditable data. The bridging gap designs a single quantitative model for assessing the integrity of data, trust management of entities, and efficiency of service under the same architecture. The authors clarify that blockchain-enabled WSN should be viewed as an auditable security architecture, suitable for public-service sensor data, rather than a substitute for all network-security controls as maintained by Da Xu et al. (2021), Khan et al. (2022), Rathod et al. (2022).

III. CONCEPTUAL FRAMEWORK

3.1 Conceptual Linkages and Mechanisms

The conceptual framework links the integration of blockchain technology to node authentication, trust management, data integrity, tampering detection, services transparency, service efficiency and e-governance reliability. Blockchain integration is seen as an autonomously designedarchitectural intervention.Node authentication works through registering node identities and the gateway credentials, trust management makes trust-score updates auditable and for

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

data integrity it records hashes and validation stage events on a ledger that is tamper-evident. The mechanisms are expected to enhance service transparency and reliability, but have an adversae effect over performance in terms of latency and energy overhead (Awan et al. 2022; Hyperledger Fabric Documentation n.d.-b; Yaga et al. 2018).

Figure 1. Conceptual Framework of Blockchain-Enabled Secure WSN for Transparent E-Governance

Source: Author generated from reproducible simulation outputs and architecture design.

3.2 E-Governance Reliability Logic

The framework assumes that e-governance reliability emerges from both security and service performance. A highly secure architecture with unacceptable latency may fail in emergency public services, while a fast architecture with weak integrity may mislead decision makers. The proposed model therefore evaluates blockchain-enabled WSN through a dual lens: integrity and trust on one side, and service efficiency on the other.

IV. PROPOSED SYSTEM ARCHITECTURE

The proposed architecture uses a layered design in which constrained sensor nodes perform sensing and lightweight signing, edge gateways perform aggregation and preliminary validation, and a permissioned blockchain records integrity metadata, trust events, and audit logs. The architecture is intended for e-governance use cases such as smart water monitoring, municipal energy services, public environmental monitoring, and rural service-status verification. Its design reflects the principle that resource-constrained WSN nodes should not carry the full burden of blockchain validation (Khan et al., 2022; Ramasamy et al., 2021).

4.1 Sensor Node Layer

A cluster head or gateway is where low-power devices of the sensor node layer perform physical measurements that are sent. Every node gets a registration status and a cryptographic identity. The node signs such outgoing packets with lightweight authentication material, and the gateway checks the identity of the node before accepting that packet. The integrity of the physical layer, which can be subjected to capturing and false data injection, should be continuously monitored rather than permanently assumed (Fagan et al., 2020; Xia et al., 2022).

4.2 Edge Gateway Layer

The edge gateway layer aggregates all the node's data together. It also filters out clear outliers and computes a hash of all accepted readings. Finally, it will submit the transaction proposals to the blockchain network. Gateways also keep local buffers so that data isn't lost when disconnected. According to the proposed design, the gateways store raw high-frequency sensors streams off-chain and on-chain only submit integrity proofs, trust updates and crucial service events to decrease the ledger load (Goyat et al., 2022; Khan et al., 2022).

4.3 Blockchain Validation Layer

The blockchain validation layer resembles a permitted network of validator peers run by public agencies, municipal utilities, or authorized audit agencies. Before a transaction is committed, validator peers endorse rules. The transaction flow of Hyperledger Fabric validates transactions for compliance with endorsement policy and ledger-state consistency before commitment which means it can be used for multi-organization public sector workflows which necessitate accountability (Hyperledger Fabric Documentation, n.d.-b; Piao et al., 2023).

4.4 Smart Contract Layer

Identity registration, trust-score calculation, data hash acceptance, anomaly flagging, penalty logic are encoded in smart contract layer. As an instance, if a sensor node constantly transmits inconsistent readings or causes packet drops, its trust score can be made less and the route manager can exclude this node from the future forwarding path. While smart

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

contracts are not a substitute for statistical anomaly detection, they can generate a consistent, auditable environment for rule execution (Awan et al. 2022; Hyperledger 2022b).

4.5 E-Governance Service Layer

The layer for e-governance services contains an administration dashboard, public-service notification, citizen grievance integration, report API, etc. When a sensor event is confirmed, the dashboard shows both the observed value and integrity asserted value. A departmental officer can check if the reading source was a high-trust node and if the hash was committed on-chain along with tamper alerts. It strengthens the chain of evidence to make service decisions (UN DESA, 2024; Yaga et al., 2018).

4.6 Citizen and Administrative Audit Layer

Authorized public citizens, oversight bodies, auditors, and administrators can verify through the audit layer whether key records were altered, delayed or excluded. Public transparency does not require exposing sensitive raw data; it can be accomplished by giving verifiable metadata, proof of inclusion, and date-stamped audit events. This is especially helpful in disputes alleging environmental readings, utility service outage, or delayed response to infrastructure (Yaga et al., 2018; UN DESA, 2024).

V. RESEARCH METHODOLOGY

5.1 Research Design

The design of the research is quantitative comparative simulation. Since the goal is to assess for architecture-level differences under controlled attack and node-density conditions, a reproducible Monte Carlo simulation was chosen. Using a fixed random seed of 20260621, the simulation was executed using Python. A total of 450 observations were generated from the three WSN architectures, five node densities, and 30 replications of each density-scenario pair. We suggest interpreting the results as controlled simulations rather than field-deployment measurements.

The three architectures that were compared include (a) a conventional sensors and wireless network architecture WSN which does not have the blockchain, (b) a WSN with a centralized secure database logging, and (c) a WSN with a blockchain that is enabled having permissioned validation, smart contract trust scoring, and tamper-evident integrity records. The comparative approach takes its cue from previous research done on WSN as well as Blockchain namely; the architecture alternatives are evaluated on common security and performance metrics (Awan et al., 2022; Hsiao & Sung, 2021; Ramasamy et al., 2021).

5.2 Simulation Environment and Data Generation

The environment for the study was reproducible and simulation rather than used public dataset. The rationale behind this choice is due to the fact that public WSN datasets do not usually contain all the variables required in this paper such as the transaction confirmation time, trust-score updates, tamper detection, malicious node detection and service response time under a common attack model. Consequently, the simulation depicts a smart municipal monitoring network with node densities of 25, 50, 75, 100, and 125 nodes in the area of 500 m x 500 m. It utilizes abstraction as per IEEE 802.15.4 and multi-hop cluster based reporting. The peer-to-peer network of the blockchain is modeled as a permissioned ledger architecture like hyperledger fabric (Hyperledger Fabric Documentation, n.d.-b; Piao et al., 2023).

Table 1. Simulation / Experimental Parameters

Parameter	Value
Simulation tool	Python 3 Monte Carlo simulation using NumPy, pandas, SciPy, statsmodels, and Matplotlib
Random seed	20260621
Total observations	450 observations
Node densities	25, 50, 75, 100, and 125 sensor nodes

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

Replications	30 replications per scenario per node density
Network area	500 m x 500 m simulated municipal service zone
Communication protocol	IEEE 802.15.4-style low-power wireless abstraction
Routing protocol	Cluster-based multi-hop routing with scenario-specific trust filtering
Blockchain type	Permissioned blockchain model patterned on Hyperledger Fabric
Consensus / ordering	Raft-style permissioned ordering abstraction
Block size	50 sensor transactions per block
Transaction rate	One reading per node per time slot; gateway aggregates and submits integrity metadata
Malicious node percentage	15% of sensor nodes treated as malicious or unreliable
Packet size	64-byte sensor payload plus 32-byte hash/signature metadata abstraction
Simulation duration	1,000 time slots per replication
Energy model	Architecture-specific per-node communication, verification, and ledger-interaction overhead
Attack model	Data tampering, false data injection, replay, unauthorized access, malicious reporting, and packet dropping
Performance metrics	PDR, latency, throughput, energy, integrity, trust, detection rates, transaction time, service response, and service efficiency

Note. The simulation is reproducible through the fixed seed and parameter set. Values are not claimed as field-deployment observations.

5.3 System Scenarios

In scenario 1, the conventional WSN is implemented with local node authentication and gateway forwarding but does not offer. In Scenario 2, there will be a secure centralized WSN logging the database with access control and the validation of the gateway. However, the trust and audit record will still be controlled centrally. In this scenario, the blockchain-enabled secure wireless sensor network uses various techniques for security.Through a three-scenario-design, we isolate the added value and costs of distributed trust relative to the weakly protected and centrally protected alternatives (Da Xu et al 2021; Goyat et al 2022).

5.4 Security and Attack Model

The simulation attack model considers existence of 15 percent stations or nodes under attack . Some of the attacks include injecting false data, tampering the data, replaying stale readings, unauthorized access attempts, malicious routing report and dropping of packets. The basic wireless sensor network is not capable of detecting compromised but authenticated nodes. The centralized way secure WSN possess enhancement in access control and logging at data base but suffers from insider alteration and central bottleneck. The use of a blockchain-enabled WSN records the identities of the nodes, accepted hashes, trust-score updates and anomaly flags in a distributed ledger making post-hoc manipulations increasingly difficult (Awan et al., 2022; Hsiao & Sung, 2021; Yaga et al., 2018).

5.5 Variables and Measurement

The kind of WSN security architecture is the independent variable. The dependent variables which were measured included data integrity score, tampering detection rate, packet delivery ratio, average latency, throughput, energy consumption, trust score, malicious node detection rate, service response time, transaction confirmation time, service efficiency index. We consider various control variables such as node density, malicious node percentage, packet size, area of network, simulation duration, and traffic model. The index for service efficiency was developed as a weighted

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

composite of packet delivery ratio, throughput, integrity score, trust score, latency and energy consumption. After taking security and network efficiency into account, the higher indices yield better service performance.

5.6 Statistical Analysis Methods

There is a mean, standard deviation, minimum and maximum values obtained with the help of descriptive statistics. The functioning of one-way ANOVA for architecturesand sphere metrics was verified next. The blockchain-enabled scenario and the conventional scenario differ in terms of significance and actual mean with a confidence of 95% as per the results from Welch t-tests.The Pearson correlation was used to measure various associations between integrity, trust, tampering detection, latency, throughput, and service efficiency.

The relationship between service efficiency and data integrity, trust score, packet delivery ratio, latency, throughput and energy consumption was estimated using multiple linear regression. A threshold of $p < .05$ was used. Very small p-values are reported as $p < .001$.Effect size for ANOVA was measured through eta squared.

VI. DATA ANALYSIS AND RESULTS

6.1 Profile of the Simulation Dataset

The produced dataset consists of 450 simulation observations; 150 observations for each architecture. In each of the scenario we will do 30 replications at each of the five node densities.

The design consequently permits interpretation at both the architectural level and the density control level. Due to the similarities in malicious node percentage, packet size, network area, and replication structure across all scenarios, we can conclude that the architectural assumptions, as well as stochastic variations owing to seed fixation simulation, are responsible for the results.

6.2 Summary of Descriptive Network Metrics

Table 2. Descriptive Statistics of Network Performance Metrics

Metric	Conventional Mean	Centralized Mean	Blockchain Mean	SD	Min	Max
Average latency (ms)	98.36	102.06	118.28	20.45	65.98	155.65
Packet delivery ratio (%)	85.30	90.03	93.02	4.10	78.37	97.35
Throughput (kbps)	157.70	167.74	159.06	9.62	139.03	187.14
Energy consumption (J/node)	0.62	0.67	0.77	0.15	0.41	1.04
Data integrity score (%)	70.47	84.21	93.88	9.80	63.68	96.52
Tampering detection rate (%)	55.26	76.36	92.03	15.28	48.00	96.14
Trust score (0-1)	0.54	0.72	0.86	0.13	0.46	0.92
Malicious node detection rate (%)	51.75	76.08	90.29	16.12	43.20	94.25
Replay attack prevention rate (%)	59.00	80.30	94.47	14.74	51.10	97.97
Unauthorized access prevention rate (%)	61.02	83.02	95.48	14.41	54.06	98.69
Transaction confirmation time	0.00	21.14	114.88	50.83	0.00	146.31

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

(ms)						
Service response time (ms)	266.44	248.10	278.09	26.07	197.74	335.71
Service efficiency index (0-100)	65.94	72.52	74.07	5.01	58.14	81.14

Note. Scenario columns report means. SD, minimum, and maximum are calculated across all 450 simulated observations for each metric.

Table 2 shows that the blockchain-enabled WSN achieved the strongest security-related averages, including data integrity, tampering detection, trust score, malicious node detection, replay prevention, and unauthorized access prevention. It also produced the highest packet delivery ratio. However, the same architecture recorded higher latency, energy consumption, and transaction confirmation time, indicating a measurable security-performance trade-off. This pattern is consistent with prior blockchain-IoT research showing that distributed validation can strengthen integrity while adding computational and communication overhead (Khan et al., 2022; Piao et al., 2023).

6.3 Comparative Architectural Performance

Table 3. Comparative Performance of Three WSN Architectures

Architecture	Latency (ms)	Throughput (kbps)	PDR (%)	Energy (J/node)	Transaction Time (ms)	Service Response (ms)	Service Efficiency
Blockchain-Enabled WSN	118.28	159.06	93.02	0.77	114.88	278.09	74.07
Centralized Secure WSN	102.06	167.74	90.03	0.67	21.14	248.10	72.52
Conventional WSN	98.36	157.70	85.30	0.62	0.00	266.44	65.94

Note. Values are scenario means from the reproducible simulation.

The comparative performance table indicates that the centralized secure WSN achieved the highest mean throughput and lowest service response time, reflecting the advantage of a lighter database-based security mechanism. The blockchain-enabled WSN achieved the highest packet delivery ratio and service efficiency index but required longer transaction confirmation time. The conventional WSN had the lowest security and packet delivery performance, which reduced its composite service efficiency despite lower ledger overhead.

6.4 Security Outcome Comparison

Table 4. Security Performance Results

Architecture	Data Integrity (%)	Tamper Detection (%)	Malicious Node Detection (%)	Trust Score	Replay Prevention (%)	Unauthorized Access Prevention (%)
Blockchain-Enabled WSN	93.88	92.03	90.29	0.86	94.47	95.48
Centralized Secure WSN	84.21	76.36	76.08	0.72	80.30	83.02
Conventional WSN	70.47	55.26	51.75	0.54	59.00	61.02

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

Note. Trust score is scaled from 0 to 1; all other security indicators are percentages.

Security results in Table 4 show that the blockchain-enabled architecture obtained a mean data integrity score of 93.88%, tampering detection of 92.03%, malicious node detection of 90.29%, and trust score of 0.86. These values are substantially above the conventional baseline and also above the centralized secure scenario. The results support RQ1 and RQ2 by showing that blockchain-enabled trust logging and integrity verification improve simulated security outcomes under malicious-node conditions.

6.5 ANOVA-Based Significance Testing

Table 5. ANOVA Test Results Across Three Architectures

Metric	F	p-value	Eta squared	Significant
Average latency (ms)	48.81	< .001	0.179	Yes
Packet delivery ratio (%)	339.94	< .001	0.603	Yes
Throughput (kbps)	60.82	< .001	0.214	Yes
Energy consumption (J/node)	53.45	< .001	0.193	Yes
Data integrity score (%)	5880.98	< .001	0.963	Yes
Tampering detection rate (%)	8549.47	< .001	0.975	Yes
Trust score (0-1)	5154.16	< .001	0.958	Yes
Malicious node detection rate (%)	9589.09	< .001	0.977	Yes
Transaction confirmation time (ms)	6503.87	< .001	0.967	Yes
Service response time (ms)	64.78	< .001	0.225	Yes
Service efficiency index (0-100)	219.68	< .001	0.496	Yes

Note. One-way ANOVA compares the three architectures. All listed effects are statistically significant at $p < .05$.

Table 5 shows statistically significant differences across the three architectures for all major metrics. The effect sizes are especially large for integrity, tampering detection, trust score, malicious node detection, transaction confirmation time, and service efficiency. The ANOVA results support RQ4 by indicating that architecture choice has a statistically meaningful effect on both security and service-performance metrics in the simulation.

6.6 Correlation Analysis

Table 6. Correlation Matrix

Metric	Data integrity score (%)	Trust score (0-1)	Tampering detection rate (%)	Average latency (ms)	Throughput (kbps)	Service efficiency index (0-100)
Data integrity score (%)	1.00	0.97	0.97	0.30	0.04	0.74
Trust score (0-1)	0.97	1.00	0.97	0.27	-0.02	0.76
Tampering detection rate (%)	0.97	0.97	1.00	0.35	0.07	0.69
Average latency	0.30	0.27	0.35	1.00	0.57	-0.36

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-38040

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

(ms)						
Throughput (kbps)	0.04	-0.02	0.07	0.57	1.00	-0.29
Service efficiency index (0-100)	0.74	0.76	0.69	-0.36	-0.29	1.00

Note. Pearson correlation coefficients. Positive values indicate that variables increase together; negative values indicate inverse association.

Figure 8. Heatmap of Correlation Matrix

Source: Author generated from reproducible simulation outputs and architecture design.

The correlation matrix shows strong positive associations among data integrity, trust score, tampering detection, and service efficiency. Latency has a negative correlation with service efficiency, which is expected because slower response reduces operational quality. The correlation pattern confirms that a secure e-governance WSN cannot be assessed by security metrics alone; network response and energy cost must also be included.

6.7 Regression Modelling of Service Efficiency

Table 7. Regression Results for Service Efficiency Index

Variable	Coefficient	Std Error	t	p	CI Lower	CI Upper
Constant	29.423	2.622	11.224	< .001	24.270	34.575
Data integrity score	0.197	0.023	8.706	< .001	0.153	0.242
Trust score	16.577	1.681	9.863	< .001	13.274	19.881
Packet delivery ratio	0.199	0.031	6.513	< .001	0.139	0.260
Latency	-0.091	0.008	-11.887	< .001	-0.106	-0.076
Throughput	0.077	0.007	11.706	< .001	0.064	0.089
Energy consumption	-10.376	1.099	-9.445	< .001	-12.535	-8.217

Note. Dependent variable: service efficiency index. Model R^2 = 0.960; adjusted R^2 = 0.959.

The regression model explains 96.0% of the variance in service efficiency. Data integrity, trust score, packet delivery ratio, and throughput have positive coefficients, while latency and energy consumption have negative coefficients. This confirms the conceptual expectation that service efficiency improves when secure data are delivered reliably and quickly, but declines when blockchain or network operations impose excessive delay and energy cost.

6.8 Graphical Results and Interpretation

Figure 3. Bar Chart Comparing Packet Delivery Ratio Across Architectures

Source: Author generated from reproducible simulation outputs and architecture design.

Figure 3 shows that blockchain-enabled WSN achieved the highest packet delivery ratio. The improvement is consistent with trust-filtered routing, which reduces the influence of nodes that drop or misreport packets. This outcome supports the view that trust management can improve routing reliability when integrated with secure identity and auditable behavior records (Awan et al., 2022; Xia et al., 2022).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, August 2026 Impact Factor: 8.2

Figure 4 shows that latency increases with node density across all scenarios. The blockchain-enabled WSN has the highest latency at each density because gateway transactions require hash preparation, endorsement, ordering, and validation. This trade-off is consistent with Hyperledger Fabric performance studies showing that endorsement and transaction processing affect latency (Hyperledger Fabric Documentation, n.d.-b; Piao et al., 2023).

Figure 5. Bar Chart Comparing Data Tampering Detection Rate

Source: Author generated from reproducible simulation outputs and architecture design.

Figure 5 demonstrates the largest security gain of the blockchain-enabled architecture. Tamper detection is strengthened because each accepted sensor record has an associated hash and validation event, and abnormal reports affect the node trust score. This does not prove that blockchain alone detects all tampering; instead, it shows that tamper-evident logging and smart-contract rules improve detection when combined with gateway validation.

Figure 6. Box Plot of Service Response Time Across Scenarios

Source: Author generated from reproducible simulation outputs and architecture design.

Figure 6 shows that centralized secure WSN has the lowest service response time because it avoids distributed transaction confirmation. Blockchain-enabled WSN has a broader response-time distribution, reflecting confirmation overhead. However, service response time alone does not capture governance quality; the blockchain scenario compensates through higher integrity, trust, and packet delivery scores.

Figure 7. Scatter Plot Showing Relationship Between Trust Score and Service Efficiency

Source: Author generated from reproducible simulation outputs and architecture design.

Figure 7 shows a positive relationship between trust score and service efficiency. Higher trust scores are generally associated with improved service efficiency because trustworthy routing and reliable sensor reporting reduce packet losses, rework, and decision uncertainty. This finding connects technical trust management with e-governance service quality.

Figure 9. Energy Consumption Comparison Chart

Source: Author generated from reproducible simulation outputs and architecture design.

Figure 9 confirms that blockchain-enabled WSN consumes more energy per node than the other scenarios. Although end nodes are not full blockchain validators, the architecture still creates additional costs through signing, hash verification, gateway interaction, and trust-message handling. Energy-aware consensus, edge batching, and adaptive transaction submission are therefore necessary for real-world deployment (Khan et al., 2022; Rathod et al., 2022).

Figure 10. Blockchain Transaction Confirmation Time Under Different Node Densities

Source: Author generated from reproducible simulation outputs and architecture design.

Figure 10 shows that transaction confirmation time increases as node density rises in the blockchain-enabled scenario. This trend is expected because more sensor readings create more gateway-submitted records and more validation work. The result suggests that public-service WSNs should use batching, off-chain storage, event prioritization, and lightweight endorsement rules rather than submitting every raw reading directly to the ledger.

VI. DISCUSSION

7.1 Impact of Blockchain on Data Integrity

The greatest finding is an improvement in data integrity. Through the integration of Block-Chain Technology, the paper will increase the mean data integrity score from 70.47% in the absence of Block Chain Technology to 93.88% in the presence of Block-Chain Technology. The Welch t-test of blockchain-enabled WSN and conventional WSN yielded a mean difference of 23.41 percentage points, 95% CI [22.97, 23.85], $p < .001$. The outcome of this RQ1 is probably in

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

line with previous studies that argue that blockchain can guarantee immutable data structures and stronger provenance of IoT and WSN data (Goyat et al., 2022; Hsiao and Sung, 2021; Yaga et al., 2018).

The key takeaway is not that blockchain guarantees the truth at the sensor source. A sensor that malfunctions is capable of giving false readings. The benefit comes from the ability of the design to make accepted readings linkable, to make alterations difficult after acceptance and to link suspect behaviour to auditable trust-score changes. In the e-governance, it matters as the veracity of the administrative records can later be examined by an auditor or other stakeholder.

7.2 Trust Management and Malicious Node Detection

The scenario of blockchain elaborated on trust management. The average score for trust was enhanced from 0.54 in the traditional WSN to 0.86 in the blockchain WSN. In addition, malicious node detection improved from 51.75% to 90.29%. The mean difference for the Welch t-test for trust score was 0.322, 95% CI [0.316, 0.328], $p < .001$. The results were similar to Awan et al. (2022) who focused on trust evaluation and routing mechanism using blockchain-based authentication of WSNs.

The institutional and technical aspect of trust management for e-governed. It assists routing in evading harmful nodes. At an institutional level, it explains why certain sensor data were accepted, downgraded, or flagged. A ledger-based trust history can help resolve disputes concerning issues like whether an agency didn't act on a warning from a sensor or whether a faulty node was producing unreliable evidence.

7.3 Service Efficiency Gains and Trade-offs

The WSN that uses blockchain attained the highest value of composite service efficiency index (CSEI) of 74.07 as compared to 72.52 for centralized secure WSN and 65.94 for conventional WSN The enhancement over the standard scenario amounted to 8.13 points, with a 95% confidence interval of [7.29, 8.98] and a p-value less than .001. It means that if the efficiency can include packet delivery, integrity, and trust, then the improvement in security can lead to improvement in efficiency too.

Nonetheless, the centralized secure wireless sensor network outperformed with greater mean throughput, and lower service response time. So, this implies, deploying blockchain just because it is techno-optimally fashionable or has some hype. In situations of multi-stakeholder governance, where values of auditability, non-repudiation, and tamper resistance justify moderate overhead, his case is strongest. This interpretation aligns with the literature on blockchain performance, which emphasizes the latencies, throughputs, and scalability limits of blockchain systems (Hyperledger Performance and Scale Working Group (2018); Piao et al. (2023)).

7.4 Cost and Latency of Blockchain Integration

The energy consumption and latency were high in blockchain-based architecture. The latency experienced an increase of 19.91 ms when compared to a conventional WSN, 95% CI [15.58, 24.25], $p < .001$. Similarly, the energy consumption increased 0.156 J/node, 95% CI [0.124, 0.187], $p < .001$. Such costs are expected because permissioned blockchain workflow necessitates transaction packaging, endorsement, ordering, validating and ledger update. Even when end nodes do not run as validators, gateways and similar trust mechanisms add communication and processing.

This finding is useful for designers. Emergency services and real-time control systems might not stand for any further delay. In such instances, blockchain should be employed for auditing metadata and verifying post-events, rather than every control-loop decision. For non-real-time governance activities such as service verification, compliance reporting, grievance proofing, and utility monitoring, the overhead may be acceptable when appropriate batching and edge processing are used.

7.5 Implications for Transparent E-Governance

The suggested framework proposes that transparent e-governance must create a chain of trust beginning from the sensor node to the administrative dashboard in a verifiable manner. There is no need for a citizen or an auditor to place

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

blind faith on a single server. Alternatively, authorized stakeholders can verify if a record hash, time stamp, node identity and trust status were indeed committed. This enhances the transparency of the procedure while protecting the raw data through off-chain storage. This design aligns with a greater focus in digital government of trustworthy, inclusive and accountable data systems (UN DESA, 2024).

7.6 Comparison with Previous Studies

The findings support blockchain-WSN efforts that demonstrate enhanced detection of malicious network actors, trust-aware routing, and data confidentiality. Hsiao and Sung (2021) highlighted blockchain technology as a way to strengthen the data security of WSN. Awan et al. (2022) predicted safe routing based authentication using blockchain. Ramasamy et al. (2021) regarded malicious node detection as a major blockchain-WSN research areas. The current paper adds to the existing literature by associating the various security enhancements with e-governance service efficiency and by conducting a comparison of blockchain-enabled WSN against both conventional and centralized secure benchmarks.

7.7 Practical Implications for Smart Cities and Public Administration

The researchers discovered that they offer smart city-manages insights regarding to use of blockchain-enabled WSN which areas most appropriate when any manipulation of data could damage public trust, violate legal/regulatory requirements, or interfere, whether to a minor or great degree, with financial allocation and/or allocation of other resources. Examples of uses include monitoring of water quality, environmental compliance, smart metering successful flood alert logging and public infrastructure verification. According to Goyat et al. (2022) and Khan et al. (2022), Edge Gateways, off-chain raw data storage, permitted Validators, and event-triggered Ledger submission should be used in this architecture to reduce overhead.

Even public agencies ought to define governance rules beforehand. Documentation is needed for all parts related to validator roles, authorisation, visibility of audit, procedures for smart-contract updates, policies for node replacements, and data retention. Complexity could increase without any enhancement of accountability, due to lack of governance.

7.8 Policy and Governance Impacts

Decision makers ought to consider blockchain incorporated WSN as an aspect of trust architecture. It must be aligned to the baselines for the cybersecurity of IoT devices, zero-trust principles, standards for purchase, and public governance of data. NIST's IoT baseline is about a device's capabilities that protect device data and ecosystems while NIST's zero-trust architecture is about the need for verification, rather than just trust (Fagan et al. 2020, Rose et al. 2020) Public sector sensor infrastructure can benefit from auditability of permissioned ledger.

VIII. CONCLUSION

The study evaluated a blockchain-enabled secure WSN architecture for transparent e-governance. A study of 450 observations using a reproducible simulation dataset were used to study conventional WSNs, centralized secure WSNs and blockchain-enabled WSNs situation. The scenario which is enabled by blockchain was found to be the most effective regarding security as it achieved the highest score for data integrity, tampering detection rate, trust score, malicious node detection rate, replay prevention rate, unauthorized access prevention rate, packet delivery ratio, and composite service efficiency index. The architecture-level differences are statistically significant for the core security and performance metrics.

Results verify the conclusion that blockchain-enabled WSN can improve e-governance transparency using a permissioned, edge-assisted, smart-contract-driven architecture. However, results also indicate that blockchain adds latency, energy, and transaction confirmation overhead. Asa result, blockchain should be exercised on audit-critical events, integrity metadata, trust-score updates, and governance record as against every raw sensor packet. The

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

integrated evaluation framework proposed in the paper connects data integrity, trust management, service efficiency and transparency in the public sector.

IX. LIMITATIONS

Limitations exist in the study. First, the data comes from a reproducible simulation and not from a field deployment. The results are valid in the assumptions stated and should not be considered as measurements from a real municipal WSN. Secondly, the simulation abstracts physical-layer behavior and does not model all environmental effects, such as interference, rain, terrain, battery aging, device diversity, or gateway failure. In addition, the validation logic guarantees permission and not a total Hyperledger Fabric test network is implemented in the Blockchain model. Moreover, the service efficiency index is a weighted composite; different public-service contexts may require different weights. In the fifth place, we include common WSN attacks in our attack model. However, we don't consider advanced attacks. For example, coordinated insider attacks by different validator organizations. Similarly, we also don't consider post-quantum cryptographic attacks.

X. FUTURE DIRECTIONS

Future implementations of the proposed architecture should be done in NS-3, Cooja/Contiki-NG, OMNeT++, or a physical WSN testbed integrated with Hyperledger Fabric and Hyperledger Caliper. The measurements of these work should real transaction throughput, endorsement latency, gateway CPU load, memory use, and battery drain. Subsequent iterations are suggested for examination of lightweight blockchain protocols, edge-AI anomaly detection, federated trust management, adaptive block sizes, event-priority submission, and energy-aware consensus. In addition, post-quantum security is another emerging area because long-lived public-sector infrastructure may need to be cryptographically resilient against future threats.

Additional research may also look at governance and policy issues. Validator peers should be operated by whom, citizens should access audit proofs how and data privacy should be preserved how, smart-contract rules should be updated how when public policy changes and why. By performing a combined technical and administrative evaluation, it will judge whether a blockchain-enabled WSN step further from a promising security design to a reliable component of transparent digital government.

XI. DATA AVAILABILITY AND REPLICATION STATEMENT

This paper presents quantitative results based on a reproducible simulation with random seed 20260621. The dataset has 450 observations consisting of three architectures, five node densities, and 30 replications per density-scenario pair. The simulation employs clearly defined parameters, attack hypotheses, and measurement variables. The outcomes are not asserted to be measurements from the real world. The code used for simulation and the generated CSV dataset could be sent along with the journal or conference.

REFERENCES

1. Abd El-Moghith, I. A., & Darwish, S. M. (2021). Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach. IEEE Access, 9, 103822-103834. https://doi.org/10.1109/ACCESS.2021.3098933
2. Almarri, S. (2024). Blockchain technology for IoT security and trust. Sustainability, 16(23), 10177. https://doi.org/10.3390/su162310177
3. Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J.-G. (2022). Blockchain based secure routing and trust management in wireless sensor networks. Sensors, 22(2), 411. https://doi.org/10.3390/s22020411
4. Da Xu, L., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473. https://doi.org/10.1109/JIOT.2021.3060508

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

5. Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076-8094. https://doi.org/10.1109/JIOT.2019.2920987
6. Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). IoT device cybersecurity capability core baseline (NISTIR 8259A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259A
7. Gharavi, H., et al. (2024). Post-quantum blockchain security for the Internet of Things. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2024.3355222
8. Goyat, R., Kumar, G., Alazab, M., Conti, M., Rai, M. K., Thomas, R., Saha, R., & Kim, T. H. (2022). Blockchain-based data storage with privacy and authentication in Internet of Things. IEEE Internet of Things Journal, 9(16), 14203-14215. https://doi.org/10.1109/JIOT.2020.3019074
9. Hsiao, S.-J., & Sung, W.-T. (2021). Employing blockchain technology to strengthen security of wireless sensor networks. IEEE Access, 9, 72326-72341. https://doi.org/10.1109/ACCESS.2021.3079708
10. Hyperledger Caliper. (n.d.). Introduction. Retrieved June 21, 2026, from https://hyperledger-caliper.github.io/caliper/
11. Hyperledger Fabric Documentation. (n.d.-a). Smart contracts and chaincode. Retrieved June 21, 2026, from https://hyperledger-fabric.readthedocs.io/en/latest/smartcontract/smartcontract.html
12. Hyperledger Fabric Documentation. (n.d.-b). Transaction flow. Retrieved June 21, 2026, from https://hyperledger-fabric.readthedocs.io/en/release-2.2/txflow.html
13. Hyperledger Performance and Scale Working Group. (2018). Blockchain performance metrics white paper. Linux Foundation. https://www.lfdecentralizedtrust.org/learn/publications/blockchain-performance-metrics
14. Khan, A. A., Laghari, A. A., Shaikh, Z. A., Dacko-Pikiewicz, Z., & Kot, S. (2022). Internet of Things (IoT) security with blockchain technology: A state-of-the-art review. IEEE Access, 10, 122679-122695. https://doi.org/10.1109/ACCESS.2022.3223370
15. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411. https://doi.org/10.1016/j.future.2017.11.022
16. Omar, Y. A. (2024). Blockchain-enabled data integrity in wireless sensor networks. International Journal of Wireless and Microwave Technologies, 14(6), 15-25. https://doi.org/10.5815/ijwmt.2024.06.02
17. Piao, X., Ding, H., & Song, H. (2023). Performance analysis of endorsement in Hyperledger Fabric concerning endorsement policies. Electronics, 12(20), 4322. https://doi.org/10.3390/electronics12204322
18. Ramasamy, L. K., Khan K. P., F., Imoize, A. L., Ogbebor, J. O., Kadry, S., & Rho, S. (2021). Blockchain-based wireless sensor networks for malicious node detection: A survey. IEEE Access, 9, 128765-128785. https://doi.org/10.1109/ACCESS.2021.3111923
19. Rathod, T., Jadav, N. K., Alshehri, M. D., Tanwar, S., Sharma, R., Felseghi, R.-A., & Raboaca, M. S. (2022). Blockchain for future wireless networks: A decade survey. Sensors, 22(11), 4182. https://doi.org/10.3390/s22114182
20. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
21. United Nations Department of Economic and Social Affairs. (2024). United Nations E-Government Survey 2024: Accelerating digital transformation for sustainable development. United Nations. https://desapublications.un.org/
22. Xia, Z., Wei, Z., & Zhang, H. (2022). Review on security issues and applications of trust mechanism in wireless sensor networks. Computational Intelligence and Neuroscience, 2022, 3449428. https://doi.org/10.1155/2022/3449428
23. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview (NISTIR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

Appendix A. Simulation Replication Note

The simulation used a fixed seed and scenario-specific equations for latency, packet delivery, throughput, energy, integrity, tamper detection, trust, malicious node detection, transaction confirmation, and service response. Random error terms were sampled from normal distributions with metric-specific standard deviations. Values were clamped to physically meaningful ranges such as 0-100% for rates and 0-1 for trust score. The service efficiency index combined packet delivery, throughput, integrity, trust, latency, and energy after normalization. This appendix is included to make clear that the reported numerical results are reproducible simulation outputs, not invented field observations.