International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain-Based Security Framework for Internet of Things in Smart Cities

Dr. Jyoti G

Submitted:05/05/2023 **Revised:**18/06/2024 **Accepted:**27/06/2024

Abstract: This paper examines a blockchain-based security framework of Internet of Things (IoT) in smart cities, resolving vital challenges of data integrity, privacy, scalability and trust. The aim is to examine how blockchain dynamics, combined with AI, software-defined networks and federated learning, have the potential to protect IoT-based municipal systems. A secondary research approach was implemented using peer-reviewed investigations and the IEEE to summarize evidence in several frameworks. This methodology was cost-efficient and helped to have the holistic picture of the role of blockchain without conducting primary data. The results indicate that decentralised blockchain regimes enhance up to 97% in accuracy in detecting anomalies, 45% risks in of denial-of-service, and even 92% on stakeholder trust. The use of smart contracts shores up transparency in governance, whereas federated learning protects privacy in distributed IoT environments. In general, the study finds that blockchain provides a scalable, robust, and transparent base on which to build security around smart city environments and add sustainable, trusted digital transformation.

Keywords: *Blockchain, IoT, Smart cities / Smart city, Security, Framework, Trust, Data, Privacy, Authentication, Decentralized*

Introduction

The rapid growth of the Internet of Things (IoT) has developed has revolutionized smart cities in managing energy successfully, in smart transport, health care monitoring, and in the management of public safety. However, this huge linking of devices results in security, privacy, and trust-related issues that are not easy to resolve using centralized solutions. The blockchain can be a great way of improving IoT security through greater transparency and immutability of data, provenance, and authentication, which does not hinge on third parties. A blockchain-powered security framework would help eliminate the potential risk of cyberattacks, authorization and manipulation of information in smart city systems. This strategy offers scale, trust and robustness, thus being a potential model of safeguarding sensitive information and increasing trust between stakeholders in the urban ecosystem in contemporary cities.

Associate Professor in Electronics
Government Science College
Nrupathunga University,
N. T. Road, Bangalore-560001
Karnataka, India.

Objectives

- To Analyse the decentralised security framework for IoT in smart cities
- To ensure data integrity, authentication, and privacy using blockchain mechanisms.
- To evaluate the framework's scalability, reliability, and resistance to cyber threats.
- To enhance trust and secure data sharing among smart city stakeholders.

Literature Review

Kumar et al. (2021) present an IoT-based smart city that embeds blockchain and machine learning and is privacy-preserving and secure through PPSF. Decentralization, immutability, and auditability addresses spoofing, tampering and the possibility of single-point-of-failure on heterogeneous devices. Federated learning with encrypted model updates provides collaborative learning in which no raw data

is shared. Members of the framework are lightweight consensus, tokenized permissions, and access control lists to authenticate devices and control data flows. Edge-cloud coordination allows reducing latency and retaining privacy because of the difference in privacy. Experiments encourage resiliency to attacks in inference and poisoning, delivery scheduling of essential services and availability.

Islam et al. (2021) propose a Blockchain-SDN that maintains coordinated energy-aware routing plus security enforcement, besides distributed trust, solutions in a smart-city IoT. Blockchain-based SDN controllers provide an immutable audit trail of logs, identities, and access privileges, whereas blockchain provides tamper-resistant logging, identities, access privileges. This solution addresses the scope of denial-of-service containment, key management and topology agility in an environment with volatile traffic. The admission control and resource allocation is ensured through smart contracts and consensus to save energy across limited nodes. Inter-domain cooperation can lessen closed down operations and amplify confidentiality, integrity of data, and availability. Evaluations focus on lowered overhead and resilience and the use of control-plane intelligence and ledger-backed assurance.

Asif et al. (2022) propose an authentication and trust mechanism that is based on blockchains and can be applied to the smart-city environment. The scheme pairs device identities with historical credential anchors in a ledger and derives trust based on prior transactions, and propagates the reputations to block malign actors. Smart contracts are used to automate recording, de-allocations, and review of policies without having centralized control. The design focuses on lightweight cryptography on limited sensors and components to applications in mobility and utilities. Local verification keeps the handshake costs down and guarantees to prevent Sybil and spoofing attacks. It takes less time to accomplish onboarding, trust updates, and is resilient to collusion and compromise attacks.

Ahmed et al. (2022) introduce a blockchain- and AI-driven intelligent IoT framework of sustainable cities, which puts secure data governance and predictive intelligence in alignment. Blockchain provides provenance, consent tracking, and fine-grained access control and AI models are used to optimize energy consumption, mobility, and maintenance on the edge. The architecture enhances federated analytics, privacy preservation and domain environment interoperability to decrease silos. Smart contracts facilitate coordination across stakeholders on incentivization, enforcement and compliances. Edge orchestration and model lifecycle management would allow learning with the varying workloads. Demonstrations point to decision pipelines that support a balance between explainability, performance, and protection of both services and citizen data.

El Bekkali et al. (2023) present blockchain-based architecture to design cybersecure smart cities in their layer-wise drilling efforts concerning sensing, networking, platforms, and applications. The identification and authentication is part of the framework, which is secure onboarding, segmentation, and monitoring, and ledgers are used to ensure integrity, non-repudiation, and policy audit. Microservices publish interfaces which are controlled by smart contracts to enforce least privilege and automate compliance. Risk modeling and threat intelligence direct the controls throughout the domains, and interoperability covers the legacy systems. The focus of operational guidance is on governance, data stewardship, and incident response toward resilience. Case analyses present deployments considerations, performance trade-offs, and migration strategies by municipalities on the path digital transformation.

Padma and Ramaiah (2024) build an upper-level privacy-guaranteed blockchain framework of smart cities in which lightweight operations are prioritised. The consensus takes the form of a narrow cryptographic primitive over an optimized consensus instance and a judicious selection on-chain storage to reduce computation and bandwidth on limited devices. Confidentiality is ensured through attribute-based access control, anonymization and secure aggregation that ensures verifiability. The use of smart contracts ensures little overhead in device lifecycle-management, consent and policy enforcement. Off-chain channels are used for bulk telemetry and edge processing reduces the latency of time sensitive services. Results show lower energy consumption, shorter authorization and resistant to replay, linkage and eavesdropping than traditional security thresholds.

Methodology

This paper has used a secondary research methodology that considers a secure blockchain-based framework model to IoT in smart cities. Primary information is extracted through peer-reviewed journals, IEEE publications, and case studies, and therefore, credible information about security, scalability, and trust mechanisms can be found. The application of secondary sources has multiple advantages that the availability of large-range empirical results, affordability, and time-saving. It allows making comparisons among different frameworks, technologies, and urban applications without a need to ensure the primary data collection data. Furthermore, the secondary analysis will make it possible to critique the existing models, e.g., blockchain-SDN, federated learning, AI integration. The approach makes research more robust by summarizing evidence-based findings, establishing knowledge gaps, and offers an in-depth understanding of how blockchain can be used in the security of the smart IoT ecosystems.

Result and Discussion

Decentralized Blockchain Framework Enhances Security in Smart City IoT Systems

The decentralized blockchain frameworks can solve this challenge by eliminating the single points of the failure and result in a resilient IoT security in smart cities. Khan et al. (2024) define how the combination of blockchain with AI enhances anomaly detection in the ecosystem of tens of thousands of interconnected sensors by securing the data provenance. Rani et al. (2022) state the importance of the blockchain in combination with software-defined networks (SDN) to achieve dynamic routing security, which would lower the chances of a denial-of-service attack by 45%. Bommu et al. (2023) present the evidence of routing protocols based on blockchain improving the packet delivery ratio by 18 pct within the large-scale and urban IoT systems.

Technology/Study	Devices/Nodes Tested	Security Improvement (%)	Availability (%)	Key Feature
Khan et al. (2024)	10,000 sensors	+40% anomaly detection	98.5	AI–Blockchain provenance
Rani et al. (2022)	8,000 SDN devices	45% DoS risk reduction	97.2	Blockchain-SDN routing
Bommu et al. (2023)	5,000 IoT nodes	18% higher packet ratio	96.1	Blockchain routing
Siddiqui et al. (2023)	12 city services	38% attack resistance	99.2	Smart contract governance

Table 1: Decentralized Blockchain Framework Enhances Security

Smart contract governance over municipal services like waste management and traffic management (Siddiqui et al., 2023) has shown 99.2 percent availability of their services. These decentralised trust on different nodes fosters security of the trust because the trust cannot be faked; consensus mechanisms achieve this, such as the use of Proof-of-Authority (PoA) or Byzantine Fault Tolerance. Ahmad et al. (2024) describe blockchain queues optimized according to secure supply chains, and dilute reduced latency by 22% applied to the logistics application. This is evidence to the fact that blockchain can decentralize security and build immutable foundations of trust in smart city IoT infrastructures to ensure reliable protection against tampering, replay, and insider threats.

Improved Data Integrity, Authentication, and Privacy through Blockchain Mechanisms

In smart cities, blockchain mechanisms enhances data security as far as integrity, authentication, and privacy are concerned. According to Khan et al. (2024) the blockchain-enabling of AI models indicates 97 percent accuracy in the detection of anomalies and immutable logs of the IoT devices of healthcare applications. In Siddiqui et al. (2023), authentication by smart contracts is introduced, according to which 5,000 access requests per day are authenticated by the municipal services themselves, with no central servers and without any risk of identity spoofing. Rani et al. (2022) describe an SDN-blockchain solution in which identity

authentication enhanced system integrity by 40 percent without incurring a high computational load.

Technology/Study	Requests/Nodes	Integrity Gain (%)	Unauthorized Access Reduction (%)	Privacy Technique
Khan et al. (2024)	10,000 healthcare IoT	97% anomaly accuracy	32%	Immutable blockchain logs
Siddiqui et al. (2023)	5,000 access requests	42% authentication speed	30%	Smart contracts authentication
Rani et al. (2022)	6,500 IoT devices	40% system integrity	28%	SDN + blockchain identities
Sefati et al. (2024)	15,000 IoT nodes	35% privacy retention	33%	Federated learning + blockchai

Table 2: Improved Data Integrity, Authentication, and Privacy

By uniting federated learning and blockchain, Sefati et al. (2024) show how to train 15,000 host IoT nodes under GDPR by not sharing the raw data, and demonstrate that the privacy-preserved training provides a comparable performance level. Bommu et al. (2023) confirm that the unauthorized network intrusion of nodes is decreased by 35 percent as established by blockchain-based device attestation within IoT-enabled traffic networks. The findings of Ahmad et al. (2024) show that they are more transparent than current supply chain exchanges of information where the chance of avoiding data manipulation can be reduced by 30%. Encryption schemes, Merkle proofs, smart contracts, and zero-knowledge proofs all provide trusted access, and the latest advances in authentication support privacy, through zero-knowledge proofs. The results confirm the ability of blockchain to provide end-to-end trust, imperturbable data transmissions, and data breach-resiliency in smart city solutions.

Scalability and Reliability Achieved with Resistance to Cyber Threats

In smart cities, blockchain frameworks improve scaling and reliability and are resilient to a wide range of cyberattacks. According to Khan et al. (2024), the blockchain AI synergy can allow real-time security orchestration across the networks at the scale of 100, 000 devices. Rani et al. (2022) reveal that blockchain-SDN integration manages the capacity of the network, with a throughput boost of 38 percent, strengthening resistance to DDoS and routing attacks. In Sefati et al. (2024), federated learning with blockchain creates scalability through secure training of distributed IoT nodes with a latency that is capped at 50 ms. In the case study put forth by Bommu et al. (2023), a blockchain-based routing mechanism saw a 28% reduction in packet loss which enhances the reliability of services in terms of traffic management.

Technology/Study	Network Size	Throughput (TPS)	Latency (ms)	Reliability (%)
Khan et al. (2024)	100,000 IoT devices	1,050 TPS	45	96.8
Rani et al. (2022)	50,000 SDN nodes	+38% throughput	52	95.3
Sefati et al. (2024)	15,000 IoT nodes	870 TPS	<50	97.1
Bommu et al. (2023)	8,500 traffic IoT	+28% packet stability	48	94.7

Table 3: Scalability and Reliability Achieved with Resistance to Cyber Threats

Ahmad et al. (2024) verify the idea that supply chain frameworks empowered by blockchain technologies are capable of supporting the transaction rates of over 1,200 TPS, in a stable manner. According to Siddiqui et al. (2023), enhancing blockchain networks through municipal blockchain-based networks does more thanconduct a joint service as the fault tolerance rate outweighs above 95 percent, or avoids manipulation by the insider. The consensus mechanism used in Elastos, Proof-of-Stake (PoS) and Delegated Byzantine Fault Tolerance (dBFT), reduces computational overhead, and still maintains attack resistance. Results substantiate that blockchain offers scalable security

and resilience standards to important systems such as health care, energy use, and intelligent transportation in smart cities.

Enhanced Trust and Secure Data Sharing among Smart City Stakeholders

Blockchain can provide improved trust in sharing and secure data across the various smart city stakeholders. Khan et al. (2024) indicate that hyper-certainty of decisions (2.7x) using AI-blockchain integration in the exchange of data between hospitals and transport networks has reduced false reporting by 33%. Siddiqui et al. (2023) show the examples of smart contracts that can govern municipal partnerships, with no central authorities with fair sharing of services among 12 departments. Rani et al. (2022) allude that blockchain-SDN integration supports transparency and integrity in multi-stakeholder applications of the IoT to gain a stakeholder trust rating of 92% in simulations. Sefati et al. (2024) corroborate the fact that federated learning and blockchain guarantee model training collaboration and increases trustworthiness without exposing sensitive datasets. According to the study by Bommu et al. (2023), distributed trust management offered by blockchain has the potential to minimize the effect of malicious nodes in IoT city networks by 40 percent.

Technology/Study	Stakeholders Covered	Trust Improvement (%)	Counterfeit/Data Manipulation Reduction (%)	Key Mechanism
Khan et al. (2024)	Healthcare + Transit	+33% trust in decisions	29%	AI–Blockchain exchange validation
Siddiqui et al. (2023)	12 city departments	36% governance trust	31%	Smart contracts for collaboration
Rani et al. (2022)	Multi-IoT domains	92% stakeholder trust	27%	Blockchain–SDN transparency
Ahmad et al. (2024)	Supply chain networks	25% counterfeit drop	25%	Auditable blockchain tracking

Table 4: Enhanced Trust and Secure Data Sharing

The blockchain platform model ensures the consumers and manufacturers are certain of their security by allowing them to track their products and not risking counterfeits given that there is a 25% reduction in counterfeits due to blockchain. This is validated by Ahmad et al. (2024). Distributed ledgers, immutable logs, and reputation scores enhance accountability and trust, across services in the urban system. These results support that blockchain is able to harmonise heterogeneous stakeholders through various modes of secure, transparent and auditable sharing of information, leading to more intelligent and collaborative city ecologies.

Conclusion

The paper ends with the conclusion that blockchain-powered models can make IoT-based smart cities notably more secure and efficient. Blockchain can decentralize a system of control and remove single points of failure, which guarantees integrity, authentication, and privacy of various elements of a density infrastructure. The testimonies available today concerning the results of contemporary research characterize the level of feasibility of blockchain to address large-scale IoT implementation, withstand malicious attacks, and achieve low latency rates without compromising the achievement of collaboration among stakeholders. The use of smart contracts, federated learning, and AI also enhances transparency, trust, and energy-efficient municipal services, healthcare, transportation, and supply chains. All in all, blockchain proves to be a reliable platform to restore smart city infrastructures, guarantee long-term development, and instill confidence in citizens in the digitalization process.

References

[1] Ahmad, A.Y.A.B., Verma, N., Sarhan, N.M., Awwad, E.M., Arora, A. and Nyangaresi, V.O., 2024. An IoT and blockchain-based secure and transparent supply chain management framework in smart cities using optimal queue model. *IEEE Access*, *12*, pp.51752-51771.

[2] Ahmed, I., Zhang, Y., Jeon, G., Lin, W., Khosravi, M.R. and Qi, L., 2022. A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city. *International Journal of Intelligent Systems*, *37*(9), pp.6493-6507.

[3] Asif, M., Aziz, Z., Bin Ahmad, M., Khalid, A., Waris, H.A. and Gilani, A., 2022. Blockchain-based authentication and trust management mechanism for smart cities. *Sensors*, *22*(7), p.2604.

[4] Bommu, S., M, A.K., Babburu, K., N, S., Thalluri, L.N., G, V.G., Gopalan, A., Mallapati, P.K., Guha, K., Mohammad, H.R. and S, S.K., 2023. Smart city IoT system network level routing analysis and blockchain security based implementation. *Journal of Electrical Engineering & Technology*, *18*(2), pp.1351-1368.

[5] El Bekkali, A., Essaaidi, M. and Boulmalf, M., 2023. A blockchain-based architecture and framework for cybersecure smart cities. *IEEE Access*, *11*, pp.76359-76370.

[6] Islam, M.J., Rahman, A., Kabir, S., Karim, M.R., Acharjee, U.K., Nasir, M.K., Band, S.S., Sookhak, M. and Wu, S., 2021. Blockchain-SDN-based energy-aware and distributed secure architecture for IoT in smart cities. *IEEE Internet of Things Journal*, *9*(5), pp.3850-3864.

[7] Khan, B.U.I., Goh, K.W., Khan, A.R., Zuhairi, M.F. and Chaimanee, M., 2024. Integrating AI and Blockchain for Enhanced Data Security in IoT-Driven Smart Cities. *Processes*, *12*(9).

[8] Kumar, P., Kumar, R., Srivastava, G., Gupta, G.P., Tripathi, R., Gadekallu, T.R. and Xiong, N.N., 2021. PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. *IEEE Transactions on Network Science and Engineering*, *8*(3), pp.2326-2341.

[9] Padma, A. and Ramaiah, M., 2024. Blockchain based an efficient and secure privacy preserved framework for smart cities. *IEEE Access*, *12*, pp.21985-22002.

[10] Rani, S., Babbar, H., Srivastava, G., Gadekallu, T.R. and Dhiman, G., 2022. Security framework for internet-of-things-based software-defined networks using blockchain. *IEEE Internet of Things Journal*, *10*(7), pp.6074-6081.

[11] Sefati, S.S., Craciunescu, R., Arasteh, B., Halunga, S., Fratu, O. and Tal, I., 2024. Cybersecurity in a scalable smart city framework using blockchain and federated learning for internet of things (iot). *Smart Cities*, *7*(5), pp.2802-2841.

[12] Siddiqui, S., Hameed, S., Shah, S.A., Khan, A.K. and Aneiba, A., 2023. Smart contract-based security architecture for collaborative services in municipal smart cities. *Journal of Systems Architecture*, *135*, p.102802.