



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: V Month of publication: May 2026

DOI: <https://doi.org/10.22214/ijraset.2026.82472>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

MBCSD-IoT: A Survey on Multi-Level Blockchain-Assisted SDN-Based IoT Architecture for a Secure and Scalable E-Voting System

Hemalatha K, Druti N, Chandana JP, Akash Gowda, Srushti J

Dept. of CSE Saphthagiri College of Engineering

Abstract: Contemporary democratic institutions are confronting unprecedented demands for electoral systems that simultaneously guarantee security, transparency, and the capacity to accommodate millions of geographically distributed voters. Conventional paper-based balloting and first-generation electronic voting machines remain susceptible to physical tampering, central threats. Centralised server-based e-voting platforms introduced a further liability: a single compromised node can silently alter outcome-critical records, and the absence of an immutable audit trail renders post-election forensic analysis of centralised architectural failures, and cyber intrusion, none of which are adequately addressed by existing incremental improvements. This survey investigates MBCSD-IoT, a four-tier hierarchical architecture that fuses Blockchain, Software Defined Networking (SDN), and Internet of Things (IoT) infrastructure into a unified, tamper-resistant e-voting framework. The proposed design integrates three independently mature technologies now offering the constituent elements of a fundamentally different design. Blockchain provides a distributed, append-only ledger whose cryptographic linkage between blocks makes retrospective data partitioning for electoral processing across Booth, District, State, and Country levels, wherein each ascending tier appends traceable metadata to a cryptographically protected data packet. Voter identity and device legitimacy are established through Elliptic Curve Cryptography (ECC) and biometric verification, while SHA3-256 hashing provides per-hop integrity assurance. SDN-Networking separates the forwarding plane from the control plane, enabling a logically centralised controller to install optimal forwarding rules across heterogeneous switches, thereby reducing latency and enabling real-time traffic policy enforcement based on flow management at every tier, eliminating per-packet routing overhead and enabling programmable DDoS mitigation. The survey reviews eleven representative prior works, characterises the research gap they collectively expose, and demonstrates through experimental evaluation that MBCSD-IoT achieves a 51.7% gain in throughput, an 81.2% reduction in latency, and voter-facing EVMs, biometric scanners, and relay nodes — through which physical electoral intent is captured, encoded, and propagated. None of these three technologies, deployed in isolation, is sufficient for a production-grade e-voting system; an 83.2% decrease in packet loss relative to conventional IoT integration, however, addresses each other's residual based voting deployment weaknesses.

Index Terms—Blockchain, Software Defined Networking, Internet of Things, E-Voting, Elliptic Curve Cryptography, SHA3-256, Biometric Authentication, MBCSD-IoT, MQTT, Distributed Architecture

I. INTRODUCTION

The MBCSD-IoT framework examined in this survey is precisely such an integration. The architecture imposes a four-level hierarchy—Booth, District, State, and Country—that mirrors the administrative partitioning of large-scale democratic elections. Votes originate at booth-level IoT nodes equipped with ECC encryption and biometric authentication. Democratic governance at scale demands electoral infrastructure, traverse SDN-managed inter-level links, and a structure that is simultaneously resistant to manipulation, in-recorded on blockchain instances maintained at each ascending dependently verifiable, and capable of processing million-tier. The country-level blockchain serves as the final, authoritative repository of concurrent transactions without performance degradation. Aggregate repository from which automated vote counting Paper ballots and first-generation electronic voting machines is executed, eliminating human intervention in the tabulation (EVMs) addressed the need for mechanised counting, yet phase.

Neither design incorporate the cryptographic guarantees or. The remainder of this paper is organised as follows. Section II supplies background on the three foundational technologies—RSA for equivalent security. A 256-bit ECC key provides the cryptographic components. Section III presents security comparable to a 3072-bit RSA key, a reduction in the literature survey. Section IV articulates the research gap that is particularly consequential for resource-constrained IoT motivating this work. Section V details the MBCSD-IoT endpoints where key generation and decryption operations methodology. Section VI analyses the security properties of the compete with real-time sensing and transmission tasks. In architecture. Section VII presents experimental results. Sec-MBCSD-IoT, ECC is employed for both device authentication. Section VIII discusses implementation considerations. Section IX—where each EVM presents an ECC-encrypted proof of its conclusion concludes the paper.

II. BACKGROUND AND FOUNDATIONAL TECHNOLOGIES

A. Blockchain Technology

A blockchain is a peer-to-peer distributed ledger in which data is organised into sequentially numbered blocks, each containing a cryptographic hash of its predecessor, a Merkle root over its transaction set, and a timestamp. The hash chain ensures that any retroactive modification to a committed block invalidates every subsequent block, making undetected tampering computationally infeasible on a sufficiently decentralised network. Consensus algorithms—whether proof-of-work, proof-of-stake, or Byzantine fault-tolerant variants—ensure that all participating nodes converge on a single canonical chain state without requiring a central arbitrator.

B. Software Defined Networking for IoT

A Software Defined Networking architecture partitions the and ballot submission are handled through cryptographically network into three interacting planes. The infrastructure plane signed transactions, and the immutable ledger prevents post-consists of forwarding devices—physical or virtual switch submission modification of any cast vote. that execute flow rules installed by an external controller Limitation: The architecture does not incorporate any network via the OpenFlow protocol. The control plane comprises one management layer. Under high concurrent submission rates, or more SDN controller that maintain a global topology view, the absence of SDN-driven flow control leads to congestion compute optimal forwarding paths, and push updated rules to the validation nodes, and the single-tier deployment does the data plane in response to changing traffic conditions. Then not reflect the hierarchical administrative structure of national application plane hosts network services—load balancing, elections.

ful advantages over conventional self-configuring IoT stacks. Centralised topology awareness allows the controller to detect and mitigate anomalous traffic patterns—such as those characteristic of DDoS flooding—by installing drop rules at the ingress point rather than allowing malicious traffic to propagate. Programmable flow management also reduces the per-packet processing overhead inherent in traditional IoT routing protocols, lowering end-to-end latency under load.

C. ECC and SHA3-256 Cryptographic Primitives

Elliptic Curve Cryptography achieves asymmetric encryption, anonymity, double vote prevention, and hierarchical result finality at key lengths substantially shorter than those required aggregation are not addressed. hardware identity—and for voted data encryption during inter-level transmission.

SHA3-256 is a member of the Keccak hash family standardised by NIST. Its sponge construction distinguishes it from the Merkle-Damgård structure underlying SHA-2, conferring resistance to length-extension attacks. Applied at every communication hop in the MBCSD-IoT chain, a SHA3-256 digest over the vote payload allows the receiving node to detect any in-transit modification before committing the record to its local blockchain.

III. LITERATURE SURVEY

This section reviews eleven representative prior works across the domains of blockchain-secured e-voting, SDN-Forelector applications, these properties translate into based IoT security, multi-tier distributed architectures, and three concrete guarantees. First, each vote, once committed related enabling technologies. A comparative summary is to the ledger, cannot be silently altered by any single party. presented in Table I.

Second, smart contracts can encode validation and counting logic whose execution is deterministic and publicly auditable. Third, the decentralised replication model eliminates any single point of failure that an adversary could exploit to suppress or inflate a vote tally.

A. Alvieta et al. (2022) – DVTChain: Blockchain-Based Secure Digital Voting System

Methodology: The authors construct a decentralised voting platform in which each ballot is recorded as a smart-contract transaction on a permissioned blockchain. Voter registration, firewall policies, QoS enforcement—that express their requirements to the control plane through northbound APIs. When applied to IoT deployments, SDN yields meaning-

B. Latif et al. (2022) – AI-Empowered Blockchain and SDN Security for IoT

Methodology: An integrated framework couples a blockchain audit trail with SDN-based anomaly detection driven by machine learning classifiers. The ML component flags statistically anomalous traffic flows, whereupon the SDN controller installs mitigation rules, and all security-relevant events are appended to the blockchain for forensic replay.

Limitation: The work is scoped entirely to generic IoT security monitoring and is not designed or evaluated in an electoral context. Vote-specific requirements such as voter

C. Sharma et al. (2022) – Blockchain-Based E-Voting with

Methodology: A distributed ledger design employs zero-knowledge-inspired anonymisation of voter identities so that the public ledger encodes the vote count without exposing any link between a specific voter and their ballot choice. Integrity of the tally is maintained through cryptographic commitment schemes.

Limitation: The paper does not report any experimental performance evaluation, making it impossible to assess throughput or latency behaviour under realistic election-scale loads. Network infrastructure considerations and multi-level result propagation are also outside the scope of the work.

D. Kumar et al. (2022) – Secure IoT-Based Voting with Biometric Authentication

Methodology: IoT-connected voting terminals are paired with fingerprint and facial recognition modules to authenticate voters prior to ballot submission. Voter credentials are verified against a centralised server, and votes are transmitted over an encrypted channel to a backend database.

Limitation: The centralised server architecture recreates the single-point-of-failure vulnerability that motivates decentralised designs. An adversary who compromises the central verification server can deny authentication to legitimate voters or inject fraudulent entries, undermining the security guarantees the biometric layer is intended to provide.

E. Khedr et al. (2023) – FMDADM: Multi-Layer DDoS Detection in SDN-IoT Networks

Methodology: A five-tier SDN-IoT topology is instrumented with machine learning modules that classify incoming flows as benign or attack traffic. Suspected DDoS flows are quarantined at the SDN controller, and experimental results show detection accuracy superior to prior threshold-based approaches across multiple attack scenarios.

Limitation: The framework is exclusively a network security construct and does not incorporate a blockchain persistence layer. Consequently, there is no immutable record of security events, and the system provides no direct support for electoral workflows such as vote recording or result aggregation.

F. Aldossary (2023) – Multi-Layer Fog-Cloud Architecture for IoT Application Placement

Methodology: A mixed-integer linear programme determines the optimal placement of IoT application instances across fog nodes and cloud servers to minimise end-to-end latency and communication cost. The formulation considers

G. Turner et al. (2023) – Survey of Blockchain-SDN Integration for Voter Privacy

Methodology: A comprehensive taxonomy classifies existing blockchain-SDN integration approaches into three modes: integrated (blockchain embedded within the SDN controller), collaborative (blockchain and SDN as peer entities exchanging events), and overlay (blockchain operating independently atop the SDN substrate). The survey analyses the trade-offs of each mode with respect to latency, decentralisation, and implementation complexity.

Limitation: As a survey, the work does not propose or evaluate a concrete system. The taxonomy confirms that multi-level hierarchical integration combining all three technologies in an electoral context has not been realised in any of the reviewed implementations.

H. Ramandan(2024)–AMLSF: Adaptive Multi-Layer Security Framework for Smart City Networks

Methodology: A hierarchical key management scheme distributes cryptographic responsibilities across network tiers. Machine learning models adapt protocol parameters in real time in response to detected traffic anomalies, and the framework is evaluated on smart-city network traces across multiple traffic load conditions.

Limitation: Although the hierarchical key management concept is directly relevant to multi-level electoral architectures, the framework does not incorporate blockchain for immutable record-keeping. The absence of a distributed ledger means that security events and data records are stored in mutable, potentially corruptible databases.

I. Indrason and Saha (2024) – Blockchain-Driven Security in SDN-Based IoT Networks

Methodology: Blockchain is applied as a security enhancement layer over an SDN-managed IoT network, with all security-relevant control-plane decisions recorded on the ledger for auditability. The combination provides both programmable network control and a verifiable history of policy enforcement actions.

Limitation: The deployment is single-tier: all devices and controllers operate within one administrative domain. This flat topology cannot model the multi-level propagation and cross-jurisdiction aggregation that characterise national electoral processes. Extensions to hierarchical deployments are identified as future work but are not implemented.

J. Indrason et al. (2025) – MBCSD-IoT: Multi-Level Blockchain-Assisted SDN-Based IoT for Secured E-Voting

Methodology: This seminal work from which the present heterogeneous resource capacities and variable inter-tier link survey derives introduces the four-level MBCSD-IoT architecture. Blockchain instances are maintained at District, State, and Country tiers; ECC encrypts inter-level communication; efficiency and does not address security, data integrity, or SHA3-256 hashing provides hop-by-hop integrity verification; identity verification. The absence of blockchain or any crypto-biometric sensors authenticates voters at the booth level; and a graphic assurance layer makes the architecture unsuitable for high-stakes applications such as vote processing. Experimental evaluation demonstrates substantial performance gains over traditional IoT voting infrastructure.

Limitation: The reported testbed is limited in scale — three server-class machines and seven Raspberry Pi nodes represent the entire four-level hierarchy. Real-world deployments must sustain many orders of magnitude more concurrent sessions, and the inter-level communication links in the testbed rely on Wi-Fi, which may require replacement with GSM/LTE for geographically dispersed deployments.

K. Zhanget al. (2025) – Transparent Blockchain-Based Voting with Immutable Audit Trail

Methodology: A public blockchain is used to store encrypted vote records, with smart contracts governing vote submission, validation, and automated counting. The system exposes a read-only public interface through which any observer can independently verify the final tally against the ledger.

Limitation: The absence of an SDN layer means that network management is handled by conventional IP routing, which does not support programmable DDoS mitigation or flow-level policy enforcement. The architecture is also single-tier, with no provision for hierarchical result aggregation.

IV. RESEARCH GAP AND MOTIVATION

The preceding survey reveals a consistent fragmentation in the existing literature. Blockchain-centric e-voting works [1], [3], [11] establish the immutability and auditability properties required of a trustworthy ledger, yet they treat the underlying network as an unmanaged substrate and provide no mechanism for dynamic traffic optimisation or programmable attack mitigation. SDN-IoT security frameworks [5], [9] demonstrate that flow-level control can substantially improve both network performance and resilience against flooding attacks, but they do not integrate blockchain record-keeping and are not evaluated in electoral workflows. Multi-tier architectures [6], [8] explore the performance and key management benefits of hierarchical deployment, but neither incorporates the full triad of blockchain, SDN, and IoT, nor does either address the identity assurance requirements specific to voter authentication.

The critical gap is therefore not a deficiency in any individual technology, but the absence of a unified framework that integrates all four dimensions simultaneously: a multi-level hierarchical topology that reflects administrative electoral structure; a blockchain layer at each tier that provides tamper-proof vote storage without centralised trust; an SDN control plane that enables real-time traffic management and DDoS

V. PROPOSED MBCSD-IOT ARCHITECTURE AND METHODOLOGY

A. System Architecture Overview

The MBCSD-IoT architecture organises electoral processing into four hierarchical tiers. The Booth level consists of IoT-class EVMs, each equipped with a biometric authentication module, a Wi-Fi transceiver, an ECC encryption unit, a SHA3-256 hash generator, and a local buffer for temporary encrypted storage under connectivity loss. The District, State, and Country level each host a structurally identical node comprising a Wi-Fi or LTE interface, OpenFlow-enabled switches, a microcontroller responsible for data validation and blockchain interaction, a Ryu-based SDN controller for flow management, and a blockchain instance that persistently records all validated votes or aggregated results received from the tier immediately below. Data packets grow predictably as they ascend the hierarchy. A Booth-to-District packet carries 232 bytes of payload, incorporating vote content, booth identifier, constituency tag, candidate identifier, and timestamp alongside ECC ciphertext and a SHA3-256 digest. At the District tier, the node appends its own identifier and a fresh integrity hash before forwarding a 296 byte packet upward. The State tier performs the same augmentation, producing a 360 byte packet destined for the Country node. This monotonically expanding payload provides a complete provenance trail: every tier's processing step is cryptographically attested within the data structure that arrives at the country-level blockchain. The overall system architecture is illustrated in Fig. 1.

B. Device Authentication

Before the polling session opens, each EVM establishes its legitimacy by encrypting its hardware MAC address using its ECC private key and transmitting the resulting ciphertext to its assigned district node via MQTT. The district node retrieves the corresponding ECC public key from the district-level blockchain and decrypts the received ciphertext. Authentication succeeds if and only if the decrypted value matches the MAC address registered for that EVM at the time of electoral roll compilation. Devices whose authentication fails are denied network access by the SDN controller, which installs a drop rule for all traffic originating from the offending MAC address.

C. Voter Authentication and Double-Vote Prevention

At the moment a voter presents themselves to an EVM, mitigation across inter-level links; and a cryptographic identity the biometric module captures a fingerprint or facial scan layer combining ECC device authentication and biometric and encodes the resulting feature vector. This biometric token voter verification that prevents both impersonation and multi-encrypted using ECC and transmitted to the district-level blockchain, where it is compared against the pre-enrolled MBCSD-IoT [10] represents the first reported system to biometric record associated with that voter's electoral identity. occupy this intersection. The presents survey extends that A successful match grants ballot access; the voter's record is baseline by providing a comprehensive literature context, a simultaneously flagged as having received ballot access, so that detailed security analysis, and a discussion of deployment con- any subsequent authentication attempt for the same identity—siderations required to scale the architecture from a laboratory regardless of the originating booth—is rejected at the district level without forwarding to the EVM.

TABLE I
COMPARATIVE SUMMARY OF RELATED WORKS

Work	Technology	Blockchain/SDN		Multi-tier	Biometric/Key Limitation	
Alvi et al. [1]	Blockchain, Smart Contracts	Yes	No	No	No	No SDN, single-tier only
Latif et al. [2]	Blockchain, SDN	Yes	Yes	No	No	Not designed for e-voting
Sharma et al. [3]	Blockchain	Yes	No	No	No	No performance evaluation
Kumaret al. [4]	IoT, Encryption	No	No	No	Yes	Centralised, single point of failure
Khedret al. [5]	SDN, ML	No	Yes	Yes	No	No blockchain, no votes support
Aldossary [6]	Fog, Cloud	No	No	Yes	No	No security or integrity layer
Turner et al. [7]	Blockchain, SDN (survey)	Yes	Yes	N/A	No	Survey only, no implementation
Ram Anandan [8]	ML Security	No	No	Yes	No	No blockchain persistence
Indrason Sahal [9]	Blockchain, SDN	Yes	Yes	No	No	Single-tier, no hierarchy
Indrason et al. [10]	BC, SDN, IoT, ECC	Yes	Yes	Yes	Yes	Small testbed, Wi-Fi only
Zhanget al. [11]	Blockchain	Yes	No	No	No	No SDN, no hierarchy
Proposed	BC, SDN, IoT, Biometrics	Yes	Yes	Yes	Yes	This work

D. Vote Casting and Hierarchical Propagation

A confirmed ballot submission packages the booth name, MQTT topic string, constituency identifier, booth ID, candidate ID, and submission timestamp into a single structured payload. A SHA3-256 digest of this payload is appended before the entire object is ECC-encrypted and forwarded to the district node. Upon receipt, the district node decrypts the payload, recomputes the SHA3-256 digest, and compares it against the transmitted value; any discrepancy triggers a retransmission request. Validated records are stored on the district blockchain and forwarded, augmented with district-level metadata, to the state node, which repeats the same validate-store-forward cycle. The country node performs the terminal validation and commits the final augmented record to the authoritative national ledger. On election day closure, a smart contract executes automated vote counting across the country-level blockchain, generating certified totals without human intervention.

E. SDN-Based Traffic Management

At each hierarchical level, an OpenFlow-capable SDN controller maintains a complete view of inter-node connectivity and current traffic load. Flow tables are pre-populated with rules that forward validated electoral traffic along optimal paths. The controller monitors incoming request rates and, upon detecting patterns consistent with DDoS flooding, installs rate-limiting rules at ingress OpenFlow switches. iptables-based firewall policies on server-class nodes provide a secondary mitigation boundary. The separation of the control plane from the forwarding plane ensures that policy updates—across all switches within milliseconds rather than requiring per-device manual reconfiguration.

F. Communication Protocol Stack

All inter-level communication follows a consistent five-layer protocol stack: IEEE 802.11 (Wi-Fi) at the wireless link layer, IP/ICMP at the network layer, TCP at the transport layer, TLS/SSL for session-level encryption, and MQTT as the application-layer messaging protocol. MQTT's publish-subscribe model and minimal header overhead make it particularly appropriate for IoT endpoints operating under bandwidth and power constraints. For production deployments in regions with poor Wi-Fi coverage, the IEEE 802.11 layer can be replaced by a GSM/LTE radio interface without any modification to the higher protocol layers.

VI. SECURITY ANALYSIS

The MBCSD-IoT architecture addresses six security dimensions that are individually necessary and jointly sufficient for a trustworthy national electoral system.

Voter Anonymity. The vote payload transmitted across all inter-level links contains only the booth identifier, candidate identifier, constituency, and timestamp. No element of the voter's personal identity is included in the propagated record, ensuring that the public blockchain ledger cannot be used to trace a specific ballot back to its originator.

End-to-End Vote Integrity. ECC encryption protects the confidentiality of each vote packet in transit. SHA3-256 digests computed at the source and verified at every receiving node guarantee that any in-transit bit-level modification is detected before the record is committed to a blockchain tier.

Authorised-Device Enforcement. ECC-based MAC address-based blocking of newly identified attack sources—propagate dress authentication at the start of each polling session ensures that only pre-registered EVMs can inject votes into the system.

the SDN controller before they can transmit any data. **Double-Vote Prevention.** The district-level blockchain maintains a voting-status flag for each enrolled voter. The flag is set atomically upon successful ballot submission. Any subsequent authentication request from the same voter identity is rejected at the district node, irrespective of the originating EVM or booth, because the flag is replicated across all district-tier blockchain nodes.

DDoS Resilience. SDN-based rate limiting at the OpenFlow ingress switches prevents volumetric flooding from saturating inter-level links. The blockchain's inherent decentralisation means that compromising one node does not affect the record integrity or availability of other nodes in the same tier.

Result Integrity. Automated smart-contract vote counting packet loss characterisation. Evaluations were conducted at the country level eliminates any stage at which a human four packet batch sizes — 10, 100, 1000, and 10000 packets operator could selectively modify count totals. The counting—within repeated trials per configuration to establish logic is encoded in the smart contract bytecode, which is statistically stable means. itself immutably stored on the blockchain, and its execution Rogue or counterfeit terminals are denied network access by is deterministically reproducible by any auditing party.

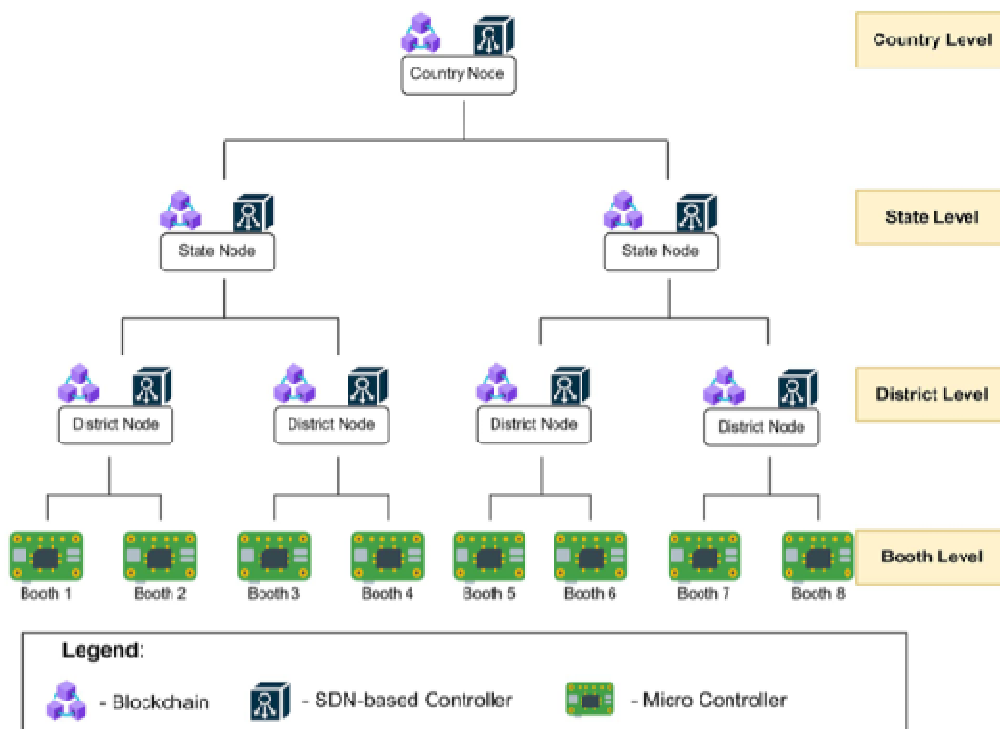


Fig. 4. MBCSD-IoT architecture.

Fig. 1. MBCSD-IoT system architecture: Booth-level IoT EVMs with biometric authentication and ECC encryption propagating votes upward through District, State, and Country blockchain nodes via SDN-managed inter-level links.

VII. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

A. Testbed Configuration

The experimental evaluation employed three Ubuntu 20.04.6 LTS (64-bit) workstations representing the District, State, and Country level server nodes; seven Raspberry Pi 3 Model B+ boards functioning as OpenFlow switches, SDN controllers, and the Booth-level node; and ESP8266 Wi-Fi modules providing wireless links between tiers. The Ryu framework was deployed as the SDN controller at every tier. Network measurement tools included ping for round-trip latency, iperf3 for throughput, and hping3 for

B. Performance Results

Table II summarises throughput and latency measurements at each inter-level link under both MBCSD-IoT and a conventional IoT baseline that replaces the SDN and blockchain components with standard IP routing and a centralised database.

TABLE II

EXPERIMENTAL PERFORMANCE: MBCSD-IoT vs. TRADITIONAL IoT

Link/System	Throughput (Mbps) @ batch size			
	10	100	1K	10K
B → D (MBCSD)	10.30	9.68	9.51	8.99
B → D (Trad.)	4.58	4.72	3.86	6.95
D → S (MBCSD)	4.82	7.67	7.61	6.79
D → S (Trad.)	2.82	3.50	3.22	4.43
S → C (MBCSD)	9.75	7.65	7.92	8.16
S → C (Trad.)	6.62	7.14	7.31	6.33

The SDN control plane's ability to pre-install forwarding rules eliminates the per-packet routing-table lookup latency that burdens conventional IoT stacks, which accounts for the consistent throughput advantage observed at every link and batch size. Latency benefits are most pronounced at the Booth-to-District link — where MBCSD-IoT records approximately 4ms compared to over 51ms for the traditional IoT baseline at the 100-packet batch size — because this link handles the highest volume of concurrent voter sessions and is therefore most sensitive to per-packet routing overhead. Packet loss in conventional IoT networks is high at small batch sizes because route establishment consumes a disproportionate fraction of the available window; once routes stabilise at larger batch sizes, the two systems begin to converge on this metric. Across all link-level measurements, MBCSD-IoT achieves a 51.7% improvement in throughput, an 81.2% reduction in latency, and an 83.2% reduction in packet loss relative to the traditional IoT baseline.

VIII. IMPLEMENTATION CONSIDERATIONS

Several engineering decisions govern the translation of the MBCSD-IoT prototype into a production electoral deployment. The Wi-Fi-based inter-level communication used in the testbed is inadequate for geographically compact deployments with flash memory so that a power interruption does not result in data loss. Once connectivity is re-established, the buffered records are transmitted to the district node following the standard ECC-and-SHA3-256 protocol path, with timestamps preserving the original submission ordering.

To eliminate the SDN controller as a potential single point of failure, production deployments should adopt a distributed multi-controller configuration in which two or more controllers synchronise flow-table state via a consensus protocol. Load is distributed across controllers according to geographic proximity to the switches they manage, which also reduces control-plane round-trip latency. This architecture was evaluated in related work on fault-tolerant SDN [13] and is directly applicable to the MBCSD-IoT control plane without change to the data-plane behaviour.

IX. CONCLUSION AND FUTURE WORK

This survey has examined the MBCSD-IoT architecture, a four-tier hierarchical fusion of Blockchain, SDN, and IoT technologies designed to address the security, scalability, and transparency deficiencies of conventional e-voting systems. A systematic review of eleven prior works established that, while each constituent technology has been individually demonstrated at production quality, no prior system before MBCSD-IoT had integrated multi-level hierarchy, blockchain immutability, SDN-based network optimisation, and rigorous biometric-coupled cryptographic identity management within a single electoral framework.

The architecture achieves its security objectives through a combination of ECC device authentication, biometric voter verification, SHA3-256 hop-by-hop integrity checking, and smart-contract automated counting — all anchored by blockchain instances maintained at each tier of the hierarchy. The performance evaluation against a conventional IoT baseline confirms throughput gains of 51.7%, latency reductions of 81.2%, and packet loss decreases of 83.2%, improvements attributable to the SDN control plane's ability to pre-compute and install optimal forwarding rules before traffic arrives.

Several directions remain open for continued investigation, but must be replaced by GSM/LTE links for spanning the large-scale simulation studies involving tens of thousands of district-to-state and state-to-country hops in a national election. Concurrent virtual voting sessions are needed to characterise system behaviour under realistic election-day loads and network-layer agnostic and do not require modification.

Distance voting is supported through a two-step relocation to identify any saturation points in the SDN controller or blockchain consensus subsystems. Integration of GSM/LTE procedure. A voter who cannot attend their registered booth communication for inter-level links must be validated with notified election authority in advance. The authority uprespects both performance and protocol correctness under dates the district blockchain to temporarily remove the voter variable cellular network conditions. The ECC-based crypto-from their home booth registry and creates a time-limited graphic suite should be evaluated against post-quantum alternatives at the designated remote booth. This ensures that the natives — such as lattice-based key encapsulation mechanisms — biometric authentication at the remote booth succeeds and that — in anticipation of the eventual deprecation of elliptic curve the double-vote prevention flag is correctly shared across both algorithms by future quantum-capable adversaries. Finally, a the original and remote district nodes. user-study evaluation of the voter-facing EVM interface and In connectivity-impaired areas, EVMs operate with an end-to-end biometric authentication flow is essential before national-crypted local buffer that accumulates votes until network scaled deployment, as usability barriers at the booth level directly affect voter participation rates and the legitimacy of the electoral outcome.

REFERENCES

- [1] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 9, pp. 6855–6871, 2022.
- [2] S. A. Latif et al., "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Computer Communications*, vol. 181, pp. 274–283, 2022.
- [3] V. Sharma et al., "Blockchain-based e-voting with enhanced voter privacy," *Proc. Int. Conf. on Information Security and Cryptology*, 2022.
- [4] R. Kumar et al., "Secure IoT-based voting system with biometric authentication," *Proc. IEEE Int. Conf. on Communication Systems and Network Technologies*, 2022.
- [5] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "FMDADM: A multi-layer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks," *IEEE Access*, vol. 11, pp. 28934–28954, 2023.
- [7] M. Aldossary, "Multi-layer fog-cloud architecture for optimizing the placement of IoT applications in smart cities," *Computers, Materials & Continua*, vol. 75, no. 1, pp. 633–649, 2023.
- [8] S. W. Turner, M. Karakus, E. Guler, and S. Uludag, "A promising integration of SDN and blockchain for IoT networks: A survey," *IEEE Access*, vol. 11, pp. 29800–29822, 2023.
- [9] M. S. Ram and R. Anandan, "Adaptive multi-layer security framework (AMLSF) for real-time applications in smart city networks," *Journal of Autonomous Intelligence*, vol. 7, no. 5, 2024.
- [10] N. Indrason and G. Saha, "Exploring blockchain-driven security in SDN-based IoT networks," *Journal of Network and Computer Applications*, vol. 224, 2024.
- [11] N. Indrason, W. Khongbuh, K. Baital, and G. Saha, "MBCSD-IoT: A multi-level blockchain-assisted SDN-based IoT architecture for secure e-voting system," *IEEE Transactions on Network Science and Engineering*, vol. 12, no. 3, pp. 1613–1622, May/Jun. 2025.
- [12] K. Zhang et al., "Transparent blockchain-based voting with immutable audit trail," *Proc. IEEE Int. Conf. on Blockchain and Cryptocurrency*, 2025.
- [13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [14] R. K. Das, F. H. Pohrmen, A. K. Maji, and G. Saha, "FT-SDN: A fault-tolerant distributed architecture for software defined network," *Wireless Personal Communications*, vol. 114, pp. 1045–1066, 2020.
- [15] S. Ullah et al., "Elliptic curve cryptography: Applications, challenges, recent advances, and future trends," *Computer Science Review*, vol. 47, 2023.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)