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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.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 Sapthagiri College of Engineering

Abstract: *Contemporarydemocraticinstitutionsarecon- architecturalredundancyrequiredtowithstandmodernad- fronting unprecedented demands for electoral systems that simul-taneously guarantee security, transparency, and the capacity to accommodate millions of geographically distributed voters. Con-ventional paper-based balloting and first-generation electronic votingmachinesremainsusceptibletophysicaltampering,cen- versarial 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 immutableaudittrailrenderspost-electionforensicanalysis tralisedarchitecturalfailures, andcyberintrusion, noneofwhich inconclusive. are adequately addressed by existing incremental improvements. This survey investigates MBCSD-IoT, a four-tier hierarchical architecture that fuses Blockchain, Software Defined Networking (SDN),andInternetofThings(IoT)infrastructureintoauni-fied,tamper-resistante-votingframework.Theproposeddesign*

Three independently mature technologies now offer the constituent elements of a fundamentally different design. Blockchain provides a distributed, append-only ledger whose cryptographiclinkagebetweenblocksmakesretrospectivedata partitionselectoralprocessingacrossBooth,District,State,and modificationcomputationallyintractable.SoftwareDefinedCountry 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 SHA3-256hashingprovidesper-hopintegrityassurance.SDN-

Networking separates the forwarding plane from the control plane, enabling a logically centralised controller to install op-timal forwarding rules across heterogeneous switches, thereby reducing latency and enabling real-time traffic policy enforcebasedflowmanagementateverytiereliminatesper-packetrout- ment.TheInternetofThingssuppliesthesmartendpoints— ing overhead and enables programmable DDoS mitigation. The survey reviews eleven representative prior works, characterises the research gap they collectively expose, and demonstrates throughexperimentalevaluationthatMBCSD-IoTachievesa 51.7 %gaininthroughput,an81.2%reductioninlatency,and voter-facing EVMs, biometric scanners, and relay nodes — through which physical electoral intent is captured, encoded, andpropagated.Noneofthesethreetechnologies,deployedin isolation, is sufficient for a production-grade e-voting system; an83.2%decreaseinpacketlossrelativetoconventionalIoTtheirintegration,however,addresseseachother'sresidualbasedvotingdeploy ments.weaknesses.

IndexTerms—Blockchain,SoftwareDefinedNetworking,In-ternetofThings,E-Voting,EllipticCurveCryptography,SHA3-256, Biometric Authentication, MBCSD-IoT, MQTT, DistributedArchitecture

I. INTRODUCTION

The MBCSD-IoT framework examined in this survey is precisely such an integration. The architecture imposes afour-levelhierarchy—Booth,District,State,andCountry that mirrors the administrative partitioning of large-scale democraticelections.Votesoriginateatbooth-levelIoTnodes equippedwithECCencryptionandbiometricauthentication

Democratic governance at scale demands electoral infras-modules,traverseSDN-managedinter-levellinks,andare tructure that is simultaneously resistant to manipulation, in-recordedonblockchaininstancesmaintainedateachascending dependently verifiable ,andcapableofprocessingmillionstier.Thecountry-levelblockchainservesasthefinal,authorita-of concurrent transactions without performance degradation.tive aggregate repository from which automated vote counting Paperballotsandfirst-generationelectronicvotingmachinesisexecuted,eliminatinghumaninterventioninthetabulation(EVMs)addressedtheneedformechanised counting,yetphase.

©IJRASET: All Rights are Reserved

Neitherdesignincorporatesthecryptographicguaranteesor Theremainderofthispaperisorganisedasfollows. SectionIIsuppliesbackground onthethreefoundationaltechnolo-by RSA for equivalent security. A 256-bit ECC key provides giesandtheircryptographiccomponents. SectionIIIpresentssecuritycomparabletoa3072-bitRSAkey,areduction the literature survey. Section IV articulates the research gapthat is particularly consequential for resource-constrained IoT motivating this work. Section V details the MBCSD-IoTendpoints where key generation and decryption operations methodology. SectionVIanalysesthesecuritypropertiesofthecompete with real-time sensing and transmission tasks. In architecture. SectionVIIpresentsexperimentalresults. Sec-MBCSD-IoT, ECC is employed for both device authentication tionVIIIdiscussesimplementationconsiderations. SectionIX—whereeachEVMpresentsanECC-encryptedproofofits concludesthepaper.

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 ensuresthatanyretroactivemodificationtoacommittedblock invalidateseverysubsequentblock,makingundetectedtamper-ing 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. *SoftwareDefinedNetworkingforIoT*

A Software Defined Networking architecture partitions theand ballot submission are handled through cryptographically network into three interacting planes. The infrastructure planesigned transactions, and the immutable ledger prevents post-consists of forwarding devices — physical or virtual switchessubmission modification of any cast vote. thatexecuteflowrulesinstalledbyanexternalcontrollerLimitation:Thearchitecturedoesnotincorporateanynetwork viatheOpenFlowprotocol.Thecontrolplanecomprisesonemanagementlayer.Underhighconcurrentsubmissionrates,ormoreSDNcontroll ersthatmaintainaglobaltopologyview,the absence of SDN-driven flow control leads to congestion compute optimal forwarding paths, and push updated rules toatthevalidationnodes,andthesingle-tierdeploymentdoes the data plane in response to changing traffic conditions. Thenot reflect the hierarchical administrative structure of national applicationplanehostsnetworkservices—loadbalancing,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 characteristicofDDoSflooding—byinstallingdroprules attheingresspointratherthanallowingmaliciousttraffic 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. *ECCandSHA3-256CryptographicPrimitives*

EllipticCurveCryptographyachievesasymmetricencryp- anonymity,double voteprevention,andhierarchicalresulttionatkeylengthssubstantiallyshorterthanthoserequired aggregation are not addressed. hardwareidentity—andforvotedataencryptionduringinter-level transmission.

SHA3-256isamemberoftheKeccakhashfamilystandard-ised by NIST. Its sponge construction distinguishes it fromtheMerkle–Damga˚rdstructureunderlyingSHA-2,conferring resistance to length-extension attacks. Applied at every com-munication hop in the MBCSD-IoT chain, a SHA3-256 digest over the vote payload allows the receiving node to detect any in-transitmodificationbeforecommittingtherecordtoitslocal blockchain.

III. LITERATURE SURVEY

This section reviews eleven representative prior works acrossthedomainsofblockchain-securede-voting,SDN-Forelectoralapplications,thesepropertiestranslateintobasedIoTsecurity,multi-tierdistributedarchitectures,and threeconcreteguarantees. First,eachvote,oncecommittedrelatedenablingtechnologies. Acomparativesummaryis totheledger, cannotbesilentlyaltered byanysingleparty. presentedinTableI.

Second,smartcontractscanencodevalidationandcounting logic whose execution is deterministic and publicly auditable. Third, the decentralised replication model eliminates any sin-gle point of failure that an adversary could exploit to suppress or inflate a vote tally.

A. Alvietal.(2022)–DVTChain:Blockchain-BasedSecure Digital Voting System

Methodology:Theauthorsconstructadecentralisedvoting platform in which each ballot is recorded as a smart-contract transactiononapermissionedblockchain.Voterregistration firewallpolicies,QoSenforcement—thatexpresstheirre-quirements to the control plane through northbound APIs. WhenappliedtoIoTdeployments,SDNyieldsmeaning-

B. Latifetal.(2022)–AI-EmpoweredBlockchainandSDN 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 flagsstatisticallyanomaloustrafficflows,whereupontheSDN 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 electoralcontext.Vote-specificrequirementssuchasvoter

C. Sharmaetal.(2022)–Blockchain-BasedE-Votingwith

Methodology: A distributed ledger design employs zero-knowledge-inspired anonymisation of voter identities so that thepublicledgerencodesthevotecountwithoutexposingany 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 per-formance evaluation, making it impossible to assess through-put 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 withfingerprintandfacialrecognitionmodulestoauthenticate voterspriortoballotsubmission.Votercredentialsareverified against a centralised server, and votes are transmitted over an encrypted channel to a backend database.

Limitation:Thecentralisedserverarchitecturerecreates the single-point-of-failure vulnerability that motivates decen-tralised designs. An adversary who compromises the central verificationservercandenyauthenticationtolegitimatevoters or inject fraudulent entries, undermining the security guaran-tees the biometric layer is intended to provide.

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

Methodology: A five-tier SDN-IoT topology is instru-mented 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-LayerFog-CloudArchitecturefor IoT Application Placement

Methodology: A mixed-integer linear programme deter-mines the optimal placement of IoT application instances across fog nodes and cloud servers to minimise end-to-end latencyandcommunicationcost.Theformulationconsiders

G. *Turneretal.(2023)–SurveyofBlockchain-SDNIntegra-VoterPrivacy*

Methodology:Acomprehensivetaxonomyclassifiesexist-ing blockchain-SDN integration approaches into three modes: integrated (blockchain embedded within the SDN controller), collaborative(blockchainandSDNaspeerentitiesexchanging events),andoverlay(blockchainoperatingindependentlyatop theSDNsubstrate).Thesurveyanalysesthetrade-offsofeach mode with respect to latency, decentralisation, and implemen-tation complexity.

Limitation: As a survey, the work does not propose or evaluateaconcretesystem.Thetaxonomyconfirmsthatmulti-level hierarchical integration combining all three technologies in an electoral context has not been realised in any of the reviewed implementations.

H. RamandAnandan(2024)–AMLSF:AdaptiveMulti-Layer Security Framework for Smart City Networks

Methodology:Ahierarchicalkeymanagementschemedis-tributes cryptographic responsibilities across network tiers. Machine learning models adapt protocol parameters in real time in response to detected traffic anomalies, and the frame-workisevaluatedonsmart-citynetworktracesacrossmultiple traffic load conditions.

Limitation: Although the hierarchical key management con-cept is directly relevant to multi-level electoral architectures, the framework does not incorporate blockchain for immutable record-keeping. The absence of a distributed ledger meansthat 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 en-hancementlayeroveranSDN-managedIoTnetwork,with all security-relevant control-plane decisions recorded on the ledger for auditability. The combination provides both pro-grammable network control and a verifiable history of policy enforcement actions.

Limitation:Thedeploymentissingle-tier:alldevicesand
controllers operate within one administrative domain. Thisflat topology cannot model the multi-level propagation and cross-jurisdiction aggregation that characterise national elec-toral 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:Theseminalworkfromwhichthepresent heterogeneous resource capacities and variable inter-tier linksurvey derives introduces the four-level MBCSD-IoT archi-bandwidths. tecture. Blockchain instances are maintained at District, State, Limitation: The work focuses entirely on resource allocationand Country tiers; ECC encrypts inter-level communication; efficiency and does not address security, data integrity, orSHA3-256 hashing provides hop-by-hop integrity verification; identity verification. The absence of blockchain or any crypto-biometric sensors authenticate voters at the booth level; and graphic assurance layer makes the architecture unsuitable forRyu-controlledOpenFlowswitchesmanagetrafficateachtier. high-stakes applications such as vote processing.Experimentalevaluationdemonstratessubstantialperformancegainsovertraditional IoTvotinginfrastructure.

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, andtheinter-levelcommunicationlinksinthetestbedrely on Wi-Fi, which may require replacement with GSM/LTE for geographically dispersed deployments.

K. Zhangetal.(2025)–TransparentBlockchain-BasedVoting with Immutable Audit Trail

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

Limitation:TheabsenceofanSDNlayermeansthatnetwork management is handled by conventional IP routing, which doesnotsupportprogrammableDDoSmitigationorflow-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 mecha-nism for dynamic traffic optimisation or programmable attack mitigation.SDN-IoTsecurityframeworks[5],[9]demonstrate thatflow-levelcontrolcansubstantiallyimprovebothnetwork performance and resilience against flooding attacks, but they do not integrate blockchain record-keeping and are not eval-uated in electoral workflows. Multi-tier architectures [6], [8] exploretheperformanceandkeymanagementbenefitsofhier-archical deployment, but neither incorporates the full triad of blockchain,SDN,andIoT,nordoeseitheraddressestheidentity assurance requirements specific to voter authentication.

The critical gap is therefore not a deficiency in any indi-vidual technology, but the absence of a unified frameworkthat integrates all four dimensions simultaneously: a multi-levelhierarchicaltopologythatreflectsadministrativeelectoral structure; a blockchain layer at each tier that provides tamper-proof vote storage without centralised trust; an SDN control planethatenablesreal-timetrafficmanagementandDDoS

V. PROPOSED MBCSD-IOT ARCHITECTURE AND METHODOLOGY

A. SystemArchitectureOverview

TheMBCSD-IoTarchitectureorganiseselectoralprocessing into four hierarchical tiers. The Booth level consists of IoT-class EVMs, each equipped with a biometric authentication module,aWi-Fitransceiver,anECCencryptionunit,aSHA3-256hashgenerator,andalocalbufferfortemporaryencrypted storageunderconnectivityloss.TheDistrict,State,andCoun-trylevelseachhostastructurallyidenticalnodecomprising a Wi-Fi or LTE interface, OpenFlow-enabled switches, a microcontrollerresponsiblefordatavalidationandblockchain interaction,aRyu-basedSDNcontrollerforflowmanagement, andablockchaininstancethatpersistentlyrecordsallvalidated votes or aggregated results received from the tier immediately below.

Data packets grow predictably as they ascend the hierar-chy. A Booth-to-District packet carries 232bytes 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 296byte packet upward. The State tier performs the same augmentation, producing a 360byte packet destined for the Countrynode.Thismonotonicallyexpandingpayloadprovides a complete provenance trail: every tier's processing step is cryptographicallyattestedwithinthedatastructurethatarrives at the country-level blockchain.

Theoverallsystemarchitectureisillustratedin Fig.1.

B. DeviceAuthentication

Beforethepollingsessionopens,eachEVMestablishes its legitimacy by encrypting its hardware MAC address using its ECC private key and transmitting the resulting ciphertextto its assigned district node via MQTT. The district node retrieves the corresponding ECC public key from the district-levelblockchainanddecryptsthereceivedciphertext.Authen-ticationsucceedsifandonlyif thedecryptedvaluematchesthe MAC address registered for that EVM at the time of electoral rollcompilation.Deviceswhoseauthenticationfailsaredenied network access by the SDN controller, which installs a drop ruleforalltrafficoriginatingfromtheoffendingMACaddress.

C. VoterAuthenticationandDouble-VotePrevention

Atthemomentavoterpresentsthemselvestoan EVM, mitigation across inter-level links; and a cryptographic identity thebiometricmodulecapturesafingerprintorfacialscan layercombiningECCdeviceauthenticationandbiometric and encodes the resulting feature vector. This biometric token voter verification that prevents both impersonation and multi-isencryptedusingECCandtransmittedtothedistrict-level ple voting. blockchain,whereitiscomparedagainstthepre-enrolled MBCSD-IoT[10]representsthefirstreportedsystemto biometric record associated with that voter's electoral identity. occupythisintersection.Thepresentsurveyextendsthat A successful match grants ballot access; the voter's record is baselinebyprovidingacomprehensiveliteraturecontext,a simultaneouslyflaggedashavingreceivedballotaccess,sothat detailed security analysis, and a discussion of deployment con- anysubsequentauthenticationattemptforthesameidentity—siderationsrequiredtoscalethearchitecturefromalaboratory regardlessoftheoriginatingbooth—isrejectedatthe district testbedtoaproductionelectoralenvironment. levelwithoutforwardingtotheEVM.

TABLEI
COMPARATIVESUMMARYOFRELATEDWORKS

Work	Technology	Blockchain	SDN	Multi-tier	Biometric	KeyLimitation
Alvietal.[1]	Blockchain,SmartContracts	Yes	No	No	No	NoSDN;single-tieronly
Latifetal.[2]	AI,Blockchain,SDN	Yes	Yes	No	No	Notdesignedfore-voting
Sharmaetal.[3]	Blockchain	Yes	No	No	No	Noperformanceevaluation
Kumaretal.[4]	IoT,Encryption	No	No	No	Yes	Centralised;singlepointoffailure
Khedretal.[5]	SDN,ML	No	Yes	Yes	No	Noblockchain;novotesupport
Aldossary[6]	Fog,Cloud	No	No	Yes	No	Nosecurityorintegritylayer
Turneretal.[7]	Blockchain,SDN(survey)	Yes	Yes	N/A	No	Surveyonly;noimplementation
RamAnanda & n[8]	MLSecurity	No	No	Yes	No	Noblockchainpersistence
IndrasonSah & a[9]	Blockchain,SDN	Yes	Yes	No	No	Single-tier;nohierarchy
Indrasonetal.[10]	BC,SDN,IoT,ECC	Yes	Yes	Yes	Yes	Smalltestbed;Wi-Fionly
Zhangetal.[11]	Blockchain	Yes	No	No	No	NoSDN;nohierarchy
Proposed	BC, SDN, IoT, ECC, Biometrics	Yes	Yes	Yes	Yes	Thiswork

D. VoteCastingandHierarchicalPropagation

A confirmed ballot submission packages the booth name, MQTT topic string, constituency identifier, booth ID, candi-date 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 tothedistrictnode.Uponreceipt,thedistrictnodedecrypts the payload, recomputes the SHA3-256 digest, and comparesit 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 recordto 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-*BasedTrafficManagement*

At each hierarchical level, an OpenFlow-capable SDN con-troller 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, upondetectingpatternsconsistentwithDDoSflooding,installs rate-limiting rules at ingress OpenFlow switches. Iptables-based firewall policies on server-class nodes provide a sec-ondary mitigation boundary. The separation of the control planefromtheforwardingplaneensuresthatpolicyupdates—
across all switches within milliseconds rather than requiring per-device manual reconfiguration.

F. CommunicationProtocolStack

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 asthe application-layer messaging protocol. MQTT's publish-subscribemodelandminimalheaderoverheadmakeitparticu-larly 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 re-placedbyaGSM/LTEradiointerfacewithoutanymodification to the higher protocol layers.

VI. SECURITY ANALYSIS

TheMBCSD-IoTarchitectureaddressessixsecuritydimen-sions that are individually necessary and jointly sufficient fora 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 di-gests 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-DeviceEnforcement.ECC-basedMACad-suchasblockinganewlyidentifiedattacksource—propagate dress authenticationat the start ofeachpollingsessionensures that only pre-registered EVMs can inject votes into the system.

theSDNcontrollerbeforetheycantransmitanydata. Double-VotePrevention.Thedistrict-levelblockchain maintainsavoting-statusflagforeachenrolledvoter. The flag is set atomically upon successful ballot submission. Any subsequentauthenticationrequestfromthesamevoteridentity is rejected at the district node, irrespective of the originating EVMorbooth,becausetheflagisreplicatedacrossalldistrict-tier blockchain nodes.

DDoS Resilience. SDN-basedratelimitingattheOpenFlow 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.

ResultIntegrity.Automatedsmart-contractvotecountingpacketlosscharacterisation.Evaluationswereconductedat at the country level eliminates any stage at which a humanfour packet batch sizes — 10, 100, 1000, and 10000 packets operatorcouldselectivelymodifycounttotals.Thecounting—withtenrepeatedtrialsperconfigurationtoestablish
logicisencodedinthesmartcontractbytecode,whichisstatisticallystablemeans. itselfimmutablystoredontheblockchain,anditsexecution
Rogue or counterfeit terminals are denied network access by is deterministically reproducible by any auditing party.

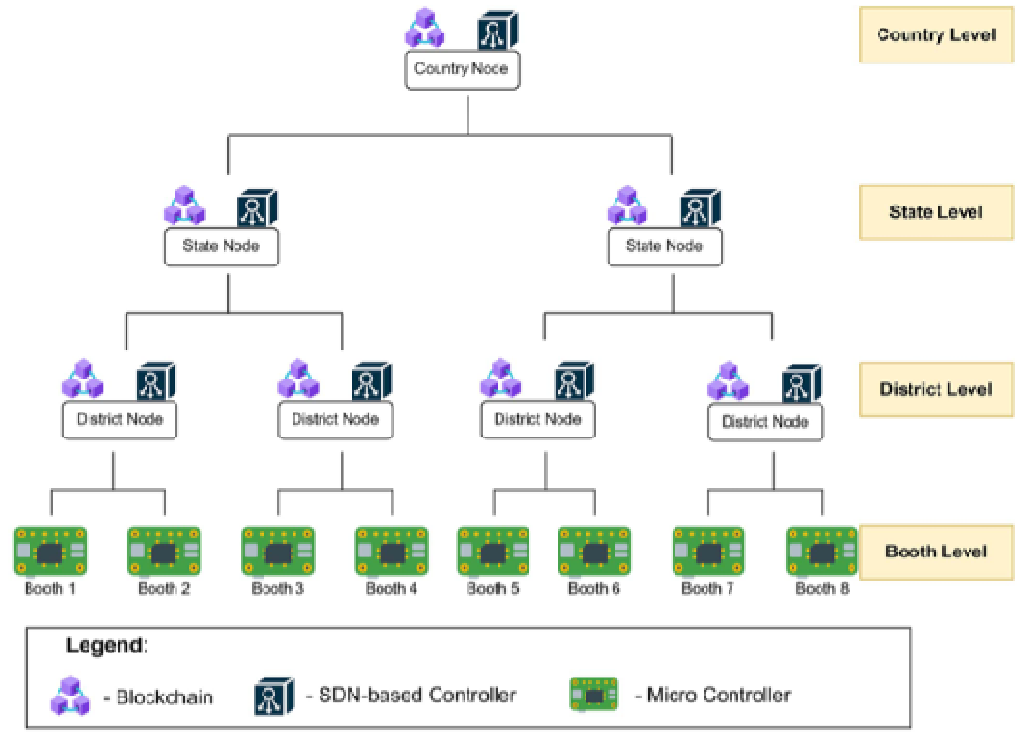


Fig. 4. MBCSD-IoT architecture.

Fig. 1.MBCSD-IoT system architecture: Booth-level IoT EVMs with biometric authentication and ECC encryption propagating votes upward through District,State,andCountryblockchainnodesviaSDN-managedinter-levellinks.

VII. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

A. TestbedConfiguration

Theexperimentalevaluationemployed threeUbuntu20.04.6LTS(64-bit)workstationsrepresenting 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.TheRyuframeworkwasdeployedastheSDNcontroller atevery tier. Network measurement tools included pingfor round-triplatency,iperf3forthroughput,andhping3for

B. PerformanceResults

Table II summarises throughput and latency measurements at each inter-level link under both MBCSD-IoT and a conven-tionalIoTbaselinethatreplacestheSDNandblockchaincom-ponents with standard IP routing and a centralised database.

TABLEII

EXPERIMENTALPERFORMANCE:MBCSD-IOTVS.TRADITIONALIOT

Link/System	Throughput(Mbps)@batchsize			
	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 batchsize.LatencybenefitsaremostpronouncedattheBooth-to-District link — where MBCSD-IoT records approximately4ms compared to over 51ms for the traditional IoT baselineat 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 conventionalIoTnetworksishighatsmallbatchsizesbecause 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.Acrossalllink-levelmeasurements,MBCSD-IoTachievesa
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 deploy-ment. The Wi-Fi-based inter-level communication used in the testbedisadequateforgeographicallycompactdeployments 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-controllerconfigurationinwhichtwoormorecontrollers synchronise flow-table state via a consensus protocol. Load is distributedacrosscontrollersaccordingtogeographicproxim-ity 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 appli-cabletotheMBCSD-IoTcontrolplanewithoutchangestothe data-plane behaviour.

IX. CONCLUSION AND FUTUREWORK

ThissurveyhasexaminedtheMBCSD-IoTarchitecture a four-tier hierarchical fusion of Blockchain, SDN, andIoT technologies designed to address the security, scalability, and transparency deficiencies of conventional e-voting sys-tems. 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 withina single electoral framework.

Thearchitectureachievesitssecurityobjectivesthrough acombinationofECCdeviceauthentication,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 base-line confirms throughput gains of 51.7%, latency reductionsof81.2%,andpacketlossdecreasesof83.2%,improvements attributable to the SDN control plane's ability to pre-compute and install optimal forwarding rules before traffic arrives.

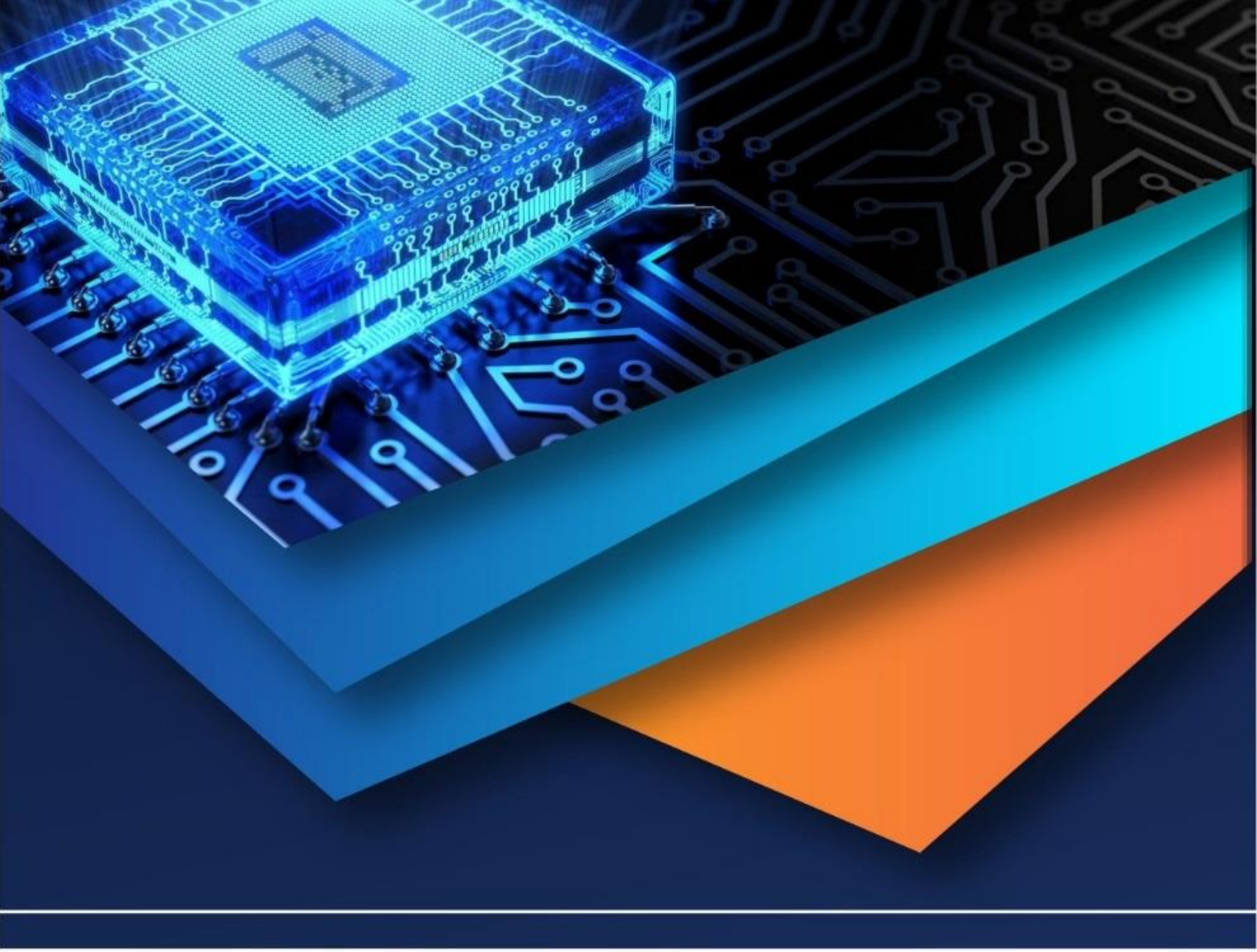
Severaldirectionsremainopenforcontinuedinvestigation. butmustbereplacedbyGSM/LTElinksforspanningthe Large-scalesimulationstudiesinvolvingtensofthousands district-to-state and state-to-country hops in a national election. ofconcurrentvirtualvotingsessionsareneededtocharac-Theupperprotocollayers—TLS/SSLandMQTT—are terise system behaviour under realistic election-day loads and network-layer agnostic and do not require modification.

toidentifyanysaturationpointsintheSDNcontrolleror Distance voting is supported through a two-step relocation blockchainconsensussubsystems.IntegrationofGSM/LTEprocedure.Avoterwhocannotattendtheirregisteredboothcommunicationforint erlevellinksmustbevalidatedwithnotifiestheelectionauthorityinadvance.Theauthorityuprespecttobothperformanceandprotocolcorrectn essunder dates the district blockchain to temporarily remove the voter variable cellular network conditions. The ECC-based crypto-fromtheirhomeboothregistryandcreatesatime-limited graphic suite should be evaluated against post-quantum alter-entryatthedesignatedremotebooth.Thisensuresthatthe natives—suchaslattice-basedkeyencapsulationmechanisms 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 algorithmsbyfuturequantum-capableadversaries.Finally,a the original and remote district nodes. user-studyevaluationofthevoter-facingEVMinterfaceand In connectivity-impaired areas, EVMs operate with an en-the biometric authentication flow is essential before national-cryptedlocalbufferthataccumulatesvotesuntilnetwork
scaledeployment,asusabilitybarriersattheboothlevel directlyaffectvoterparticipationratesandthelegitimacyof the electoral outcome.

REFERENCES

[1] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "DVTChain: Ablockchain-based decentralized mechanism to ensure the security ofdigitalvotingsystem,"JournalofKingSaudUniversity–ComputerandInformationSciences,vol.34,no.9,pp.6855–6871,2022.
[2] S. A. Latif et al., "AI-empowered, blockchain and SDN integrated secu-rity architecture for IoT network of cyber physical systems," ComputerCommunications, vol. 181, pp. 274–283, 2022.
[3] V. Sharma et al., "Blockchain-based e-voting with enhanced voterprivacy," Proc. Int. Conf. on Information Security and Cryptology, 2022.
[4] R. Kumar et al., "Secure IoT-based voting system with biometricauthentication," Proc. IEEE Int. Conf. on Communication Systems andNetwork Technologies, 2022.
[5] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "FMDADM: A multi-layer DDoS attack detection and mitigation framework using machinelearningforstatefulSDN-basedIoTnetworks,"IEEEAccess,vol.11,
[6] pp.28934–28954,2023.
[7] M. Aldossary, "Multi-layer fog-cloud architecture for optimizing theplacementofIoTapplicationsinsmartcities,"Computers,Materials& Continua, vol. 75, no. 1, pp. 633–649, 2023.
[8] S. W. Turner, M. Karakus, E. Guler, and S. Uludag, "A promisingintegration of SDN and blockchain for IoT networks: A survey," IEEEAccess, 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 ofAutonomous 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: Amulti-level blockchain-assisted SDN-based IoT architecture for securede-voting system," IEEE Transactions on Network Science and Engineer-ing, vol. 12, no. 3, pp. 1613–1622, May/Jun. 2025.
[12] K. Zhang et al., "Transparent blockchain-based voting with immutableaudit 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," WirelessPersonal 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.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



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)