Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Blockchain-Based Secure Voting System with Integrated Complaint Management Portal

Lalithambikai S
Department of Information Technology
Knowledge Institute of Technology
Tamilnadu, India

Kavinkumar R
Department of Information Technology
Knowledge Institute of Technology
Tamilnadu, India

Sowndariya K
Department of Information Technology
Knowledge Institute of Technology
Tamilnadu, India

Barath M
Department of Information Technology
Knowledge Institute of Technology
Tamilnadu, India

Dharani M
Department of Information Technology
Knowledge Institute of Technology
Tamilnadu, India

***Abstract*—While digital shifts have radically redefined modern governance and civil operations, the practice of casting ballots electronically continues to grapple with persistent obstacles concerning data transparency and operational robustness. Conventional, centralized digital voting systems typically harbor singular vulnerability points that attract cyber offensives, compounded by a distinct lack of mechanisms to rapidly manage arising voter concerns. In response to these pressing flaws, this study introduces a multifaceted architecture merging distributed ledger technologies with an intelligent, machine-learning-driven grievance resolution interface. Specifically, our model leverages a decentralised blockchain framework for immutable ballot storage, ensuring that individual vote modifications are virtually impossible and establishing a trustless verification environment devoid of centralized oversight. graphic hashing, this schematic aims to seamlessly preserve data fidelity and supreme voter anonymity. Our comprehensive investigation of these distributed consensus rules and AI-guided triage methods indicates that unifying rigid cryptographic ballot handling together with responsive, automated complaint mechanisms dramatically elevates overall electoral resilience while reinforcing public faith in democratic workflows.**

***Index Terms*—Blockchain, Electronic Voting, Cryptography, RSA Encryption, Complaint Management, Machine Learning, Decentralized Networks.**

I. Introduction

Elections represent a cornerstone of democratic societies, granting populations the authority to shape administrative trajectories and public legislation. Consequently, safeguarding the integrity and visibility of these procedures is fundamental to maintaining citizen trust in government institutions. Recently, an accelerated push toward digitized administration has amplified the necessity for sound, easily scalable digital voting alternatives [1]. Nonetheless, despite the swift progression of technology, global adoption of e-voting remains stifled by widespread public anxiety over potential data exploitation, unauthorized monitoring, and system fraud. Conversely, legacy paper-driven polling—while physically verifiable—entails immense logistical burdens, is susceptible to human calculation errors, and routinely disappoints the electorate due to sluggish result tabulation [2]. Consequently, scholars have increasingly investigated decentralized ledger innovations, specifically blockchain architectures, to pioneer transparent and immutable voting infrastructures that prevent unauthorized data manipulation entirely.

Equally vital to any robust election framework is its capacity to properly adjudicate disputes and real-time voter complaints. Historically, grievance resolution has depended heavily on manual bureaucratic paths, demanding substantial human intervention and systematically resulting in delayed mitigations or effectively marginalized voters. Amid major national polls, hardware failures or reported coercion incidents can severely bottleneck conventional support hotlines. Contemporary digital service networks already encounter enormous strain when attempting to address mass user feedback efficiently [3]. Absent a coherent, automated apparatus for processing such grievances promptly, even the most impenetrable cryptographic voting networks risk alienating their user base. Citizens facing technical hurdles demand a clear, transparent, and instantly trackable avenue to file their issues, enabling governance bodies to swift neutralize localized disruptions before they degrade the broader legitimacy of the event.

Despite the availability of conceptual secure-voting blueprints, numerous existing implementations fall short of contemporary democratic needs due to glaring structural faults. Primarily, dominant electronic voting forms still lean on centralized server arrangements, making them inherently weak to targeted strikes or systemic outages [4]. Within these centralized setups, a singular successful breach or coordinated inside sabotage could quietly rewrite electoral histories without alerting the public. Secondly, available literature overwhelmingly dwells on the mathematical cryptography behind vote counting, largely ignoring the critical need for embedded dispute management layers. When digital polling platforms function without integrated live-complaint avenues, oversight authori-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

ties remain entirely unaware of localized system breakdowns, which blocks immediate corrective actions and corrodes public assurance.

II. Literature Review

Exploring decentralized election frameworks intertwined with algorithmic complaint-handling spans multiple scientific disciplines, notably applied cryptography, distributed network engineering, and semantic text analysis. The subsequent review synthesizes prior studies connected to our conceptual model, segmenting the literature into three thematic streams: the inherent flaws of legacy polling tactics, privacy-centric blockchain adaptations, and cutting-edge mechanisms for automated feedback interpretation.

Fig. 1. Traditional Electronic Voting Machine.

A. Issues in Traditional voting systems

Conventional paper-ballot strategies, along with server-centric digital platforms, have historically served as the primary vehicles for democratic decision-making. These methodologies, however, exhibit distinct weaknesses that arguably compromise electoral transparency. Physical voting necessitates enormous operational synchronization and painstaking manual oversight, drastically elevating the probability of tabulating errors and extending the timeline for result declarations [2].

Similarly, server-based digital voting generates profound cybersecurity anxieties. When ballot records reside on a singular cloud node or administrative server, the architecture is intrinsically exposed to catastrophic failures or hacking campaigns, potentially compromising the total dataset [4]. Furthermore, consolidating authority over demographic registries and incoming votes triggers valid doubts regarding the accountability of the administrative bodies supervising the event.

Another prominent hurdle plaguing legacy setups is the notoriously slow pace of aggregating final statistics. Disconnected manual audits and centralized validations stretch verification timelines, breeding confusion within the electorate and fostering generalized suspicion around the declared outcome [2]. Such administrative latency proves especially damaging to overall morale following sprawling, nationwide campaigns.

Moreover, safeguarding individual privacy while guaranteeing procedural transparency introduces complex paradoxes under a monolithic administrative entity. If all foundational data is held by a single party, the public is forced to implicitly trust those specific administrators. Acknowledging this, researchers forcefully advocate for distributed architectures designed to systematically offset the reliance on monopolized central agencies and inject mathematically provable fairness into the voting lifecycle.

B. Blockchain-Based Voting and Privacy Protocols

In pursuit of more resilient architectures, academics have turned to Internet of Things (IoT) paradigms and distributed ledgers. Blockchain constructs inherently supply a dispersed consensus mechanism that substantially boosts the auditability of electronic elections. By disseminating the ballot ledger uniformly across diverse geographic network participants, the technology successfully mitigates illicit data alteration. Still, realizing these decentralized ideals in full-scale societal elections poses distinct efficiency conflicts regarding cryptographic overhead and voter confidentiality [1]. Although standard consensus loops like Proof of Work and Proof of Stake frequently appear in literature, their intense computational demands render them suboptimal for massive electoral events. Consequently, newer proposals suggest adopting lightweight, hybrid proof algorithms specifically tuned to manage national-level polling constraints [9].

Within these dispersed computing models, 'self-tallying' protocols represent a compelling departure from standard hierarchical vote auditing. Here, the network collectively processes and publishes the final tally via automated cryptography without needing an overseer. This algorithmic calculation drastically refines transparency whilst eliminating traditional disputes over the post-election ballot opening and tallying phases [4].

Nevertheless, ensuring true voter anonymity remains a formidable puzzle precisely because distributed ledgers are designed for total transparency. To reconcile this, advanced studies advocate for 'collectively secure' dynamics where individual voters or distinct nodes act as fractional keepers of a shared secret. Techniques involving shared key generation and smart-contract execution allow the network to validate a vote's authenticity without unmasking its originator [5].

Collectively, these modernized cryptographic methodologies suggest it is entirely feasible to build election models that exhibit formidable privacy protections without sacrificing overarching verifiability. By weaving stringent security protocols directly into the ledger's fabric, engineers hope to pilot highly reliable voting solutions fit for tangible, high-stakes democratic environments [5].

C. Complaint Management System

Applying deep learning algorithms alongside NLP has radically optimized how modern systems parse user feedback.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

These AI-driven approaches ingest massive batches of unstructured text, systematically isolating recurrent themes to help organizations rapidly mitigate emerging dilemmas. Historically, similar semantic parsing was deployed during the 2011 Singapore Presidential Race to gauge shifting public attitudes on social media networks, although researchers acknowledged lingering risks regarding unpredictable digital sampling bias [6].

Current governance portals are frequently swamped by user comments, rendering manual grievance checks wholly impractical. To circumvent this bottleneck, engineers have proposed algorithmic pipelines utilizing techniques from TF-IDF term-weighting to XGBoost predictive classification. Implementing such architectures allows systems to autonomously rank and file issue reports, remarkably accelerating the triage phase and diminishing the need for human oversight [3].

An additional layer of complexity appears when parsing code-mixed dialects or hybrid phrasing, such as 'Hinglish', commonly utilized by diverse populations. Standard natural language analyzers predictably fail when confronted with intersecting linguistics. Modern transformer networks, however, powerfully address this limitation. Variations like HingRoBERTa demonstrate remarkable aptitude in deducing semantic context across mixed vocabularies, ensuring that hybrid user complaints are accurately digested and effectively classified [7].

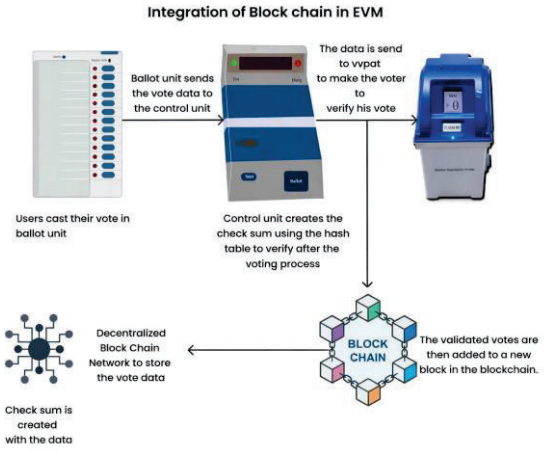

Fig. 2. Voting System Architecture.

Furthermore, in exceptionally nuanced fields like public finance, researchers have introduced multimodal complaint analyzers that evaluate simultaneous visual and auditory clues from video-based grievances. Specialized dual-encoder designs allow these systems to dynamically synthesize different forms of media, yielding highly accurate interpretations of the underlying user frustration [8].

In sharp contrast to prior conceptualizations that isolate either ledger security or NLP text routing, our blueprint tightly fuses blockchain-secured ballot recording directly with a smart, automated grievance interface. By uniting tamper-proof data storage with rapid-response problem parsing, this combined paradigm actively boosts both election security and the operational capacity to resolve voter difficulties.

III. Architectural Blueprint and Ledger Fabrication

Driven by the need for an impregnable yet highly accessible polling ecosystem, our methodology merges a dispersed blockchain backbone with an intuitive, machine-learning-supported issue tracking portal. This dual-pronged blueprint governs the entirety of the democratic cycle—from the initial cryptographic masking of voter identities to the incorruptible, final compilation of cast ballots and simultaneous mitigation of procedural anomalies.

Core architectural decisions were driven primarily by the ambition to dismantle centralized chokepoints, preserve absolute ballot anonymity, and facilitate lightning-fast grievance triage.

A. Distributed Ledger Core

The bedrock of this model is a decentralized blockchain network sustained by an array of distinct validation points, theoretically encompassing election monitors, regional polling hubs, and independent civic auditors. Subverting the standard centralized database model, our framework replicates the full ledger of cast votes across all active nodes, legally ensuring that no lone actor can unilaterally falsify histories. To optimize throughput without sacrificing structural security, the network embraces a streamlined, hybrid consensus algorithm engineered explicitly to navigate the intense computational load anticipated during national polling scenarios [1]. This tailored consensus rapidly authenticates and seals incoming ballot batches, maintaining exceptional responsiveness even during peak traffic windows.

Access to this network mandates a rigorous, decentralized identity-proofing stage before voters earn their cryptographic token. Through the application of advanced zero-knowledge proofs, our system confirms the legal standing of the participant without tethering their exact personal details to the transaction history, flawlessly meeting stringent privacy mandates [4]. Structurally, the identity verification tier is strictly alienated from the ballot transaction tier. Following authentication, the user engages primarily with an intuitive front-end interface that entirely masks the intricate cryptographic operations governing the transaction layer [5].

B. Vote Recording In Blockchain

The permanent storage of votes centers completely around self-enforcing smart contracts embedded within the ledger. The moment a voter confirms their choice, the terminal app encrypts the selection and compiles a secure network transaction. Following propagation through the peer-to-peer web, designated validator nodes apply the consensus protocol to ensure the token hasn't been double-spent. Upon successful authentication, the encrypted ballot is firmly cemented into a nascent block and securely chained to the existing sequence.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

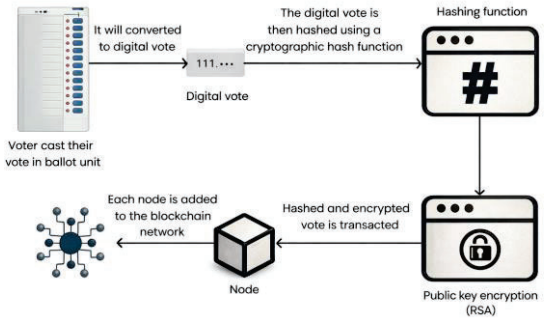

Fig. 3. Addition of each vote to the blockchain.

A defining characteristic of this transaction layer is the profound reliance on automated self-tallying mechanics. Centralized counting requires authorities to manually initiate decryption procedures, briefly creating an attack vector for malicious actors. Conversely, our self-executing framework is mathematically hardwired to aggregate encrypted submissions progressively [4]. Leveraging homomorphic principles or partitioned cryptographic keys, the ultimate results surface immediately when the voting window closes without selectively decrypting discrete inputs [5]. This elegant mathematical property guarantees supreme operational fairness and thoroughly eliminates post-election tally disputes, as the final values can be mathematically corroborated by any participating node.

C. Hash-Based Verification Sync

Synchronized hash validations act as the ultimate safeguard against in-transit data manipulation. Within our design, digital checksums are independently produced at both the user's local terminal and the ledger entry point to ascertain structural integrity. This cryptographic footprint guarantees that unauthorized intrusions are flagged instantaneously.

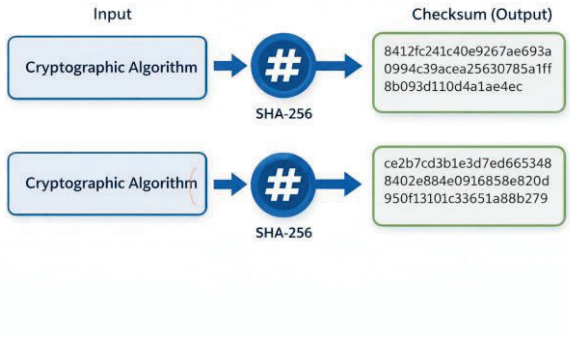

Fig. 4. Checksum verification process.

Initially, a primary checksum is fabricated at the localized voting booth the moment the ballot is formulated, utilizing SHA-256 or comparable hashing primitives. The one-way orientation of SHA-256 enforces high sensitivity to modification, meaning even a miniscule adjustment dramatically alters the resulting alphanumeric string. Concurrently, the distributed ledger module crafts a secondary checksum upon receiving the transaction block. Enforcing identical hashing subroutines across both hardware checkpoints mathematically links the pre-transmission state with the permanently stored record.

The actual authentication phase requires an automated comparison between the local terminal's checksum and the blockchain's newly minted footprint. Identical values firmly assure the network that no interference occurred during the packet's journey. Conversely, failing the checksum parity test instantly isolates and discards the affected transaction, blocking compromised data drops from polluting the election pool [9].

D. Infusion of the Grievance Subsystem

Running adjacent to the cryptographic ballot framework is a dynamic Complaint Management interface specifically scaled to absorb and parse voter issues immediately. Recognizing that sprawling demographics predictably yield immense volumes of unstructured commentary, our design fundamentally rejects sluggish manual routing as prone to oversight and bias [7].

To that end, the system embraces a bespoke machine-learning pipeline calibrated to decode textual grievances contextually. Should a voter face a systemic error—such as biometric sensor failures or targeted interference—they engage the dedicated portal to log their issue, seamlessly annexing critical trace metadata like precise node IDs or pseudo-anonymous participation hashes.

Subsequent to submission, advanced Natural Language Processing arrays—akin to those deployed in modern cyber-security threat sorting—scrub and digest the text [7]. Our multi-layered classifiers stratify these responses into actionable urgency buckets (e.g., 'Biometric Snag', 'Intimidation Tactic', 'Connectivity Drop') [3]. Priority alerts touching upon severe network breaches or physical coercion are instantaneously forwarded to emergency technical or security response modules. Establishing this live feedback loop guarantees that cascading administrative friction is resolved prior to causing widespread disenfranchisement.

IV. Theoretical Insights: Hashing Protocols And Secure Routing

The impregnability of this proposed blueprint is deeply anchored in precise cryptographic logic. The ensuing paragraphs outline the conceptual findings concerning data encapsulation, hashing dynamics, and asymmetric key exchanges necessary to guarantee absolute digital immutability [9].

In place of empirical field testing, these theoretical conclusions demonstrate how the interlacing of cryptographic primitives fundamentally nullifies traditional cyber-assault techniques.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

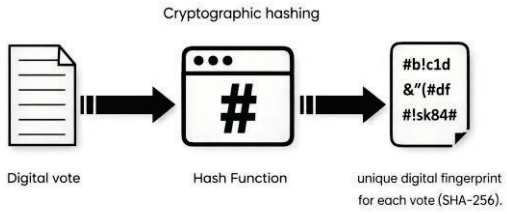

Fig. 5. Outline of cryptographic hashing.

A. Processing Each Block

Operating within our finalized architecture, each continuous ledger block acts as a permanent, timestamped snapshot of specific ballot transactions. The formation of a block initiates by gathering authenticated transactions temporarily resting in the network's processing queue.

Constructing the block's header involves merging vital variables: temporal stamps, randomized consensus nonces, the strict cryptographic hash of the antecedent block, and an all-encompassing Merkle root denoting the present batch of votes.

Adopting a Merkle tree topology stands as a paramount finding concerning operational scalability. Resolving individual transaction IDs recursively until a singular hash footprint remains enables Lightning-fast Simplified Payment Verification (SPV). This mathematical shortcut empowers everyday participants and monitoring bodies to independently prove a ballot's successful integration without requiring them to store the entire multi-gigabyte blockchain.

B. Mechanics of the Hashing Algorithm

Robust cryptographic mapping—led by the rigid SHA-256 framework—constitutes the foundational defense line of the system's ledger. Investigative analysis verifies that deploying SHA-256 supplies three vital protections: pre-image blocking, collision avoidance, and immense chaotic variance. Pre-image defenses guarantee that deciphering the original ballot from the public hash is mathematically unviable for hostile actors. Moreover, collision prevention ensures it is nearly impossible to artificially synthesize a fraudulent document matching an authentic block's hash footprint.

Critically, the pronounced avalanche effect dictating SHA-256 behaviors dictates that shifting merely one pixel or character in the input payload violently distorts the generated hash code. Throughout the voting lifecycle, all digital actions—spanning basic ballot casting to formal complaint submission—are strictly hashed and securely timestamped, forming a crystal-clear, unauditable sequence. Any malicious attempt by insiders or external entities to alter recorded ballots or suppress valid complaints will effortlessly trigger hash verification failures universally across the network, immediately freezing the compromise.

C. Asymmetric Shielding for In-Transit Ballots

To completely obfuscate ballot choices as they jump from local voter terminals to the broader network, our blueprint relies comprehensively on RSA (Rivest-Shamir-Adleman) public-key infrastructures [9]. RSA's formidable defense stems from the staggering computational difficulty associated with factoring incredibly large prime multiples. Within our theoretical scope, network administrators broadcast public keys for widespread user encryption, whereas the essential private decryption key undergoes complex algorithmic fragmentation across a cohort of trusted civic nodes [5].

During active voting, individual ballot preferences are transformed into undecipherable ciphertexts locally using this broadcasted key. Crucially, retrieving the plaintext is entirely impossible without cooperative key-assembly by the network's designated secret holders. Because encryption executes thoroughly at the physical terminal ahead of any internet routing, the submission fiercely repels packet sniffing and advanced MitM (Man-in-the-Middle) hijacking. Following ledger confirmation, the smart contracts mathematically tally these hidden values sequentially. This delicate integration of threshold RSA protocols practically guarantees that hostile servers and eavesdroppers remain entirely blind to specific ballot contents.

V. Discussion – Security Measures

Synthesizing an immutable ledger with an AI-guided complaint triage network represents a paradigm shift in modern democratic methodologies. This segment delves into the applied countermeasures deployed against mass cyber-intrusions, the transparent handling of disputes, and the overarching implications and developmental hurdles associated with decentralized governance.

A. Intrusion and Manipulation Prevention

The dispersed topology intrinsic to blockchain technology fundamentally short-circuits the standard attack vectors that routinely decimate centralized e-voting platforms. Traditional mainframes frequently succumb to sprawling Distributed Denial of Service (DDoS) campaigns, abruptly severing public access. By stark contrast, intentionally decentralizing the verification network drastically dilutes these attacks; forcefully disconnecting scattered polling hubs merely redirects traffic, guaranteeing zero-downtime ledger continuity.

Additionally, strict anti-Sybil mechanisms strictly enforce fairness. By obligating voters to fulfill zero-knowledge credential checks ahead of transaction engagement, automated spam botnets are decisively blocked from swamping the network [4]. Collectively spreading the 'secret keeping' responsibilities further ensures that verifying nodes do not wield unilateral power over the collected data, substantially reducing the likelihood of a coordinated internal compromise tearing down the election [5].

B. Complaint Verification and Tracking

Weaving deep learning complaint-handlers straight into the election portal cultivates unmatched levels of systemic accountability. Following submission, nuanced language arrays immediately dissect grievance descriptions to ascertain relative priority and specific themes [7]. Vitally, a distinct,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

cryptographically-sealed hash representing the complaint's receipt is published to an auxiliary ledger. This public-facing confirmation fundamentally destroys any capability for bureaucratic officials to quietly delete or ignore damning user feedback.

Operating via aspect-centric learning, the integrated AI routinely untangles convoluted user narratives—such as a solitary grievance highlighting both a software timeout and improper physical supervision—swiftly bifurcating the issues to distinct administrative departments [8]. Meanwhile, end-users retain an immutable ledger receipt to trace their case resolution dynamically. Merging blockchain inflexibility with rapid AI interpretation forces governing bodies to publicly, effectively, and swiftly navigate localized crises.

VI. Conclusion

This investigation proposes an advanced, comprehensive framework conceptualizing a decentralized digital election infrastructure fortified by a real-time, algorithmic complaint triage application. Diverting from the fragile, monolithic structures of past electronic implementations, this architecture utilizes rigid cryptographic hashing alongside RSA protections to facilitate supreme ledger immutability and complete voter shielding. Crucially, weaving automated, self-executing smart contracts directly into the tallying phase obliterates standard administrative processing lags and drastically cuts the margin for human-driven fraud.

Ultimately, bridging natural language intelligence with cryptographic voting bridges a crucial gap in legacy setups: resolving unformatted, chaotic user friction instantly. Sorting incoming grievances through AI drastically mitigates the marginalization of vulnerable voters and pushes continuous, live administrative accountability. Realizing nationwide deployment admittedly hinges on resolving prevailing challenges surrounding algorithmic impartiality and raw computational scale. However, intertwining ledger certainty with responsive, automated governance firmly maps an actionable route toward building resilient, digitally-native democracies perfectly calibrated for the modern technological landscape.

References

[1] Kiashemshaki, Kiana, Chukwuani, Elvis Nnaemeka, Torkamani, Mohammad Jalili, Mahmoudi, Negin, "Secure and Scalable Blockchain Voting: A Comparative Framework and the Role of Large Language Models," 2025. https://arxiv.org/pdf/2508.05865v2

[2] Bulut, Rumeysa, Kantarcı, Alperen, Keskin, Safa, Bahtiyar, S¸ erif, "Blockchain-Based Electronic Voting System for Elections in Turkey," 2019 4th International Conference on Computer Science and Engineering (UBMK) (2019) 183-188, 2019. https://doi.org/10.1109/UBMK.2019.8907102

[3] C, Venkatesh, Oberoi, Harshit, Pandey, Anurag Kumar, Goyal, Anil, Sikka, Nikhil, "RE-GrievanceAssist: Enhancing Customer Experience through ML-Powered Complaint Management," 2024. https://arxiv.org/pdf/2404.18963v1

[4] Li, Yannan, Susilo, Willy, Yang, Guomin, Yu, Yong, Liu, Dongxi, Guizani, Mohsen, "A Blockchain-based Self-tallying Voting Scheme in Decentralized IoT," 2019. https://arxiv.org/pdf/1902.03710v1

[5] Li, Zhuolun, Sonmezler, Haluk, Shirazi, Faiza, Shaji, Febin, Mroczkowski, Tymoteusz, Lardner, Dexter, Camus, Matthew Alain, Pournaras, Evangelos, "Are Voters Willing to Collectively Secure Elections? Unraveling a Practical Blockchain Voting System," 2025. https://arxiv.org/pdf/2510.08700v1

[6] Choy, Murphy, Cheong, Michelle L. F., Laik, Ma Nang, Shung, Koo Ping, "A sentiment analysis of Singapore Presidential Election 2011 using Twitter data with census correction," 2011. https://arxiv.org/pdf/1108.5520v1

[7] Rani, Nanda, Singh, Divyanshu, Saha, Bikash, Shukla, Sandeep Kumar, "Automated Classification of Cybercrime Complaints using Transformer-based Language Models for Hinglish Texts," 2024. https://arxiv.org/pdf/2412.16614v1

[8] Das, Sarmistha, Mujavarsheik, Basha, Lyngkhoi, R E Zera, Saha, Sriparna, Maurya, Alka, "Deciphering the complaint aspects: Towards an aspect-based complaint identification model with video complaint dataset in finance," 2025. https://arxiv.org/pdf/2503.00054v1

[9] A. Gomathi, P. Sachidhanandam, R. Kavinkumar, K. Sowndariya, P. Sanju, and R. Ram Kumar, "Blockchain Technology in Secure Voting Systems: Enhancing Transparency and Trust," 2024. https://ieeexplore.ieee.org/document/10860165