Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DIGITAL TOOLS FOR MONITORING THE ELECTORAL PROCESS IN UKRAINE UNDER MARTIAL LAW

OLEKSANDR HRYHORIEV[1], LIUDMYLA PAVLOVA[2], OLENA KARCHEVSKA[3], GANNA MALKINA[4], ALINA VOICHUK[5]

[1]Postgraduate Student, Private Higher Educational Establishment «European University», Department of Information, Library, Archival Affairs and Socio-Political and Humanitarian Discipline, Ukraine

[2]Associate Professor, Volodymyr Dahl East Ukrainian National University, Faculty of Law, Department of Economic Law and Socio-Political Discipline, Ukraine

[3]Associate Professor, Volodymyr Dahl East Ukrainian National University, Faculty of Law, Department of Economic Law and Socio-Political Disciplines, Ukraine

[4]Professor, Taras Shevchenko National University of Kyiv, Faculty of Philosophy, Department of Political Sciences, Ukraine

[5]Assistant, Taras Shevchenko National University of Kyiv, Faculty of Philosophy, Department of Political Sciences, Ukraine

E-mail: [1]oleksandrlawenu@gmail.com, [2]pavlovaliudmyla_vdeuu@gmail.com, [3]karchevskaolenavdeunu@gmail.com, [4]gannamalkinaknudps@gmail.com, [5]alinavoichukknu@gmail.com

ABSTRACT

Relevance of the research
The relevance of the study is determined by the need to ensure electoral integrity, traceability, and trust in digital voting procedures under martial law and an increased level of cyber threats.
Aim of the research
The aim of the research is the formalization of a digital voting framework to ensure transparency and electoral integrity under martial law through the integration of legal, technical, and organizational solutions.
Research methods
The research employed the following methods: structural-functional analysis, comparative law, typology and cluster grouping, technological classification and ranking, cross-validation functional modelling, Unified Modelling Language (UML) modelling.
Obtained results
The study formalizes a framework for digital will expression relevant to martial law restrictions. Structural-functional analysis and comparative law identified critical threats (security, regulatory, cognitive), while cross-validation modelling identified digital technologies with maximum compensatory potential (blockchain, e-/i-Voting, audit trail). The proposed UML architecture provides multi-level authentication, traceable verification, and civic oversight, which guarantees electoral integrity and regulatory validity in times of crisis.
Academic novelty of the research
The academic novelty of the study is the stratification of electoral threats under martial law and the formalization of a framework for digital expression of will, which integrates multi-factor authentication, blockchain storage, traceological audit, and citizen oversight, ensuring the stability of procedures, the legitimacy of results, and the autonomy of subjects of will declaration.
Prospects for further research
Prospects for further research include launching a controlled pilot project to implement a digital will declaration framework in a limited jurisdiction with subsequent validation of its operational stability, regulatory compatibility, and behavioural integrativity. Based on the results of the testing, it is appropriate to develop adaptive optimization modules aimed at increasing cyber resilience, minimizing transactional load, and ensuring institutional scalability.

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Keywords: *Digital Suffrage Framework, Blockchain Voting Architecture, Multi-Factor Authentication (MFA), End-to-End Verifiability (E2EV), Smart Contracts, Legal Compliance Modelling, Civic Audit Infrastructure.*

1. INTRODUCTION

The transformation of electoral processes by digital technologies attaches strategic importance to the problem of preserving electoral integrity, especially under martial law, which generates extraordinary risks of political destabilization, cognitive manipulation, and legitimization erosion. Digital will declaration requires not only technological modernization, but also an institutional redesign of the architecture of trust that integrates the principles of transparency, subject verifiability, regulatory compliance and operational resistance.

The relevance of this research is determined by the need for a unified framework capable of reducing security, legal, and techno-social threats through formalized stratification of electoral infrastructure elements. In view of the growing use of decentralized technologies (blockchain, smart contracts, multi-factor authentication) and increasing demands for civic oversight, there is a need for a systematic conceptualization of such approaches to ensure democratic legitimacy during crisis regimes of statehood.

The aim of the study is to formalize a conceptual framework for digital will declaration, capable of ensuring electoral integrity, transparency, and subject responsibility in extraordinary political circumstances, in particular under martial law, by integrating legal, technological, and organizational solutions into a single architectural model.

Research objectives:

- Perform a structural-functional decomposition of the electoral process with identification of vulnerabilities of components to security, regulatory, and cognitive threats.
- Perform a comparative law assessment of compliance with international standards (the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights (ECHR), CDL-AD opinions) by comparing with cases of electoral distortions.
- Build a typological cluster model of threats to electoral infrastructure with a hierarchy by risk categories.
- Conduct a classification and ranking of digital monitoring technologies according to the criteria of verifiability, tamper-resistance, scalability, and legal compliance.
- Develop a functional cross-validation matrix of compliance of technological solutions with threat types based on their compensatory potential.
- Formalize the synthesized framework of digital will expression using UML diagrams for visualization of architecture, interactions and behavioural scenarios in a crisis context.

2. LITERATURE REVIEW

Key Terms:

Electoral integrity – a systemic condition ensuring legality, transparency, verifiability, and resistance of electoral procedures to manipulation or coercion, aligned with international democratic standards (ICCPR, ECHR, OSCE).

Electoral sovereignty – the state's capacity to independently organize elections and safeguard citizens' right to vote under extraordinary political or security circumstances.

Digital enfranchisement – the use of electronic and online platforms (e-Voting, i-Voting) to expand accessibility, inclusiveness, and participation of citizens, including displaced populations.

Blockchain registers – distributed ledger infrastructures that guarantee tamper-resistance, immutability, and cryptographic verifiability of electoral transactions.

Risk-Limiting Audit (RLA) – a statistical post-election procedure designed to verify electoral outcomes with minimal sampling, ensuring evidence-based confidence in results.

Civic audit – participatory monitoring by citizens and NGOs through digital platforms, providing oversight, anomaly detection, and additional transparency.

Resilience of electoral infrastructure – the capacity of electoral systems to maintain operational validity, legal legitimacy, and functional continuity under multi-vector threats (security, legal, informational, legitimacy).

The organization of electoral processes under martial law and the implementation of digital monitoring tools remain isolated research areas. The lack of integrated approaches to digital verification of electoral procedures under emergency legal regimes indicates a methodological vacuum and necessitates a comprehensive analysis.

In particular, authors [1] identified a structural problem, who demonstrated the dominance of the executive vertical and parliamentary institutional subjectivity, which complicates the implementation of electoral sovereignty under martial law. Despite the partial erosion of parliamentary functionality and trust, the established stable model of intergovernmental interaction creates the prerequisites for a limited but potentially manageable restoration of electoral procedures under martial law.

Researchers [2] found the same institutional deformation, stating that the electoral process was controlled by the bureaucratic military system under latent martial law, as well as political and institutional instability. The dominance of undemocratic actors caused the institutional encapsulation of electoral procedures and the systemic desubstantialization of electoral legitimacy.

The destruction of state institutions is also found in the results of authors [3], who determined that the organization of the electoral process underwent functional destabilization and loss of procedural neutrality under martial law and nationalist polarization. The escalation of conflict between elites stimulated the instrumentalization of electoral mechanisms for political revanchism and delegitimization of democratic competition.

At the same time, researcher [4] proved that the organization of the electoral process lost its institutional autonomy in the conditions of political polarization and martial law, becoming an object of forceful usurpation pressure. The militarization of state administration led to the suspension of electoral legitimation and the establishment of an anti-democratic emergency regime.

Authors [5] pointed to the main problem, proving that the organization of the electoral process under martial law required constant electoral securitization and preventive neutralization of risks at all stages of the electoral cycle. The functioning of electoral procedures was ensured through the operational involution of force agents in the protection of electoral infrastructure and subjects to the electoral process.

At the same time, the scientometric horizon demonstrates the development of digital technologies for monitoring electoral processes. In particular, Researchers [6] showed that the Election Transparency technology functioned as a digital monitoring tool with a log-oriented architecture that provided public registration, decentralized storage, and collaborative verification of electoral data. The use of transparency logs increased the traceability of electoral events, minimized the risks of manipulation, reduced the costs of post-election audit and re-validation of results.

Authors [7] proposed a similar solution. They proved that the Smart Voting System, built on a combination of machine learning (ML), computer vision and blockchain-based registration, acted as a cyber-physical monitoring module with automated detection, validation, and traceology of electoral actions. The integration of multimodal authentication, adaptive accessibility, and cryptographic non-repudiation ensured the integrity, inclusiveness and operational stability of the electoral process at the level of local electoral centres.

Researchers [8] investigated a separate tool in detail, demonstrating that blockchain-based monitoring tools provided decentralized validation, cryptographic invariance, and biometric identification of subjects of will declaration. The implementation of non-repudiation mechanisms and a distributed registry increased electoral traceability and resilience to institutional compromise. Authors [9] demonstrated the effectiveness of comprehensive supporting solutions . They proved that integrated ICT monitoring tools built on multifactor authentication, encryption, and real-time provided electoral validation, transparent aggregation of results, and public traceability. The use of a web-based architecture with analytical visualization increased transparency, reducing the risks of fraud and counting delays.

However, there are problems with the use of new technologies. In particular, authors [10] found that digital election monitoring tools increased transparency and accountability, but remained vulnerable to cyberinterference, algorithmic opportunism and digital stratification in the context of a state of emergency. Limited regulatory congruence and a lack of techno-ethical verification reduced their effectiveness as mechanisms of electoral accountability.

The generalization of the reviewed publications indicates a structural dichotomy in the academic field. On the one hand, studies on the organization of the electoral process under martial law are distinguished, which recorded the dominance of the executive vertical, the functional erosion of parliamentary subjectivity, the securitization of electoral procedures, and the institutional encapsulation of will declaration. On the other hand, a cluster of studies on the implementation of digital monitoring tools (blockchain, log-oriented systems, non-repudiation protocols, biometric validation, cryptographic traceology, real-time aggregation) that increase procedural transparency, aggregate invariance, and operational stability of electoral systems in stable political and legal conditions is outlined. At the same time, there are no studies that integrate these vectors and demonstrate the possibility of using digital monitoring infrastructure to ensure electoral legitimacy in terms of military securitization. Such methodological asymmetry between the technological monitoring infrastructure and the legal regime of securitization of the electoral sphere justifies both the epistemological novelty and the applied relevance of this study.

3. METHODS

3.1. Research design.

The study was conducted according to a phased scheme - Figure 1.

Figure 1. Phased research design

Source: developed by the authors

3.2. Methods.

The study applied a number of complementary methods for a comprehensive risk assessment and modelling of the digital framework for will declaration under martial law:

1. Structural-functional analysis was used to decompose the electoral process into key components (authentication, administration, verification) and assess their vulnerability to security, regulatory and cognitive threats.

2. Comparative law was employed to compare international norms (ICCPR, ECHR, CDL-

AD) with identified cases of electoral distortions, which allowed for the verification of the degree of violation of basic standards of democratic will declaration.

3. Typologization and clustering was used to build a hierarchical model of threats with a division into security, information, procedural, socio-legal, and legitimation categories (Table 3), which ensured semantic consistency of subsequent cross-validation.

4. Technological classification and ranking was used to evaluate digital monitoring solutions according to the parameters of verifiability, tamper-resistance, scalability, and legal compliance (Table 4), which allowed to identify tools with the highest compensatory potential.

5. The cross-validation functional modelling was used to build a matrix of relevance of technologies to threat types (Table 5) in order to compare the functional capabilities of tools with risk profiles.

6. UML modelling (component, sequence, and precedent diagrams) was used to formalize the synthesized framework of digital will declaration (Figures 2–4), which provided visualization of the architecture, interaction logic, and behavioural scenarios of subjects in a crisis environment.

These methods provided systematic stratification of threats, empirical validation of countermeasure tools, and the construction of a normatively oriented digital architecture with high institutional interoperability.

3.3. Sample.

A systematic identification of digital technologies used to monitor electoral processes in the public, procedural, and institutional dimensions was carried out as part of the sampling. Particular attention was paid to the mechanisms of application of digital tools, the legal regulation of their use, as well as judicial practice that reveals legal conflicts in the context of electoral transparency, legitimacy, and cybersecurity (Table 1).

Table 1. Sample of digital technologies for monitoring the electoral process

Technology	Description and mechanism of application	Legal regulation	Court conflict / precedent	Academic research
Log-oriented transparency logs	Cryptographically secure public transaction log architecture with collaborative verification and traceology	Draft General Data Protection Regulation (GDPR) (EU, 2016); OSCE/ODIHR (2010) recommendations for open monitoring	—	Dommett, Luke & Gordon [11]
Blockchain platforms (non repudiation)	Distributed vote register with digital signatures, consensus transaction validation, data invariance	E-IDAS Regulation-EU (2014); Estonian Election Act (2005, Estonia) from mix-net tally	—	Ohize et al. [12]
Biometric identification	Voter verification via fingerprints, facial recognition at the entrance and during vote registration	GDPR (EU, 2016); Malaysia PDPA (2010)	Case law: Rideout v. Gardner (2016, USA, First Circuit struck bans on ballot selfies)	Omoze, Omaji & Edegbe [13]
Mob-apps for ballot selfies	Ballot photo for crowd voting transparency via social media	State laws (NY 1890; Michigan ban lifted 2019)	Silberberg v. BOE (2017, USA) — confirmation of registration ban	Stojanoski & Vukovich [14]
Computer Vision + ML Analysis	Automated ballot counting, anomaly detection,	NIST SP 800-207 (USA, 2021) — Zero Trust;	—	Usharani [15]

Technology	Description and mechanism of application	Legal regulation	Court conflict / precedent	Academic research
	statistical forensics	Verified Voting Standards (USA, 2018)		
Multi-factor authentication	2FA + crypto token for access to electronic voting	e-IDAS (2014, EU); NIST SP 800-63B (2017, USA)	—	Vedantam, et al. [16]
Real-time dashboards	Real-time visualization of results, open data access	Freedom of Information Act (USA, 1967+); Open Data Act (EU, 2019)	—	Kargbo & Turay [17]
Citizen-reporting platforms (Uchaguzi, FAFEN)	Crowdsourcing of violation reports, GPS metadata, photos	Kenya Election Observers Act (2013); Pakistan ECP regulations (2017)	—	Bhanye & Shayamunda [18]
Post-election audit (RLAs)	Selective verification of results with VVPAT or paper ballots	RLA legislation (USA, 2010-til now)	—	Koza [19]
e-voting / i-Voting (Estonia)	Online voting with end-to-end verifiability, mix-net tally	Estonian Internet Voting Act (2005); OSCE/ODIHR recommendations (2007, 2011)	Client hacking incident with programmer sparks legal proceedings and credibility assessment 2011 2019	Marouan, et al. [20]
Electronic voting machines	Computers without paper trails	Help America Vote Act (2002, USA); Verified Voting Standards	Shelby Advocates v. SAVE (2020, Tennessee) — the court recognized the vulnerability of computers	Alown, Kiraz & Bingol, [21]
Federal election observers (digital + analogue)	Ground and digital monitoring by observers	Voting Rights Act (1965, USA)	Missouri v. DOJ (2024) – states' objections to digital/federal watchdogs	Wagner [22]

Source: developed by the authors

The sample analysis (Table 1) proves that modern digital technologies (cryptographic journals, blockchain, biometrics, AI, dashboards, citizen-reporting) have the potential for electoral verification and traceology. However, their integration into the electoral process in the legal field is still limited by the lack of specialized norms and clear judicial precedents. This determines the relevance of research aimed at adapting digital tools to the emergency or war.

3.4. Instruments.

PlantUML [23] was used as an ontological modelling tool to visualize the component architecture of a synthetic framework for digital will declaration. Its use provided the formalization of structural and functional dependencies between agents, transaction modules, and verification subsystems in the form of UML diagrams (Class, Component, Sequence, Deployment). PlantUML ensured traceability, machine readability and semantic coherence of the model thanks to its declarative notation and compatibility with CI/CD.

4. RESULTS

Under martial law, electoral processes are subject to multi-vector influence of risk factors that

cause functional destabilization of the will declaration mechanisms. The systematic analysis of threats and legal distortions was carried out for a sample of challenges, which includes institutional, legal, security, informational, and cognitive components relevant to the violation of electoral sovereignty in the conditions of an emergency legal regime – Table 2.

Table 2. Analysis of threats to the electoral process under martial law

Challenge name	Threats to the will declaration process	Violation of legal norms	Political consequences	Historical precedents
Suspension of electoral procedures	Cancellation or postponement of the electoral cycle, violation of the principle of the election interval	ICCPR (1966), Art. 25(b); Venice Commission's Code of Good Practice (2002), Principle 6	Delegitimization of mandates, erosion of constitutional legitimacy	Mali, 2020; Burkina Faso, 2022
Militarization of electoral administration	Institutional replacement of the Central Election Commission (CEC) by executive and power agencies	Venice Commission, CDL-AD(2002)023rev	Usurpation of election administration, reduction of civilian control	Egypt, 2013; Thailand, 2014
Securitization of electoral infrastructure	Direct involvement of armed forces in the protection of polling stations, risk of violent pressure	Declaration on Criteria for Free and Fair Elections (2002), §4	Shift towards authoritarian proceduralization, imitation of electorality	Belarus, 2020; Iran, 2009
Threat to the lives of voters and administrators	Forced refusal to participate, creation of existential danger	GDPR (1948), Art. 3; Geneva Conventions (1949)	Erosion of mass participation, destruction of voter subjectivity	Iraq, 2005; Syria, 2012
Information destabilization	Systemic manipulation of voters' cognitive attitudes, spread of disinformation	OSCE, Copenhagen Document (1990), §7.8	Violation of the principle of conscious will, delegitimization of the campaign	Росія, 2022; Філіппіни, 2022
Restrictions on IDP participation	Territorial inaccessibility of the electoral procedure, loss of electoral rights	UN Guiding Principles on Internal Displacement (1998), §22; ECHR, Article 3 of Protocol No. 1	Systemic exclusion of marginalized groups	Syria, 2012; Congo, 2006
Media censorship	Limitations of independent information, monopolization of electoral discourse	ECHR, Art. 10; UNESCO Declaration (1991)	Erosion of the public sphere, demobilization of critical electorates	Turkey, 2016; Russia, 2022
Lack of international monitoring	Lack of external verification of the electoral process	UN Declaration on Democratic Elections (2005), §3	Loss of external legitimacy, non-recognition of results	Belarus, 2020; Russia, 2022
Intimidation of process participants	Psychological coercion, threat of violence, repressive influence on the will declaration	OSCE, Copenhagen Document (1990), §7.7	Self-reduction effect of participation, establishment of informal authoritarianism	Afghanistan, 2009; Venezuela, 2018
Legal indetermination of election status	Lack of clear regulation of elections under martial law	Venice Commission, CDL-AD(2007)012	Regulatory delegitimization of results, legal nullity of the	Cameroon, 2018; Libya, 2021

Challenge name	Threats to the will declaration process	Violation of legal norms	Political consequences	Historical precedents
			process	

Source: developed by the authors

The analysis of the identified challenges (Table 2) demonstrates the complex destruction of the electoral process under martial law, which is manifested through institutional inversion of administration, legal indeterminacy of procedures, securitization of infrastructure, cognitive manipulation, and erosion of basic guarantees of will declaration. Documented violations of international standards (ICCPR, ECHR, OSCE documents, Venice Commission) correlate with historical cases of loss of legitimacy, which confirms the need for formalized legal stratification of electoral activity under emergency regimes.

The next stage of the study involved a systematic typologization and hierarchical ranking of the identified challenges to the electoral process under martial law. A classification by threat type (security, regulatory and procedural, informational, socio-legal, legitimacy) was applied, taking into account the destructive potential for institutional stability, subject participation, and normative validity of the electoral cycle - Table 3.

Table 3. Hierarchical ranking (by threat level) and typology of challenges to the electoral process under martial law

Challenge name	Threat type	Description of damage and political consequences
Threat to the lives of voters and administrators	Security	Creation of existential threat, mass demobilization of the electorate
Securitization of electoral infrastructure	Security	Forcible control over the procedure, escalation of forced will declaration
Intimidation of process participants	Security	Repressive atmosphere, reduction of participation, delegitimization of democracy
Suspension of electoral procedures	Regulatory and procedural	Violation of the principle of interval, rupture of the mandate legitimacy cyclicality
Militarization of electoral administration	Regulatory and procedural	Usurpation of administration, elimination of institutional autonomy
Legal indetermination of election status	Regulatory and procedural	Lack of regulatory certainty, annulment of results
Information destabilization	Informational	Disorientation of the electorate, violation of the voter's cognitive autonomy
Media censorship	Informational	Erosion of public space, violation of the right to information
Restrictions on IDP participation	Socio-legal	Territorial segregation, exclusion of groups from the electoral process
Lack of international monitoring	Legitimacy	Loss of external trust, undermining of the recognition of results

Source: developed by the authors

The hierarchical typology of electoral challenges under martial law (Table 3) demonstrates the dominance of security threats that violate the principles of non-discrimination, free will, and the voter's subjective autonomy. The security priority in the destructiveness scale is accompanied by regulatory and procedural indeterminacy and information destabilization, which together pose the risk of systemic delegitimization of the electoral process.

The next stage of the study was the systematization of digital technologies for monitoring the electoral process by type of functional purpose and conditional effectiveness. The classification was based on evidence, cyber resilience, interoperability, scalability and regulatory compliance, taking into account the principles of electoral verification and transparency - Table 4.

Table 4. Hierarchical ranking (by level of conditional effectiveness) and typologization of digital technologies for monitoring electoral processes (under normal conditions)

Technology title	Type	Description of function/mechanism	Effectiveness rating*
Post-election audit (RLAs)	Post-factum audit	Statistical sampling and voter verifiable paper audit trail (VVPAT)	★★★★★
Blockchain platforms	Distributed registry infrastructure	A secure environment with consensus validation of votes and transaction provability	★★★★★
e-Voting / i-Voting (Estonia)	Electronic voting	An online platform with end-to-end verification and cryptographic protection	★★★★☆
Computer Vision + ML Analytics	Automated audit	Ballot anomaly detection, visual inspection, vote counting	★★★★☆
Log-oriented transparency logs	Cryptographic traceology	Public immutable transaction history with verification of administrator actions	★★★★☆
Biometric identification	Identification security	Voter verification by biometric markers (face, fingerprints)	★★★★☆
Multi-factor authentication	Cyber access identification	Login using 2FA or crypto tokens to increase cybersecurity	★★★☆☆
Real-time dashboards	Visualization analytics	Online data visualization for rapid response and verification	★★★☆☆
Citizen reporting platforms (FAFEN, Uchaguzi)	Crowdsourcing monitoring	Mobile evidence collection services, GPS, and photo capture of violations	★★★☆☆
Federal observers (digital/analogue)	Institutional oversight	Digital support of ground surveillance, photo/video capture	★★☆☆☆
Ballot selfies / mob apps	Civic monitoring	Voter self-reporting via photo ballot for transparency control	★☆☆☆☆
Electronic voting machines (without VVPAT)	Machine voting	Standalone voting devices without transparent audit	★☆☆☆☆

**★ — composite performance indicator (1–5 stars) consisting of the following parameters:*

- *verifiability of results*
- *tamper-resistance*
- *interoperability*
- *scalability*
- *regulatory compliance*

Source :developed by the authors

The hierarchical ranking of digital technologies for electoral monitoring (Table 4) showed the dominance of tools with a high level of verifiability, cryptographic invariance, and regulatory institutionalization (RLAs, blockchain, e-voting). Technologies with a low verifiability and legal validation (ballot selfies, EVM without VVPAT) show limited effectiveness in ensuring procedural legitimacy, which reduces their suitability for use as forensic or oversight mechanisms in the electoral process conducted under normal conditions. The next stage of the study was to conduct a cross-validation analysis of digital technologies for electoral monitoring in order to assess their relevance in neutralizing typical threats to the voting process under martial law. The typified technologies were correlated with the classified threats on a scale of conditional effectiveness (from minimal to high reduction potential), which enabled creating a formalized matrix of functional relevance - Table 5.

Table 5. Cross-validation matrix of the ability of digital technologies to monitor electoral processes to reduce threats of martial law to the will-expression procedure, ranked hierarchically in relation to the effectiveness rate

Digital technology	Threat to life	Securitization	Intimidation	Suspension	Militarization	Indef. status	Infodestabilization	Media censorship	Restrictions on IDPs	Lack of monitoring	∑★*
e-Voting / i-Voting (Estonia)	★★★	★★★	★★	★★★	★★	★★★	★★	★	★★★	★★	24
Citizen reporting platforms	★★	★★	★★★	★★	★★	★★	★★	★★	★★	★★	22
Blockchain platforms	★★	★★	★	★★★	★★	★★	★★	★	★★★	★★	20
Log-oriented transparency logs	★	★★	★★	★★	★★	★★	★★★	★	★	★	17
Post-election audit (RLAs)	★	★	★	★★★	★★	★★★	★	★	★	★	14
Real-time dashboards	★	★	★	★	★	★	★★★	★★★	★	★	13
Federal observers (digital/analogue)	★	★★	★★	★	★	★	★	★★	★	★★★	13
Biometric identification	★★	★★	★	★	★	★	★	★	★★	★	11
Multi-factor authentication	★★	★★	★	★	★	★	★	★	★★	★	11
Computer Vision + ML Analytics	★	★	★	★	★	★	★★	★	★	★	10
Ballot selfies / mob apps	★	★	★	★	★	★	★	★	★	★	10
Electronic voting machines (withut VVPAT)	★	★	★	★	★	★	★	★	★	★	10

** Explanation of the effectiveness scale:*

- *★ – minimal or indirect impact on threat reduction*
- *★★ – moderate effectiveness or contextual relevance*
- *★★★ – high potential for threat neutralization due to the functional specifics of the technology*

Source: developed by the authors

The cross-validation analysis (Table 5) showed that the most relevant risk reduction tools for the electoral process under martial law are technologies with a high level of cryptographic security, traceable verification, and institutionalized crowdsourcing. The integrated ranking demonstrates that e-Voting/i-Voting, citizen observation platforms, and blockchain registries have the highest potential to compensate for security, procedural, and legitimacy distortions due to their ability to be scalable verifiability, tamper-resistance, participatory oversight, and regulatory adaptability.

e-Voting/i-Voting technology reduces existential risks for voters through remote voting and increases inclusivity through accessibility for internally displaced persons, but is characterized by increased cyber vulnerability, lack of procedural

transparency, and dependence on critical infrastructure. Crowdsourcing citizen monitoring platforms enhance horizontal oversight and mobilize digital evidence, but have low ontological validation of messages, fragmented geographic coverage, and limited institutional relevance. Blockchain registries guarantee invariance and attestation of transactions in non-repudiation mode, but do not provide full identity verification and do not eliminate the risks of manipulation until the moment of voting. These limitations justify the need to develop a synthesized framework for digital will declaration that combines cryptographic integrity, distributed monitoring, and regulatory sanctioned modularity optimized for martial law: Figure 2 - Figure 4.

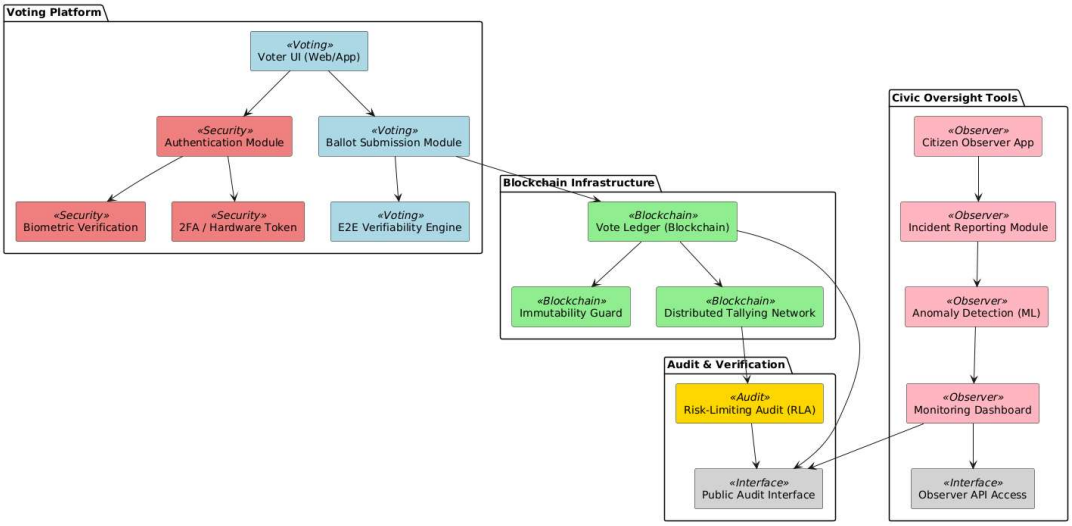

Figure 2. Ontological model (component diagram) of the synthesized framework for digital will declaration under martial law

Source: created by the authors in a modelling environment [23]

The component diagram (Figure 2) formalizes the synthesized framework for digital will declaration under martial law as a modular-stratified system with integrated subsystems of authentication, cryptographic vote capture, audit verification, and civic oversight. The architecture provides end-to-end verifiability, immutability, multi-level cyber-identification (MFA, biometrics), ML anomaly detection, and an open interface for civic audit, which cumulatively increases the system's resistance to martial law threats.

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

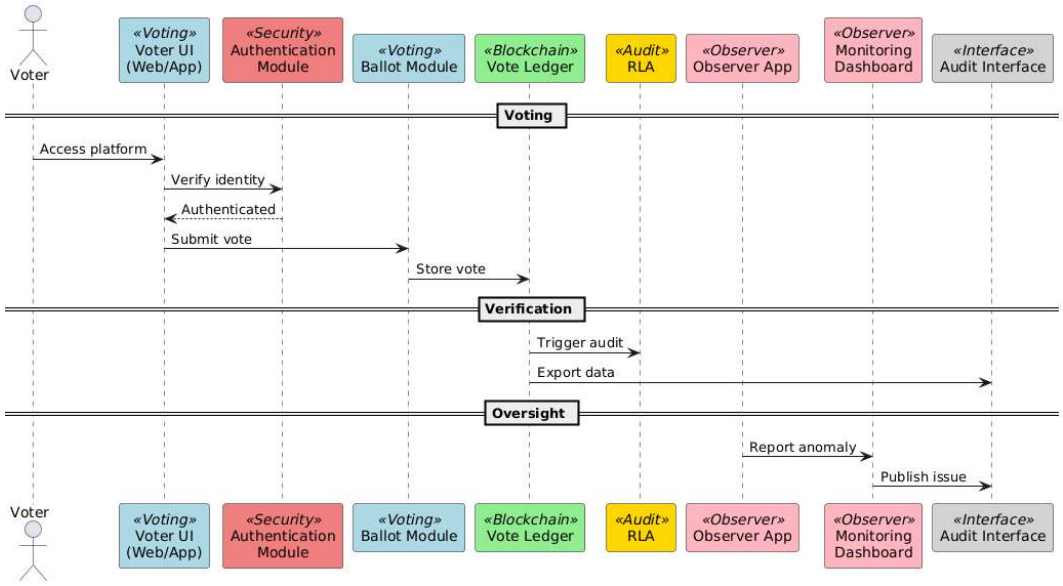

Figure 3. Ontological model (sequence diagram) of the synthesized framework for digital will declaration under martial law

Source: created by the authors in a modelling environment [23]

The sequence diagram (Figure 3) illustrates the compact integration of key components of digital voting, providing end-to-end transaction traceability (end-to-end verifiability), modular voter authentication, decentralized recording of voting data on a blockchain registry, and multi-source citizen oversight. The built-in interaction between Ledger, RLA, and Audit Interface forms a transparent verification chain, and the participation of the Observer Dashboard implements a context-sensitive violation detection mechanism, which increases the operational resilience of the system in crisis conditions.

Journal of Theoretical and Applied Information Technology
15th December 2025. Vol.103. No.23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

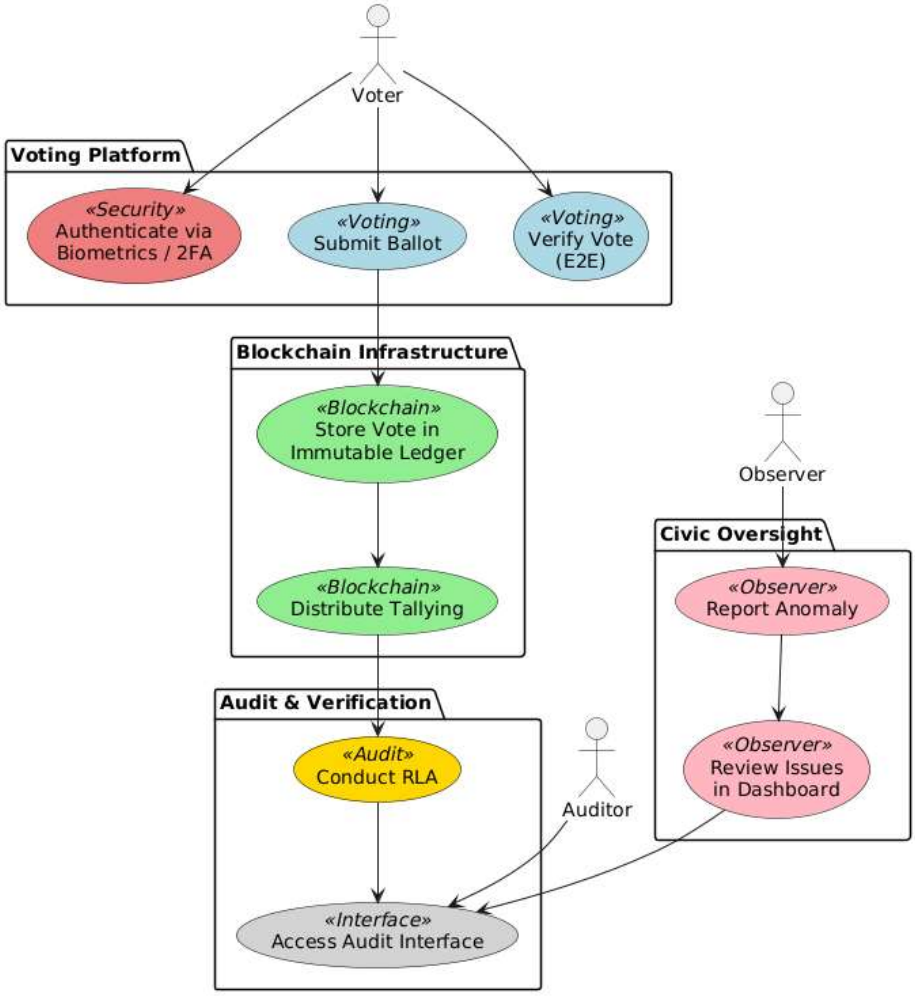

Figure 4. Ontological model (precedent diagram) of the synthesized framework for digital will declaration under martial law

Source: created by the authors in a modelling environment [23]

The use case diagram (Figure 4) formalizes the functional architecture of a synthetic framework for digital will declaration, where each use case represents a critical stage of interaction of subjects (voter, observer, auditor) with the subsystems of authentication, voting, blockchain storage, verification, and public monitoring. The integration of E2E verification, Risk-Limiting Audit (RLA) and decentralized ballot processing ensures traceability, non-repudiation, and trust in election results under military turbulence.

UML modelling of the synthesized digital will declaration framework for under martial law (Figure 2 - Figure 4) formalizes a holistic, stratified modular architecture that combines elements of multifactor authentication, blockchain-oriented vote storage, audit trail, algorithmic oversight, and open verification interaction. The use of component, sequence, and precedent diagrams reflects not only the structural composition, but also the logic of interaction between entities, subsystems, and services, which increases the interoperability, transparency, and operational resistance of the digital electoral process to security threats.

The implementation of the synthesized framework for digital will declaration under martial law forms the political and institutional legitimacy of the electoral process, minimizes the risks of delegitimization of results, strengthens trust in the electoral infrastructure, enhances the democratic stability of the regime, and creates a precedent for inclusive citizen participation under an emergency legal regime.

5. DISCUSSION

In the context of intensifying threats to digital electoral security and regulatory instability caused by martial law, the discursive analysis focuses on a comparative assessment of relevant models of digital will declaration. The aim is to verify the institutional relevance, functional resistance and regulatory compliance of the synthesized framework as a tool for stabilizing the electoral process under emergency legal regime.

Authors [24] empirically confirmed the effectiveness of a descriptive prototyping approach to developing a mobile application for e-voting in an institutional context, with an emphasis on interface, accessibility, and transparency. Instead, our study formalizes a high-level framework with multi-factor authentication, blockchain traceability and civic audit, relevant to martial law settings.

Researchers [25] focused on the regulatory stratification of political content and transparency of digital campaigning according to the DSA, TTPA and G-E–DSA requirements. In contrast, the synthesized framework of digital will declaration is oriented not only to regulatory compliance, but also to ensuring electoral integrity through multi-agent traceability, blockchain fixation and civic oversight in crisis political conditions.

Authors [26] proved that the perceived transparency of blockchain-oriented e-voting systems, according to the UTAUT2 model, is a key mediator between the user's cognitive-behavioural factors and the implementation intention. In the same study, transparency is implemented technically and functionally — through E2E-verifiability, audit trail, civic oversight and decentralized verification, which ensures institutional trust regardless of behavioural factors.

Researchers [27] demonstrated the effectiveness of a blockchain voting architecture based on the hybrid consensus HPBFTA, the HAHE cryptographic scheme, as well as the VEcSBP and CNN-based Threat Detection mechanisms. In contrast, our study focuses on architectural modularity, civic oversight, and legally traceable verification, shifting the emphasis from purely technical optimization to the regulatory and institutional resilience of the electoral process under martial law.

Authors [28] conceptualized blockchain as a techno-political guarantor of electoral integrity, promoting Ethereum 2.0 and smart contracts as tools for anonymity, verification, and decentralization. Our study extends this approach by formalizing a layered framework with MFA, audit trail, civic oversight, and algorithmic detection, focused on political stability under military turbulence.

Authors [29] presented a Blockchain-based Voting Mechanism (BVM) that integrates Zero-Knowledge Proof (ZKP) and Improved Master-key Administration (IMA) to provide authentication, integrity, and tamper resistance. This study extends this paradigm by modelling a comprehensive architecture with multi-level authentication, civic audit, ML analytics, and a traceable audit chain focused on elections under legal emergency.

Researchers [30] substantiated the context-dependent effectiveness of m-Participation, driven by political apathy, mistrust of institutions, and digital divide. This study synthesizes these findings by modelling institutionalized civic oversight as a structural element of a digital will framework with a focus on interoperability, transparency, and increased civic agency under martial law.

Authors [31] systematized the techno-social prerequisites for implementing a blockchain-based e-voting architecture, emphasizing the critical role of cryptographic security, consensus mechanisms, and regulatory compliance. Our study formalizes such a framework in the form of a stratified UML model that balances anonymity, ballot integrity, and trust in digital voting in the context of military turbulence.

Author [32] presented a blockchain-based digital voting model with biometric verification, smart contracts, and decentralized processing aimed at increasing institutional trust, scalability, and electoral integrity. In this study, these approaches are integrated into a UML-formalized framework with multifactor authentication, audit traceability, and civic oversight, which cumulatively increases the resilience of electoral infrastructure to security risks.

Researchers [33] developed a blockchain e-voting architecture for universities using smart contracts, a decentralized registry, and a secure UI that ensures transparency and procedural legitimacy. This study extends this approach to a crisis scale by integrating E2E verification, MFA, audit trails, and civic oversight to enhance institutional resilience.

The reviewed publications confirm significant progress in the technical and regulatory evolution of digital voting systems, with an emphasis on transparency, cryptographic security, behavioural acceptability, regulatory compliance, and procedural verification. At the same time, the

key difference of the proposed framework is its ability to reduce systemic risks caused by legal uncertainty and security turbulence of martial law by integrating multi-factor authentication, audit trail, civic oversight, and UML-stratified modularity as a political and institutional tool for stabilizing the electoral process.

6. LIMITATIONS

A limitation of the study is the lack of empirical validation of the synthesized framework in a real electoral cycle, which does not allow assessing its operational stability, techno-legal interoperability, and behavioural acceptability by the subjects of will expression. The study also does not cover modelling of scenarios for responding to contingent cyber threats and does not include a formalized assessment of the level of regulatory compliance in a cross-border context.

7. RECOMMENDATIONS

It is recommended to initiate a pilot controlled project of implementation of the digital will framework in a limited administrative environment in order to assess its functional stability, regulatory compliance, and behavioural adaptability. Based on the results of the testing, it is appropriate to develop optimization solutions aimed at increasing resistance to threats, reducing operational workload and ensuring institutional scalability.

8. CONCLUSION

In the context of martial law, the electoral process is subject to systemic destruction due to the combined effect of security, regulatory and procedural, informational and legitimization threats that violate the principles of interval, voluntariness, and non-discrimination of will declaration. The conducted hierarchical typologization of risks has shown the priority of security factors (existential threat, securitization, intimidation), which destabilize the functional subjectivity of the voter, delegitimize administrative procedures, and induce normative indeterminacy of results.

Cross-validation analysis of digital technologies has shown that the maximum potential for reducing identified threats is demonstrated by the combination of e-Voting/i-Voting, blockchain-based registries, and crowdsourcing monitoring due to their scalable verifiability, tamper-resistance, participatory oversight, and regulatory adaptability. The synthesized framework of digital will expression, modelled in the form of an ontological architecture, provides end-to-end traceability, decentralized authentication and institutionalized auditability, forming a technologically and normatively valid infrastructure for holding elections in times of crisis.

Academic novelty of the study. This study if the first time to provide a systematic stratification of electoral threats in the context of martial law with a formalized typology of their destructive potential in relation to subject autonomy, procedural validity, and legitimacy of will declaration. An ontologically formalized framework for digital will declaration is proposed with the integration of elements of multi-factor authentication, cryptographic storage, traceological audit, and citizen oversight, which ensures the resistance of the electoral infrastructure to multi-vector crisis influences.

Practical significance of the research results. The developed framework can be implemented as a model of adaptive electoral administration under the emergency legal regime, in particular through the institutionalization of e-Voting/i-Voting with support for blockchain fixation and civic audit. The obtained results enable the formation of regulatory protocols, technical standards, and risk-neutralization scenarios for electoral processes under military turbulence, while maintaining regulatory continuity, political legitimacy, and security stability of the will-expression procedure.

REFERENCES:

[1]. K. Pelchar, E.S. Herron, and G. Flikke, “Legislative–Executive relations in ukraine’s wartime conditions”, *PS: Political Science & Politics*, Vol. 58, No. 1, 2025, pp. 125–127. https://doi.org/10.1017/s1049096524000763

[2]. D.A.J. Butt, D.S. Ali, M.U. Shamim, and M.A.M. Raza, “Political instability and institutional interplay: A study of pakistan’s fragile democratic journey 1947-1969”, *Contemporary Journal of Social Science Review*, Vol. 3, No. 1, 2025, pp. 400-407. https://contemporaryjournal.com/index.php/14/article/view/321/276

[3]. J.E. Cho, and A. Hur, “The perils of south korean democracy”, *Journal of Democracy*, Vol. 36, No. 2, 2025, pp. 38–46. https://doi.org/10.1353/jod.2025.a954560

[4]. J. Lee, “Not too unrealistic a future of liberal democracy: A reflection on the self-coup attempt in south korea”, *The Political*

Quarterly, 2025. https://doi.org/10.1111/1467-923x.13539

[5]. A.C. Okoye, H.C. Ezeanya, and A.E. Chikezie, "Securing election processes: Interrogating the role of security agents in nigeria's elections", *African Journal of Social Sciences and Humanities Research*, Vol. 8, No. 1, 2025, pp. 61–74. https://doi.org/10.52589/ajsshr-cftnaono

[6]. L.T. Kimura, G. Fumagali, Y.R. Venturini, and M.A. Simplicio, "Election Transparency: Monitoring Elections with Transparency Logs-Brazil as a case study", *Authorea Preprints. TechRxiv,* Vol. 14, No. 8, 2025. https://doi.org/10.36227/techrxiv.174062888.82211159/v1

[7]. R. Sujatha, A.Naseem, S. Navabharathi, D. Thirukkumaran, and M.R. Prabakaran, "Decentralized smart voting system using blockchain and deep learning", in: *2025 international conference on intelligent computing and control systems (ICICCS).* Piscataway: IEEE, 2025, pp. 493–498. https://doi.org/10.1109/iciccs65191.2025.10985618

[8]. M.S. Peelam, G. Kumar, K. Shah, and V. Chamola, "DemocracyGuard: Blockchain-based secure voting framework for digital democracy", *Expert Systems,* Vol. 42, 2025. https://doi.org/10.1111/exsy.13694

[9]. I. Kona, and A.U. Imouokhome, "Real-time election voting and results display system (REVORDS)", *Journal of Electrical Engineering, Electronics, Control and Computer Science*, Vol. 10, No. 2, 2025, pp. 29-36. https://jeeeccs.net/index.php/journal/article/view/368\

[10]. J G. Asimakopoulos, H. Antonopoulou, K. Giotopoulos, and C. Halkiopoulos, "Impact of information and communication technologies on democratic processes and citizen participation", *Societies*, Vol. 15, No. 2, 2025. https://doi.org/10.3390/soc15020040

[11]. K. Dommett, S. Luke, and H.C. Gordon, "Making elections more transparent? Lessons from the implementation of digital imprints at the 2024 UK General Election", *Policy Studies*, 2025, pp. 1–24. https://doi.org/10.1080/01442872.2025.2482869

[12]. H.O. Ohize, A.J. Onumanyi, B.U. Umar, L.A. Ajao, R.O. Isah, E.M. Dogo, B. K. Nuhu, O. M. Olaniyi, J. G. Ambafi, V. B. Sheidu, M.M. Ibrahim, "Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges", *Cluster Computing*, Vol. 28, No. 2, 2025. https://doi.org/10.1007/s10586-024-04709-8

[13]. S. Omoze, S. Omaji, and G.N. Edegbe, "Machine learning-based multimodal biometric authentication system (facial and fingerprint recognition) for online voting systems", *ABUAD Journal of Engineering Research and Development (AJERD)*, Vol. 8, No. 1, 2025, pp. 122–128. https://doi.org/10.53982/ajerd.2025.0801.13-j

[14]. M. Stojanoski, and Vukovich, L. (). "Use of smartphone applications in the democratic decision-making process", in: *Science, technology, policy and international law*. London: Routledge, 2025, pp. 175–192. https://doi.org/10.4324/9781003472421-9

[15]. B. Usharani, "Combating digital election fraud", in: *Democracy and democratization in the age of AI*, Hershey: IGI Global, 2025, pp. 103–120. https://doi.org/10.4018/979-8-3693-8749-8.ch006

[16]. H. Vedantam, S. Panthangi, A. Pesarakayala, and G. Kunchala, "Online voting system using cyber security", *SSRN Electronic Journal,* 2025. https://doi.org/10.2139/ssrn.5276799

[17]. H.A. Kargbo, and A. Turay, "Enhancing electoral transparency in sierra leone through data visualization and mapping", *International Journal of Innovative Science and Research Technology*, 2025, pp. 3303–3314. https://doi.org/10.38124/ijisrt/25apr1970

[18]. J. Bhanye, and R. Shayamunda, "The promise of civic-tech: Digital technologies and transparent, accountable governance", in: *Studies in national governance and emerging technologies*. Cham: Springer Nature Switzerland, 2025, pp. 93–122. https://doi.org/10.1007/978-3-031-75079-3_5

[19]. J. Koza, "Call for correction of false statements in the paper claiming that the national popular vote compact would undermine election integrity", 2025. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5140329

[20]. A. Marouan, M. Badrani, A. Zannou, N. Kannouf, and A. Chetouani, "E-Voting system based on blockchain for enhanced university elections", *SN Computer Science*, Vol. 6, No. 3, 2025. https://doi.org/10.1007/s42979-025-03671-5

[21]. M. Alown, M.S. Kiraz, and M.A. Bingol, "Enhancing democratic processes: A survey of DRE, internet, and blockchain in electronic voting systems", *IEEE Access*, Vol. 13, 2025, pp. 20512 - 20545. https://doi.org/10.1109/access.2025.3531349

[22]. R. Wagner, "Electoral resilience of citizen election observers: A case study of the republic of Kyrgyzstan", *Election Law Journal: Rules, Politics, and Policy,* 2025. https://doi.org/10.1089/elj.2024.0019

[23]. PlantUML. "PlantUML at a Glance", 2025. https://plantuml.com/

[24]. E.G. Tabanao, and J.C. Cece, "Development of student government e-voting application", *Journal of Interdisciplinary Perspectives*, Vol. 3, No. 2, 2025. https://doi.org/10.69569/jip.2024.0675

[25]. M.T. Sekwenz, and R. Gsenger, "Mapping compliance: A taxonomy for political content analysis under the EU's digital electoral framework", *arXiv preprint arXiv:2501.01738,* 2025. https://doi.org/10.48550/arXiv.2501.01738

[26]. A.Z. Abbasi, S. Bashir, M. Albashrawi, and D.H. Ting, "Blockchain enabled e-voting system adoption: Examining the mediating role of perceived transparency", *Journal of Asia Business Studies,* Vol. 19, No. 3, 2025, pp. 660–683. https://doi.org/10.1108/jabs-06-2024-0304

[27]. M. Elhoseny, H. Alyami, M. Altuwairiqi, P. Dutta, B.D. Veerasamy, and P.K. Shukla, "An efficient and secured voting system using blockchain and hybrid validation technique with deep learning", *Peer-to-Peer Networking and Applications*, Vol. 18, No. 2, 2025. https://doi.org/10.1007/s12083-024-01849-x

[28]. D. Upadhyay, S. Shakkarwal, and S. Vibuti, "Enhancing democracy through blockchain-enabled electronic voting systems.", in: *Advances in knowledge acquisition, transfer, and management*. Hershey: IGI Global, 2025, pp. 293–304. https://doi.org/10.4018/979-8-3693-3956-5.ch010

[29]. S. Gupta, K.K. Gupta, and P.K. Shukla, "Improving the end-to-end protection in e-voting using bvm—blockchain-based e-voting mechanism", *Concurrency and Computation: Practice and Experience,* Vol. 37, No. 2, 2025. https://doi.org/10.1002/cpe.8324

[30]. J. Montoya, S. Ramirez, and L.L. van der Meer, "Enhancing electoral participation in low-and middleincome countries: A mobile-digital technology (MParticipation) framework", *Journal of Information Systems and Digital Transformation-JISDT*, Vol. 3, No. 01, 2025. https://ditrn.org/pub/index.php/JISDT/article/view/7

[31]. C. Eremia, N. Shivananjappa, and R. Creutzburg, "Digital voting: Blockchain enabled democracy", *Electronic Imaging*, Vol. 37, 2025, pp. 1-8. https://doi.org/10.2352/EI.2025.37.3.MOBMU-311

[32]. A. Shaikh, N. Adhikari, A., Nazir, A.S. Shah, S. Baig, and H. Al Shihi, (2025). "Blockchain-enhanced electoral integrity: A robust model for secure digital voting systems in Oman", *F1000Research*, Vol. 14. https://doi.org/10.12688/f1000research.160087.2

[33]. M.S. Minu, K.S. Dattatreya, J. Mitesh, G. Raghunath, B. Vaidianathan, and R. Regin, (). "Blockchain-Enabled e-voting on reinventing electoral processes for university elections", in: *Advances in computational intelligence and robotics*. Hershey: IGI Global, 2025, pp. 309–330. https://doi.org/10.4018/979-8-3693-9375-8.ch018