# Dissertation Topic:

**‘’Enhancing E-Voting Security through Integrated Blockchain, Zero-Knowledge Proofs and Multimodal Biometric Authentication: A Post-Quantum Cryptographic Approach’’**

# Table 1: Research Gaps Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| **Paper** | **Identified Research Gaps** | **Proposed Solutions** | **Limitations** |
| Kumar et al. (2025) - Modernizing Voting Systems | Scalability issues with blockchain networks; Limited post-quantum security; Privacy vs transparency trade-offs | Hyperledger Fabric + ZKP + Biometrics integration | Limited scalability testing; No real-world deployment analysis |
| ZKP-BLOCKCHAIN (2025) - E-Voting Using Blockchain | High computational overhead; Limited real-world testing; Quantum vulnerability of current cryptographic methods | Three-layer architecture with DID, Triple-blind signatures, zk-SNARKs | Theoretical framework only; Missing performance benchmarks |
| Marcellino et al. (2024) - Zero-knowledge Identity Authentication | Limited biometric integration; Centralized identity provider dependency; Gas cost optimization needed | ZK-SNARK with ECDSA for identity authentication | Single blockchain platform; Limited voter authentication methods |
| Kaim et al. (2022) - Post-Quantum Online Voting Scheme | Implementation complexity; Limited performance evaluation; Trusted setup requirements | Blind signature + threshold encryption + lattice cryptography | Complex implementation; No practical deployment study |
| Aikata et al. (2022) - KaLi Post-Quantum Security | Resource constraints for IoT devices; Energy consumption issues; Hardware-software co-design challenges | Unified KaLi architecture for Kyber and Dilithium | ASIC-specific optimization; Limited to specific algorithms |
| Mao et al. (2025) - ZKP-based Anonymous Biometric Authentication | Limited multimodal biometric fusion; Computational complexity of ZKP verification; Privacy-utility balance | MCBG technology with Pedersen vector commitment | E-health focus only; Limited to specific biometric modalities |
| Jayakumari et al. (2024) - Cloud-based Hybrid Blockchain | Consensus mechanism efficiency; Authentication delay issues; Hybrid blockchain security analysis needed | PBFT consensus with timestamp-based authentication | Simulation-based evaluation only; Missing large-scale testing |
| Usha et al. (2025) - Systematic Review on ZKP Algorithms | Lack of standardization; Interoperability challenges; Quantum-resistant ZKP algorithms needed | Comprehensive analysis of ZKP models and applications | Survey paper - no implementation provided |

# Table 2: Base Papers Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Paper Title** | **Authors** | **Year** | **Journal/Conference** | **Relevance Score** | **Key Contributions** |
| Modernizing Voting Systems: A Comprehensive Approach Using Blockchain, Biometrics and Zero Knowledge Proofs | Kumar et al. | 2025 | International Journal of Electrical, Computer and Biomedical Engineering | High | Hyperledger Fabric + ZKP + Biometric integration |
| Zero-knowledge Identity Authentication for E-voting System | Marcellino et al. | 2024 | Journal of Internet Services and Information Security | High | ZK-SNARK identity authentication framework |
| A ZKP-based anonymous biometric authentication scheme for the E-health systems | Mao et al. | 2025 | PLoS One | Medium | MCBG with ZKP for e-health authentication |
| Post-Quantum Online Voting Scheme | Kaim et al. | 2022 | IFCA Conference Proceedings | High | Lattice-based post-quantum voting scheme |
| E-voting system using cloud-based hybrid blockchain technology | Jayakumari et al. | 2024 | Journal of Safety Science and Resilience | Medium | Cloud-based hybrid blockchain voting |

# Table 3: Research Questions Based on Identified Gaps

|  |  |  |  |
| --- | --- | --- | --- |
| **Research Question** | **Research Gap Addressed** | **Methodology** | **Expected Contribution** |
| RQ1: How can the integration of blockchain technology, zero-knowledge proofs, and multimodal biometric authentication enhance the security and privacy of electronic voting systems while maintaining scalability? | Integration challenges, privacy-security trade-offs, scalability issues | Experimental design with prototype development, performance benchmarking, security analysis | Novel integrated framework, security enhancement guidelines, scalability solutions |
| RQ2: What are the performance implications of implementing post-quantum cryptographic algorithms (lattice-based cryptography) in blockchain-based e-voting systems compared to traditional cryptographic methods? | Quantum vulnerability, performance evaluation, future-proofing | Comparative analysis, simulation studies, cryptographic security evaluation | Post-quantum readiness assessment, performance benchmarks, migration strategies |
| RQ3: How can a hybrid consensus mechanism combining Practical Byzantine Fault Tolerance (PBFT) and Delegated Proof-of-Stake (dPoS) improve the efficiency and security of e-voting systems? | Consensus mechanism efficiency, Byzantine fault tolerance, energy consumption | Consensus protocol design, network simulation, fault tolerance testing | Improved consensus mechanism, energy efficiency, fault tolerance enhancement |
| RQ4: What is the optimal architecture for integrating multimodal cancelable biometric generation (MCBG) technology with zero-knowledge proofs to ensure voter privacy while preventing identity fraud? | Biometric privacy, identity verification, cancelable biometrics | Biometric algorithm development, privacy analysis, authentication accuracy testing | Privacy-preserving biometric framework, identity protection protocols |
| RQ5: How can smart contracts be optimized to reduce gas costs and computational overhead while maintaining the integrity and auditability of the voting process? | Gas optimization, smart contract efficiency, cost-effectiveness | Smart contract optimization, gas analysis, transaction throughput measurement | Cost-effective smart contracts, gas optimization techniques, efficiency improvements |
| RQ6: What are the scalability challenges of implementing ZK-SNARKs in large-scale e-voting systems, and how can sharding and layer-2 solutions address these limitations? | ZKP scalability, large-scale deployment, performance bottlenecks | Scalability testing, layer-2 implementation, sharding protocol evaluation | Scalable ZKP implementation, layer-2 solutions, performance optimization |