IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, January 2026
Impact Factor: 7.67

A Comprehensive Review of Secure Remote E-Voting and Credibility-Aware Election Forecasting Using Cryptography and Deep Learning

Dipayan Roy[1], Abhinav Shukla[2], Dr. Ram Krishna Akuli[3]
[12]Department of Information Technology and Computer Science,
Dr. C. V. Raman University, Bilaspur, India
[3]Tata Consultancy Services, Kolkata, India
[1]dipayanr@yahoo.com, [2]amitshukla9611@gmail.com, [3]drakulirk@gmail.com

Abstract: *The increasing adoption of digital technologies in democratic processes has accelerated the development of secure remote electronic voting systems and intelligent election forecasting frameworks. While cryptographic mechanisms such as Elliptic Curve Cryptography (ECC), blockchain, digital signatures, and authentication protocols have significantly improved the security, privacy, and integrity of electronic voting systems, advances in machine learning and deep learning have transformed election forecasting through predictive analytics, sentiment analysis, and poll aggregation techniques. Despite these developments, existing approaches often address voting security and election prediction as independent research domains. Furthermore, most election forecasting models fail to incorporate poll credibility assessment, anomaly detection, and trust evaluation mechanisms into the predictive learning process, leading to potential forecasting biases and reliability concerns. This review presents a comprehensive analysis of recent advancements in secure remote e-voting and credibility-aware election forecasting by examining cryptographic frameworks, deep learning architectures, hybrid forecasting models, explainable artificial intelligence techniques, and trust assessment mechanisms. The review categorizes existing research into five major themes: cryptographic security frameworks, deep learning-based election forecasting, hybrid and ensemble prediction models, explainable and trustworthy AI systems, and credibility-aware poll aggregation approaches. The strengths, limitations, and emerging challenges of each research direction are critically analyzed. The study identifies significant research gaps related to credibility integration, anomaly-resilient forecasting, and trust-aware decision support. Finally, future research directions are proposed toward the development of unified frameworks that combine cryptographic security, credibility assessment, explainable intelligence, and deep temporal learning for trustworthy digital democracy systems.*

Keywords: Remote E-Voting, Election Forecasting, Elliptic Curve Cryptography, Deep Learning, Explainable Artificial Intelligence, Poll Credibility Assessment, Anomaly Detection, Trustworthy AI.

I. INTRODUCTION

The rapid digital transformation of governance and public administration has significantly influenced the evolution of electoral systems worldwide. Traditional voting mechanisms often face challenges related to accessibility, transparency, operational costs, and security, motivating governments and researchers to investigate secure remote electronic voting solutions. Remote e-voting systems enable citizens to participate in democratic processes regardless of geographical constraints while reducing administrative overhead and increasing voter convenience. However, the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, January 2026 Impact Factor: 7.67

success of such systems depends heavily on ensuring voter privacy, authentication, data integrity, confidentiality, and resistance against cyberattacks. Consequently, cryptographic techniques such as Elliptic Curve Cryptography (ECC), digital signatures, blockchain technologies, and secure authentication protocols have emerged as critical components for protecting electoral processes.

Simultaneously, election forecasting has become an important research area due to the increasing availability of polling data, demographic information, social media content, and voter behavior analytics. Machine learning and deep learning algorithms have demonstrated remarkable capabilities in identifying complex patterns from large-scale electoral datasets. Models based on Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), Transformers, ensemble learning, and sentiment analysis have significantly improved forecasting accuracy compared to conventional statistical approaches. Recent studies have also explored multimodal learning frameworks that integrate polling data, social media sentiment, demographic indicators, and historical election records.

Despite substantial progress in both domains, significant challenges remain unresolved. Most election forecasting frameworks assume equal reliability among data sources and rely on simplistic weighting mechanisms that fail to account for credibility variations among polling agencies. Similarly, explainable AI techniques primarily focus on post hoc interpretation rather than incorporating trustworthiness into predictive learning. Furthermore, existing e-voting security frameworks and election forecasting systems are generally developed independently, limiting the potential benefits of integrated trust-aware electoral intelligence.

This review aims to provide a comprehensive synthesis of recent developments in secure remote e-voting and credibility-aware election forecasting. The study critically examines cryptographic security mechanisms, intelligent forecasting architectures, explainable AI techniques, anomaly detection approaches, and credibility assessment strategies. By identifying existing limitations and emerging opportunities, this review establishes a foundation for future research toward secure, transparent, explainable, and trustworthy digital democracy ecosystems.

II. LITERATURE REVIEW

- **Cryptographic Frameworks for Secure Remote E-Voting**

Research on secure remote e-voting has primarily focused on strengthening voter authentication, privacy preservation, ballot confidentiality, and attack resistance through cryptographic mechanisms. Yan (2022), Ullah et al. (2022), and Sakkari and Ulla (2022) comprehensively highlighted the advantages of Elliptic Curve Cryptography (ECC) in providing strong security with reduced computational complexity. Abarzúa et al. (2019) examined the mathematical characteristics of Edwards curves, demonstrating their suitability for efficient cryptographic implementations. Shah et al. (2024) reviewed modern ECC advancements and their applications in IoT, blockchain, and cloud environments. Additional studies by Choi and Kim (2025), Nguyen and Pham (2022), and Fournaris et al. (2018) focused on performance optimization and side-channel attack resistance. Collectively, these works establish ECC as a reliable foundation for secure electronic voting systems. However, most studies emphasize computational security and implementation efficiency while overlooking intelligent trust evaluation, adaptive threat detection, and integration with predictive electoral analytics.

- **Deep Learning-Based Election Forecasting**

Deep learning techniques have significantly improved election prediction by learning complex nonlinear relationships from electoral data. Myilvahanan et al. (2023) demonstrated the effectiveness of machine learning models in electoral forecasting. Puspanath et al. (2025) proposed the Neural Democracy Prognosticator for analyzing voter behavior and election outcomes. Veeramani et al. (2025) utilized multimodal deep learning to combine electoral, demographic, and social media data. Khan et al. (2023) integrated location-aware sentiment analysis with social media analytics to improve election prediction. Ghosh et al. (2025) combined Twitter sentiment with traditional polling information to enhance forecasting accuracy. These studies confirm the effectiveness of AI-driven political forecasting. Nevertheless, most models prioritize prediction accuracy while ignoring polling credibility, trust assessment, and anomaly detection, limiting their reliability in real-world electoral environments.

- **Hybrid and Ensemble Forecasting Models**

Hybrid and ensemble learning frameworks have emerged as powerful approaches for improving forecasting performance. Bhuiyan et al. (2025) integrated CNN, LSTM, and attention mechanisms for temporal prediction tasks. Shi et al. (2025) introduced the HO-CAL framework combining optimization and intelligent learning techniques. Elo et al. (2024) applied Stack Ensemble Classification for voting behavior prediction. Liu et al. (2020) combined Twitter analytics with predictive modeling for election forecasting. Lewis-Beck and Dassonneville (2015) proposed synthetic forecasting models integrating political and economic variables. These approaches demonstrate that combining multiple learning paradigms improves forecasting accuracy and robustness. However, existing hybrid frameworks lack mechanisms for trust-aware learning, credibility integration, and adaptive anomaly detection, which are crucial for reliable election forecasting systems.

- **Explainable AI, Robustness, and Trustworthy Forecasting**

Explainable Artificial Intelligence (XAI) has gained considerable importance in high-stakes decision-making applications. Sampaio et al. (2024) explored explainability in digital governance systems. Y and Challa (2023) compared various XAI methods for enhancing model transparency. Rumapea et al. (2025) investigated interpretable deep learning approaches for trustworthy AI. Şahin et al. (2024) reviewed interpretability and reliability frameworks in deep learning. Asal and Demir (2024) integrated SHAP and LIME with voting classifiers to improve transparency. These studies demonstrate that explainability enhances user confidence and accountability. However, most existing methods provide post hoc explanations and fail to incorporate trust, credibility, and reliability directly into the model learning process.

- **Credibility Assessment, Poll Aggregation, and Anomaly Detection**

Credibility assessment and anomaly detection have emerged as critical challenges in election forecasting. Vasist and Sebastian (2022) demonstrated the importance of detecting misinformation in digital ecosystems. Steorts (2023) emphasized the role of data cleaning and quality assurance in predictive modeling. N et al. (2025) highlighted the growing significance of big data analytics in voter behavior analysis. Cruces (2024) discussed challenges associated with biased and noisy social media data. Doumard et al. (2022) proposed quantitative evaluation methods for explanation reliability. While these studies address trustworthiness from different perspectives, they do not provide integrated credibility-aware forecasting frameworks capable of learning from source reliability, temporal consistency, and anomaly patterns simultaneously.

III. RESEARCH GAP

Current research has achieved significant progress in secure electronic voting, election forecasting, deep learning, and explainable artificial intelligence. However, most existing studies treat voting security and election prediction as separate domains. Cryptographic frameworks focus on secure vote transmission without incorporating intelligent credibility assessment, while forecasting models primarily emphasize prediction accuracy and overlook polling reliability. Existing poll aggregation methods employ static weighting strategies that fail to capture multidimensional trust characteristics. Furthermore, explainable AI techniques largely provide post hoc interpretations rather than integrating credibility into predictive learning. Therefore, a unified framework combining cryptographic security, credibility-aware learning, anomaly detection, and explainable deep forecasting remains largely unexplored.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, January 2026
Impact Factor: 7.67

Table 1: - Research Gap Analysis Table

Research Area	Existing Approaches	Limitation	Required Improvement
ECC-Based E-Voting	Secure communication and authentication	No intelligent trust assessment	Credibility-aware cryptographic security
Election Forecasting	High prediction accuracy	Ignores poll reliability	Credibility-integrated forecasting
Poll Aggregation	Static weighting methods	Limited trust representation	Multi-dimensional credibility scoring
Explainable AI	Post hoc explanations	No trust-aware learning	Embedded explainability mechanisms
Anomaly Detection	Separate detection modules	Not integrated with forecasting	Unified anomaly-resilient forecasting

IV. CONCLUSION

The integration of secure remote electronic voting and credibility-aware election forecasting represents a critical advancement in modern digital democracy systems. This review examined recent developments in cryptographic security mechanisms, deep learning architectures, hybrid forecasting models, explainable artificial intelligence, and trust assessment frameworks. The findings indicate that Elliptic Curve Cryptography remains one of the most effective approaches for ensuring secure vote transmission and voter privacy, while deep learning techniques significantly enhance election forecasting performance. Nevertheless, existing studies largely focus on either security or prediction accuracy and rarely address credibility assessment as an intrinsic component of model learning. Furthermore, conventional poll aggregation methods fail to adequately capture multidimensional trust characteristics, and explainable AI approaches often provide only post hoc interpretations. Future research should focus on developing unified frameworks that combine cryptographic protection, credibility-aware learning, anomaly detection, explainability, and deep temporal forecasting to improve reliability, transparency, and public trust in digital electoral ecosystems.

REFERENCES

1. Abarzúa, M., Martínez, F., Mendoza, M., & Thériault, M. (2019). Same-value analysis of Edwards curves and their cryptographic properties. *Journal of Cryptographic Engineering*, *9*(3), 215–228.
2. Asal, M., & Demir, H. (2024). Explainable artificial intelligence for software defect prediction using SHAP and LIME integrated voting classifiers. *Applied Artificial Intelligence*, *38*(2), 1–18.
3. Awais, M., Hassan, S., & Ahmed, R. (2019). Big data analytics for political forecasting: Predicting Pakistan general election outcomes. *Journal of Big Data Analytics*, *6*(4), 45–58.
4. Bhuiyan, M. R., Rahman, M. S., Islam, M. T., & Hasan, M. A. (2025). Hybrid CNN-LSTM-attention framework for scalable grocery sales forecasting. *Expert Systems with Applications*, *257*, 125436.
5. Bhowmik, S., Sadik, M., Akanda, M. A. M., & Pavel, M. I. (2024). Sentiment analysis using FNet architecture on hotel customer reviews. *International Journal of Intelligent Systems*, *39*(5), 1021–1038.
6. Choi, J., & Kim, H. (2025). A lightweight Curve25519-based ECC accelerator for resource-constrained devices. *IEEE Access*, *13*, 15621–15635.
7. Cruces, G. (2024). Forecasting executive approval ratings using social media data: Opportunities and challenges. *Government Information Quarterly*, *41*(2), 101915.
8. Danger, J. L., Guilley, S., Hoogvorst, P., Murdica, C., & Naccache, D. (2013). A synthesis of side-channel attacks on elliptic curve cryptography in smart cards. *Journal of Cryptographic Engineering*, *3*(4), 241–265.
9. Doumard, M., et al. (2022). Quantitative comparison of additive local explanation methods in explainable artificial intelligence. *Artificial Intelligence Review*, *55*(8), 6421–6445.

10. Elo, P., Ghansah, B., & Kwaa-Aidoo, K. (2024). Stack ensemble classifier for predicting voting behavior based on parental political affiliations: A critical review. *Journal of Political Analytics*, *12*(1), 55–71.
11. Fournaris, A. P., Dimopoulos, I., Moschos, T., & Koufopavlou, O. (2018). Side-channel attack-resistant Binary Edwards elliptic curve digital signature architectures. *Microprocessors and Microsystems*, *61*, 20–31.
12. García-Sigüenza, J., Llorens-Largo, F., Tortosa, L., & Vicent, J. F. (2023). Explainability in graph neural network-based road traffic forecasting. *Information Sciences*, *640*, 119086.
13. Ghosh, A., Boettcher, T., Johnston, M., & Lahiri, S. (2025). THANOS: Predicting electoral campaign outcomes using Twitter data and opinion polls. *Decision Support Systems*, *184*, 114274.
14. Jebrane, A., Chhaybi, M., Lazaar, M., & Nitaj, A. (2024). Machine learning applications in elliptic curve cryptography: Opportunities and challenges. *Journal of Information Security and Applications*, *81*, 103705.
15. Khan, M., Boudjellal, A., Zhang, Y., Ahmad, S., & Khan, R. (2023). Location-aware sentiment analysis for election prediction using social media data. *Knowledge-Based Systems*, *275*, 110708.
16. Kumar, P., Aggarwal, A., Sharma, S., & Goyal, N. (2021). Active learning approaches for elliptic curve cryptosystems and RFID authentication protocols. *Wireless Personal Communications*, *119*(3), 2573–2594.
17. Kurniawan, D., Romadhoni, M., Zahrona, F., & Hammad, A. (2022). Comparative analysis of LSTM and CNN models for COVID-19 Twitter sentiment analysis. *International Journal of Advanced Computer Science and Applications*, *13*(7), 314–323.
18. Lewis-Beck, M. S., & Dassonneville, R. (2015). Forecasting elections in Europe using synthetic models. *Electoral Studies*, *39*, 358–369.
19. Liu, X., Yao, Y., Guo, Z., & Wei, J. (2020). Forecasting presidential elections using Twitter data: An integrative modeling approach. *Social Network Analysis and Mining*, *10*(1), 58.
20. Liu, Y., et al. (2022). BERT-POS: Enhancing sentiment analysis through part-of-speech integrated transformer models. *Applied Intelligence*, *52*(14), 16247–16261.
21. Myilvahanan, S., et al. (2023). Election prediction using machine learning techniques: A comparative analysis. *Journal of Computational Social Science*, *6*(2), 845–861.
22. Nguyen, T., & Pham, H. (2022). Combined blinding-shuffling countermeasures against online template attacks using randomized-domain Montgomery multiplication. *IEEE Transactions on Information Forensics and Security*, *17*, 3214–3227.
23. N, S., Thangavel, R., & Toyirov, B. (2025). Big data analytics and predictive modeling for voter behavior analysis. *Journal of Big Data*, *12*(1), 42.
24. Puspanath, R., Ramesh, K., Muthusamy, P., & Pandian, V. (2025). Neural Democracy Prognosticator: An AI framework for electoral prediction. *Expert Systems with Applications*, *259*, 125921.
25. Renuka, S., & Radhakrishnan, P. (2024). BERT-based sentiment analysis for Twitter data classification. *International Journal of Intelligent Computing and Cybernetics*, *17*(1), 88–104.
26. Rumapea, H., Manalu, M., & Rumapea, J. (2025). Interpretable deep learning for trustworthy artificial intelligence systems. *Artificial Intelligence Review*, *58*(4), 1–25.
27. Saha, D., Bag, S., Jap, D., Mukhopadhyay, D., & Bhasin, S. (2021). Security analysis of countermeasures against combined side-channel and fault attacks. *IEEE Transactions on Computers*, *70*(10), 1698–1712.
28. Sakkari, S., & Ulla, M. (2022). A comprehensive review of elliptic curve cryptography: Principles, applications, and challenges. *International Journal of Computer Applications*, *184*(15), 12–23.
29. Sampaio, R., Fontes, J., Andrade, R., Bernardini, F., & Viterbo, J. (2024). Explainable artificial intelligence for collusion and corruption detection in digital government systems. *Government Information Quarterly*, *41*(1), 101884.
30. Şahin, M., Arslan, A., & Özdemir, E. (2024). Interpretability, explainability, and reliability in deep learning: A comprehensive review. *Artificial Intelligence Review*, *57*(6), 154.

31. Shah, R., Bhadauria, S., Thakkar, J., Shah, P., & Kaur, H. (2024). Recent advancements in elliptic curve cryptography and emerging applications. *Journal of Cyber Security Technology*, *8*(2), 143–165.
32. Shi, Y., Ibrahim, A., & Hashim, H. (2025). HO-CAL: A hybrid optimization and computational intelligence framework for stock index prediction. *Engineering Applications of Artificial Intelligence*, *138*, 108915.
33. Steorts, R. (2023). Data cleaning pipelines for reliable predictive modeling and statistical analysis. *Annual Review of Statistics and Its Application*, *10*, 231–255.
34. Ullah, I., et al. (2022). Elliptic curve cryptography: Applications, challenges, and future directions. *IEEE Access*, *10*, 75682–75705.
35. Van Zyl, T., Ye, Y., & Naidoo, R. (2023). Explainable AI techniques for feature selection in time-series energy forecasting. *Energy and AI*, *14*, 100294.
36. Vasist, P., & Sebastian, M. (2022). Machine learning and artificial intelligence algorithms for fake news detection during COVID-19. *Information Processing & Management*, *59*(5), 103042.
37. Veeramani, P., Thilagavathy, S., Deebalakshmi, S., & Meganathan, K. (2025). Multimodal deep learning framework for predictive political decision-making. *Neural Computing and Applications*, *37*(8), 10231–10248.
38. Yan, X. (2022). An overview of elliptic curve cryptography and its applications in modern communication systems. *Journal of Information Security*, *13*(2), 77–91.
39. Y, K., & Challa, R. (2023). Comparative analysis of explainable artificial intelligence techniques for model interpretability. *Applied Soft Computing*, *137*, 110110.
40. Zhao, H., et al. (2022). Interpretable machine learning for electrochemical impedance spectroscopy parameter prediction using global optimization. *Engineering Applications of Artificial Intelligence*, *114*, 105016.