Vol. 11, No. 1, 2026, pp. 204-212
DOI: https://doi.org/10.29210/30036840000

Contents lists available at Journal ELORA

JRTI (Jurnal Riset Tindakan Indonesia)
ISSN: 2502-079X (Print) ISSN: 2503-1619 (Electronic)

Journal homepage: https://jrti.eloracenter.org/jrti

Integration of artificial intelligence in e-voting systems for anomaly detection and prevention of electoral data manipulation

Abdurrohman Abdurrohman[1], Afiyati Afiyati[2], Rasiban Rasiban[3]
[1] Universitas Teknologi Bandung,
[2] Universitas Mercu Buana
[3] Stikom Cipta Karya Informatika, Jakarta

Article Info

Article history:

Received May 19th, 2026
Revised Jun 14th, 2026
Accepted Jun 22th, 2026

Keyword:

Artificial intelligence;
Anomaly detection;
Electoral data integrity

ABSTRACT

The increasing adoption of electronic voting (e-voting) systems has improved electoral efficiency and accessibility while simultaneously introducing new challenges related to cybersecurity and electoral data integrity. This study aims to examine the integration of Artificial Intelligence (AI) in e-voting systems for anomaly detection and the prevention of electoral data manipulation. Using a library research approach, data were collected through the analysis of books, scientific journals, research reports, and other relevant academic literature related to Artificial Intelligence, anomaly detection, and electoral data integrity. The findings indicate that AI-based anomaly detection mechanisms can effectively identify unusual patterns, suspicious activities, and potential manipulation attempts within electoral datasets. Furthermore, machine learning algorithms enable continuous monitoring and adaptive threat detection, overcoming several limitations of traditional security approaches. The study concludes that integrating AI into e-voting systems can strengthen electoral data integrity, improve security performance, and enhance public trust in digital electoral processes while supporting transparent, reliable, and accountable democratic governance.

Corresponding Author:

Abdurrohman Abdurrohman
Universitas Teknologi Bandung
Email: abdurrohman1970@gmail.com

Introduction

The rapid digitalization of public administration has encouraged many countries to explore electronic voting systems as an alternative to conventional election mechanisms. While e-voting offers advantages in terms of efficiency, accessibility, speed of vote counting, and reduction of administrative costs, it also introduces significant concerns regarding the security and integrity of electoral data. Recent developments in information technology have demonstrated that electoral infrastructures are increasingly vulnerable to cyberattacks, unauthorized access, data tampering, and sophisticated manipulation techniques that can compromise democratic processes. Several reported incidents involving electoral systems worldwide have raised concerns about the possibility of altering vote records, manipulating transmission channels, or exploiting software vulnerabilities to influence election outcomes. As elections represent one of the most critical pillars of democratic governance, any compromise in electoral data integrity can undermine public trust, create political instability, and weaken the legitimacy of elected governments(Ertel, 2024). The growing complexity of cyber threats further exacerbates these challenges because traditional security mechanisms often focus on preventing unauthorized access rather than continuously detecting abnormal activities that may indicate manipulation attempts. Consequently, the reality of evolving cybersecurity threats within digital election environments highlights an

urgent need for advanced technological approaches capable of safeguarding electoral data and preserving the credibility of democratic institutions. Therefore, addressing vulnerabilities in e-voting systems has become a strategic priority for governments, election authorities, and technology researchers seeking to ensure secure and trustworthy electoral processes(Simoes & MacCarthaigh, 2023).

Existing academic literature has extensively discussed the relationship between e-voting security, cybersecurity frameworks, and electoral transparency, providing valuable theoretical foundations for understanding the challenges associated with digital elections. Research has examined cryptographic protocols, blockchain-based voting architectures, authentication mechanisms, and secure communication channels as potential solutions for protecting electoral information. These studies have significantly contributed to enhancing confidentiality, integrity, and availability within electronic voting infrastructures. However, despite these advancements, many theoretical and practical approaches remain predominantly preventive rather than adaptive, making them less effective against emerging threats characterized by dynamic attack patterns and previously unseen manipulation strategies(Kühl et al., 2022). Traditional security models often rely on predefined rules, signatures, or static verification procedures that may fail to identify subtle anomalies hidden within large-scale voting datasets. Furthermore, the increasing sophistication of cyberattacks has demonstrated that malicious actors can exploit legitimate system activities to disguise manipulation attempts, thereby reducing the effectiveness of conventional monitoring techniques. Although anomaly detection has received attention within broader cybersecurity research, its integration into electoral systems remains relatively underexplored and fragmented. As a result, current theoretical frameworks have not fully addressed how intelligent systems can continuously analyze electoral data, recognize suspicious behavioral patterns, and respond proactively to potential manipulation efforts. This theoretical and practical gap indicates the necessity of developing more adaptive approaches capable of strengthening electoral data integrity within modern e-voting environments(Mwansa, 2023).

Based on the challenges identified in practical electoral environments and the limitations observed within existing literature, this study aims to investigate the integration of Artificial Intelligence into e-voting systems as a mechanism for anomaly detection and prevention of electoral data manipulation. Specifically, the research seeks to examine how AI-driven analytical models can identify irregular voting patterns, detect suspicious activities within electoral datasets, and support the protection of electoral data integrity throughout the voting process. In addition, the study intends to evaluate the effectiveness of machine learning and intelligent monitoring techniques in distinguishing legitimate electoral activities from potentially malicious actions that may indicate data tampering attempts. The research also aims to explore the operational benefits and implementation considerations associated with embedding AI-based security mechanisms within digital voting infrastructures. By focusing on the interaction between artificial intelligence, anomaly detection, and electoral data integrity, the study seeks to contribute to both theoretical understanding and practical development within the field of secure electronic elections. Furthermore, the findings are expected to provide insights for policymakers, election management bodies, and system developers regarding the adoption of intelligent technologies capable of enhancing transparency, reliability, and trustworthiness in electoral processes. Therefore, the research is designed to address a critical knowledge gap while offering practical implications for strengthening democratic governance in increasingly digital societies(Peelam et al., 2025).

The importance of conducting this research is grounded in the argument that artificial intelligence possesses unique capabilities that can significantly enhance the resilience of e-voting systems against increasingly sophisticated forms of electoral data manipulation. Given the reality that conventional security mechanisms often struggle to identify complex and evolving threats, AI-driven anomaly detection offers a promising alternative through its ability to learn behavioral patterns, analyze large volumes of electoral data in real time, and recognize deviations that may indicate malicious activities. This study is based on the hypothesis that the integration of intelligent analytical models into electronic voting infrastructures can improve the detection accuracy of anomalous events while simultaneously reducing the risk of successful manipulation attempts. Such an approach aligns with the identified need for adaptive security mechanisms capable of responding to emerging cyber threats that cannot always be anticipated through traditional rule-based frameworks. Moreover, by supporting continuous monitoring and predictive analysis, artificial intelligence may contribute to strengthening public confidence in digital electoral systems and enhancing the overall integrity of election outcomes. The significance of this research therefore extends beyond technological innovation, encompassing broader democratic objectives related to transparency, accountability, and institutional legitimacy. Consequently, investigating the integration of artificial intelligence within e-voting systems represents a timely and necessary effort to advance both cybersecurity research and the sustainable development of secure digital democracy(Peelam et al., 2025).

Method

The object of this research focuses on the phenomenon of electoral data manipulation risks within electronic voting systems and the challenges associated with detecting anomalous activities that may threaten electoral integrity. The increasing adoption of digital voting technologies has transformed the administration of elections by improving efficiency, accessibility, and vote-counting speed. However, alongside these benefits, e-voting systems have become potential targets for cyberattacks, unauthorized access, data tampering, and sophisticated manipulation techniques capable of influencing election outcomes(Lee, 2020). Such vulnerabilities create concerns regarding the reliability and transparency of digital electoral processes, particularly when conventional security mechanisms fail to identify subtle irregularities hidden within large-scale electoral datasets. The phenomenon becomes increasingly significant as malicious actors continuously develop more advanced methods to exploit system weaknesses while avoiding detection. Consequently, ensuring electoral data integrity requires innovative approaches capable of monitoring, identifying, and preventing suspicious activities in real time. Within this context, the integration of Artificial Intelligence for anomaly detection emerges as a promising solution to address the limitations of traditional security frameworks. Therefore, the research object examined in this study encompasses the relationship between artificial intelligence, anomaly detection mechanisms, and the prevention of electoral data manipulation in contemporary electronic voting environments(Milea & Siminiuc, 2025).

This study employs a library research approach, which is conducted through the systematic examination and analysis of various written sources relevant to the research problem. Library research was selected because it enables a comprehensive understanding of theoretical developments, empirical findings, and technological innovations associated with Artificial Intelligence, Anomaly Detection, and Electoral Data Integrity. The primary data utilized in this study consist of scholarly literature directly discussing cases, phenomena, and challenges related to electoral data manipulation, cybersecurity threats in e-voting systems, and the implementation of intelligent detection mechanisms within digital election infrastructures(McCarthy, 2022). These sources provide foundational insights into the nature of the problem being investigated and the potential solutions proposed by previous researchers. Meanwhile, the secondary data comprise broader literature associated with the study's key concepts, including Artificial Intelligence, machine learning applications, anomaly detection techniques, cybersecurity frameworks, electoral governance, and data integrity management. Such secondary sources were obtained from academic books, peer-reviewed journals, conference proceedings, research reports, and other scientific publications. Through the integration of both primary and secondary sources, the study establishes a comprehensive knowledge base that supports the analysis of how artificial intelligence can contribute to securing electoral systems against manipulation attempts(Mulli, 2024).

The theoretical foundation of this research is primarily based on the theory of Artificial Intelligence proposed by John McCarthy in 1956, a foundational framework that defines Artificial Intelligence as the science and engineering of creating intelligent machines capable of performing tasks that typically require human intelligence. McCarthy's conceptualization established the basis for the development of computational systems that can learn, reason, solve problems, and adapt to changing environments through data-driven processes. Within the context of this study, the theory provides an essential framework for understanding how intelligent systems can be designed to identify unusual patterns, recognize behavioral deviations, and support decision-making processes in complex digital environments. Furthermore, the study incorporates principles derived from anomaly detection theory, which emphasizes the identification of observations that significantly deviate from expected patterns within datasets(Jarrahi et al., 2022). These theoretical perspectives collectively support the assumption that intelligent computational models possess the capability to distinguish between legitimate electoral activities and potentially malicious actions indicative of data manipulation. By integrating Artificial Intelligence theory with anomaly detection principles, the research establishes a conceptual framework that explains how machine learning algorithms and predictive analytical techniques can strengthen electoral data integrity. Consequently, these theoretical foundations serve as the primary source of information and assumptions guiding the entire research process(Ababio & Olatokun, 2023).

The research process was conducted through several systematic stages designed to ensure the collection of relevant and reliable information. The initial stage involved identifying the research problem and determining the scope of investigation concerning the integration of Artificial Intelligence in e-voting systems for anomaly detection and prevention of electoral data manipulation. Following this stage, relevant literature was searched, selected, and classified according to its relationship with the research objectives and key concepts. Data collection was subsequently performed through an extensive review of written sources, including academic books, previous research studies, scientific journals, conference papers, articles, reports, and other scholarly publications related to electronic voting security, anomaly detection, and artificial intelligence applications.

During this process, information was carefully documented, categorized, and organized based on thematic relevance to facilitate further analysis. The collected materials were then critically evaluated to identify significant findings, theoretical perspectives, and empirical evidence associated with the research topic. This structured approach enabled the researcher to gather comprehensive information from diverse sources while maintaining consistency with the objectives of the study. Therefore, the research process emphasized systematic literature exploration as the primary means of obtaining data and developing a coherent understanding of the investigated phenomenon(Chigova & Hofisi, 2025).

The data analysis technique employed in this study is content analysis, a method that facilitates the systematic examination and interpretation of information obtained from various literature sources. Content analysis was selected because it allows researchers to study, process, and evaluate textual data in order to identify patterns, relationships, themes, and significant information relevant to the research objectives. The analytical process began with the organization and classification of collected data according to predetermined categories associated with Artificial Intelligence, anomaly detection mechanisms, electoral data integrity, and electronic voting security(Chatterjee, 2020). Subsequently, the content of each source was examined to identify recurring concepts, theoretical arguments, empirical findings, and technological approaches related to the prevention of electoral data manipulation. Through comparative analysis, similarities and differences among various scholarly perspectives were explored to generate a comprehensive understanding of the subject matter. The identified patterns and relationships were then synthesized into an integrated analytical framework capable of explaining the role of Artificial Intelligence in enhancing electoral security. By employing content analysis, the study was able to transform extensive textual information into meaningful insights that support the formulation of conclusions and recommendations. Consequently, this analytical approach provides a rigorous foundation for understanding the potential contributions of intelligent technologies to safeguarding electoral integrity within modern e-voting systems(Ajao et al., 2025).

Results and Discussions

Results

The literature review results indicate that electoral data manipulation remains one of the most significant security challenges in contemporary e-voting systems. Various studies demonstrate that digital election infrastructures are exposed to threats ranging from unauthorized access and vote alteration to database tampering and transmission interception. The findings reveal that attackers increasingly employ sophisticated methods that are difficult to detect using conventional rule-based security mechanisms. As a result, election authorities face growing difficulties in maintaining the integrity, transparency, and reliability of electoral outcomes. These findings suggest that the protection of electoral data requires adaptive security mechanisms capable of continuously monitoring system behavior and identifying suspicious activities before they affect election results.

Another important finding concerns the limitations of traditional cybersecurity approaches in e-voting environments. Existing security mechanisms generally focus on authentication, encryption, and access control. Although these technologies effectively prevent many common attacks, they often struggle to identify previously unknown threats. The reviewed literature shows that cybercriminals frequently exploit legitimate system processes to disguise malicious activities, thereby reducing the effectiveness of static security controls. Consequently, the inability of traditional approaches to recognize evolving attack patterns creates vulnerabilities that may compromise electoral data integrity(Sujatha et al., 2024).

The analysis further reveals that Artificial Intelligence has emerged as a promising solution for enhancing electoral security. AI systems possess the capability to process large volumes of data, identify complex patterns, and generate predictive insights in real time. Several studies demonstrate that machine learning algorithms can successfully distinguish normal system behavior from abnormal activities that may indicate fraud or manipulation attempts. This capability enables election management systems to detect suspicious events earlier than conventional monitoring approaches. Therefore, AI contributes not only to threat detection but also to proactive risk mitigation(Ohize et al., 2025).

The reviewed literature identifies anomaly detection as one of the most effective applications of Artificial Intelligence in cybersecurity. Anomaly detection refers to the process of identifying data patterns that deviate significantly from established norms. Within e-voting systems, such deviations may include unusual voting frequencies, abnormal access attempts, unexpected changes in vote counts, or irregular network traffic. The findings indicate that anomaly detection models can recognize subtle indicators of manipulation that may remain invisible to human operators. Consequently, these systems provide an additional layer of protection for electoral infrastructures(Rafi, 2025).

The analysis also reveals that supervised and unsupervised machine learning techniques are widely used in anomaly detection frameworks. Supervised learning models rely on previously labeled datasets to classify suspicious activities, whereas unsupervised learning methods identify anomalies without requiring predefined labels. The literature suggests that unsupervised techniques are particularly valuable in electoral contexts because novel attack patterns may not have historical examples available for training. This flexibility increases the capability of AI systems to respond to emerging threats and changing attack strategies(Jafar et al., 2024).

Another finding concerns the role of real-time monitoring in preserving electoral data integrity. Studies consistently demonstrate that continuous monitoring systems significantly improve the ability to detect and respond to suspicious activities before substantial damage occurs. AI-powered monitoring platforms can analyze system logs, voting records, and network communications simultaneously. This capability enables immediate identification of irregular behavior and supports rapid intervention by election authorities. As a result, real-time monitoring contributes to maintaining public confidence in digital electoral processes(Zhuravlov & Zhuravlov, 2025).

The literature further indicates that integrating AI into e-voting systems improves operational efficiency. Traditional auditing procedures often require extensive human resources and lengthy verification processes. In contrast, AI systems automate data analysis, reduce manual workload, and accelerate threat identification. These efficiencies allow election administrators to allocate resources more effectively while maintaining high levels of security oversight. Consequently, AI integration offers both security and administrative benefits within modern electoral environments(Maphephe, 2025b).

The findings also reveal several implementation challenges. The effectiveness of AI-based anomaly detection depends heavily on data quality, computational resources, and model training processes. Inadequate datasets may lead to inaccurate predictions and increased false-positive rates. Furthermore, concerns regarding algorithmic transparency and explainability remain significant, particularly in democratic processes where accountability is essential. These challenges highlight the importance of establishing robust governance frameworks for AI deployment in electoral systems.

Overall, the results demonstrate a strong relationship between Artificial Intelligence, anomaly detection, and electoral data integrity. The reviewed evidence consistently suggests that AI-driven anomaly detection mechanisms improve the ability of e-voting systems to identify, prevent, and respond to electoral data manipulation attempts. Therefore, the integration of intelligent technologies represents a valuable strategy for strengthening the security, reliability, and legitimacy of digital election infrastructures(Novelli & Sandri, 2024).

Table 1. Summary of Main Findings

Research Aspect	Key Findings	Implications for E-Voting Security
Electoral Data Manipulation	Increasingly sophisticated cyber threats	Requires adaptive protection mechanisms
Traditional Security Systems	Limited against unknown attacks	Need for intelligent detection methods
Artificial Intelligence	Capable of pattern recognition and prediction	Enhances proactive security
Anomaly Detection	Identifies abnormal behavior effectively	Improves fraud detection capability
Machine Learning	Supports automated threat identification	Strengthens system resilience
Real-Time Monitoring	Enables immediate response	Reduces manipulation risks
Operational Efficiency	Automates auditing processes	Improves administrative performance
Implementation Challenges	Data quality and transparency issues	Requires governance and oversight

Discussion

The findings support the argument that traditional security mechanisms alone are insufficient to address the growing complexity of cyber threats targeting e-voting systems. Although security measures such as encryption, authentication, access control, and digital signatures remain fundamental components of electronic voting infrastructures, their primary function is generally limited to preventing unauthorized access and protecting data confidentiality(Tussyadiah, 2020). These mechanisms often operate within predefined security parameters and may not effectively identify sophisticated attacks that exploit legitimate system functions. The reviewed literature indicates that modern cyber threats increasingly involve advanced persistent attacks, insider threats, and covert manipulation techniques that can bypass conventional security controls without immediately triggering alerts.

Attackers frequently disguise malicious activities as normal system behavior, making detection significantly more difficult through static monitoring approaches. Consequently, electoral institutions face substantial challenges in ensuring the integrity and transparency of election outcomes when relying solely on traditional cybersecurity frameworks. This situation demonstrates the necessity of adopting adaptive and intelligent security solutions capable of continuously monitoring system behavior and identifying irregular activities in real time. Therefore, the findings suggest that the evolution of cyber threats within digital electoral environments requires a corresponding evolution in security strategies, emphasizing proactive detection and predictive analysis rather than solely preventive protection mechanisms.

The results also confirm the relevance of Artificial Intelligence theory proposed by John McCarthy, who conceptualized Artificial Intelligence as the science and engineering of creating intelligent machines capable of performing tasks that normally require human intelligence(Natale & Ballatore, 2020). Within the context of e-voting systems, this theoretical perspective provides a strong foundation for understanding how intelligent computational systems can enhance electoral security through advanced analytical capabilities. The literature reviewed in this study demonstrates that AI technologies possess the ability to process extensive volumes of electoral data, identify hidden relationships among variables, recognize irregular behavioral patterns, and generate predictive insights that support informed decision-making(Hopgood, 2021). Unlike conventional monitoring systems that depend on predefined rules and manual supervision, AI-based systems can autonomously learn from historical and real-time data to improve detection performance continuously. These capabilities align closely with McCarthy's theoretical assumptions regarding machine intelligence and adaptive problem-solving. Furthermore, AI enables election management systems to respond more effectively to emerging threats by identifying potential vulnerabilities before they can be exploited. As a result, the study reinforces the theoretical proposition that intelligent systems can provide a higher level of analytical sophistication and operational effectiveness than traditional cybersecurity approaches, particularly within complex and dynamic electoral environments(Battista, 2025).

Furthermore, the effectiveness of anomaly detection identified in the reviewed literature supports previous research emphasizing the importance of data-driven cybersecurity strategies. Anomaly detection operates on the principle of identifying patterns, behaviors, or observations that significantly deviate from established norms within a dataset. In electronic voting environments, these anomalies may manifest as unusual voting frequencies, unexpected modifications to vote records, abnormal user access behavior, suspicious network activity, or inconsistencies in data transmission processes. Unlike traditional rule-based security systems that require predefined attack signatures, anomaly detection models continuously learn from system behavior and adapt to evolving operational conditions(Ahmed et al., 2022). This adaptive capability is particularly valuable in electoral settings because cyber threats often evolve faster than static security policies can be updated. Machine learning algorithms enable anomaly detection systems to recognize previously unseen attack patterns and respond to emerging risks with greater flexibility. Consequently, these systems offer a proactive approach to cybersecurity by identifying suspicious activities before they develop into significant security incidents. Therefore, the integration of anomaly detection mechanisms contributes substantially to creating a more resilient, responsive, and adaptive electoral security infrastructure capable of addressing both known and unknown threats(Aniche et al., 2021).

The findings additionally highlight the strong relationship between anomaly detection and electoral data integrity, a connection that is fundamental to maintaining the legitimacy of democratic processes. Electoral data integrity refers to the accuracy, consistency, completeness, and authenticity of voting information throughout all stages of the election cycle, including voter registration, ballot casting, vote transmission, vote counting, and result reporting(Samoili et al., 2020). Any unauthorized modification, deletion, duplication, or manipulation of electoral records can compromise election outcomes and undermine public confidence in democratic institutions. The literature demonstrates that AI-powered anomaly detection systems can effectively identify suspicious changes in electoral datasets by continuously monitoring transactional behavior and comparing current activities against established behavioral baselines. Through this process, potential threats can be detected and investigated before they significantly impact election results. Furthermore, anomaly detection enhances transparency by providing detailed analytical evidence regarding suspicious events and system irregularities. This capability strengthens accountability and facilitates more effective auditing procedures. Consequently, the findings indicate that anomaly detection functions not only as a technical security mechanism but also as an essential safeguard for preserving electoral integrity, public trust, and democratic legitimacy(Maphephe, 2025a).

Another significant discussion point concerns the practical implications of AI adoption for election management institutions and governmental organizations responsible for administering elections. Beyond its contribution to cybersecurity enhancement, Artificial Intelligence offers substantial operational benefits through automation and intelligent decision support(Aliyu et al., 2024). Traditional electoral auditing procedures often

require considerable human resources, extensive documentation review, and lengthy verification processes, particularly in large-scale elections involving millions of voters. AI technologies can significantly reduce these burdens by automating data analysis, continuously monitoring electoral processes, and generating timely alerts regarding potential security concerns. Such capabilities allow election administrators to allocate resources more efficiently while maintaining high standards of oversight and accountability. However, the successful implementation of AI within electoral systems depends on several critical factors, including technological infrastructure readiness, data availability, algorithm quality, and human expertise. Moreover, regulatory frameworks must be established to ensure transparency, accountability, and ethical governance in the use of AI technologies. Therefore, while AI presents significant opportunities for improving electoral security and operational performance, its adoption must be accompanied by comprehensive institutional preparation and governance mechanisms to maximize benefits and minimize associated risks(Novelli & Sandri, 2024).

Finally, the study suggests that the future development of secure e-voting systems should prioritize the integration of intelligent analytical technologies as a central component of electoral cybersecurity strategies. The evidence synthesized from the literature consistently indicates that AI-driven anomaly detection systems can significantly strengthen the capacity of election infrastructures to identify, prevent, and respond to electoral data manipulation attempts(Krishnamoorthy & Rajeev, 2018). By enabling continuous monitoring, predictive analysis, and adaptive threat detection, Artificial Intelligence addresses many limitations associated with conventional security frameworks and contributes to greater transparency, accountability, and operational efficiency. Nevertheless, the findings also emphasize the importance of addressing challenges related to algorithmic explainability, fairness, privacy protection, and public trust. Electoral processes operate within highly sensitive democratic contexts where transparency and legitimacy are essential. Consequently, AI systems must be designed and implemented in ways that ensure accountability and maintain stakeholder confidence. Future research should further explore methods for improving the interpretability and reliability of AI-based electoral security mechanisms while examining their effectiveness across different electoral environments. Therefore, Artificial Intelligence should be viewed not merely as a technological innovation but as a strategic instrument capable of safeguarding democratic values and strengthening the integrity of digital electoral systems in the modern era(Ainur et al., 2024).

Table 2. Discussion of AI Contributions to Electoral Data Integrity

AI Capability	Function in E-Voting Systems	Expected Outcome
Pattern Recognition	Identifies normal and abnormal voting behavior	Early detection of manipulation
Predictive Analytics	Forecasts potential security threats	Preventive security measures
Real-Time Monitoring	Continuously evaluates electoral activities	Immediate incident response
Automated Auditing	Reviews large datasets efficiently	Reduced human error
Machine Learning Adaptation	Learns from evolving attack patterns	Increased resilience against new threats
Data Integrity Verification	Detects unauthorized modifications	Greater election reliability
Decision Support	Assists election authorities in risk assessment	Improved governance and accountability

Conclusions

This study concludes that the integration of Artificial Intelligence into e-voting systems provides a promising and effective approach for enhancing electoral security through anomaly detection and the prevention of electoral data manipulation. The findings indicate that conventional security mechanisms, while important, are often insufficient to address increasingly sophisticated cyber threats that target digital election infrastructures. Artificial Intelligence, particularly through machine learning and anomaly detection techniques, demonstrates the capability to identify abnormal patterns, detect suspicious activities in real time, and support proactive responses to potential manipulation attempts. Furthermore, the implementation of AI contributes to strengthening electoral data integrity by ensuring the accuracy, consistency, and reliability of voting information throughout the electoral process. Despite challenges related to data quality, algorithm transparency, and implementation complexity, the overall evidence suggests that AI-driven security frameworks can significantly improve the resilience, efficiency, and trustworthiness of e-voting systems. Therefore, the adoption of Artificial Intelligence should be considered a strategic measure for protecting democratic processes, maintaining public confidence in election outcomes, and supporting the development of secure, transparent, and accountable digital electoral systems.

References

Ababio, H., & Olatokun, W. (2023). Artificial Intelligence, Social Inclusion, And Representation In General Elections In Lesotho: Challenges, Prospects And A Framework For Implementation. *Journal Of Contemporary Society & Education (Jcse)*, *3*(1), 43–63.

Ahmed, I., Jeon, G., & Piccialli, F. (2022). From Artificial Intelligence To Explainable Artificial Intelligence In Industry 4.0: A Survey On What, How, And Where. *Ieee Transactions On Industrial Informatics*, *18*(8), 5031–5042.

Ainur, J., Gulzhan, M., Amandos, T., Venera, R., Bulat, S., Zauresh, Y., & Aizhan, S. (2024). The Impact Of Blockchain And Artificial Intelligence Technologies In Network Security For E-Voting. *International Journal Of Electrical And Computer Engineering (Ijece)*, *14*(6), 6723–6733.

Ajao, L. A., Umar, B. U., Ohize, H., Dogo, E. M., Esenogho, E., & Cameron, M. (2025). Blockchain Integration With Multimodal Biometric Authentication System For Secure Smart Verifiable Electronic Voting System. *Ieee Access*.

Aliyu, A. A., Liu, J., & Gilliard, E. (2024). A Decentralized And Self-Adaptive Intrusion Detection Approach Using Continuous Learning And Blockchain Technology. *Journal Of Data Science And Intelligent Systems*.

Aniche, C., Yinka-Banjo, C., Ohalete, P., & Misra, S. (2021). Biometric E-Voting System For Cybersecurity. In *Artificial Intelligence For Cyber Security: Methods, Issues And Possible Horizons Or Opportunities* (Pp. 105–137). Springer.

Battista, D. (2025). From Electronic Voting To Ai: Lessons From The Estonian Case On The Transformation Of Digital Democracy. *Em Questão*, *31*, E-145465.

Chatterjee, R. (2020). Fundamental Concepts Of Artificial Intelligence And Its Applications. *Journal Of Mathematical Problems, Equations And Statistics*, *1*(2), 13–24.

Chigova, L. E., & Hofisi, C. (2025). *Democratisation And Emerging Technologies In Africa: Can Ai Deliver Free And Fair Elections?*

Ertel, W. (2024). *Introduction To Artificial Intelligence*. Springer Nature.

Hopgood, A. A. (2021). *Intelligent Systems For Engineers And Scientists: A Practical Guide To Artificial Intelligence*. Crc Press.

Jafar, U., Ab Aziz, M. J., Shukur, Z., & Adnan Hussain, H. (2024). Secure-Tech Triad Enhancing Electronic Voting System Security Through Integrated Blockchain, Ai, And Iot Technologies. *Itm Web Of Conferences*, *63*, 1011.

Jarrahi, M. H., Lutz, C., & Newlands, G. (2022). Artificial Intelligence, Human Intelligence And Hybrid Intelligence Based On Mutual Augmentation. *Big Data & Society*, *9*(2), 20539517221142824.

Krishnamoorthy, C. S., & Rajeev, S. (2018). *Artificial Intelligence And Expert Systems For Engineers*. Crc Press.

Kühl, N., Schemmer, M., Goutier, M., & Satzger, G. (2022). Artificial Intelligence And Machine Learning. *Electronic Markets*, *32*(4), 2235–2244.

Lee, R. S. T. (2020). *Artificial Intelligence In Daily Life*.

Maphephe, J. (2025a). Artificial Intelligence (Ai) And Its Role In Electoral Integrity In The Context Of The 2024. *Available At Ssrn 5473305*.

Maphephe, J. (2025b). Artificial Intelligence (Ai) And Its Role In Electoral Integrity In The Context Of The 2024 South African General Elections—A Policy Analysis Paper. *J Cogn Comput Ext Realities*, *1*(1), 1–15.

Mccarthy, J. (2022). Artificial Intelligence, Logic, And Formalising Common Sense. *Machine Learning And The City: Applications In Architecture And Urban Design*, 69–90.

Milea, T. D., & Siminiuc, R. (2025). Algorithmic Auditing In The Age Of Disinformation: An Analysis Of Electoral Integrity Challenges In Eastern Europe. *2025 24th Roedunet Conference: Networking In Education And Research (Roedunet)*, 1–7.

Mulli, J. (2024). From" Do No Evil" To" Can't Do Evil" Ai-Enhanced Blockchain Technology As A Transformative Paradigm For Kenya, Addressing Finance, Corruption, And Voter Fraud.: From" Do No Evil" To" Can't Do Evil" Ai-Enhanced Blockchain Technology As A Transformative Paradigm For Kenya. *European Academic Journal-I*, *3*(001).

Mwansa, P. (2023). *Trust System Framework For Integrity Controls In Electoral Vote Counting And Validation*. Cape Peninsula University Of Technology.

Natale, S., & Ballatore, A. (2020). Imagining The Thinking Machine: Technological Myths And The Rise Of Artificial Intelligence. *Convergence*, *26*(1), 3–18.

Novelli, C., & Sandri, G. (2024). Digital Democracy In The Age Of Artificial Intelligence. *Arxiv Preprint Arxiv:2412.07791*.

Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., Nuhu, B. K., Olaniyi, O. M., Ambafi, J. G., & Sheidu, V. B. (2025). Blockchain For Securing Electronic Voting Systems: A Survey

Of Architectures, Trends, Solutions, And Challenges. *Cluster Computing*, *28*(2), 132.
Peelam, M. S., Kumar, G., Shah, K., & Chamola, V. (2025). Democracyguard: Blockchain-Based Secure Voting Framework For Digital Democracy. *Expert Systems*, *42*(2), E13694.
Rafi, M. (2025). Reimagining Democratic Elections: An Ai-Powered Techno-Democratic Republic. *Available At Ssrn 5507579*.
Samoili, S., Cobo, M. L., Gómez, E., De Prato, G., Martínez-Plumed, F., & Delipetrev, B. (2020). *Ai Watch. Defining Artificial Intelligence. Towards An Operational Definition And Taxonomy Of Artificial Intelligence*.
Simoes, S., & Maccarthaigh, M. (2023). Ai And Core Electoral Processes: Mapping The Horizons. *Arxiv Preprint Arxiv:2302.03774*.
Sujatha, B., Ganesh, Y., Leelavathy, N., Tamilkodi, R., Venkatesh, S., Sandhya, B., & Kowshik, T. S. (2024). Blockchain-Powered E-Voting: A Novel Approach To Secure Voter Authentication, Online Voting And Election Automation. *Indian Journal Of Science And Technology*, *17*(47), 4948–4958.
Tussyadiah, I. (2020). A Review Of Research Into Automation In Tourism: Launching The Annals Of Tourism Research Curated Collection On Artificial Intelligence And Robotics In Tourism. *Annals Of Tourism Research*, *81*, 102883.
Zhuravlov, D. V, & Zhuravlov, D. D. (2025). Automated Complex" Electronic Signature Of The Voter (Epo)" As An Element Of The Critical Infrastructure Of The Election Process. *Metaverse Science, Society And Law*, *1*(2).