The Development of an Artificial Intelligent (AI) Driven Election Monitoring System

Umebe Anthony Chukwudumebi (IFT/19/0687)

Department of Information Technology, Federal University of Technology, Akure (FUTA)

DOI: https://dx.doi.org/10.51584/IJRIAS.2025.10100000189

Received: 12 November 2025; Accepted: 18 November 2025; Published: 22 November 2025

ABSTRACT

This paper explored the creation of an Artificial Intelligent (AI) Driven Election Monitoring System that will enhance transparency, accuracy, and credibility in the voting process. This project has aided in overcoming the long time difficulties in manual election monitoring with the implementation of automated surveillance, fraud detection and report generation on an integrated digital platform. The system examined the information in electronic voting databases, social media trends, and live feeds of monitoring to identify abnormalities and identify potential risk factors in real time using artificial intelligence (AI) algorithms. The front end of the system was created with React.js and the backend was created with Node.js and data was stored in PostgreSQL. The social analysis and fraud detection algorithms were represented as AI module using natural language processing and fraud detection algorithms. The results indicated that the built system was effective in minimizing human error, enhancing the response time, and making better decisions during elections. The findings confirm the ability of the system as a useful model in enhancing electoral integrity and accountability in the democratic processes.

Keywords: Artificial Intelligence, Election Monitoring, Anomaly Detection, Transparency, Accountability

INTRODUCTION

Elections are what democracy is all about as they offer a main mechanism that allows citizens to elect their representatives and legitimize the government. Political stability and trust of institutions by the population therefore depend on the credibility of electoral processes.

The establishment of strong election monitoring is known to be very crucial in most countries and particularly in the emerging democracies in protecting this legitimacy. There are major limitations with conventional methods of election monitoring, use of human monitors, however. Human checkers are only able to survey a small part of voting sites and would in most cases be unable to check fraud schemes that are more intricate or hidden, particularly those that are manifested in a statistical irregularity or in cyber space. The flaws of the traditional approaches are even more evident as the elections become more and more electronic and affected by social media.

The development of artificial intelligence (AI) provides new opportunities to eliminate these limitations. AI-powered systems are able to process large volumes of data in real time whether it is polling station reports or content on social media well beyond what human monitors are capable of processing. The algorithms of machine learning can identify the spikes of reported votes that are unusual, campaigns of misinformation can be identified by the algorithms of natural language processing, and the irregularities in the activities in the live video feeds in the polling stations can be identified by the algorithms of computer vision. Although potentially promising, AI in election monitoring comes with some serious ethical and technical issues, such as bias in the algorithms, voter privacy, or the fact that it requires transparency and accountability.

The present project overcomes these obstacles by creating an Election Monitoring System (Poll Secure) that is an integrated system based on AI. The system integrates various AI tools into a single unit to offer election observers real-time monitoring and decision support, and improve their capability of identifying and acting in response to irregularities as they occur. The main objective of this research was to design and deploy this system with the view of enhancing integrity of elections by real-time reporting and detection of electoral irregularities.

MATERIALS AND METHODS

The creation and testing of the system of the Poll Secure were based on the organised and quantitative research method. This section describes system architecture, data sources, implementation of AI model and evaluation metrics.

System Architecture

Poll Secure is an automated voting monitoring system that is meant to combine AI with real-time data stream. The architecture is modular, which guarantees scalability and maintainability. Once the secure login, an observer communicates with a central dashboard that gives an in-depth view of the election. A set of AI models runs on the back-end of the system and its data processing pipeline is event-driven thus ensuring that high input volumes are processed with low latency.

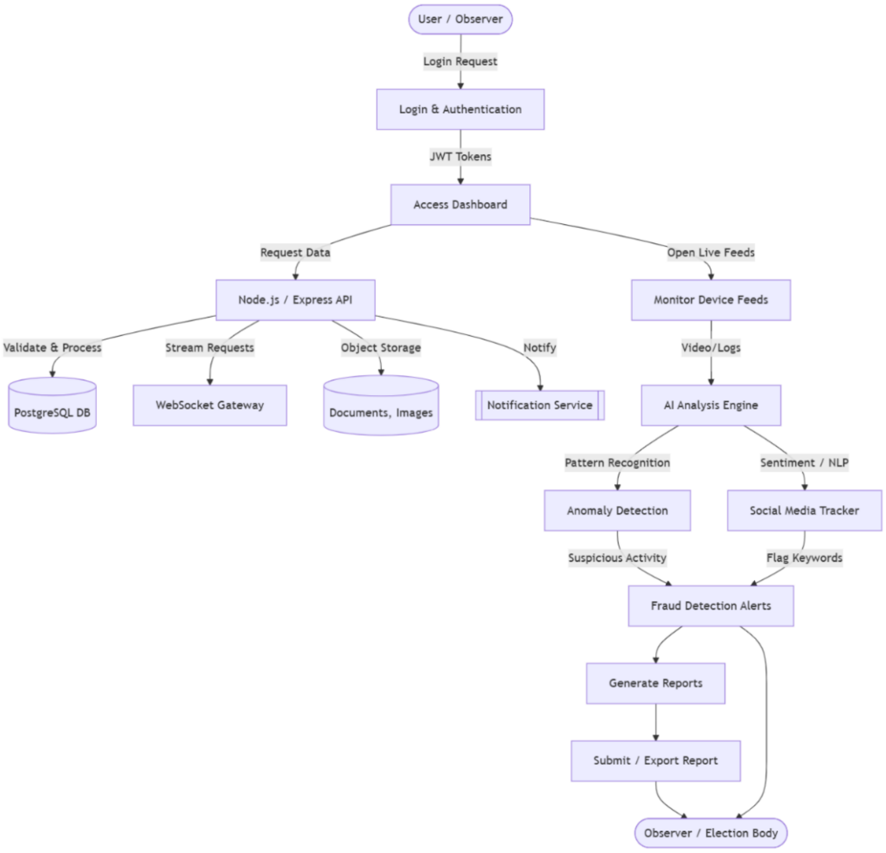


Figure 1: System Architecture Diagram for Poll Secure

The system is designed in such a way that it consists of five main functional modules that can be accessed via a friendly interface:

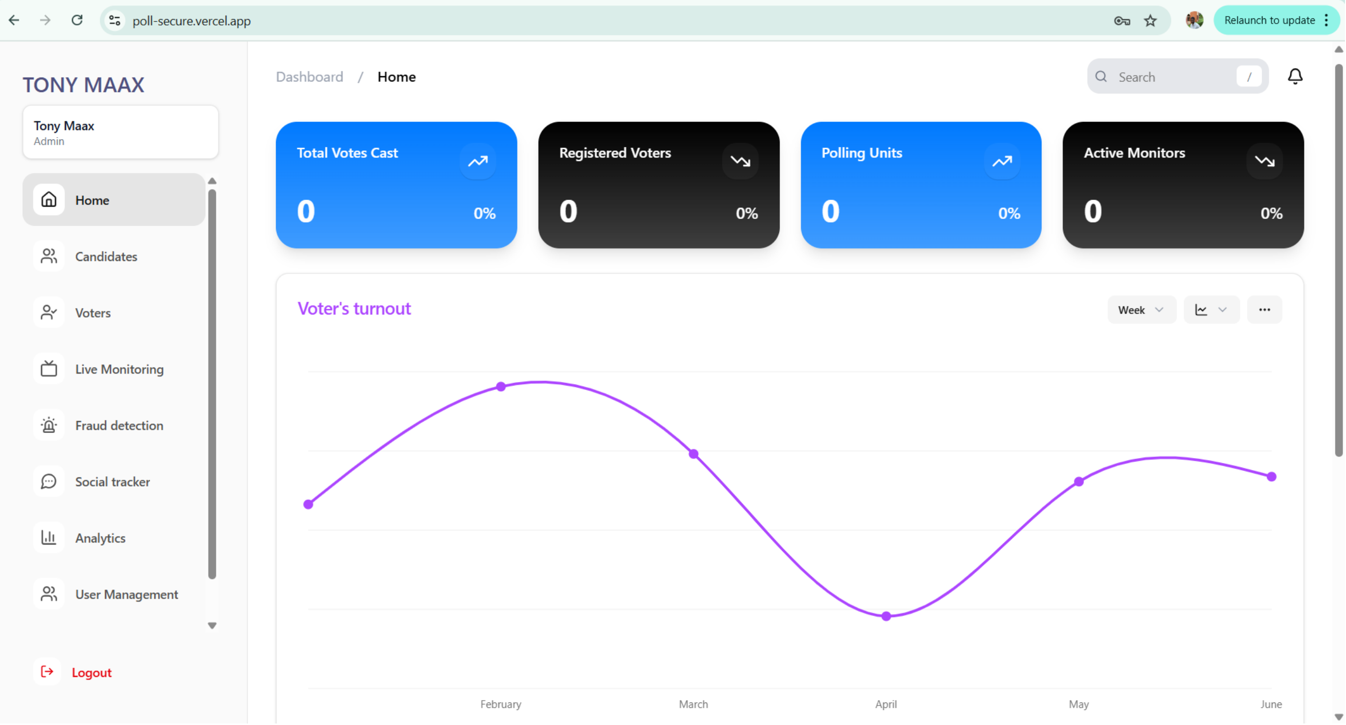
Dashboard (Overview): It is the main entry point where we can see the real-time overview of the most important election indicators, such as voter turnout, cast votes, active voting points, and high-priority notifications.

Live Monitoring: Provides live video streaming and live statistical coverage of polling units, and interactive geospatial map which overlays the polling station status.

Fraud Detection: An AI-based module that verifies the data in voting and real-time to recognize possible malpractices like ballot stuffing, anomalous voting patterns, or differences between the number of registered voters and voters casting their ballots.

Social Tracker: Surveillance of online discussion on the most popular social media, identifying and preventing misinformation, hate speech, or coordinated actions that can provoke unrest or manipulate voters through the application of NLP.

Reports: It is an integrated tool that enables the user to create, label, and export organized summaries of watched actions, gathering data of all different modules together to be reviewed by the official.


poll-secure.vercel.app

Relaunch to update

TONY MAAX

Tony Maax
Admin

Home
Candidates
Voters
Live Monitoring
Fraud detection
Social tracker
Analytics
User Management

Logout

Dashboard / Home

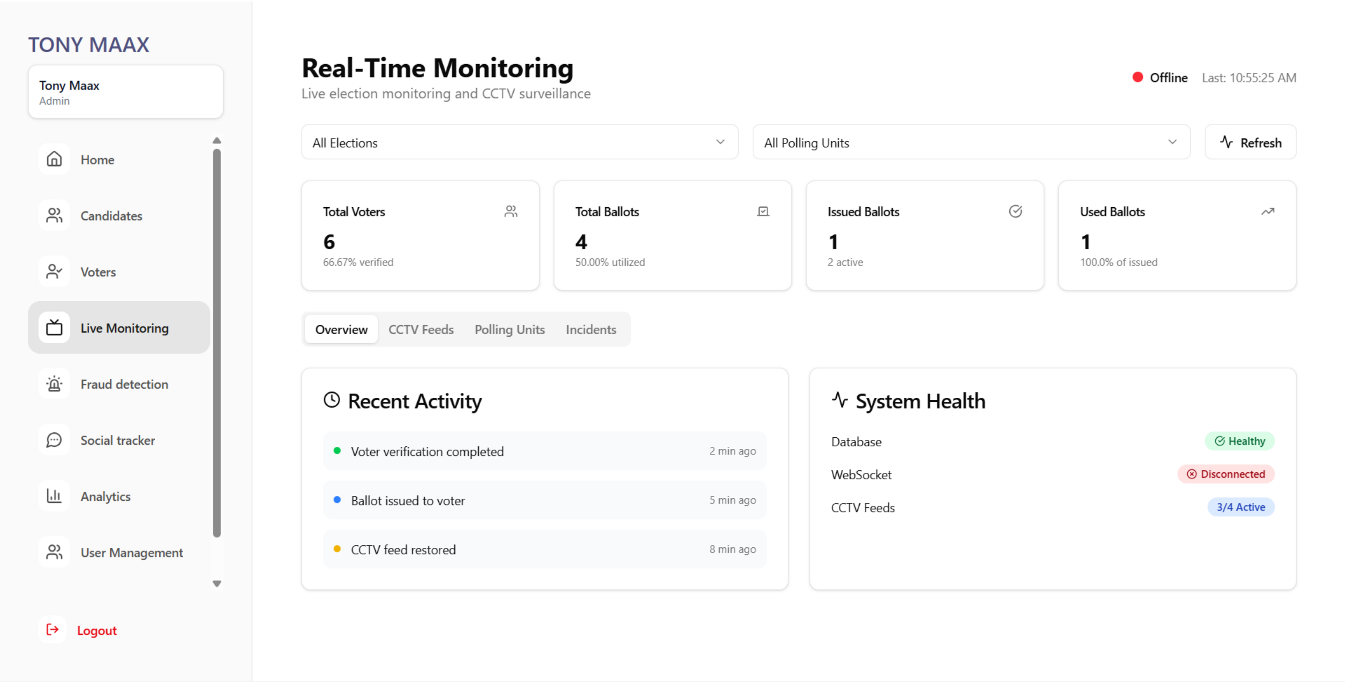
Search

Total Votes Cast 0 0%
Registered Voters 0 0%
Polling Units 0 0%
Active Monitors 0 0%

Voter's turnout

Week

Figure 2: Dashboard (Overview) interface of Poll Secure


TONY MAAX

Tony Maax
Admin

Home
Candidates
Voters
Live Monitoring
Fraud detection
Social tracker
Analytics
User Management

Logout

Real-Time Monitoring
Live election monitoring and CCTV surveillance

Offline Last: 10:55:25 AM

All Elections
All Polling Units
Refresh

Total Voters
6
66.67% verified

Total Ballots
4
50.00% utilized

Issued Ballots
1
2 active

Used Ballots
1
100.0% of issued

Overview CCTV Feeds Polling Units Incidents

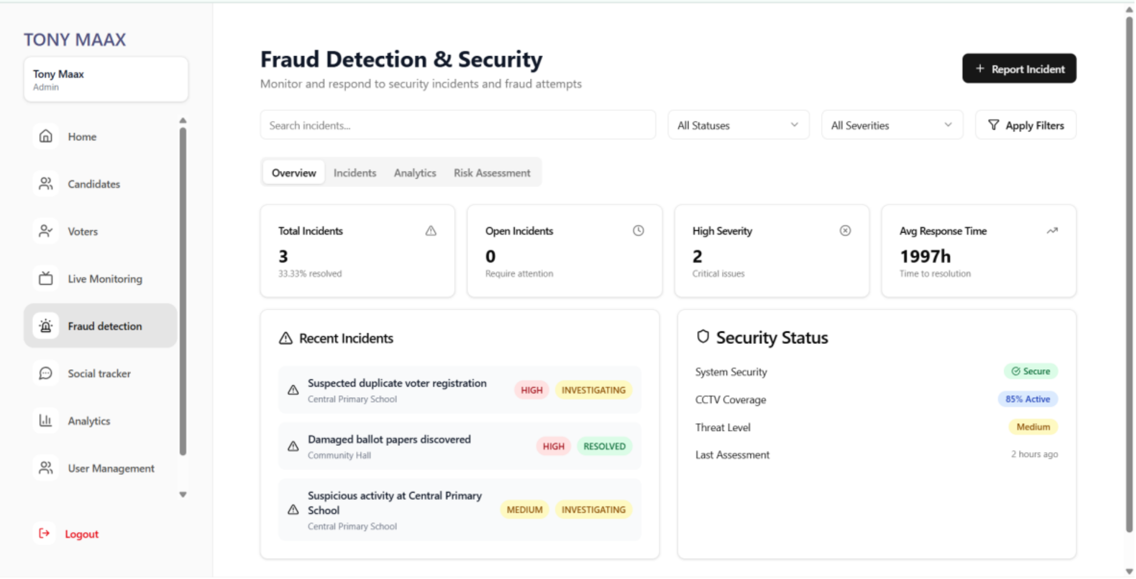
Recent Activity

Voter verification completed 2 min ago
Ballot issued to voter 5 min ago
CCTV feed restored 8 min ago

System Health

Database Healthy
WebSocket Disconnected
CCTV Feeds 3/4 Active

Figure 3: Real-time monitoring interface for Poll Secure



Fraud Detection & Security

Monitor and respond to security incidents and fraud attempts

Total Incidents 3 — 33.33% resolved

Open Incidents 0 — Require attention

High Severity 2 — Critical issues

Avg Response Time 1997h — Time to resolution

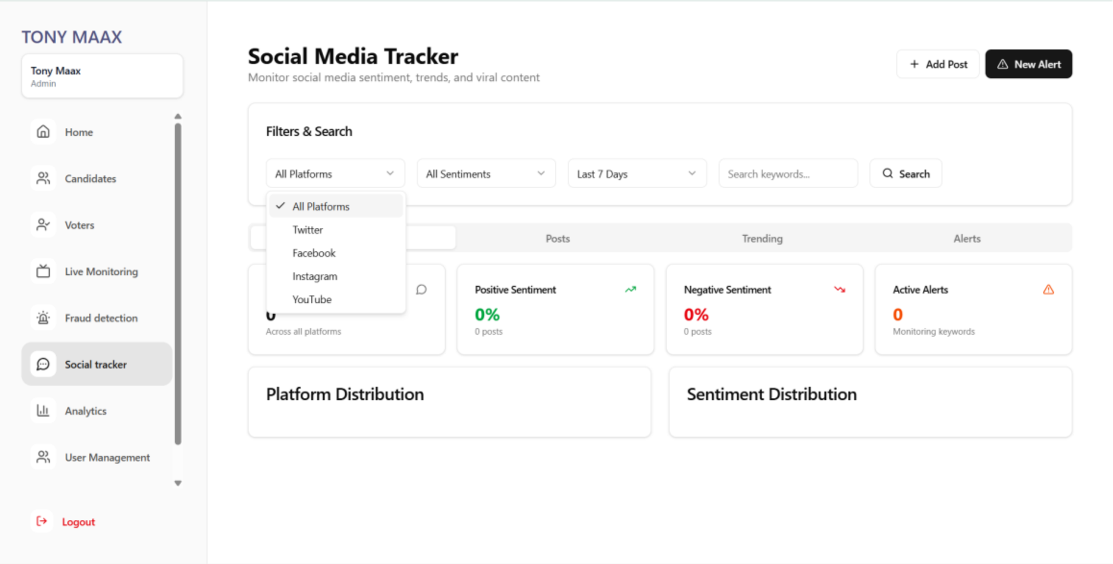
Recent Incidents

- Suspected duplicate voter registration — Central Primary School — HIGH — INVESTIGATING
- Damaged ballot papers discovered — Community Hall — HIGH — RESOLVED
- Suspicious activity at Central Primary School — Central Primary School — MEDIUM — INVESTIGATING

Security Status

System Security	Secure
CCTV Coverage	85% Active
Threat Level	Medium
Last Assessment	2 hours ago

Figure 4: Fraud Detection Interface



Social Media Tracker

Monitor social media sentiment, trends, and viral content

Filters & Search

0 — Across all platforms

Positive Sentiment 0% — 0 posts

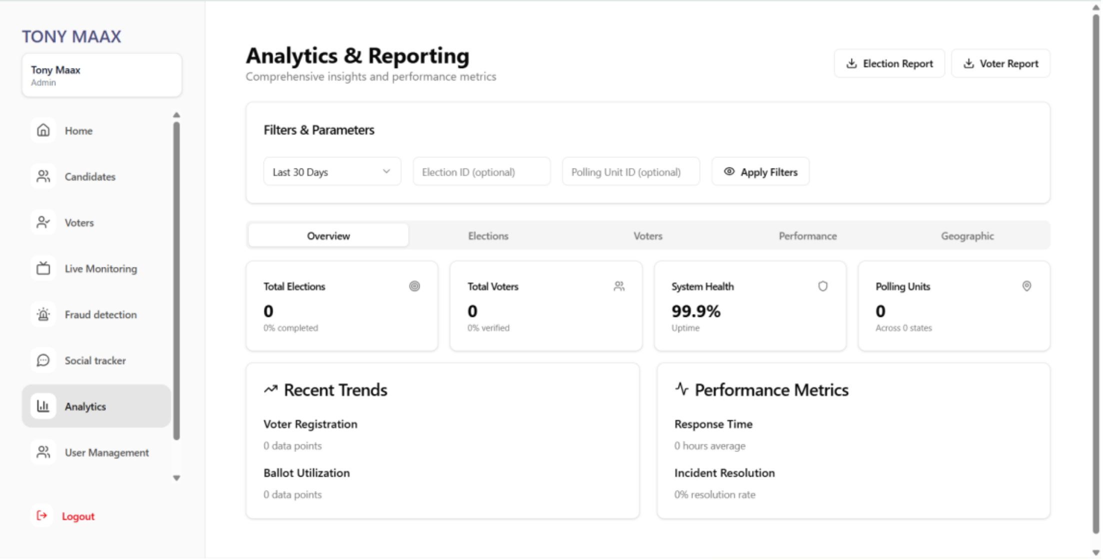
Negative Sentiment 0% — 0 posts

Active Alerts 0 — Monitoring keywords

Platform Distribution

Sentiment Distribution

Figure 5: Social Media Tracking Interface



Analytics & Reporting

Comprehensive insights and performance metrics

Filters & Parameters

Total Elections 0 — 0% completed

Total Voters 0 — 0% verified

System Health 99.9% — Uptime

Polling Units 0 — Across 0 states

Recent Trends

Voter Registration — 0 data points

Ballot Utilization — 0 data points

Performance Metrics

Response Time — 0 hours average

Incident Resolution — 0% resolution rate

Figure 6: Analytics and Reporting Interface

Data Sources and Preprocessing

The sensitivity of the work, as well as the logistical difficulties in getting the live election data, led to the use of a mix between publicly available anonymized datasets, and carefully designed synthetic data, used as training and validation data. This method gave a regulated and ethical setting of model development.

- Polling Unit Data: Artificial data on voter turnout and biometric scans and vote counts was created to represent the electoral tendencies. These datasets were biased with a range of anomalies (e.g. sudden spiking of turnout, abnormal temporal distributions) on the basis of known cases of electoral malpractice in the real world.
- Social Media Data: Publicly available datasets of historical social media posts were screened based on election related key words. There were also simulated real time text streams that were used to train the NLP models to recognize misinformation, hate speech and propaganda.
- Video Feed Data: The simulated video scenarios were created to mimic polling stations activities. These were regular processes as well as simulated anomalies like tampering of ballot boxes, intrusion, or suspicious human movements that were used to train the computer vision models.

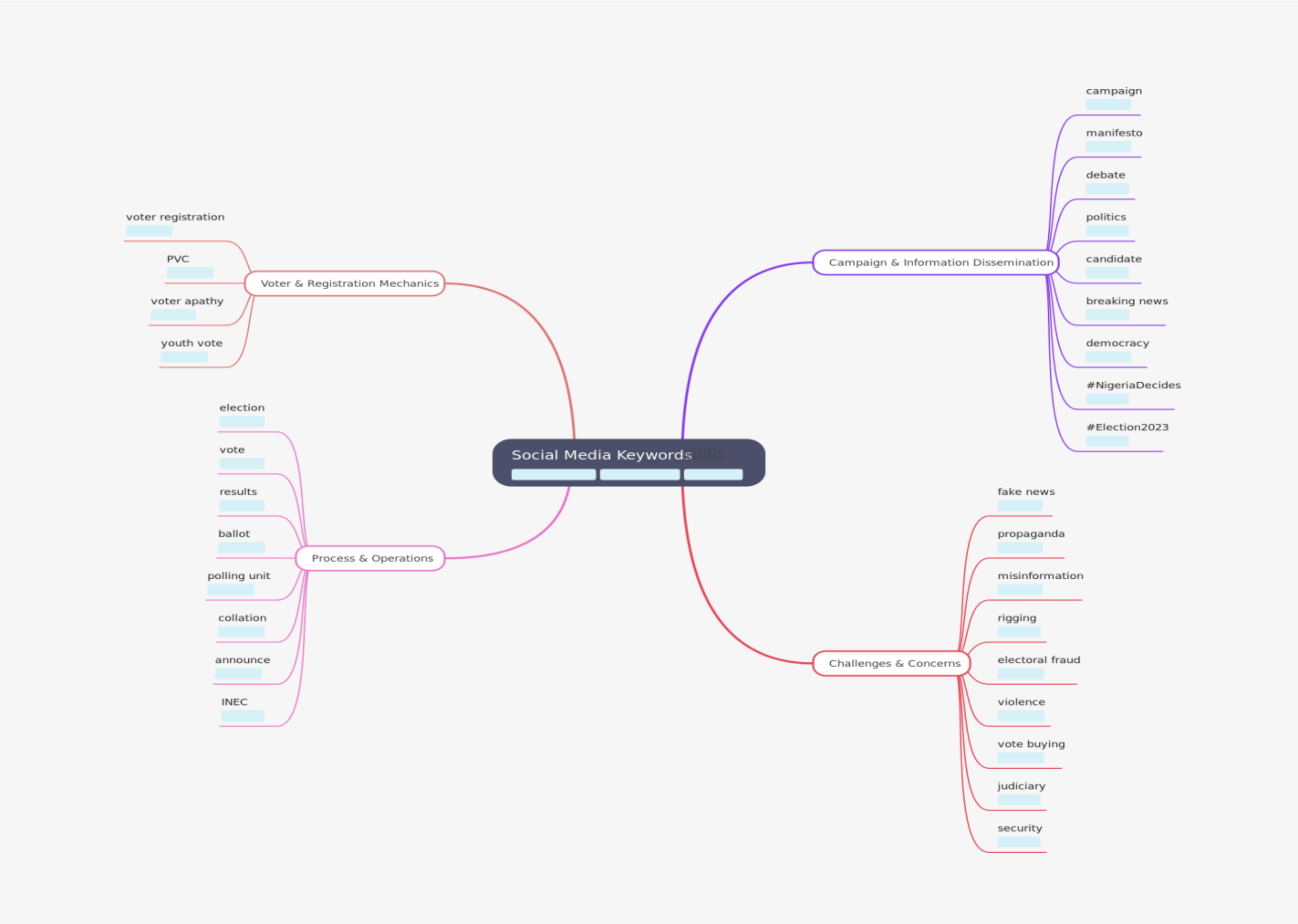


Figure 7: Social media keywords used for sentiment analysis

AI Model Implementation

The essence of the concept of Poll Secure lies in the fact that it incorporates a multi-modal AI framework that uses specific and specialized models to examine data streams in order to provide proper classification of anomalies in physical, digital, and statistical space. In order to track physical activities in polling stations, Convolutional Neural Network (CNN) is used to process live video frames in real time. Being trained on simulated video data of normal and irregular activity, this model makes use of its convolutional, max-pooling and fully connected layers to classify an event such as ballot box tampering or the appearance of unauthorized personnel, placing a confidence score upon it to be flagged and alerted upon immediately. At the same time, a powerful Natural Language Processing (NLP) pipeline is used in the Social Tracker module to track social conversations. Text on the Facebook, X and Instagram platforms is ingested and pre-processed by this pipeline, where a hybrid process based on a pre-trained sentiment analysis model (VADER) is used and combined with key-matching algorithms to determine the tone of emotion and identify high-risk content. It also examines the trends in posting in order to identify organized misinformation campaigns or hate speech. In addition to these, the Fraud Detection module uses an unsupervised Isolation Forest algorithm that detects statistical anomalies in electoral data. This model defines a baseline of normal voting data then evaluates incoming polling information to raise newsworthy alarms on statistical anomalies, e.g. unlikely voter turnout spikes or inconsistency in vote counts, which are raised to high-priority handling as alarms requiring human intervention.

Evaluation Methodology

The performance of the system was evaluated in a quantitative manner with respect to the precision of the functional modules that the system has in reference to traditional manual monitoring. The assessment system was based on a list of key performance indicators (KPIs) and conventional machine learning metrics in order to be able to offer a comprehensive and objective evaluation.

1) Accuracy: This measure indicates the percentage of correct identifications or identifications of the number of instances. It was considered as a primary measuring tool of overall performance of each functional module. Although it helped obtain a general overview, it was supplemented by other metrics to ensure that there were no imbalances in the data in terms of classes. The components were established during evaluation as follows.

True Positive (TP): A real anomaly that was detected by the system as such (e.g., a known ballot box tampering).

True Negative (TN): The system correctly not notified a legitimate event (e.g. a normal voter queue is considered a non-threatening event).

False Positive (FP): A legitimate event that was inaccurately detected as an irregularity by the system (a false alarm, i.e. a high, but valid, voter turnout).

False Negative (FN): An actual anomaly that the system was unable to identify (a missed threat (e.g. coordinated misinformation campaign) that was not detected).

2) Precision and Recall: The two measures were essential when assessing the classification models in the Fraud Detection and Social Tracker modules.

Precision is defined as the percentage of true positive identifications of all positive identifications of the system. Precision was a high value to make sure that whenever the system indicated an occurrence as an irregularity, there was a high probability of a real occurrence meaning that any load of false alarms was minimized.

Recall (or Sensitivity) is the measure of the percentage of the real positive instances that the system has recognized. An important factor was high recall to guarantee the capability of the system to capture most of actual electoral threats minimizing chances of overlooking some important irregularities.

3) F1-Score: it is the harmonic mean of Precision and Recalls, which gives one score that balances Precision and Recall. It was applied to give a more detailed evaluation of the performance of the classification models in situations where there is a trade-off between false positives reduction and a reduction in false negative.

4) Detection Speed: This KPI determined the interval between the receipt of data and the creation of an alert about a detected irregularity. It was a decisive step towards the effectiveness of the system in the real-

time monitoring since the promptness in the case of timely intervention is reliant on the detection of possible problems.

5) Scalability: This was measured by examining how many streams of concurrent data (e.g. thousands of polling units) patchable by the system without showing a significant decrease in system performance. This played a vital role in the determination of whether the system was viable to conduct large scale and national elections.

6) Reliability: This was evaluated by determining the stability of the system outputs when similar inputs were used and comparing the objective data-driven analysis with the subjective nature of the human observer and his/her fatigue and bias. This parameter was critical in achieving credibility in the automated monitoring procedure.

RESULTS AND DISCUSSION

The modules of the system were tested under a controlled and simulated environment to determine the accuracy of the modules, and comparative analysis was done with the manual monitoring process. The tests have been conducted on the hardware and software stack that was described above and an example of a live system prototype is publicly available to use as a demonstration at https://poll-secure.vercel.app/.

Accuracy of Functional Modules

The individual module level assessment showed good performance in the board. Live Monitoring module was most accurate with a score of 93 and this was credited to the fact that live video feeds were well processed and metadata could be synchronized accurately. The Reports Module had 91% accuracy, which means that it is a trustworthy observer submission and AI-generated insights management. The Insights Module achieved a score of 90 per cent. The lowest accuracy of 88 was registered in Sentiment Analysis Module since the analysis of subtle language on social media is difficult.

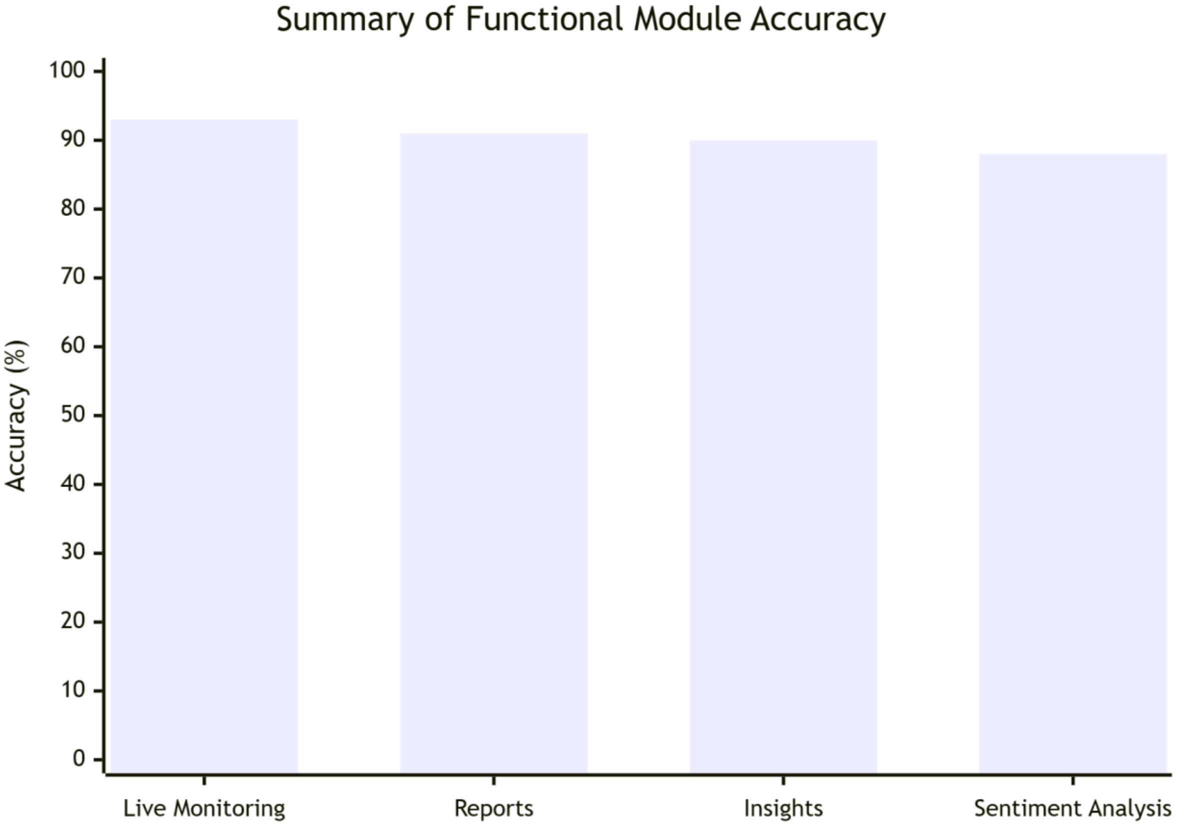


Figure 8: Results from Accuracy Testing of Poll Secure

Comparison of the performance of a manual and the AI-driven system

The AI-based system was far superior to the traditional manual monitoring in three main indicators of speed of its detection, scalability, and reliability. By automatically identifying anomalies in a real-time, the AI system attained a score of more than 90 on detection speed, compared to less than 50 with the manual ones. To be able to scale, the AI system achieved almost 95% results by absorbing data and processing it across a range of sources at once, which with manual monitoring is at a severely reduced result (scoring at around 40%). Lastly, the AI system was more reliable (more than 90%), because individual steps are consistent and objective, and manual operations (around 55) are prone to fatigue and prejudice.

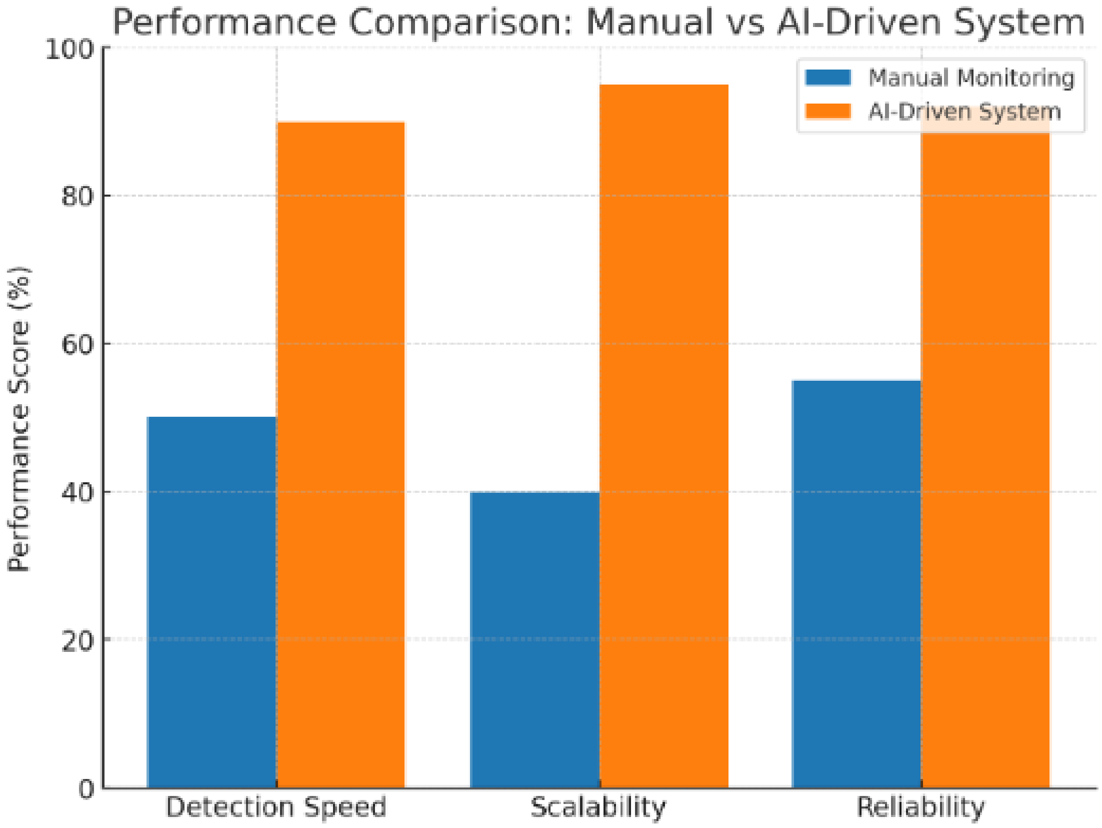


Figure 9: Performance Comparison Results: Poll Secure vs Manual Methods

Discussion

The findings of the experiments prove that the purpose of the system, which was to increase the transparency, efficiency, and accountability of the election monitoring, was reached by the "Poll Secure" system. The fact that its functional modules are very accurate especially in live monitoring and reporting proves that the system can offer real-time oversight with high accuracy.

The fact that the AI-driven system has a high level of efficiency as opposed to manual approaches underscores how technology can be transformed to enhance democracy. The capability to uncover irregularities much faster, conduct elections on a bigger scale, and deliver more trustworthy data decreases human error and allows the interested parties to act proactively to threats to electoral integrity. This is in line with other past researches that suggest the use of technology as a way of addressing the constraints of conventional supervision.

Nevertheless, there were weaknesses identified during the assessment. The 88% precision of the sentiment analysis module highlights the persistence of the NLP issues particularly with regards to deciphering sarcasm, local dialects and ambivalent language posts. In addition to this, the system requires steady internet access to live data feeds thereby making it a practical challenge to be deployed in the rural or poorly-infrastructure area.

Such restrictions imply some obvious guidelines about the future efforts, such as improving NLP models by providing them with more diverse training data and creating offline features

CONCLUSION AND RECOMMENDATIONS

This paper has effectively proven the feasibility and effectiveness of an integrated AI based system to be used to monitor elections. Through the creation and execution of the so-called Poll Secure, we have demonstrated that the constraints of the traditional, manual observation could be eliminated with the use of automated surveillance and fraud detection and real-time reporting. The system offers a powerful platform that empowers the sanctity of the democratic processes because it is able to identify the abnormality in a timely manner and thus breed confidence in the citizens toward the election results.

Regardless of the difficulties associated with the data access and calculations, this project provides a viable basis of the AI use in election oversight. The development of a more sophisticated AI model, the inclusion of such technologies as biometrics and blockchain to enhance the security level, the creation of mobile and offline versions to ensure a higher level of accessibility, and the establishment of collaborations with electoral institutions to implement the models in practice and constantly improve their functionality should be considered future work. The results of this project add a practical and theoretical improvement to the existing expansive area in AI to benefit civic good, providing a solution, which can be scaled to manage elections with credibility and accountability.

ADDITIONAL INFORMATION

Author Contributions: All the authors have gone through the final copy that will be published and they have accepted to bear the full responsibility of the work.

- Concept and design: Anthony C. Umebe, Olutayo K. Boyinbode.
- Purchasing, examining, or interpreting information: Anthony C. Umebe.
- Manuscript writing: Anthony C. Umebe.
- Important intellectual material critical review of the manuscript: Olutayo K. Boyinbode.
- Supervision: Olutayo K. Boyinbode.

Disclosures

- Human subjects: The authors have ensured that this research was not a case of human subjects or tissue.
- Animal subjects: An animal subject or tissue was not involved in this study, as it has been confirmed by all authors.
- Conflicts of interest: All the authors state that they do not have any conflicts of interest in accordance with the ICMJE uniform disclosure form.

REFERENCES

1. Asiryan, S. S. (2023). Artificial intelligence use in elections: Practice, endangerment of the right to vote and how to resist it. Uzhhorod National University Herald, Series: Law.
2. Bacelar, M. (2021). The bias and fairness in machine learning models: A review. ScienceOpen Preprints.
3. Bhujel, S., Bhattarai, S., Neupane, N., and Adhikari, S. (2023). Artificial intelligence and blockchain voting system. KEC Journal of Science and engineering, 7(1), 99-104.
4. Chennupati, A. K. (2024). Artificial intelligence poses a threat to elections all over the world: A 2024 overview. World Journal of Advanced engineering technology and sciences 12(1), 29-34.
5. Jain, N., & Patil, S. (2024). Fraud detection models based on artificial intelligence: Progress, issues and future opportunities. International Journal of Global Innovations and Solutions, 3(1) 45-61.
6. Lacasa, L., & Fernandez-Gracia, J. (2018). Election forensics Quantitative electoral fraud detection. Forensic Science International, 294, e19-e22.

7. Maine, I. M., & Esiefarienrhe, B. M. (2024). Effects of artificial intelligence and ethical considerations and technologies on the election process. E-Journal of Humanities, Arts and social sciences, 5(16), 3211-3219.
8. Manheim, K. M., & Kaplan, L. (2019). Artificial intelligence: Privacy and democracy risks. Yale Journal of Law and Technology 21(1), 106-134.
9. Olufunmilayo, O., & Ibukunoluwa, B. O. (2023). How effective are electronic voting systems in Nigeria: Evaluating electro-voting systems in Nigeria. African Journal of Politics and Administrative Studies, 16(2), 84-104.
10. Srivastava, B., Nikolich, A., and Koppel, T. (2023). Artificial Intelligence and elections: Special issue introduction. AI Magazine, 44(3), 7-10.
11. Islam, T., Islam, S. M., Sarkar, A., Rahman, A. J. M. O., Khan, R., Paul, R., and Bari, M. S. (2024). Fraud detection and financial risk mitigation with artificial intelligence: Future trends and business purpose. International Journal of Multidisciplinary Research.