LAUTECH Journal of Computing and Informatics (LAUJCI) – ISBN : 2714-4194
Volume 5 No.1, April 2026 – www.laujci.lautech.edu.ng

Design and Implementation of an Online Whistle-Blower Reporting System to Combat Public Property Vandalism in Lagos State

Ayorinde Felix Ajibaye
Department of Information Systems & Technology
National Open University of Nigeria (NOUN)
ajibaye@gmail.com

O.M. Olaniyan
Department of Computer Engineering
Federal University Oye-Ekiti (FUOYE)
olatayo.olaniyan@fuoye.edu.ng

ABSTRACT
Public property vandalism presents a growing challenge in Lagos State, with existing whistle-blowing mechanisms often constrained by inadequate anonymity, weak feedback mechanisms, and limited citizen trust. This study presents the design and implementation of an Online Whistle-Blower Reporting System aimed at addressing these gaps. The system was developed using the Design Science Research Methodology (DSRM) and informed by the Technology Acceptance Model (TAM) and trust-based privacy principles. It was implemented using the MERN (MongoDB, Express.js, React.js, Node.js) stack and deployed on AWS cloud infrastructure. Key features include anonymous and confidential reporting, multimedia evidence submission, password-protected case tracking, and role-based dashboards for administrators and relevant agencies. The system was evaluated through functional testing, usability assessment, performance testing, and penetration testing, with results indicating a 93.3% functional pass rate, a 90% task completion rate for usability, and average response times of under two seconds. The system also demonstrated resilience against common vulnerabilities based on assessments using OWASP ZAP and Burp Suite. Comparative analysis with existing whistle-blowing platforms in Nigeria suggests improvements in usability, accessibility, and reporting transparency. While the system was evaluated in a controlled environment, the findings indicate its potential to support more effective reporting mechanisms and contribute to civic engagement in Lagos State.

Keywords: whistleblowing, vandalism, Lagos State, civic technology, digital governance.

1. INTRODUCTION

Public property vandalism has emerged as a persistent challenge in Lagos State, Nigeria, undermining infrastructure development and diverting public resources to costly replacements. Damage to critical infrastructure such as streetlights, manhole covers, underground cables, and government buildings leads to substantial replacement costs and slow urban progress (Oluwakayode et al., 2024). In fact, these researchers found that property-related crimes significantly hinder infrastructure development in Nigerian cities by diverting funds from developmental to non-developmental expenditures. Despite various government efforts to address this issue, existing reporting mechanisms remain limited and often ineffective.

Current reporting channels in Lagos, such as web-based forms (e.g., CitizensGate) and telephone hotlines, face several challenges, including poor user experience, weak feedback mechanisms, and limited support for anonymity. These limitations reduce citizen engagement in reporting vandalism incidents. Prior research suggests that web-based reporting systems are more effective than conventional reporting channels in safeguarding whistleblowers' identities, as they incorporate mechanisms that enhance anonymity, confidentiality, and data security (Hauser, 2021).

Web-based systems can support anonymous reporting, multimedia evidence submission, and real-time feedback, thereby improving accessibility and responsiveness. However, there is currently no

dedicated, integrated whistle-blower reporting platform tailored to the Lagos State context, highlighting a gap in both practice and research.

This study addresses this gap by designing and implementing a secure, user-friendly whistle-blower reporting system for Lagos State. The objectives of the study are to: (i) design a platform that supports anonymous and confidential reporting, (ii) implement features such as multimedia uploads, case tracking, real-time notifications, and role-based dashboards, (iii) evaluate the system's usability, performance, and security through controlled testing, and (iv) compare its performance with selected existing reporting platforms in Nigeria.

This study contributes by developing and evaluating a secure, user-friendly whistle-blower reporting system tailored to the Lagos State context. Grounded in the Technology Acceptance Model (TAM) and trust-based privacy principles, the system integrates anonymity, multimedia evidence submission, case tracking, and role-based dashboards within a unified platform. It also provides empirical evaluation of functional accuracy, usability, performance, and security in a controlled environment, offering insights into the design of trustworthy civic reporting systems in developing contexts.

2. LITERATURE REVIEW

2.1 Theoretical Frameworks

This study is grounded in the Technology Acceptance Model (TAM) and trust-based privacy frameworks to explain user adoption of whistle-blowing systems. The Technology Acceptance Model, proposed by Davis (1989), posits that user adoption of technology is primarily determined by two constructs: Perceived Usefulness (PU) and Perceived Ease of Use (PEOU). In the context of whistle-blowing platforms, citizens are more likely to adopt a system if they perceive it as effective in reporting incidents and easy to use.

However, for platforms handling highly sensitive information, TAM alone is insufficient. Research extending TAM into e-services and digital governance demonstrates that "Trust" must be integrated as a foundational construct alongside PU and PEOU (Wu et al., 2011). Trust and perceived anonymity play a critical role in whistle-blowing behavior; individuals are significantly more willing to report illicit activities when they are confident that their identity is protected and that the system ensures a high level of confidentiality and data security (Hauser, 2021).

Based on these theories, this study integrates key design features such as anonymous reporting, password-based case tracking, secure data handling, and user-friendly interfaces to enhance perceived usefulness, ease of use, and institutional trust. These elements form the conceptual foundation guiding the design, implementation, and evaluation of the proposed whistle-blower reporting system for Lagos State.

2.2 Review of Related Works

Public property vandalism encompasses the intentional destruction, defacement, or theft of infrastructure such as streetlights, manhole covers, rail tracks, and transformers. In Lagos State, this issue has become increasingly significant due to rapid urbanization. Oluwakayode et al. (2024)

examined how vandalism and theft hinder urban development in the Lagos metropolis, noting that such activities divert resources from developmental to non-developmental expenditures. While their study highlights the importance of security partnerships and citizen engagement, it does not propose concrete technology-based interventions, which are particularly relevant in contexts like Nigeria where comprehensive whistle-blowing legislation offering statutory protection to citizens is still lacking (Ojobo, 2023). Similarly, Khalilikhah et al. (2016) demonstrated that infrastructure vandalism is non-random and correlated with socio-demographic variables such as poverty and population density. However, their work focuses primarily on predictive modelling and does not address proactive, citizen-driven mitigation strategies.

Digital civic engagement has been identified as a potential approach to addressing such challenges. Kumare (2024) notes that digital platforms can support collective action by enabling citizens to participate more actively in governance processes. In this context, online whistle-blower systems can provide structured channels through which citizens can report incidents and contribute to infrastructure protection.

The effectiveness of such systems, however, depends significantly on user trust and perceived safety. In environments where reporting misconduct may expose individuals to risk, confidentiality and anonymity are critical. Rabaiotti and Smith (2023), in their study of the Crimestoppers initiative in England and Wales, identify anonymity as a key factor influencing citizens' willingness to report crimes. Their findings suggest that when individuals perceive that their identities are protected, their likelihood of participation increases.

In addition to anonymity, the reporting medium plays an important role. Hauser (2021) analysed whistle-blowing channels across European organizations and found that web-based systems provide stronger protection for user identity compared to conventional channels such as hotlines. This is largely due to the ability of digital systems to incorporate structured anonymity and data protection mechanisms more effectively. However, anonymity alone is insufficient. Muskita et al. (2019) emphasise the importance of feedback mechanisms, noting that visible organizational responses can increase user engagement and reporting intention. While global platforms tend to integrate anonymity, feedback, and case tracking within unified systems, existing platforms in Nigeria often implement these features in isolation, limiting their overall effectiveness.

Based on the reviewed literature, this study adopts a conceptual model in which system design features such as anonymity, data security, usability, and feedback mechanisms influence user trust and perceived usefulness. These factors, in turn, affect users' willingness to report incidents, which ultimately determines the effectiveness of the whistle-blowing system. This conceptual model guides the design and evaluation of the proposed system by linking system features to user behaviour and overall system effectiveness.

3. METHODOLOGY

This study adopted Design Science Research Methodology (DSRM) as proposed by Peffers et al. (2007), which provides a structured approach for developing and evaluating artefacts that address

identified problems. DSRM consists of six key stages: problem identification, definition of objectives, design and development, demonstration, evaluation, and communication.

In the problem identification stage, the study established that existing reporting mechanisms in Lagos are limited by weak anonymity, poor feedback mechanisms, and low user trust. This problem was identified through a review of relevant literature and analysis of existing whistle-blower platforms, which revealed that these limitations reduce citizen participation in reporting vandalism incidents.

In the objectives definition stage, the study aimed to develop a secure, user-friendly whistle-blower reporting system that supports anonymous reporting, multimedia evidence submission, and real-time feedback.

The design and development stage involved translating these objectives into system requirements. The system design was informed by the theoretical framework (TAM and trust-based privacy principles), ensuring that perceived usefulness, ease of use, and anonymity were central to the artefact. Key design features included anonymous reporting, password-based case tracking, secure evidence handling, and role-based dashboards.

The system was implemented using the MERN stack (MongoDB, Express.js, React.js, Node.js), with Amazon Web Services (AWS) providing cloud hosting, secure storage, and notification services.

In the demonstration stage, the developed system was tested through simulated reporting scenarios, where users submitted reports, tracked cases, and interacted with the platform's features.

The evaluation stage involved functional, usability, performance, and security testing to assess the effectiveness of the artefact. Feedback from testing informed minor refinements to system features, particularly in improving user interface clarity and report submission flow.

Finally, the communication stage is achieved through the documentation of the system design, implementation, and evaluation in this study.

3.1 System Architecture

The proposed system follows a three-tier architecture comprising the presentation layer, the application layer, and the data layer. The presentation layer, built with React.js, provides citizens, administrators, and agencies with role-based interfaces. The application layer, implemented with Express.js and Node.js, manages authentication, case routing, evidence upload through pre-signed URLs, and system notifications. The data layer, powered by MongoDB and AWS S3, supports secure persistence of reports, user credentials, and evidence files. This architecture was designed with scalability and reliability considerations and is adaptable to future integration with mobile platforms.

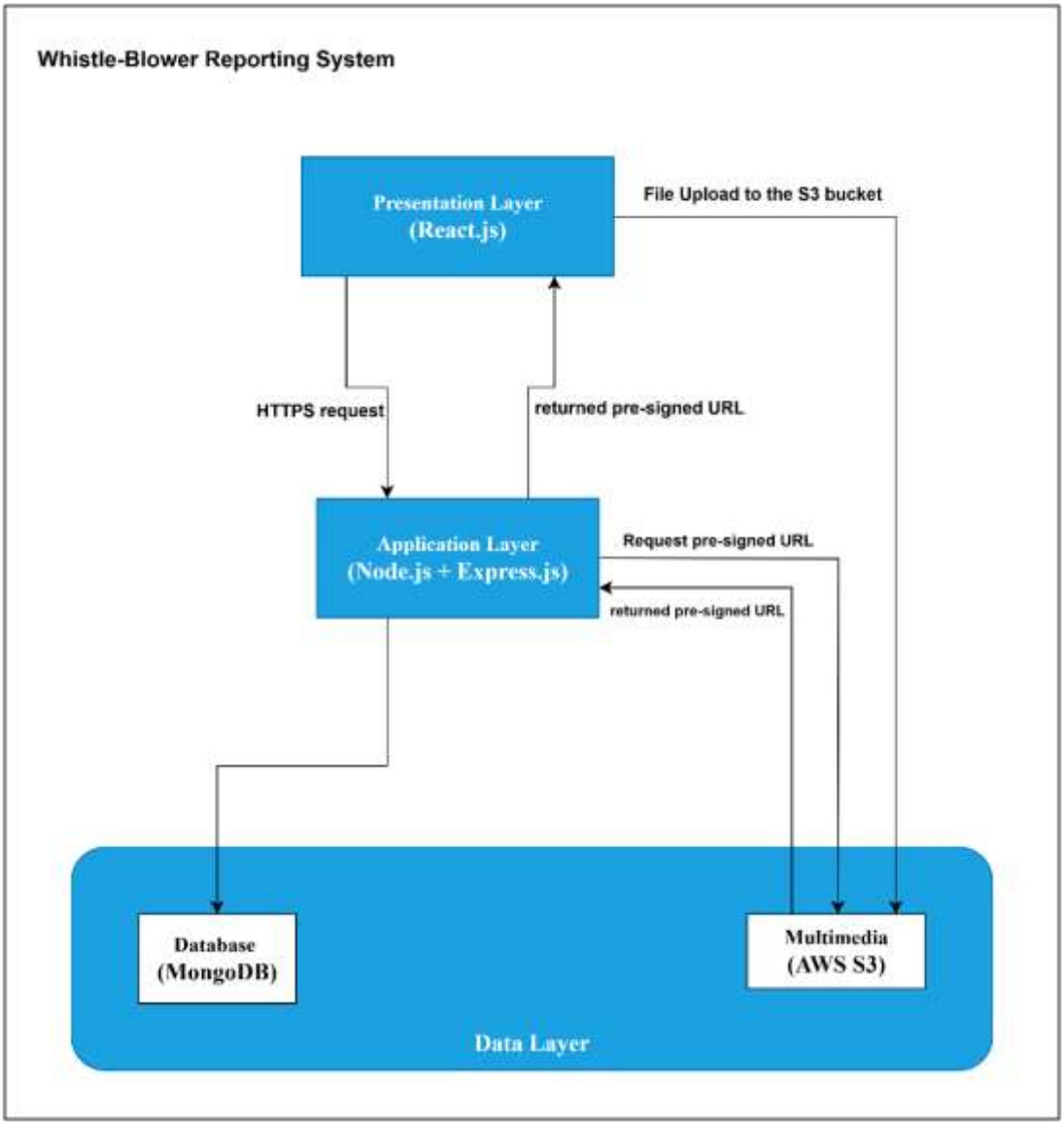

Figure 1: High-Level System Architecture of the Whistle-Blower Reporting Platform

3.2 System Modelling

The logical model of the system was formalized using structured design techniques to represent workflows between whistle-blowers, administrators, and agencies. The central process flow guiding the platform is expressed in the core algorithm for report submission, which ensures that anonymity is preserved while maintaining continuity of case feedback.

Core Algorithm for Whistle-Blower Report Submission

1. Begin ReportSubmission

2. Receive input data (text, multimedia evidence)

3. Validate input fields

4. If input invalid:

    Display error message

    Request resubmission

  Else:

    Strip metadata from evidence

    Generate unique CaseID + password

    Store evidence in AWS S3

    Save report details in MongoDB

    Notify administrator of new report

5. End ReportSubmission

3.3 System Implementation

The system was implemented as a responsive web application. React.js and Material-UI provided a clean, mobile-friendly interface for whistle-blowers, while administrators and agencies accessed role-based dashboards with case management and analytics functions. The backend, built with Express.js, handled secure authentication using JSON Web Tokens (JWTs), evidence uploads with AWS S3, and notifications with Amazon SES. Password-only case tracking enabled anonymous users to monitor progress without disclosing personal identifiers, while confidential users could optionally receive notifications via email.

3.4 Evaluation Methods

The developed system was evaluated through functional, usability, performance, and security testing, as well as comparative benchmarking against existing whistle-blower reporting platforms in Nigeria. Functional testing measured the accuracy of report submission, evidence upload, and case tracking workflows. Usability testing involved a purposive sample of 30 volunteer participants (17 male, 13 female, aged 18–45), comprising 20 ordinary citizens, 5 IT professionals, and 5 civil servants to represent a diverse user base. The testing followed a moderated think-aloud protocol where participants performed representative tasks such as report submission, case tracking, and dashboard navigation. Task completion rates and qualitative feedback were recorded to assess ease of use and interaction flow. Performance testing measured response times of core functions, while security testing was conducted using the OWASP Top 10 methodology to assess the system's resilience against common vulnerabilities such as SQL injection, cross-site scripting (XSS), and brute-force login attempts. Automated vulnerability scanning was performed using OWASP ZAP, supplemented by manual penetration testing using Burp Suite Community Edition to verify access control flaws and session management vulnerabilities. Comparative benchmarking examined differences in accessibility, anonymity, efficiency, and transparency relative to existing reporting channels in Nigeria.

The design process involved iterative refinement based on evaluation outcomes. Initial usability testing revealed challenges in report submission flow and navigation clarity. In response, the interface was simplified by reducing the number of required input steps and improving form validation feedback. Additionally, the case tracking process was refined to enhance clarity for anonymous users. These iterative improvements contributed to better usability and system performance in subsequent evaluations.

Table 1: Evaluation Criteria Summary

Criterion	Description	Measurement Method	Success Threshold
Functional Accuracy	System performs required tasks correctly	Functional Testing	≥ 90% pass rate
Response Time	Average processing time for key operations	Performance Testing	≤ 2 seconds
Usability	Ease of use for representative users	Task completion rate + feedback	≥ 85% completion rate
Data Security	Anonymity and confidentiality preserved	OWASP ZAP automated scans & Burp Suite manual testing	No critical vulnerabilities identified during testing
Comparative Advantage	Improvements over existing mechanisms	Benchmarking analysis	≥ 3 documented advantages

3.5 Design Principles

Based on the design and evaluation process, the study derives the following design principles for whistle-blower reporting systems:

i. anonymity should be preserved through minimal data collection and metadata protection
ii. user interfaces should be simple and accessible to encourage participation
iii. feedback mechanisms should be integrated to sustain user engagement, and
iv. secure data handling should be implemented to ensure confidentiality and system integrity.

4. RESULTS AND DISCUSSION

The implementation of the Online Whistle-Blower Reporting System achieved its objectives and addressed the shortcomings of existing mechanisms in Lagos State. The platform enabled both anonymous and confidential submissions, allowing whistle-blowers to report incidents with essential details such as subject, description, location, and multimedia evidence. Confidential users received email notifications, while anonymous users remained fully protected. This dual-mode design reflects the importance of anonymity and trust in encouraging citizen participation.

A password-based case tracking feature provided continuity of communication and accountability, enabling whistle-blowers to securely monitor the progress of their submissions and add clarifications where necessary. The administrator and agency dashboards offered tools for case intake, categorisation, routing, and resolution, supported by analytics visualisations for identifying trends and monitoring performance. Additionally, the Public Agency Accountability Scorecard displayed on the homepage introduced a transparency mechanism by making agency responsiveness visible to citizens, thereby reinforcing trust and governance.

The evaluation confirmed these design choices. Functional testing showed a 93.3% pass rate (e.g., successfully executing 14 out of 15 core system workflows), and moderated usability testing demonstrated a high overall task completion rate of 90% among the 30 participants. There were slightly lower completion rates (80%) for case tracking and agency updates, suggesting areas for minor interface refinement. Performance testing demonstrated response times under two seconds, and security testing utilizing OWASP ZAP and Burp Suite reported no critical vulnerabilities. Comparative benchmarking further revealed that the system demonstrates structural advantages over existing platforms in terms of transparency, accessibility, and anonymity.

Usability Test Results

Table 2: Summary table of usability test results

Task	Completion Rate (%)
Submit Anonymous Report	90.0
Submit Confidential Report	90.0
Upload Evidence	90.0
Track Case	80.0
Update Case Status (Agency)	80.0

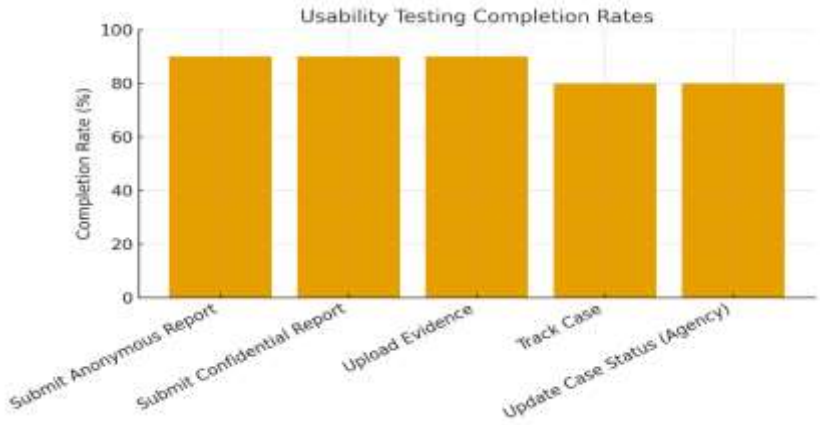

Figure 2: Usability Task Completion Rates

Implementation Evidence

Figures 3–5 provide screenshots of the implemented system. Figure 3 illustrates the homepage showing the Public Agency Scorecard, which publicly displays agency responsiveness and fosters transparency. Figure 4 shows the Report Submission Interface, which allows both anonymous and confidential reporting with multimedia uploads. Figure 5 presents the Administrator Dashboard, where submitted reports are verified, categorised, and routed to relevant agencies.

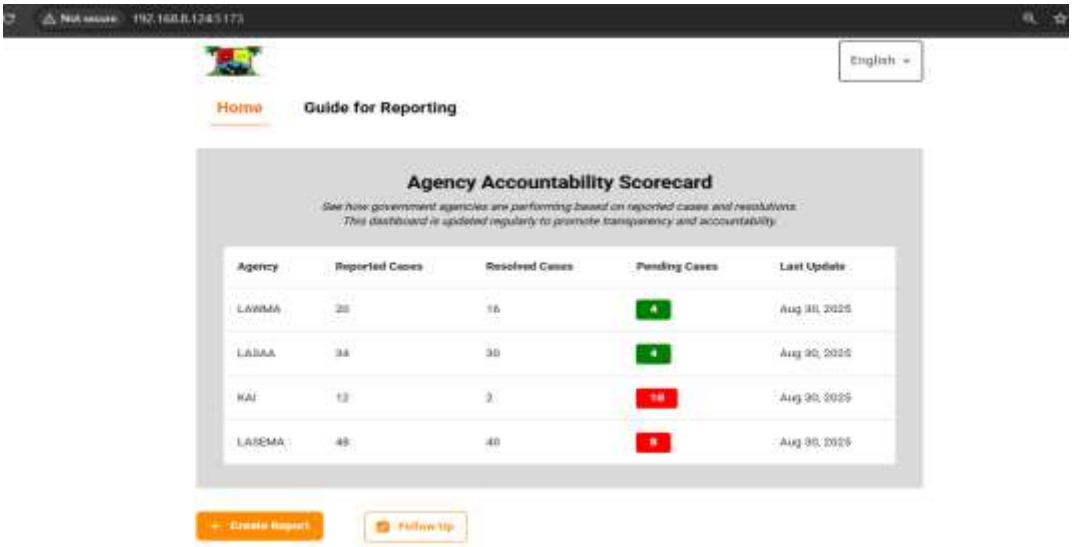

Figure 3: User's Homepage showing Public Agency Scorecard

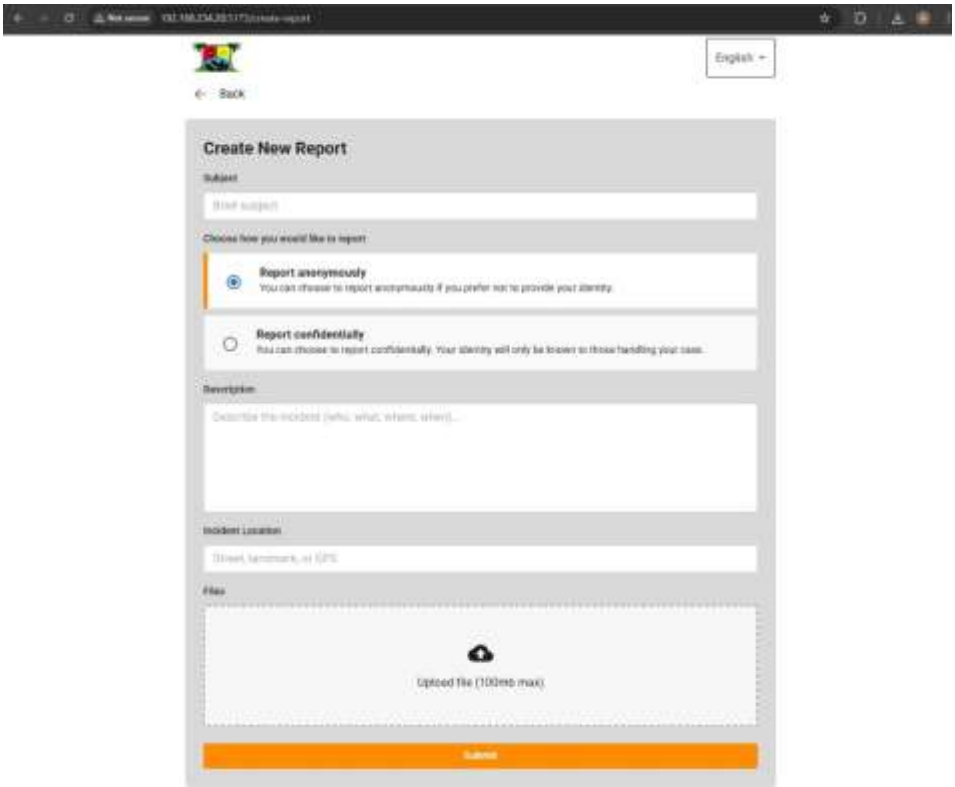

Figure 4: Report Submission Interface (Anonymous/Confidential Mode)

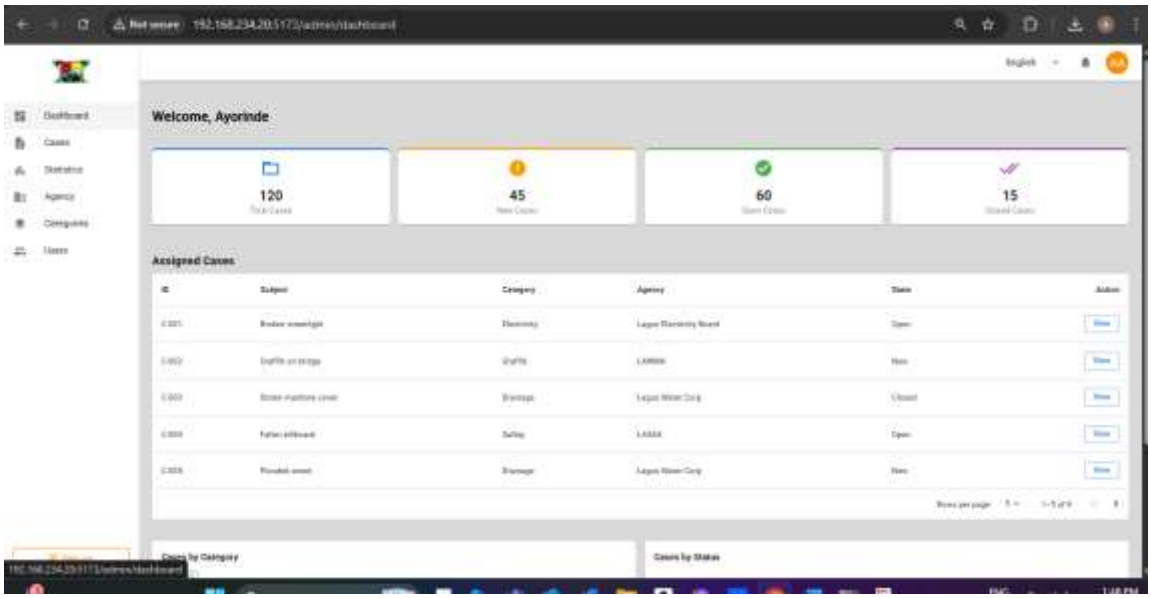

Figure 5: Administrator Dashboard for Case Management

Overall, the system's design and results demonstrate that integrating anonymity, feedback mechanisms, secure communication, and transparency features can strengthen accountability mechanisms and citizen engagement in Lagos State and beyond. These findings are consistent with the Technology Acceptance Model (TAM) and trust-based frameworks, which emphasize usability, perceived usefulness, and trust as key drivers of system adoption.

5. CONCLUSION

This research has demonstrated that a secure, transparent, and user-friendly whistle-blower reporting platform holds the potential to significantly improve how cases of public property vandalism are reported and managed in Lagos State. By combining anonymity, confidentiality, and feedback mechanisms within a single system, the study addressed key barriers that have limited the effectiveness of existing reporting channels in Lagos State.

The objectives set at the beginning of the study were achieved. The system provided a functional web-based platform supporting anonymous and confidential submissions, integrated evidence uploads and case tracking and introduced role-based dashboards for administrators and agencies. Evaluation confirmed that the system is both usable and effective, with strong performance and resilience to common security threats. Comparative benchmarking further showed measurable improvements in accessibility, anonymity, efficiency, and transparency over traditional mechanisms.

Although some features, such as geo-tagging and comprehensive real-time notifications, remain partially implemented, these limitations do not diminish the system's contribution. Instead, they highlight opportunities for incremental improvement as the platform matures. Furthermore, because this prototype was evaluated in a controlled environment, future research should focus on pilot deployments with actual government agencies and citizens to validate these findings in real-world scenarios. In conclusion, the study affirms that technology-driven whistle-blowing systems, when

grounded in theoretical frameworks like the Technology Acceptance Model (TAM) and trust-based privacy principles, can foster trust, promote citizen participation, and strengthen accountability in public governance.

This study contributes to knowledge by contextualizing global best practices for whistle-blower platforms in Nigeria, deriving actionable design principles for civic technology, demonstrating a prototype for a secure and scalable MERN–AWS implementation model, and providing empirical benchmarks that can guide the design and evaluation of future civic technology systems.

6. ACKNOWLEDGEMENTS

We give thanks to Almighty God for the success of this work.

7. REFERENCES

[1] Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

[2] Hauser, C. (2021). The role of web-based reporting systems in safeguarding whistleblowers' anonymity. *Academy of Management Proceedings*, *2021*(1), 15728. https://doi.org/10.5465/AMBPP.2021.15728abstract

[3] Khalilikhah, M., Heaslip, K., & Hancock, K. (2016). Traffic sign vandalism and demographics of local population: A case study in Utah. *Journal of Traffic and Transportation Engineering (English Edition)*, *3*(3), 192–202. https://doi.org/10.1016/j.jtte.2015.11.001

[4] Kumare, M. S. (2024). Civic engagement and public policy: connecting the people to government. *EPRA International Journal of Multidisciplinary Research (IJMR)*, *10*(7), Article 7.

[5] Muskita, F. I., Utami, I., & Hapsari, A. N. S. (2019). Effectiveness testing of reporting systems and organizational responses toward whistleblowing intentions. *Journal of Contemporary Accounting*, 131–144. https://doi.org/10.20885/jca.vol1.iss3.art1

[6] Ojobo, E. (2023). A Review of the Effectiveness of the Nigerian Whistleblowing Stopgap Policy of 2016 and the Whistleblower Protection Bill of 2019. *Journal of African Law*, *67*(3), 487–494. https://doi.org/10.1017/S0021855323000098

[7] Oluwakayode, A. S., Afiqah, A. F., & Salfarina, S. (2024). The Impact of Property Crime on Public Infrastructure Development in the Nigerian Cities. *International Journal of Research and Innovation in Social Science*, *8*(8), 1153–1172.

[8] Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *J. Manage. Inf. Syst.*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

[9] Rabaiotti, E., & Smith, R. (2023, May 16). *The power of anonymity: An exploratory study into the role of Crimestoppers in reporting and investigating crime in England and Wales—Ella Rabaiotti, Richard Smith, 2024*. https://journals.sagepub.com/doi/10.1177/0032258X231171029

[10] Wu, K., Zhao, Y., Zhu, Q., Tan, X., & Zheng, H. (2011). A meta-analysis of the impact of trust on technology acceptance model: Investigation of moderating influence of subject and context type. *International Journal of Information Management*, *31*(6), 572–581. https://doi.org/10.1016/j.ijinfomgt.2011.03.004

Author's Brief Profile

Ayorinde Felix AJIBAYE holds a Diploma in Data Processing from Olabisi Onabanjo University, Ago-Iwoye, Ogun State, Nigeria. He obtained a Bachelor of Science (B.Sc.) degree in Computer Science and a Master of Science (M.Sc.) degree in Information Technology from the National Open University of Nigeria. His research interests include machine learning, artificial intelligence, e-health systems, secure information systems, and software development, with a focus on developing practical, data-driven solutions for real-world challenges. He can be reached via email at ajibaye@gmail.com

Olatayo Moses OLANIYAN is a Professor of Computer Engineering at Federal University, Oye-Ekiti, Nigeria. Having more than fifteen years' experience in academics, he has graduated several Masters and PhD students, he is an authority in AI and embedded systems. He has more than 60 publications which include books, journals and proceedings. Email: Olatayo.olaniyan@fuoye.edu.ng