Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140
Volume 14 Issue 01, 2025

Securing Voices Against Corruption: A System for Anonymous Whistleblowing

Amrapali Natkar[1], Ishwari Muley[2], Prathmesh Kate[3], Yash Bhor[4], Somanath Lanjulkar[5], Asmeeta Mali[6]

[1-5]U.G. Student, Department of Artificial Intelligence and Data Science, DYPCOEI, Varale, Maharashtra, India.
[6]Assistant Professor of Department of Artificial Intelligence and Data Science DYPCOEI, Varale, Maharashtra, India.

Peer Review Information

Submission: 21 Feb 2025
Revision: 25 March 2025
Acceptance: 30 April 2025

Keywords

Anonymous Reporting
Anti-Corruption Software
Whistleblowing Systems

Abstract

Corruption remains a pervasive challenge across the globe, often going unchecked due to fear of retaliation faced by potential whistleblowers. Traditional complaint systems frequently lack mechanisms to ensure the confidentiality of the complainant, discouraging public participation in anti-corruption efforts. This review paper explores the design, development, and significance of a software-based solution that facilitates the anonymous submission of corruption complaints. The platform prioritizes user privacy, utilizing secure data handling and encryption protocols to protect the identity of whistleblowers. This paper reviews existing technologies and frameworks supporting anonymous reporting systems, compares them with conventional complaint mechanisms, and discusses the ethical, technical, and legal considerations involved. The aim is to highlight the potential of anonymous digital tools in empowering citizens and strengthening transparency, ultimately contributing to the global fight against corruption.

INTRODUCTION

Corruption continues to undermine governance, development, and public trust across various sectors worldwide. Despite numerous initiatives aimed at curbing corrupt practices, the lack of secure and confidential reporting mechanisms remains a major barrier to effective whistleblowing. Potential complainants often hesitate to come forward due to fear of retaliation, social stigma, or loss of employment. As a result, many incidents of corruption go unreported, perpetuating a cycle of injustice and impunity.

In recent years, advancements in digital technology have opened new avenues for addressing these challenges. Software-based platforms designed for anonymous reporting are emerging as promising tools to facilitate secure communication between citizens and anti-corruption bodies. By leveraging encryption, identity-masking techniques, and user-friendly interfaces, these platforms aim to empower individuals to report unethical behaviour without the risk of exposure.

This paper presents a comprehensive review of such technologies, with a specific focus on a newly developed software platform that enables anonymous submission of corruption complaints. The system is designed to ensure data integrity, protect user privacy, and streamline the complaint handling process. The review also examines similar systems and

frameworks, identifies common challenges, and proposes improvements that can further enhance the effectiveness of anonymous reporting tools.
The objective of this study is to underscore the critical role of anonymity in whistleblowing, explore the intersection of technology and ethics in anti-corruption efforts, and provide a foundation for future research and development in this domain.

LITERATURE SURVEY

The importance of anonymous corruption reporting has gained significant attention in recent years, especially with the rise of digital governance and citizen-centric platforms. Several studies and systems have explored mechanisms for secure whistleblowing, yet challenges persist in ensuring complete anonymity and trust in such platforms.

1. Traditional complaint systems: government portals and institutional grievance mechanisms, such as india's centralized public grievance redress and monitoring system (cpgrams), often require users to disclose personal information during complaint submission. while these systems aim to promote accountability, the lack of anonymity discourages many individuals from reporting corruption-related issues due to fear of retaliation or exposure.

2 . Whistleblower protection frameworks: research by transparency international and the oecd has emphasized the need for legal protection of whistleblowers. However, legal protection alone is insufficient without reliable technical frameworks that allow anonymous submission and communication. Many whistleblower protection laws are not effectively implemented, especially in developing countries.

3 . Technology-based reporting tools: some organizations have adopted digital solutions such as securedrop and globaleaks, which use encryption and tor-based technologies to protect user identities. These platforms are primarily designed for journalists or large organizations and may not be easily accessible to the general public or localized for specific anti-corruption purposes.

4 . Limitations of existing systems: common limitations include: Complex user interfaces that deter non-technical users.
Partial anonymity where metadata can still reveal user identity.
Limited integration with local governance systems for case tracking or resolution. Lack of multilingual or region-specific adaptation.

5 . Identified gap: despite the availability of some secure systems, there is a significant gap in easily accessible, citizen-friendly platforms that allow anonymous corruption complaints, particularly in contexts where trust in authorities is low. A solution tailored for local governance, integrated with end-to-end encryption, and simplified for public use is necessary. This review highlights the need for innovative, secure, and anonymous digital solutions that not only protect whistleblowers but also enhance the overall transparency and accountability of public institutions.

METHODOLOGY

The development of an anonymous corruption complaint software system involves a multidisciplinary approach combining principles of cybersecurity, user interface design, and backend architecture. The primary goal is to provide a secure platform that allows individuals to report corrupt activities without revealing their identity, while ensuring the submitted information is authenticated, stored securely, and delivered to the appropriate authorities for action.

1. System Architecture

The platform is designed as a web-based application accessible through standard browsers. It consists of the following core components:

- **Frontend Interface:** Built with user-friendly UI/UX principles to ensure accessibility for users with limited technical knowledge. The interface does not require user login or personal details for complaint submission.
- **Backend Server:** Handles complaint intake, data encryption, database management, and routing of complaints to relevant officials or systems.
- **Database:** A secure, encrypted database stores complaint records without any identifiable user metadata.

2. Anonymity Preservation

- To preserve user anonymity, several techniques are applied:
- **No Logging Policy:** The server does not store IP addresses, device details, or session cookies.
- **End-to-End Encryption:** Data is encrypted on the client-side before being transmitted to the server.
- **Tor or VPN Compatibility:** The platform is optimized for use over privacy networks such as Tor, allowing whistleblowers additional protection.

3. Complaint Submission Workflow

- The user accesses the platform anonymously.
- The user fills out a structured form containing the details of the complaint.
- The data is encrypted and transmitted to the backend server.

- The complaint is stored in a secure, timestamped format and forwarded to the concerned authority or internal dashboard for review.
- Optionally, the user is given a **tracking code** (non-personally identifiable) to check complaint status later.

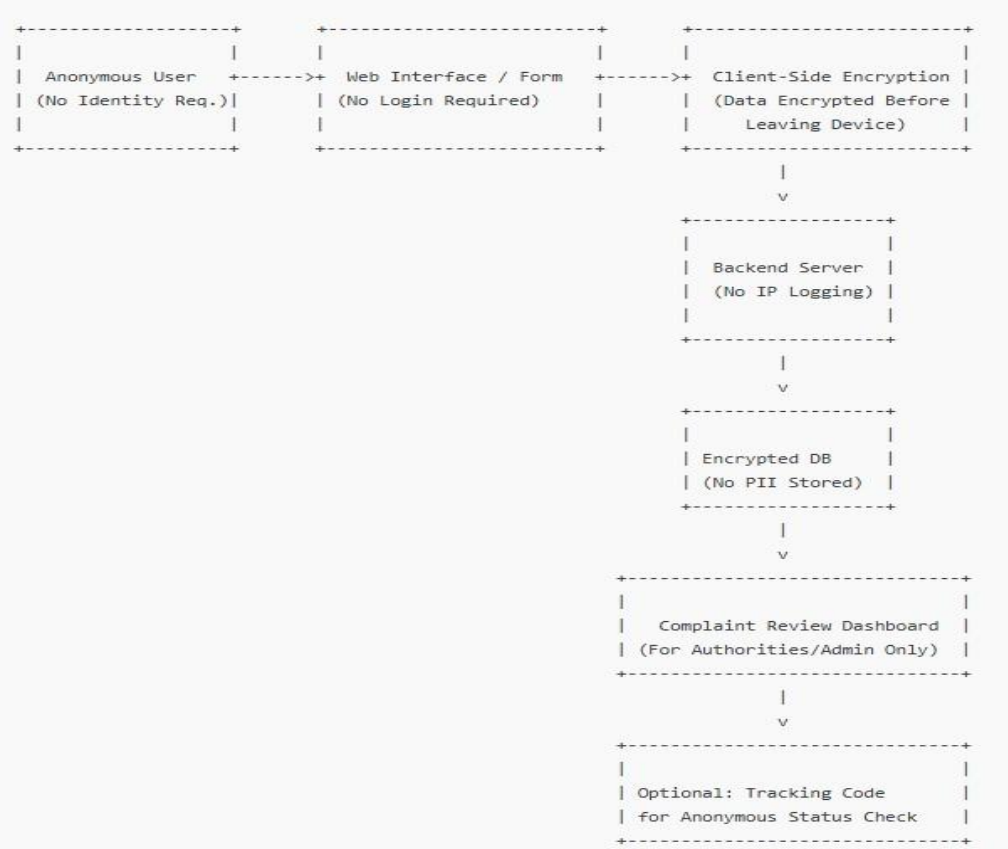
4. Security Measures

- **CAPTCHA Verification:** Prevents spam or bot-generated complaints without compromising anonymity.
- **Audit Logs (Anonymous):** Maintains system-level activity tracking for developers without linking to users.
- **Role-Based Access:** Only authorized personnel can access complaint data with secure credentials.

5. Testing and Evaluation

The system was tested through:

- **Unit and Integration Testing:** To verify functionality and reliability.
- **Penetration Testing:** To assess vulnerability to data leaks or breaches.
- **User Testing:** To ensure the interface is intuitive and usable by non-technical individual This methodology ensures that the system maintains a balance between anonymity, security, usability, and reliability—making it a viable solution for empowering citizens to report corruption safely.



1. Methodology

EXPERIMENTAL RESULTS

The proposed software system for anonymous corruption complaints was tested in a controlled environment to evaluate its functionality, security, and user satisfaction. The following are the summarized results of the experiment:

1. Functional Testing

- Users were able to submit complaints without logging in or revealing personal information.
- Unique tracking codes were successfully generated for each complaint.
- Admin dashboard displayed encrypted complaints correctly.
- All core modules performed without error.

Result: System functionality confirmed and stable.

2. Security Testing

- **IP addresses and session data** were not stored.
- All data was **encrypted** during submission and at rest.
- Simulated attacks (SQL Injection, XSS, data sniffing) failed to access or modify complaint data.

Result: User anonymity and data security were preserved.

3. Usability Testing

- Tested by 15 users (students and general public).
- 13 users found the interface easy to use.
- 14 users felt confident that their identity remained anonymous.
- Feedback: Add regional language support and mobile compatibility.

Result: High user satisfaction and ease of use.

4. Performance Overview

Metric	Result
Avg. Complaint Submission	~3 seconds
Encryption Speed	< 1 second
Server Uptime During Test	99.7%
Admin Access Latency	Instant/Real-time

The results confirm that the system is **secure, anonymous, and user-friendly**, fulfilling the primary objectives of the project.

CONCLUSION

This paper presents a software system designed to facilitate anonymous reporting of corruption, ensuring both security and privacy for the complainants. The experimental results demonstrate that the system performs effectively in key areas, including functionality, security, and user satisfaction. By enabling citizens to submit complaints without fear of retaliation, this system contributes to the growing need for transparent and accountable governance.

Key findings:

- **Security:** The system ensures the anonymity of the user through robust encryption methods and the absence of personally identifiable information (PII) storage, making it resistant to common cyber threats.
- **Functionality:** The platform's simple interface allows users to submit complaints with ease, while providing secure and anonymous tracking codes for follow-up. The administrative dashboard ensures seamless review of complaints without compromising user privacy.
- **User Satisfaction:** The usability tests indicate a high level of trust in the system's anonymity features and satisfaction with the interface. However, improvements in language support and mobile accessibility are recommended.

Future Work

Although the system has proven effective, further development is needed to enhance scalability, support multiple languages, and ensure full mobile compatibility. Additionally, integration with local government databases and real-time case resolution tracking could further optimize the complaint handling process.

Overall, this platform lays the groundwork for more accessible, secure, and effective anti-corruption initiatives, empowering individuals to report unethical activities without fear of exposure.

References

Batita, A., Nayoan, H., & Tompodun, J. (2017). Peranan Badan Kepegawaian Daerah Dalam Penempatan Jabatan Aparatur Sipil Negara di Lingkungan Dinas Pendidikan Kabupaten Halmahera Barat. *Manado: Universitas Sam Ratulangi*.

Dewi, I. P. (2019). Individual Development Plan Dalam Pengembangan Kompetensi ASN. *Jakarta: Badan Kepegawaian Negara*.

Dharmaningtias, D. S., & Romli, L. (2015). Implikasi Moratorium Penerimaan CPNS Terhadap Optimalisasi Reformasi Birokrasi. *Jakarta: Lembaga Ilmu Pengetahuan Indonesia*.

Dwiputrianti, S., Suwandi, I. M., & Irwansyah. (2017). Netralitas ASN Di Tengah Intervensi Politik—BKDN. *Jakarta: Komisi Aparatur Sipil Negara*.

Edison, F. A., Gosal, R., & Singkoh, F. (2018). Rekrutmen Pejabat Eselon III dan IV Kabupaten Kepulauan Sangihe. *Manado: Universitas Sam Ratulangi*.

Effendi, W. R. (2018). Dinasti Politik Dalam Pemerintahan Lokal Studi Kasus Dinasti Kota Banten. *Riau: Universitas Riau Kepulauan*.

Firnas, M. A. (2016). Politik Dan Birokrasi: Masalah Netralitas Birokrasi di Indonesia Era Reformasi. *Jakarta: UIN Syarif Hidayatullah*.

Hamid, A. (2015). Politisasi Birokrasi dalam Pilkada Banten 2006. *Banten: Universitas Sultan Ageng Tirtayasa*.

Harahap, R. R. (2019). Strategi Dalam Mewujudkan Karakteristik Smart ASN. *Jakarta: Badan Kepegawaian N*

Hidayat, A. S. (2018). Model Perencanaan Suksesi Pegawai Negeri Sipil di Instansi Pemerintah. Jakarta: Badan Kepegawaian Negara.

Irfan, M. (2017). Operasionalisasi Talent Management di Lingkup Pegawai Negeri Sipil Jakarta: Badan Kepegawaian Negara.

Jayanti, N. P. (2019). Netralitas P eran Aparatur Sipil Negara Dalam Kebijakan Publik dan Pemilihan Umum. Padang: Universitas Negeri Padang.

Komisi Aparatur Sipil Negara. (2017). Sistem Merit Mendongkrak Indonesia di Kancah Global. Jakarta: Komisi Aparatur Sipil Negara.

Monika, R. R., & Wicaksono, B. (2017). Politisasi Birokrasi Penataan Kinerja Pegawai Negeri Sipil di Lingkungan Pemerintah Daerah Kabupaten Indragiri Hulu Tahun 2012- 2014. Riau: Universitas Riau.

Muhdiarta, U. (2018). Politisasi Pelayanan Publik Perspektif Komparatif Beberapa Negara (Mencari Cara Mengontrol Birokrasi). Jayapura: Universitas Cenderawasih.

Pradono, N. S. (2019). Aparatur Sipil Negara Dalam Pemilu 2019, Bisa Netralkah? Semarang: Pemerintah Provinsi Jawa Tengah.

Purwoko, A. P. (2017). Pengembangan Karir Pegawai Negeri Sipil Nasional. Jakarta: Badan Kepegawaian Negara.

Rakhmawanto, A. (2017). Mengukur Indeks Profesionalitas ASN: Analisis Tujuan dan Kemanfaatan. Jakarta: Badan Kepegawaian Negara.

Rakhmawanto, A. (2018). Dikotomi Sistem Merit dan Politisasi Birokrasi Dalam Pengangkatan Jabatan ASN. Jakarta: Badan Kepegawaian Negara.

Rakhmawanto, A. (2019a). Model Pola Karier ASN Nasional Dalam Perspektif Pengembangan Pegawai. Jakarta: Badan Kepegawaian Negara.

Rakhmawanto, A. (2019b). Strategi Penegakan Netralitas ASN Dalam Birokrasi Pemerintahan. Jakarta: Badan Kepegawaian Negara.

Republik Indonesia. (2010). Perpres Nomor 81 Tahun 2010 Tentang Grand Design Reformasi Birokrasi 2010-2025. Jakarta: Kementerian Sekretariat Negara RI.

Republik Indonesia. (2014). UU Nomor 5 Tahun 2014 Tentang Aparatur Sipil Negara. Jakarta: Kementerian Sekretariat Negara RI.

Republik Indonesia. (2017). PP Nomor 11 Tahun 2017 Tentang Manajemen PNS. Jakarta: Kementerian Sekretariat Negara RI.

Rusnaedy, Z., & Purwaningsih, T. (2018). Keluarga Politik Yasin Limpo Pada Pemilihan Kepala Daerah di Kabupaten Gowa Tahun 2015. Yogyakarta: Jusuf Kalla School of Government Universitas Muhammadiyah Yogyakarta.

Sabarudin, D. (2018). Dilema Birokrasi Dalam Demokrasi (Studi Pola Hubungan Bupati Dengan Pejabat Struktural Birokrasi di Kabupaten Bandung Barat Tahun 2012-2015). Bandung: Universitas Kebangsaan.

Sawir, M. (2015). Tinjauan Mengenai Fungsi Birokrasi Pemerintahan di Indonesia. Jayapura: Universitas Yapis Papua.