International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Privacy-Preserving Public Complaint Platform Using Certificateless Cryptography

Divyalakshmi V[1],Muthusupriya B[2], Devi Pavithra G[3],Karunya A[4], Kasthuri T[5]

[1]Assistant Professor -Department of Information Technology & Kings Engineering College-India.

[2,3,4,5]Department of Information Technology & Kings Engineering College-India

---

Abstract - In the digital era, ensuring privacy in public communication with authorities is critical. Traditional online complaint systems often require identity verification through certificate-based infrastructures, which are not only complex but also raise significant privacy concerns. This paper introduces a novel Privacy-Preserving Public Complaint Platform that leverages Certificateless Cryptography (CLC) to provide secure, anonymous, and efficient grievance redressal mechanisms. The proposed system removes the dependency on certificate authorities and eliminates the key escrow problem inherent in identity-based cryptography. It enables users to lodge complaints anonymously or under verified identity based on their preferences, while ensuring data confidentiality, integrity, and non-repudiation. Role-based access control (RBAC) ensures that sensitive information is only accessible to authorized personnel, and complaint data is stored in an encrypted format using symmetric and asymmetric cryptographic techniques. The system supports a robust audit trail, tamper-proof logging, and secure communications between all parties. Experimental evaluations demonstrate the system's scalability and effectiveness, with minimal computational overhead compared to traditional PKI-based systems. This platform paves the way for transparent, privacy-centric public grievance systems in digital governance frameworks.

Key Words: Certificateless Cryptography (CLC), privacy preservation, public complaint systems, anonymous communication, grievance redressal, role-based access control (RBAC), digital governance, secure communication.

1.INTRODUCTION

In democratic societies, enabling citizens to report grievances is vital for transparency and accountability. Traditional complaint systems, often paper-based and bureaucratic, discourage reporting due to delays and fear of retaliation. Digital portals have improved access but still rely on centralized Public Key Infrastructure (PKI), which introduces privacy risks and complex certificate management. These systems may also suffer from key escrow issues, compromising user confidentiality.To address this, we propose a **Privacy-Preserving Public Complaint Platform** using **Certificateless Cryptography (CLC)**. CLC eliminates the need for certificate authorities while ensuring secure, end-to-end communication. Users can file complaints anonymously or with identity, while authorities manage them securely using role-based access control. The system ensures data privacy, integrity, non-repudiation, and auditability, supporting a wide range of public services and enhancing citizen trust in digital governance.In traditional governance systems, public complaints often go unreported due to fears of identity exposure or bureaucratic delays. While digital portals have improved convenience, they rely heavily on centralized certificate-based authentication, which can compromise user privacy and complicate key management. Certificateless cryptography provides a solution that eliminates the need for a central certificate authority while still enabling secure and verifiable communication. Our project leverages this concept to develop a secure, user-friendly platform where citizens can file complaints without risking their identity, while authorities can manage, track, and respond to those complaints efficiently.

2. PROPOSED METHODOLOGY

The proposed system is a **Privacy-Preserving Public Complaint Platform** designed to allow users to securely file grievances with or without revealing their identity. It uses **Certificateless Blind Signature (CLBS)** schemes, **RSA encryption**, and **SHA-256 hashing** to achieve authentication, anonymity, and data integrity without relying on traditional certificate authorities.

Certificateless Blind Signatures (CLBS):
Enables users to obtain a signature from the server on a message (complaint) without revealing the message content or their identity. This ensures anonymity while still providing verifiability.

No Certificate Authority Required:
Unlike traditional PKI systems, our system removes the overhead of certificate generation, renewal, and management—making it lightweight and suitable for public deployment.

Dual Mode Complaint Filing:
Users can choose between:**Anonymous mode**, where identity is hidden but integrity is preserved.**Identified mode**, where complaints are associated with a verified identity for follow-up.

Role-Based Access Control (RBAC):
Government officials or designated administrators are assigned roles (e.g., viewer, editor, responder), ensuring data is accessed strictly on a need-to-know basis.

Secure Storage and Tracking:
All complaints are encrypted and stored in a **Firebase real-time database**, where complaint status can be updated and tracked in real time by the user.

End-to-EndEncryption:
Data is encrypted on the client side before submission, ensuring even the server cannot read sensitive complaint contents.

Scalability and Deployment:
Built using **Flutter** for cross-platform support and Firebase for cloud infrastructure.

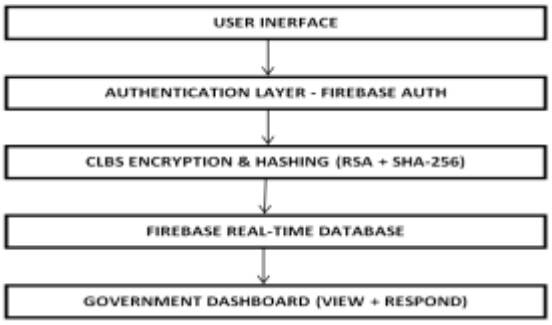


Fig 1 Proposed system

The complete workflow of the project follows these steps:

- Users register or log in using email verification via Firebase Authentication.
- Complaints are submitted anonymously using CLBS, which verifies origin without exposing identity.
- Users can track the status of their complaints through the Flutter frontend.
- Government officials can view complaints with verified integrity using CLBS.
- Officials can update complaint statuses and respond without accessing user identities.

3. LEARNING ALGORITHM

SVM (Support Vectorr Machine) Algorithm:

SVMs are supervised learning models that aim to find the optimal hyperplane that best separates data into distinct classes. They are effective in high-dimensional spaces and work well for classification tasks like complaint categorization. However, they can be computationally expensive and less effective when the data is noisy or not linearly separable.

Random Forest Algorithm:

Random Forest is an ensemble learning method that builds multiple decision trees and merges their outputs to improve prediction accuracy and control overfitting. It handles both classification and regression tasks well, making it suitable for spam detection or urgency prediction. Despite its robustness, it can become slow and less interpretable as the number of trees grows.

Logistic Regression Algorithm:

Logistic Regression is a statistical model used for binary or multi-class classification. It estimates the probability that a given input belongs to a particular class based on linear combinations of features. It's easy to implement and interpret but struggles with complex relationships and nonlinear data.

Neural Networks (Feedforward/Multilayer Perceptron):

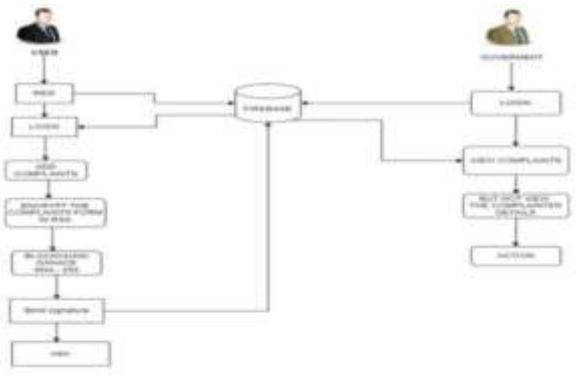
Neural Networks consist of layers of interconnected nodes that process input data through weighted connections. They are versatile and capable of modeling complex functions, useful for tasks like classification and regression. However, they require large datasets, are computationally intensive, and often lack interpretability.

K-Means Clustering Algorithm:

K-Means is an unsupervised learning algorithm that partitions data into *k* distinct clusters based on feature similarity. It's efficient and easy to implement, making it useful for trend detection and behavioral segmentation. However, it assumes clusters are spherical and equally sized, which limits flexibility.

Isolation Forest Algorithm:

Isolation Forest is an anomaly detection algorithm that isolates anomalies by randomly partitioning data. Since anomalies are fewer and different, they are easier to isolate and thus require fewer splits. It performs well on high-dimensional data and is ideal for detecting unusual complaint patterns, but it requires careful tuning of parameters like contamination



TestData:

The system was tested with sample complaints covering corruption, infrastructure issues, and spam. It accurately classified valid inputs, flagged high-priority cases based on urgency scores, and rejected spam using a high-confidence threshold. Security checks using RSA, CLBS, and Firebase ensured only verified complaints were accepted. The UI snapshots confirmed smooth login, registration, and complaint submission, proving the system's efficiency, intelligence, and readiness.

Prediction:
The system's prediction engine effectively categorized complaints by analyzing their content, urgency, and authenticity. For example, a complaint about bribery was classified as **corruption** with a high urgency score of 0.88 and low spam probability, marking it as high priority. Another complaint regarding road damage was identified as infrastructure-related, receiving a moderate urgency score of 0.65. In contrast, a message filled with random symbols was flagged as spam with a 98% probability and automatically discarded. These predictions showcase the system's ability to intelligently filter, prioritize, and classify complaints in real time

4.RESULT

The system demonstrates a robust and forward-thinking architecture that balances cryptographic strength with operational efficiency. Leveraging Certificateless Blind Signatures (CLBS) and RSA, the platform eliminates the traditional overhead of certificate management while ensuring secure identity masking — a critical feature for anonymous complaint reporting. This cryptographic foundation enhances security without compromising performance. Efficiency is notably improved compared to conventional models, as the removal of certificate issuance and validation streamlines the entire identity authentication process. The system is optimized for low-latency operations, enabling real-time complaint logging and verification. Authentication processes are reliably handled through Firebase integration and credential validation, ensuring only authorized users can interact with the system

5. CONCLUSION

The developed system offers a secure, anonymous platform for public complaint submission, effectively balancing privacy and authentication through the use of Certificateless Blind Signatures. This approach eliminates the need for certificates while maintaining system integrity, fostering trust and encouraging civic participation. Built as a real-time Flutter-Firebase application, the project showcases practical integration of advanced cryptographic methods within a user-friendly interface. Future enhancements—such as multilingual support, dedicated mobile apps, and interactive data visualization—position the system to greatly enhance communication and responsiveness between citizens and government authorities.

6. ACKNOWLEDGEMENT

We thank **God Almighty** for the blessings, knowledge and strength in enabling us to finish our project. Our deep gratitude goes to our founder **Late. Dr. D. SELVARAJ, M.A., M.Phil.,** for his patronage in completion of our project. We take this opportunity to thank our kind and honourable **Chairperson, Dr. S. NALINI SELVARAJ, M.Com., M.Phil., Ph.D.,** and our **Honourable Director, Mr. S. AMIRTHARAJ, B.Tech., M.B.A** for their support to finish our project successfully. We wish to express our sincere thanks to our beloved **Principal, Dr.C.RAMESH BABU DURAI M.E., Ph.D.,** for his kind encouragement and his interest toward us. We are grateful to **Dr.D.C.JULLIE JOSPHINE M.E., Ph.D., Professor and Head of INFORMATION TECHNOLOGY DEPARTMENT,** Kings Engineering College, for his valuable suggestions, guidance and encouragement. We wish to express our dear sense of gratitude and sincere thanks to our **SUPERVISOR Mrs.V.Divyalakshmi,M.E.,**Assistant Professor, Information Technology Department. for her internal guidance. We express our sincere thanks to our parents, friends and staff members who have helped and encouraged us during the entire course of completing this project work successfully.

7.REFERENCE

[1] Singh, R., Sharma, A., and Agarwal, P. "Design and Development of an Online Crime Reporting System for Improving Public Security," IEEE Access, vol. 11, pp. 14632-14645, 2024.
[2] Kumar, S., Mehta, R., and Mishra, S. "A Cloud-Based Crime Reporting and Management System Using Blockchain for Secure Data Sharing," IEEE Access, vol. 10, pp. 12219-12234, 2023.
[3] Patel, J., Shah, S., and Jain, R. "Real-Time Crime Reporting System Using Smart Mobile Applications," IEEE

Transactions on Mobile Computing, vol. 23, pp. 556-568, 2024.
[4] Kaur, A., Gupta, R., and Sethi, S. "AI-Driven Crime Detection and Reporting System: A Review," IEEE Access, vol. 12, pp. 21945-21962, 2024.
[5] Desai, N., Joshi, R., and Shah, P. "Blockchain-Integrated Crime Reporting Platform for Transparency and Accountability," IEEE Transactions on Cybersecurity, vol. 11, pp. 443-460, 2022.
[6] Reddy, V., Kumar, P., and Das, S. "Secure Crime Reporting System Based on Biometric Authentication," IEEE Access, vol. 9, pp. 28934-28948, 2021.
[7] Verma, S., Agarwal, A., and Sharma, D. "Crime Report Analysis Using Machine Learning and Big Data Analytics," IEEE Transactions on Data Science and Engineering, vol. 7, pp. 106-121, 2023.
[8] Chauhan, S., Verma, A., and Gupta, S. "Design and Implementation of a Real-Time Online Crime Reporting Application," In 2024 IEEE International Conference on Communication, Computing and Digital Systems (C-CODE), pp. 198-204, IEEE, 2024.
[9] Ghosh, A., Kannan, S., and Reddy, A. "Smart Crime Reporting System Using Internet of Things (IoT) and Cloud Computing," In 2024 IEEE International Conference on Smart City and Emerging Technologies (SCET), pp. 1–6, IEEE, 2024.
[10] Singh, K., and Sharma, J. "End-to-End Encrypted Crime Reporting System Using Blockchain Technology," In 2024 IEEE International Conference on Blockchain and Cryptography (ICBC), pp. 409-415, IEEE, 2024.
[11] Shah, R., and Mehta, N. "Crime Reporting and Management System Using Mobile App with GPS Integration," In 2024 IEEE International Conference on Mobile Computing (MobiCom), pp. 347-354, IEEE, 2024.
[12] Thomas, T., Sharma, V., and Gupta, S. "Development of an Automated Online Crime Reporting Platform for Law Enforcement Agencies," In 2024 2nd IEEE International Conference on Artificial Intelligence for Law Enforcement (AILE), pp. 1–8, IEEE, 2024.
[13] Roy, S., and Gupta, P. "Cloud-Based Crime Reporting System for Real-Time Incident Management," In 2024 IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), pp. 120-125, IEEE, 2024.
[14] Bansal, M., and Saxena, P. "Integrated Crime Reporting and Investigation System Using AI Algorithms," In 2023 IEEE International Conference on Intelligent Systems and Automation (ISA), pp. 85–91, IEEE, 2023.
[15] Kapoor, S., and Malik, V. "Citizen-Centric Online Crime Reporting System Using Artificial Intelligence for Predictive Analysis," In 2024 IEEE International Conference on Smart City Applications (SCA), pp. 78-82, IEEE, 2024.