# Privacy Preserving Public Complaint Reporting Platform

Ms. POORNASHREE S[1], Mr. MARIMUTHU[2]
[1]*POORNASHREE S, M.Sc., CFIS, Dr. M.G.R. Educational and Research Institute, Chennai.*
[2] *Mr. MARIMUTHU R, Faculty. Center for Cyber Forensic and Information Security, University of Madras, Chepauk, Chennai.*

***Abstract*—In today's digital landscape, safeguarding the privacy and security of public grievances submitted to government bodies is crucial. This research introduces a Secured Public Grievance System leveraging Certificateless Blind Signatures (CLBS) to ensure anonymity while maintaining authenticity. The primary challenge addressed is the need for a system that allows citizens to submit complaints confidentially while enabling government agencies to verify legitimacy without compromising user privacy. To achieve this, the system integrates certificateless public key cryptography, removing the dependence on traditional certificates for key validation, thereby streamlining key management. Furthermore, the adoption of blind signatures ensures that complaint details remain undisclosed to the signing authority, preserving the complainant's anonymity. This approach enhances security, simplifies cryptographic operations, and upholds privacy, making it a robust solution for secure grievance redressal in government systems.**

***Index Terms*—Certificateless Blind Signatures (CLBS), Cryptographic Authentication, Cybersecurity in E-Governance, Data Anonymity, Flutter, Public Grievance Redressal.**

## I. INTRODUCTION

The paper "Privacy Preserving Public Complaint Reporting Platform" proposes a Secured Public Grievance System using Certificateless Blind Signatures for anonymous, government-verified complaints, ensuring privacy and confidentiality. The Public Complaint Framework uses Certificateless Visually Impaired Marks (CLBS) to securely submit complaints to government organizations, ensuring privacy and enabling public authorities to verify entries without compromising complainants' privacy.

The Secured Public Grievance System aims to enhance public trust in government processes by providing a secure platform for citizens to submit complaints anonymously. It uses certificateless blind signatures, a user-friendly interface, and real-time notifications. The system also includes reporting, analytics, and user support resources to improve transparency and accountability in government processes over the internet through smartphones. Smartphones store personal information, posing data security challenges. Android unlock pattern, has limitations like low efficiency, high latency, and poor security. Blockchain technology, known as the foundation of Bitcoin [1], has been used in various fields with its rapid development, resulting in the dawn of a new economy [2].

The previous research has featured the difficulties looked at by the citizens in reporting complaints to the Police, particularly in situations where the crime is carried out by influential or powerful, or strong individuals, or where the actual Police might be engaged in crimes. The existing complaints system is often complicated, time-consuming, and hazardous, leading to further dissatisfaction, frustration, and inconvenience for victims. Furthermore, the absence of legitimate documentation and record-keeping systems in many Police departments can prompt a deferral or even loss of complaints. These issues have added to a lack of confidence in the Police and diminished accountability [3].

A statistic shows that, in 2015, 179,880 criminal cases are filed in Bangladesh among which more than 63,571 cases are filed for cognizable offenses like murders, rapes, and robbery. But many offenders remain untouched because of the lack of information, evidence or the time-consuming process and paperworks. Evidence associated with a criminal case is crucial as it provides essential information for law enforcement, aiding in crime prevention, suspect identification, and maintaining public safety through informed decision-making and strategic planning. But there is an undeniable threat of data breaches which can be assumed from a recent example in July 2023,

when a major data breach occurred in a Bangladesh Government website, resulting in the unauthorized exposure and compromise of personal data belonging to more than 50 million Bangladeshi citizens [4]. And at quite a few cases the complaints are withdrawn by the victims due to death threats. Our system uses Blockchain technology, in its essence, is a decentralized and secure system that allows for the transparent and immutable recording of digital transactions [5].

## II. LITERATURE REVIEW

Andreas Humm and et al., [6] had proposed Combined Handwriting and Speech Modalities for User Authentication presenting an efficient user authentication system using online pen and speech signals. The system records both modalities simultaneously, resulting in better accuracy and increased difficulty for forgers. The system was tested on two scenarios: spoken signatures and spoken handwriting. Data from 70 users was collected, and the system was designed to model independently both streams of data and perform a fusion at the score level. The use of both modalities outperforms the modalities used alone, demonstrating the effectiveness of this multimodal approach.

Nader, J., and et al., [7] had proposed Designing Touch-Based Hybrid Authentication Method for Smartphones proposes a hybrid authentication scheme combining continuous authentication (CA) and implicit authentication (IA) based on touch gestures. The model uses adaptive machine learning classifiers and a normal-behavioural model. The study evaluates the effectiveness of different classifiers, with the PSO-RBFN classifier showing an average error rate of 1.9%. Combining the CA scheme with an IA scheme reduces the error rate to nearly 0.

Robert, G., and et al., [8] had proposed Graphical Authentication Systems are a potential replacement or supplement for conventional authentication systems. Several studies have suggested graphical authentication may offer greater resistance to guessing and capture attacks but there are other attacks against graphical authentication including social engineering, brute force attacks, shoulder surfing, intercepted communication and spyware. In this paper we give a brief description and classification of different graphical password schemes followed by information about vulnerabilities in the various schemes and recommendations for future development.

Jian Liu and et al., [9] had proposed Enabling Finger-touch-based Mobile User Authentication via Physical Vibrations on IoT Device proposes a hybrid authentication scheme based on touch gestures for mobile devices. The system uses a normal-behavioural model and adaptive machine learning classifiers to authenticate users. The system uses 14 gestures extracted from users' interaction with Android smartphones. The proposed system uses a neural network classifier and the Practical Swarm Optimisation (PSO) - Radial Basis Function Network (RBFN) classifier, with an average error rate of 1.9%. Combining the CA scheme with an IA scheme reduces the error rate to nearly 0. The system extends finger-input authentication beyond touch screens to any solid surface for IoT devices, providing a low-cost, tangible, and enhanced security solution. Extensive experiments show high accuracy (over 97% within two trials), low false positive rate, and robustness to various types of attacks.

Matsuda, T., [10] had proposed Cryptography in Public Systems addresses the growing challenges of managing certificates and cryptographic keys in large-scale public systems. Matsuda proposes using certificateless frameworks to enhance scalability and reduce costs associated with traditional PKI. The study also discusses real-world applications, including privacy-preserving e-governance platforms and secure public grievance systems, highlighting the potential for cryptographic innovations in improving user trust and system efficiency.

Weilin Zheng, and et al., [11] had proposed Blockchain, originating from Bitcoin, is gaining attention due to its decentralization, persistency, anonymity, and auditability. However, its complexity makes it difficult for developers to build, maintain, and monitor a blockchain network. This paper proposes NutBaaS, a BaaS platform that provides blockchain services over cloud computing environments, allowing developers to focus on business code and application without maintaining and monitoring the system.

Christiana Aristidou and et al., [12] had proposed Blockchain is a promising technology that has the potential to revolutionize government applications. However, its true potential is often misunderstood due to its potential to address issues like corruption, fraud,

and lack of transparency. To effectively utilize blockchain in government, governments must adopt a need-based approach, focusing on the development of blockchain standards. These standards enable governments to appreciate blockchain applications effectively, allowing them to use it for various applications outside the government context. This approach can help restore government reputation and efficiency towards citizens.

## III. PROPOSED METHODOLOGY

The framework's core relies on certificateless public key cryptography, which enhances the key administration procedure by eliminating the need for traditional declarations to authorize public keys. Additionally, the visually impaired mark fuse ensures that the protest's content remains hidden from the endorser, maintaining the secret. In this paper, we introduce a new paradigm for public key cryptography, which we name certificateless public key cryptography (CL-PKC). Our concept grew out of a search for public key schemes that do not require the use of certificates and yet do not have the built-in key escrow feature of ID-PKC. The solution we propose enjoys both of these properties; in this way, it is a model for the use of public key cryptography that is intermediate between traditional PKI and ID-PKC. Our concept shares some features in common with the self-certificated keys of and with Gentry's recently proposed certificate-based encryption [13].

Java code is organized around objects and classes rather than just functions, which enables the reuse of code in a very structured manner. Although Java syntax is similar to C++, it has not suffered from feature overload and is much less complex. In addition, some Java features, like garbage collection, are not entirely new but were pioneered by languages such as Lisp and Smalltalk. The paper discusses Java language features such as: inheritance, robustness, type safety, access modifiers, null pointer checking, array bounds checking, memory management, multithreading, garbage collection and security [14]. With the advent of new mobile technologies, the mobile application industry is advancing rapidly. Consisting of several operating systems like Symbian OS, iOS, blackberry, etc., Android OS is recognized as the most widely used, popular and user-friendly mobile platform [15]. Java is used to program android applications. Developers make use of existing java IDEs which provides flexibility.

### 1. FLUTTER

A software that runs on the Android Operating system makes up a Mobile application. Since the Android platform is designed for portable devices, a typical Android app is created for a smartphone or tablet computer that runs the Android Operating system. The majority of Android applications are transferred and disseminated through the Android Advertise, a dedicated online commercial hub for portable programmes, despite the fact that Android app creators can post their apps on their own websites. The Android app store advertises both free and paid apps. Java-written Android apps make use of Java center libraries. Just on Android website, you can obtain the Android software development kit (SDK). The SDK contains tools, test code, and core data for developing Android apps. In this project, we'll create an application that provides us with projects in a variety of programming languages as well as the project's source code and documentation for educational purposes [16].

### 2. FIREBASE

Android applications use various databases for their back-end. The popular ones used commercially have been SQLite, Realm DB, ORM Lite, Berkeley DB and Couchbase Lite. Firebase gives you a chance to construct all the more dominant, secure and versatile applications, utilizing worldclass foundation [17]. Firebase accelerates the cloud database integration automatically in both web and mobile app, and directs to settle the required massive tasks which should be accomplished by developers. By charging no cost under limited usage, Firebase is available to be commenced and clients are able to upgrade when the app tasks are requested to be equipped with more advanced features.

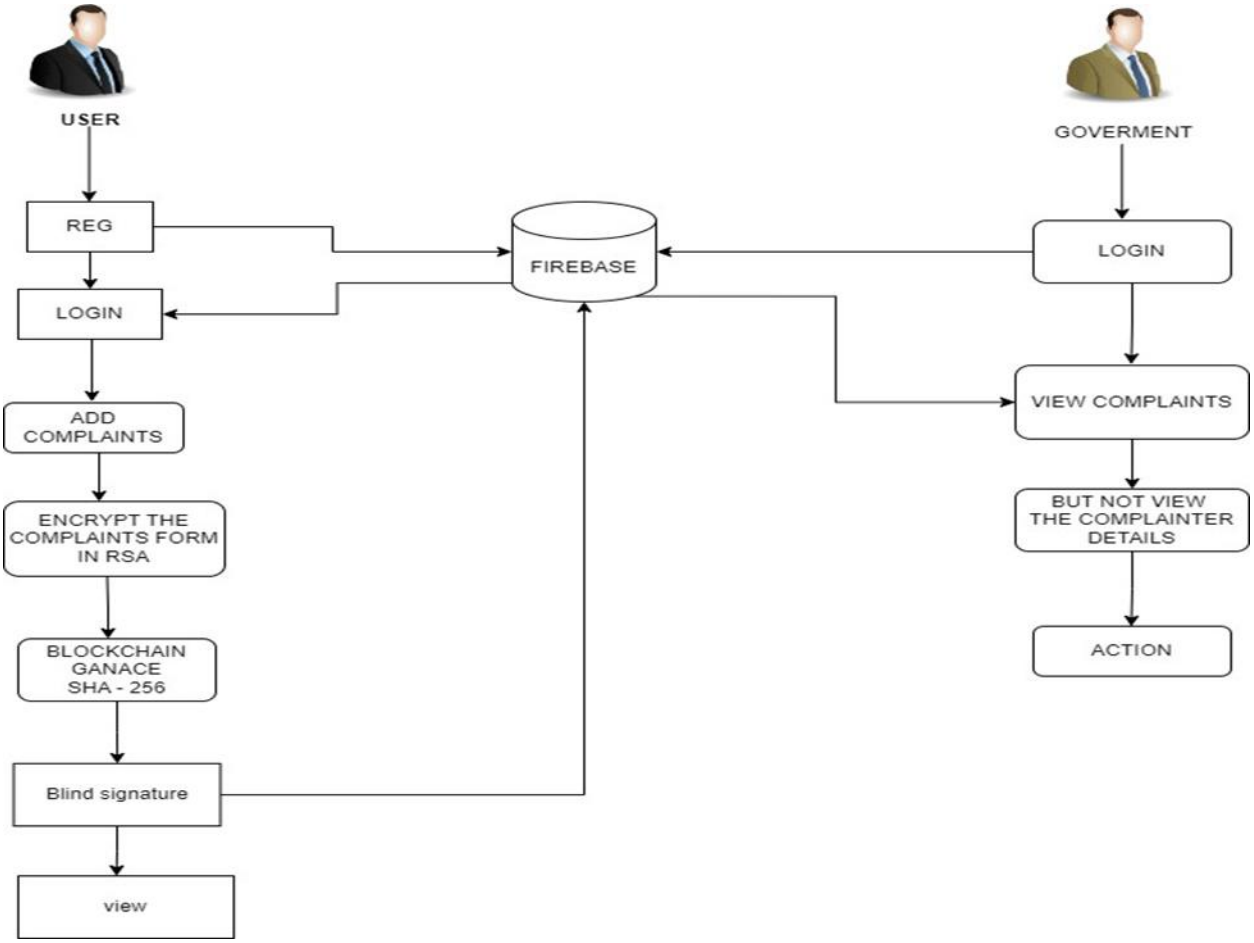


Fig 1 ARCHITECTURE DIAGRAM

Developers could uplift the infrastructure on the Google-based app, focus on the app content and user's satisfaction in a secure system [18]. Firebase has become increasingly popular over the past couple of years. Major application companies have adopted it due its perfect fit with agile development. Colleges usually have their own applications that are created and maintained by a

third-party organization. In this case, this Android application has the capability of being handled by the creator due to Firebase being the backend that provides all the features in a go. With this, even small institutions can adopt this model and run this application to connect all the members [17]

## 3. RSA ALGORITHM

Encryption is one of the principal means to grantee the security of sensitive information. It not only provides the mechanisms in information confidentiality, but also functioned with digital signature, authentication, secret sub- keeping, system security and etc. Therefore, the purpose of adopting encryption techniques is to ensure the information's confidentiality, integrity and certainty, prevent information from tampering, forgery and counterfeiting [19].

In general, the algorithms that implicated asymmetric keys are much more secure than others using one key. RSA algorithm used asymmetric keys; one of them for encryption the message, and is known as a public key and another used to decrypt the encrypted message and is called a private key. The main disadvantage of the RSA algorithm is that extra time is taken to perform the encryption process [20].

## 4. BLOCKCHAIN GANACE

Blockchain is a decentralized, distributed digital ledger that records transactions across multiple computers, ensuring immutability and transparency. It is a technology that underpins cryptocurrencies like

Bitcoin and has applications in various industries. Blockchain is immutable, ensuring a permanent record of transactions. It is transparent, secure, and acts as a shared ledger, allowing participants to track assets and transactions across a network. Ganache is a private Ethereum blockchain environment that lets us engage with smart contracts on our own private blockchain by simulating the Ethereum blockchain.

5. SHA 256 ALGORITHM

The SHA-2 family is a set of cryptographic hash functions designed and published by the US National Institute of Standards and Technology (NIST) in 2002. The SHA-2 family includes six hash functions named SHA-224, SHA- 256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256. They are actually the same algorithm but with different word lengths, constant parameters, and initialization values. SHA-256 is known as representative of the SHA-2 family and is currently applied to secure data in many applications such as decentralized blockchain, DSA, and HMAC. SHA- 256 calculates a 256-bit hash value for an input message of 512 bits [21].

6. BLIND SIGNATURE SYSTEM

A blind signature is a digital signature where a signer signs a message without knowing its content, ensuring privacy and anonymity, i.e., the user's details are anonymous. The blind signature is used to utilize various cloud services anonymously. The primary aim is to supply the anonymous tickets as credentials. This enables the client to register complaints anonymously for using the services provided [22]

## IV. FINDINGS

This paper employs Certificateless Blind Signatures (CLBS) to ensure anonymous and secure complaint submissions. Whereas the prior literature reviews other authentication methods like handwriting and speech recognition, enhancing accuracy but limiting privacy preservation [6], touch-based hybrid authentication model using machine learning [7], finger-touch authentication system leveraging vibrations on IoT devices [9], and graphical authentication techniques, addressing security challenges like shoulder surfing and brute force attacks [8]. Unlike these works, which primarily enhance biometric authentication, this paper prioritizes user anonymity and privacy in public grievance reporting system.

This paper discusses about the CL – PKC (Certificateless Public Key Cryptography) which removes the dependence on traditional certificates, improving efficiency and security. Whereas Matsuda discussed public key cryptography and certificate management in large-scale systems, highlighting scalability issues in PKI [10]. Here we eliminate the need for certificates while maintaining strong authentication using blind signatures. As we speak of CL – PKC, the blockchain is the critical component discussed in this paper which ensures immutability and transparency in public complaint records. Weilin Zheng and Christiana Aristidou discusses a Blockchain-as-a-Service (BaaS) platform, simplifying blockchain implementation for developers and blockchain adoption in government applications, highlighting its potential for transparency and fraud prevention [11 – 12]. It majorly discusses the blockchain for trust and security and this paper mainly focuses blockchain specifically to anonymous public grievance reporting, addressing real-world privacy concerns.

## V. CONCLUSION

The Secured Public Grievance System is a significant step towards improving accountability, efficiency, and transparency in governmental procedures. It uses advanced technology like Certificateless Blind Signatures to ensure citizens can file complaints anonymously, boosting public confidence in government organizations. The system features a user-friendly interface, real-time support, and robust tracking systems to enhance the user experience. It prioritizes data security and privacy, allowing citizens to express concerns while providing government agencies with the necessary resources. The ultimate goal is to create a more responsive and participatory governance model, ensuring that every citizen's opinion is heard and considered in a safe environment. The system is set to undergo enhancements to improve user experience, security, and functionality.

REFERENCES


[1] Nakamoto, S., ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Tech. Rep., 2008.

[2] Swan, M., Blockchain: Blueprint for a New Economy. Newton, MA, USA: O’Reilly Media, 2015

[3] Ullah, A., Singha, T., Sarker, H., Pia, F. and Hossain, A., “Citizen-Centric Complaint Reporting and Analyzing Mechanism. Journal of Software Engineering and Applications”,2023.

[4] Tanjim, M., Chowdhury, R. A., Amin, R., Ahmed, T., Chowdhury, M.D., and Lysuzzaman, M., "SafetyNet: A Decentralized Police Complaint Management System for Bangladesh Using Blockchain Technology," 2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS), Dhaka, Bangladesh, 2024.

[5] S. Vignesh, L. Anil Kumar and M. S. Reddy, "Blockchain: online police complaint management system," 2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA), Namakkal, India, 2024.

[6] Andreas Humm, Jean Hennebert, “Combined Handwriting and Speech Modalities for User Authentication”, 2009.

[7] Nader, J., Elchouemic, A., Singh, A. K., “Designing Touch-Based Hybrid Authentication Method for Smartphones”2015.

[8] Robert, G., Rittenhouse, Malrey Lee, “Security in Graphical Authentication”, 2013.

[9] Jian Liu, Xin Yang, Chen Wang,” Enabling Finger-touch-based Mobile User Authentication via Physical Vibrations on IoT Device”, 2021.

[10] Matsuda, T., “Cryptography in Public Systems”, 2018.

[11] Weilin Zheng, Zibin Zheng, Xiangping Chen, Kemian Dai, Peishan Li, Renfei Chen, “NutBaaS: A Blockchain-as-a- Service Platform”, 2019.

[12] Christiana Aristidou, Evdokia Marcou, “Blockchain Standards and Government Applications”, 2019.

[13] Baek, Joonsang, Reihaneh Safavi-Naini, and Willy Susilo. "Certificateless public key encryption without pairing." International conference on information security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.

[14] Van Hoff, A., "The case for Java as a programming language," in IEEE Internet Computing, vol. 1, no. 1, pp. 51-56, Jan.-Feb. 1997, doi: 10.1109/4236.585172

[15] Sarkar, A., Goyal, A., Hicks, D., Sarkar, D., and Hazra, S., "Android Application Development: A Brief Overview of Android Platforms and Evolution of Security Systems," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2019, pp. 73-79, doi: 10.1109/I-SMAC47947.2019.9032440.

[16] Nagaraj, K., Prabakaran, B., and Ramkumar, M. O., "Application Development for a Project using Flutter," 2022, 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 947-951, doi: 10.1109/ICOSEC54921.2022.9951938.

[17] Sharma, D., & Dand, H., “Firebase as baas for college android application. International Journal of Computer Applications”, 2019, 178(20), 1-6.

[18] Tram, M., “Firebase”, 2019.

[19] Zhou, X., & Tang, X., “Research and implementation of RSA algorithm for encryption and decryption”, 2011 In Proceedings of 2011 6th international forum on strategic technology, (Vol. 2, pp. 1118-1121). IEEE.

[20] Obaid, T. S., “Study a public key in RSA algorithm. European Journal of Engineering and Technology Research”, 2020, 5(4), 395-398.

[21] Tran, T. H., Pham, H. L., & Nakashima, Y., “A high-performance multimem SHA-256 accelerator for society 5.0”, 2021, IEEE Access, 9, 39182-39192.

[22] Vora, J., DevMurari, P., Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M. S., “Blind signatures based secured e- healthcare system”, 208, In 2018 International conference on computer, information and telecommunication systems (CITS) (pp. 1-5). IEEE